

Aruba Central (on-premises) 2.5.4.x User Guide



Copyright Information

© Copyright 2022 Hewlett Packard Enterprise Development LP.

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US \$10.00 to:

Hewlett Packard Enterprise Company
6280 America Center Drive
San Jose, CA 95002
USA

Contents	3
About this Guide	8
Intended Audience	8
Related Documents	8
Conventions	8
Terminology Change	9
Contacting Support	9
About Aruba Central (on-premises)	11
Key Features	11
Scaling Devices for Aruba Central (on-premises)	11
Supported Web Browsers	13
Supported Devices	13
Aruba Central (on-premises) 2.5.4.x What's New	27
What's New in Aruba Central (on-premises) 2.5.4.3	27
New Features	27
What's New in Aruba Central (on-premises) 2.5.4.2	27
New Features	27
What's New in Aruba Central (on-premises) 2.5.4.0	27
Important Notes	28
New Features	28
Enhancements	34
Getting Started with Aruba Central (on-premises)	43
Aruba Central Subscriptions	43
Provisioning Workflow	43
Scaling Devices for Aruba Central (on-premises)	44
Creating a Group	46
Onboarding Devices	47
Assigning Devices to Groups	51
Assigning Labels	52
Assigning Sites	52
Connecting Aruba APs to Aruba Central	53
Connecting Aruba Controllers to Aruba Central	53
Connecting Aruba Switches to Aruba Central	54
Configuring Communication Ports	54
Configuring User Roles	56
Predefined User Roles	56
Custom Roles	57
Module Permissions	58

System Setup as Node or Cluster	59
Verifying Device Configuration Status	59
Local Overrides	60
Viewing Status for Devices Assigned to a Template Group	61
Viewing Configuration Status for a UI Group	62
Viewing Configuration Status for Devices Assigned to a UI Group	63
Using the Search Bar	63
About the Network Operations App User Interface	67
Types of Dashboards in the Network Operations App	68
Navigating to the Switch, Access Point, or Controller Dashboard	69
Workflow to Configure, Monitor, or Troubleshoot in the Network Operations App	69
The Global Dashboard	70
The Access Point Dashboard	72
The Switch Dashboard	74
The Controller Dashboard	97
The Group Dashboard	98
The Client Dashboard	100
The Site Dashboard	101
The Label Dashboard	102
The Health Bar	103
Account Home Page	112
Command Line Interface	113
Accessing the Aruba Central CLI	113
Syntax	113
Common Command Options	113
Password Recovery	114
Main Menu Options	114
List of CLI Commands	114
Network Structure	140
Viewing the Network Structure Page	140
Managing Groups	142
Group Operations	143
Group Configuration Modes	143
Default Groups and Unprovisioned Devices	143
Best Practices and Recommendations	144
Groups	144
Provisioning Devices Using UI-based Workflows	155
Provisioning Devices Using Configuration Templates	157
Managing APs	170
Configuring APs	170
Monitoring APs	348
Managing AOS-CX Switches	387
Getting Started with AOS-CX Deployments	388
Using Configuration Templates for AOS-CX Switch Management	407
Configuring AOS-CX Switches in UI Groups	410
Managing an AOS-CX VSF Stack	467
Configuring AOS-Switches	492
Getting Started with AOS-Switch Deployments	492
Using Configuration Templates for AOS-Switch Management	509

Configuring AOS-Switches in UI Groups	513
AOS-Switch Stack	559
Managing Controllers	568
Before You Begin	568
Supported Aruba Mobility Controllers	569
Adding Mobility Controllers	569
Deleting a Controller	571
The Controller Dashboard	571
Managing Users and Roles	583
Configuring System Users	583
Configuring User Roles	585
Two-Factor Authentication	589
Support Access	590
Managing Sites and Labels	592
Managing Sites	592
Creating a Site	592
Adding Multiple Sites in Bulk	593
Assigning a Device to a site	593
Convert Existing Labels to Sites	594
Editing a Site	594
Deleting a Site	595
Managing Labels	595
Device Classification	595
Creating a Label	596
Assigning a Device to a Label	596
Detaching a Device from a Label	596
Editing a label	597
Deleting a label	597
Managing Sites	597
Managing Labels	601
Managing Certificates	604
Device Certificates	604
Uploading Device Certificates	605
Deleting Device Certificates	606
Appliance Certificates	606
Viewing the Certificate Store Parameters	606
Uploading Appliance Certificates	607
Deleting Appliance Certificates	608
Certificate Signing Request	608
Supported Certificate Formats	609
Wildcard Certificates	609
Managing Licenses	613
Changes to the Legacy Licensing Model	613
Supported Devices	614
Managing License Assignments	615
Configuring External Authentication	618
Configuring SAML SSO for Aruba Central	618
Configuring RADIUS Authentication and Authorization	647
Viewing Audit Logs for Federated Users in Aruba Central	650
Viewing Federated Users in Aruba Central	650

Monitoring Your Network	652
Network Overview	652
Network Health	735
AI Insights	745
All Clients	771
Application Visibility	799
About Floorplans	802
Alerts & Events	811
Reports	827
Viewing Audit Trail	844
RAPIDS	845
Monitoring Sites in the Topology Tab	849
Upgrading Device Firmware	861
System Management	874
Viewing System Management in the Account Homes Page	874
Viewing System Performance	874
Upgrade Watcher	877
Version	880
Network	881
External Services	883
Backing up and Restoring Aruba Central System Data	884
Migrating the AirWave Server	887
Validating the Migration Process	894
Using Troubleshooting Tools	898
Troubleshooting Network Issues	898
Troubleshooting Device Issues	910
Advanced Device Troubleshooting	912
Troubleshooting System Issues	917
Unified Communications	920
Licensing	920
Configuring UCC	921
Monitoring UCC in List View	926
Monitoring UCC in Summary View	929
Aruba Central APIs	931
API Gateway	931
List of Supported APIs	934
Creating Application and Token	935
Using OAuth 2.0 for Authentication	937
Obtaining Token Using Offline Token Mechanism	940
Obtaining Token Using OAuth Grant Mechanism	940
Viewing Usage Statistics	948
Changes to Aruba Central APIs	949
Webhook	956
Streaming APIs	961
Related Information	965
Aruba Central (on-premises) Release Notes	965
Aruba Central (on-premises) 2.5.4.3 PDF Documents	965
Aruba Central (on-premises) 2.5.4.0 PDF Documents	965
Aruba Central (on-premises) APIs	965
ArubaOS and Aruba Instant Documentation	965
Aruba Switch Documentation	966

This user guide describes the features supported by Aruba Central (on-premises) and provides detailed instructions to set up and configure devices such as Campus APs, Instant APs, Switches, and Controllers. In Aruba Central, the only access points that you can configure are Instant APs. However, monitoring is supported for both Campus APs and Instant Access Points.

Intended Audience

This guide is intended for system administrators who configure and monitor their network using Aruba Central.

Related Documents

In addition to this document, the Aruba Central (on-premises) product documentation includes the following documents:

- *Aruba Central (on-premises) Installation and Setup Guide*
- *Aruba Central (on-premises) Migration Guide*
- *Aruba Central (on-premises) API Reference Guide*
- *Aruba Central (on-premises) Release Notes*

Conventions

The following conventions are used throughout this guide to emphasize important concepts:

Table 1: *Typographical Conventions*

Type Style	Description
<i>Italics</i>	This style is used to emphasize important terms and to mark the titles of books.
System items	This fixed-width font depicts the following: <ul style="list-style-type: none">■ Sample screen output■ System prompts
Bold	<ul style="list-style-type: none">■ Keys that are pressed■ Text typed into a GUI element■ GUI elements that are clicked or selected

The following informational icons are used throughout this guide:



Indicates helpful suggestions, pertinent information, and important things to remember.



Indicates a risk of damage to your hardware or loss of data.



Indicates a risk of personal injury or death.

Terminology Change

As part of advancing HPE's commitment to racial justice, we are taking a much-needed step in overhauling HPE engineering terminology to reflect our belief system of diversity and inclusion. Some legacy products and publications may continue to include terminology that seemingly evokes bias against specific groups of people. Such content is not representative of our HPE culture and moving forward, Aruba will replace racially insensitive terms and instead use the following new language:

Usage	Old Language	New Language
Campus Access Points + Controllers	Master-Slave	Conductor-Member
Instant Access Points	Master-Slave	Conductor-Member
Switch Stack	Master-Slave	Conductor-Member
Wireless LAN Controller	Mobility Master	Mobility Conductor
Firewall Configuration	Blacklist, Whitelist	Denylist, Allowlist
Types of Hackers	Black Hat, White Hat	Unethical, Ethical

Contacting Support

Table 2: *Contact Information*

Main Site	arubanetworks.com
Support Site	asp.arubanetworks.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	arubanetworks.com/support-services/contact-support/
Software Licensing Site	lms.arubanetworks.com
End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team	Site: arubanetworks.com/support-services/security-bulletins/

	Email: aruba-sirt@hpe.com
Open Source License	Site: https://myenterpriselicense.hpe.com/cwp-ui/free-software/ArubaCentralOn-Premises-OSP

Aruba Central (on-premises) is a variant of Aruba Central, a SAAS platform that offers you a single intelligent console to monitor, analyze, and configure WLAN and wired networks. Aruba Central makes it easy and efficient to manage your networks by combining industry-leading functionality with an intuitive user interface, and enables network administrators and help desk staff to support and control even the largest networks.

Network Operations is one of the apps in Aruba Central that helps you to manage, maintain, and analyze your network.

Key Features

Aruba Central offers the following key features and benefits:

- **Streamlined configuration and deployment of devices**—Leverages the ZTP capability of Aruba devices to bring up your network in no time. Aruba Central supports group configuration of devices, which allows you to provision and manage multiple devices at once, with less administrative overhead.
- **Integrated wired and wireless Infrastructure management**—Offers a centralized management interface for managing wireless and wired networks in distributed environments.
- **Advanced analytics and assurance**—With continuous monitoring, AI-based analytics like NI-Lite provide real-time visibility and insight into what's happening in the Wi-Fi network. The NI-Lite utilizes machine learning that leverage a growing pool of network data and deep domain experience.
- **Health and usage monitoring**—Provides a comprehensive view of your network, device status and health, and application usage. You can monitor, identify, and address issues by using data-driven dashboards, alerts, reports, and troubleshooting workflows. Aruba Central also utilizes the DPI feature of the devices to monitor, analyze, and block traffic based on application categories, application type, web categories, and website reputation. Using this data, you can prioritize business critical applications, limit the use of inappropriate content, and enforce access policies on a per user, device, or location basis.
- **Rogue AP detection and classification**—Supports rogue detection and classification. The network administrators can view the intrusion events and unauthorized or rogue devices detected in their WLAN network, and take appropriate measure to secure their networks.
- **Value Added Services**—Supports value added service such as Unified Communications.
 - The Unified Communication application actively monitors and provides visibility into Lync/Skype for Business traffic and allows you to prioritize sessions.

Scaling Devices for Aruba Central (on-premises)

Aruba Central supports switches, controllers, Instant APs, and Campus APs. Aruba Central can be implemented on multiple nodes. Accordingly, the number of supported devices increase.

Supported Number of Devices - Summary Table

The following table provides a summary of the number of devices supported across multiple nodes

Table 3: Maximum Number of Supported Devices

Node Size	Campus APs (AP and Controller)	Instant AP only	Switches only (AOS-Switch and AOS-CX)	Mixed-Mode
Single Node	2000	2000	1000	1600 APs (Instant AP or Campus AP) and 400 Switches (AOS-Switch or AOS-CX)
Three Node	8000	8000	3000	6000 APs (Instant AP or Campus AP) and 2000 Switches (AOS-Switch or AOS-CX)
Five Node	16000	12000	4000	12000 APs (Instant AP or Campus AP) and 4000 Switches (AOS-Switch or AOS-CX)
Seven Node	25000	16000	10000 (AOS-Switch) / 4000 (AOS-CX)	16000 APs (Instant AP or Campus AP) and 7000 Switches (AOS-Switch) [AOS-CX up to 4000 Switches]

Supported Number of Devices - Detailed Table

The following table details the number of devices that Aruba Central supports across multiple nodes.

Table 4: Maximum Number of Supported Devices

Nodes	Maximum Number of Supported Devices	Modes
Single Node	2000	<ul style="list-style-type: none"> ■ 2000 APs where APs can be either Instant APs, Campus APs, or controllers that manage APs; or a mixed deployment of any of these devices. ■ 1000 switches where switches can be AOS-Switches or AOS-CX switches or a mix of the two. ■ In a mixed-mode of switches and APs, up to 1600 APs and 400 switches are supported.
Three Node	8000	<ul style="list-style-type: none"> ■ 8000 APs, where APs can be either Instant APs, Campus APs, or APs along with the controllers that manage APs; or a mix of any of these devices. ■ 3000 AOS-Switches or AOS-CX switches or a mix of the two can be deployed in switch-only deployment. ■ In a mixed-mode of switches and APs, up to 6000 APs (Instant APs or Campus APs) and 2000 switches (AOS-Switch or AOS-CX) are supported. ■ 80000 total clients; tested and qualified with the scale of 10 clients per AP.
Five Node	16000	<ul style="list-style-type: none"> ■ 16000 Campus APs along with the controllers that manage APs can be deployed. ■ 12000 Instant APs can be deployed. ■ 4000 AOS-Switches or AOS-CX switches or a mix of the two can be deployed in switch-only deployment. ■ In a mixed-mode of switches and APs, up to 12000 (Instant APs or Campus APs) and 4000 (AOS-Switch or AOS-CX) switches are supported.

Nodes	Maximum Number of Supported Devices	Modes
		<ul style="list-style-type: none"> 160000 total clients; tested and qualified with the scale of 10 clients per AP.
Seven Node	25000	<ul style="list-style-type: none"> 25000 Campus APs along with the controllers that manage APs can be deployed. 10000 AOS-Switches can be deployed in AOS-Switches only deployment. 4000 AOS-CX switches can be deployed in AOS-CX switches only deployment. In a mixed-mode of switches and APs, up to 16000 APs (Instant AP or Campus APs), 7000 AOS-Switches and 4000 (AOS-Switch or AOS-CX) switches are supported. 240000 total clients; tested and qualified with the scale of 10 clients per AP.

You can check maximum number of supported devices of the Aruba Central setup in the **Account Home > Global Settings > Subscription Assignment** page.

If the device limit is exceeded, the device added to the system is displayed as *Unsubscribed* in the **Account Home > Global Settings > Device Inventory** page.

Supported Web Browsers

Aruba recommends that you use the following browsers to access the Aruba Central application.

Browser Versions	Operating System
Google Chrome 39.0.2171.65 or later	Windows
Mozilla FireFox 34.0.5 or later	Windows
Internet Explorer 11	Windows
Internet Explorer 10	Windows



To view the Aruba Central UI, ensure that JavaScript is enabled on the web browser.

Supported Devices

This section provides the following information:

- [Supported APs](#)
- [Supported AOS-Switch Platforms](#)
- [Supported AOS-CX Switch Platforms](#)
- [Supported Aruba Mobility Controllers](#)

Supported APs

Aruba Central (on-premises) supports following types of Aruba access points (APs).

- Instant APs—The Instant Access Point (IAP) based WLAN solution consists of a cluster of access points in a Layer 2 subnet. The IAPs serve a dual role as both Virtual Controller (VC) and member APs. The IAP WLAN solution does not require a dedicated controller hardware and can be deployed through a simplified setup process appropriate for smaller organizations, or for multiple geographically dispersed locations without an on-site administrator. IAPs run on the Aruba Instant. Aruba Central (on-premises) supports both monitoring and management of IAPs. With Aruba Central (on-premises), network administrators can configure, monitor, and troubleshoot IAP WLANs, upload new software images, monitor devices, generate reports, and perform other vital management tasks from remote locations.
- Campus APs—The Campus Access Point (CAP)s are used in private networks where APs connect over private links (LAN, WLAN, WAN, or MPLS) and terminate directly on controllers. CAPs are deployed as part of the indoor campus solution in enterprise office buildings, warehouses, hospitals, universities, and so on. Aruba Central (on-premises) supports only onboarding and monitoring the CAPs.

Supported IAP

Aruba Central (on-premises) supports the following IAP platforms and Aruba Instant software versions:

Table 5: *Supported Instant AP Platforms*

Instant AP Platform	Installation Mode	Latest Validated Aruba Instant Software Version	Power Draw Support
AP-655	Indoor	8.10.0.0	Yes
AP-635	Indoor	8.9.0.0	Yes
AP-567EX	Outdoor	8.7.1.0	No
AP-567	Outdoor	8.7.1.0	Yes
AP-565EX	Outdoor	8.7.1.0	No
AP-565	Outdoor	8.7.1.0	Yes
AP-503H	Indoor	8.7.1.0	Yes
AP-577EX	Outdoor	8.7.0.0	Yes
AP-577	Outdoor	8.7.0.0	Yes
AP-575EX	Outdoor	8.7.0.0	Yes
AP-575	Outdoor	8.7.0.0	Yes
AP-574	Outdoor	8.7.0.0	Yes

Instant AP Platform	Installation Mode	Latest Validated Aruba Instant Software Version	Power Draw Support
AP-518	Outdoor	8.7.0.0	Yes
AP-505H	Indoor	8.7.0.0	Yes
AP-505	Indoor	8.6.0.0	Yes
AP-504	Indoor	8.6.0.0	Yes
AP-535	Indoor	8.6.0.7 8.5.0.0	No
AP-534	Indoor	8.6.0.7 8.5.0.0	No
AP-515	Indoor	8.6.0.7 8.4.0.0	Yes
AP-514	Indoor	8.6.0.7 8.4.0.0	Yes
AP-555	Indoor	8.5.0.0	No
AP-387	Outdoor	8.4.0.0	Yes
AP-303P	Indoor	8.4.0.0	No
AP-377EX	Outdoor	8.3.0.0	No
AP-377	Outdoor	8.3.0.0	Yes
AP-375EX	Outdoor	8.3.0.0	No
AP-375	Outdoor	8.3.0.0	Yes
AP-374	Outdoor	8.3.0.0	Yes
AP-345	Indoor	8.3.0.0	Yes
AP-344	Indoor	8.3.0.0	Yes
AP-318	Indoor	8.3.0.0	Yes
AP-303	Indoor	8.3.0.0	No
AP-203H	Indoor	8.3.0.3 6.5.4.8 6.5.3.7	No
AP-367	Outdoor	8.3.0.3 6.5.4.8 6.5.3.7	No

Instant AP Platform	Installation Mode	Latest Validated Aruba Instant Software Version	Power Draw Support
AP-365	Outdoor	8.3.0.3 6.5.4.8 6.5.3.7	No
AP-303HR	Indoor	6.5.2.0	No
AP-303H	Indoor	8.3.0.3 6.5.4.8 6.5.3.7	Yes
AP-203RP	Indoor	8.3.0.3 6.5.4.8 6.5.3.7	No
AP-203R	Indoor	8.3.0.3 6.5.4.8 6.5.3.7	No
IAP-305	Indoor	8.3.0.3 6.5.4.8 6.5.3.7	Yes
IAP-304	Indoor	8.3.0.3 6.5.4.8 6.5.3.7	Yes
IAP-207	Indoor	8.3.0.3 6.5.4.8 6.5.3.7	No
IAP-335	Indoor	8.3.0.3 6.5.4.8 6.5.3.7	Yes
IAP-334	Indoor	8.3.0.3 6.5.4.8 6.5.3.7	Yes
IAP-315	Indoor	8.3.0.3 6.5.4.8 6.5.3.7	No
IAP-314	Indoor	8.3.0.3 6.5.4.8 6.5.3.7	Yes
IAP-325	Indoor	8.3.0.3	No

Instant AP Platform	Installation Mode	Latest Validated Aruba Instant Software Version	Power Draw Support
		6.5.4.8 6.5.3.7 6.4.4.8-4.2.4.10 6.4.3.4-4.2.1.0	
IAP-324	Indoor	8.3.0.3 6.5.4.8 6.5.3.7 6.4.4.8-4.2.4.10 6.4.3.4-4.2.1.0	No
IAP-277	Outdoor	6.5.4.3 6.5.3.7 6.4.4.8-4.2.4.10 6.4.3.4-4.2.1.0	No
IAP-228	Indoor	6.5.4.3 6.5.3.7 6.4.4.8-4.2.4.10 6.4.3.4-4.2.1.0	No
IAP-205H	Indoor	6.5.4.8 6.5.3.7 6.4.4.8-4.2.4.10 6.4.3.4-4.2.1.0	No
IAP-215	Indoor	6.5.4.3 6.5.3.7 6.4.4.8-4.2.4.10 6.4.3.4-4.2.1.0	No
IAP-214	Indoor	6.5.4.3 6.5.3.7 6.4.4.8-4.2.4.10 6.4.3.4-4.2.1.0	No
IAP-205	Indoor	6.5.4.8 6.5.3.7 6.4.4.8-4.2.4.10 6.4.3.4-4.2.1.0	No
IAP-204	Indoor	6.5.4.8 6.5.3.7 6.4.4.8-4.2.4.10 6.4.3.4-4.2.1.0	No
IAP-275	Outdoor	6.5.4.3 6.5.3.7	No

Instant AP Platform	Installation Mode	Latest Validated Aruba Instant Software Version	Power Draw Support
		6.4.4.8-4.2.4.10 6.4.3.4-4.2.1.0	
IAP-274	Outdoor	6.5.4.3 6.5.3.7 6.4.4.8-4.2.4.10 6.4.3.4-4.2.1.0	No
IAP-103	Indoor	6.5.4.8 6.5.3.7 6.4.4.8-4.2.4.10 6.4.3.4-4.2.1.0	No
IAP-225	Indoor	6.5.4.3 6.5.3.7 6.4.4.8-4.2.4.10 6.4.3.4-4.2.1.0	No
IAP-224	Indoor	6.5.4.3 6.5.3.7 6.4.4.8-4.2.4.10 6.4.3.4-4.2.1.0	No
IAP-115	Indoor	6.5.4.8 6.5.3.7 6.4.4.8-4.2.4.10 6.4.3.4-4.2.1.0	No
IAP-114	Indoor	6.5.4.8 6.5.3.7 6.4.4.8-4.2.4.10 6.4.3.4-4.2.1.0	No

-
- IAP-214, IAP-215, IAP-224, IAP-225, IAP-228, IAP-274, IAP-275, and IAP-277 IAPs are no longer supported from Aruba Instant 8.7.0.0 onwards.
 - IAP-103, IAP-114, IAP-115, IAP-204, IAP-205, and IAP-205H IAPs are no longer supported from Aruba Instant 8.3.0.0 onwards.
 - By default, AP-318, AP-374, AP-375, and AP-377 IAPs have Eth1 as the uplink port and Eth0 as the downlink port. Aruba does not recommend you to upgrade these IAPs to Aruba Instant 8.5.0.0 or 8.5.0.1 firmware versions, as the upgrade process changes the uplink port from Eth1 to Eth0 port thereby making the devices unreachable.
-



Supported Campus APs

Aruba Central (on-premises) supports the following CAP platforms and ArubaOS software versions:

AP Platform	Latest Validated ArubaOS Software Versions
AP-567EX	8.9.0.0 8.8.0.0
AP-565EX	8.9.0.0 8.8.0.0
AP-505HR	8.9.0.0 8.8.0.0
AP-503HR	8.9.0.0 8.8.0.0
AP-375EX	8.9.0.0 8.8.0.0
AP-228	8.9.0.0 8.8.0.0
AP-207	8.9.0.0 8.8.0.0
AP-577EX	8.7.1.0 8.6.0.7
AP-577	8.7.1.0 8.6.0.7
AP-575EX	8.7.1.0 8.6.0.7
AP-575	8.7.1.0 8.6.0.7
AP-574	8.7.1.0 8.6.0.7
AP-567	8.7.1.0
AP-565	8.7.1.0
AP-555	8.7.1.0 8.6.0.7
AP-518	8.7.1.0 8.6.0.7
AP-535	8.7.1.0 8.6.0.7
AP-534	8.7.1.0 8.6.0.7

AP Platform	Latest Validated ArubaOS Software Versions
AP-515	8.7.1.0 8.6.0.7
AP-514	8.7.1.0 8.6.0.7
AP-505H	8.7.1.0 8.6.0.7
AP-505	8.7.1.0 8.6.0.7
AP-504	8.7.1.0 8.6.0.7
AP-503H	8.7.1.0
AP-377EX	8.7.1.0 8.6.0.7 6.5.4.16
AP-377	8.7.1.0 8.6.0.7 6.5.4.16
AP-375	8.7.1.0 8.6.0.7 6.5.4.16
AP-374	8.7.1.0 8.6.0.7 6.5.4.16
AP-367	8.7.1.0 8.6.0.7 6.5.4.16
AP-365	8.7.1.0 8.6.0.7 6.5.4.16
AP-345	8.7.1.0 8.6.0.7
AP-344	8.7.1.0 8.6.0.7
AP-335	8.7.1.0 8.6.0.7 6.5.4.16
AP-334	8.7.1.0 8.6.0.7 6.5.4.16
AP-325	8.7.1.0 8.6.0.7

AP Platform	Latest Validated ArubaOS Software Versions
	6.5.4.16
AP-324	8.7.1.0 8.6.0.7 6.5.4.16
AP-318	8.7.1.0 8.6.0.7
AP-315	8.7.1.0 8.6.0.7 6.5.4.16
AP-314	8.7.1.0 8.6.0.7 6.5.4.16
AP-305	8.7.1.0 8.6.0.7 6.5.4.16
AP-304	8.7.1.0 8.6.0.7 6.5.4.16
AP-303P	8.7.1.0 8.6.0.7
AP-303H	8.7.1.0 8.6.0.7
AP-303	8.7.1.0 8.6.0.7
AP-277	8.7.1.0 8.6.0.7 6.5.4.16
AP-275	8.7.1.0 8.6.0.7 6.5.4.16
AP-274	8.7.1.0 8.6.0.7 6.5.4.16
AP-225	8.7.1.0 8.6.0.7 6.5.4.16
AP-224	8.7.1.0 8.6.0.7 6.5.4.16
AP-215	8.7.1.0 8.6.0.7 6.5.4.16

AP Platform	Latest Validated ArubaOS Software Versions
AP-214	8.7.1.0 8.6.0.7 6.5.4.16
AP-205H	8.2.1.0 6.5.4.8 6.5.3.7
AP-205	8.7.1.0 8.6.0.7 6.5.4.16
AP-204	8.7.1.0 8.6.0.7 6.5.4.16
AP-203RP	8.7.1.0 8.6.0.7 6.5.4.16
AP-203H	8.7.1.0 8.6.0.7 6.5.4.16
AP-203R	8.7.1.0 8.6.0.7 6.5.4.16
AP-175P	8.7.1.0 8.6.0.7 6.5.4.16
AP-175DC	8.7.1.0 8.6.0.7 6.5.4.16
AP-175AC	8.7.1.0 8.6.0.7 6.5.4.16
AP-135	8.7.1.0 8.6.0.7 6.5.4.16
AP-134	8.7.1.0 8.6.0.7 6.5.4.16
AP-115	8.7.1.0 8.6.0.7 6.5.4.16
AP-114	8.6.0.7 6.5.4.16
AP-104	8.7.1.0 8.6.0.7

AP Platform	Latest Validated ArubaOS Software Versions
	6.5.4.16
AP-105	8.7.1.0 8.6.0.7 6.5.4.16
AP-103H	8.7.1.0 8.6.0.7 6.5.4.16



- For more information about Aruba's End-of-life policy and the timelines for hardware and software products at the end of their lives, see: <https://www.arubanetworks.com/support-services/end-of-life/>
- Data sheets and technical specifications for the supported AP platforms are available at: <https://www.arubanetworks.com/products/networking/access-points/>

Supported AOS-Switch Platforms



- To manage your AOS-Switches using Aruba Central (on-premises), ensure that the switch software is upgraded to 16.09.0010 or a later version. However, if you already have switches running lower software versions in your account, you can continue to manage these devices from Aruba Central (on-premises).
- Changing AOS-Switches firmware from latest version to earlier major versions is not recommended if the switches are managed in UI groups. For features that are not supported or not managed in Aruba Central (on-premises) on earlier AOS-Switch versions, changing firmware to earlier major versions might result in loss of configuration.

The following tables list the switch platforms, corresponding software versions supported in Aruba Central (on-premises), and switch stacking details.

Table 6: Supported AOS-Switch Series, Software Versions, and Switch Stacking

Switch Platform	Supported Software Versions	Recommended Software Versions	Switch Stacking Support	Supported Stack Type (Frontplane (VSF) / Backplane (BPS))	Supported Configuration Group Type for Stacking (UI / Template)
Aruba 2540 Switch Series	<ul style="list-style-type: none"> ■ YC.16.08.0019 or later ■ YC.16.09.0015 or later ■ YC.16.10.0012 or later 	<ul style="list-style-type: none"> ■ YC.16.08.0019 or later ■ YC.16.09.0015 or later ■ YC.16.10.0012 or later 	N/A	N/A	UI and Template

Switch Platform	Supported Software Versions	Recommended Software Versions	Switch Stacking Support	Supported Stack Type (VSF) / Backplane (BPS))	Supported Configuration Group Type for Stacking (UI / Template)
Aruba 2930F Switch Series	<ul style="list-style-type: none"> ■ WC.16.08.0019 or later ■ WC.16.09.0015 or later ■ WC.16.10.0012 or later 	<ul style="list-style-type: none"> ■ WC.16.08.0019 or later ■ WC.16.09.0015 or later ■ WC.16.10.0012 or later 	Yes Switch Software Dependency: <ul style="list-style-type: none"> ■ WC.16.08.0019 or later ■ WC.16.09.0015 or later ■ WC.16.10.0012 or later 	VSF	UI and Template
Aruba 2930M Switch Series	<ul style="list-style-type: none"> ■ WC.16.08.0019 or later ■ WC.16.09.0015 or later ■ WC.16.10.0012 or later 	<ul style="list-style-type: none"> ■ WC.16.08.0019 or later ■ WC.16.09.0015 or later ■ WC.16.10.0012 or later 	Yes Switch Software Dependency: <ul style="list-style-type: none"> ■ WC.16.08.0019 or later ■ WC.16.09.0015 or later ■ WC.16.10.0012 or later 	BPS	UI and Template
Aruba 3810 Switch Series	<ul style="list-style-type: none"> ■ KB.16.08.0019 or later ■ KB.16.09.0015 or later ■ KB.16.10.0012 or later 	<ul style="list-style-type: none"> ■ KB.16.08.0019 or later ■ KB.16.09.0015 or later ■ KB.16.10.0012 or later 	Yes Switch Software Dependency: <ul style="list-style-type: none"> ■ KB.16.08.0019 or later ■ KB.16.09.0015 or later ■ KB.16.10.0012 or later 	BPS	UI and Template
Aruba 5400R Switch Series	<ul style="list-style-type: none"> ■ KB.16.08.0019 or later ■ KB.16.09.0015 or later ■ KB.16.10.0012 or later 	<ul style="list-style-type: none"> ■ KB.16.08.0019 or later ■ KB.16.09.0015 or later ■ KB.16.10.0012 or later 	Yes Switch Software Dependency: <ul style="list-style-type: none"> ■ KB.16.08.0019 or later ■ KB.16.09.0015 or later ■ KB.16.10.0012 or later 	VSF	Template only



Provisioning and configuring of aruba 5400Aruba 5400R switches and Aruba 5400R switch stacks is supported only through configuration templates. Aruba Central (on-premises) does not support moving Aruba 5400R switches from the template group to a UI group. If an Aruba 5400R switch is pre-assigned to a UI group, then the device is moved to an unprovisioned group after it joins.

Data sheets and technical specifications for the supported switch platforms are available at: <https://www.arubanetworks.com/products/networking/switches/>.

Supported AOS-CX Switch Platforms

The following table lists the AOS-CX platforms, corresponding software versions supported in Aruba Central (on-premises), and switch stacking details.

Table 7: Supported AOS-CX Switch Series, Software Versions, and Switch Stacking

Switch Platform	Supported Software Versions	Recommended Software Versions	Switch Stacking Support	Supported Stack Type	Maximum Number of Stack Members	Supported Configuration Group Type (UI / Template)
AOS-CX 4100i Switch Series	10.08.0001	10.08.0001	-N/A-	-N/A-	-N/A-	UI and Template
AOS-CX 6000 Switch Series	10.08.1010 or later	10.08.1010	-N/A-	-N/A-	-N/A-	UI and Template
AOS-CX 6100 Switch Series	10.06.0110 or later	10.06.0150 or 10.07.0030	-N/A-	-N/A-	-N/A-	UI and Template
AOS-CX 6200 Switch Series	10.05.0021 or later	10.06.0150 or 10.07.0030	Yes Switch Software Dependency : 10.05.0021	VSF	8	UI and Template
AOS-CX 6300 Switch Series	10.05.0021 or later	10.06.0150 or 10.07.0030	Yes Switch Software Dependency : 10.05.0021	VSF	10	UI and Template
AOS-CX 6300 Switch Series [JL762A] Back 2 Front Power Supply SKU only	10.06.0001 or later	10.06.0150 or 10.07.0030	Yes Switch Software Dependency : 10.05.0021	VSF	10	UI and Template
AOS-CX 6405 Switch Series	10.05.0021 or later	10.06.0150 or 10.07.0030	-N/A-	-N/A-	-N/A-	Template only

Switch Platform	Supported Software Versions	Recommended Software Versions	Switch Stacking Support	Supported Stack Type	Maximum Number of Stack Members	Supported Configuration Group Type (UI / Template)
AOS-CX 6410 Switch Series	10.05.0021 or later	10.06.0150 or 10.07.0030	-N/A-	-N/A-	-N/A-	Template only
AOS-CX 8320 Switch Series	10.05.0021 or later	10.06.0150 or 10.07.0030	-N/A-	-N/A-	-N/A-	UI and Template
AOS-CX 8325 Switch Series	10.05.0021 or later	10.06.0150 or 10.07.0030	-N/A-	-N/A-	-N/A-	UI and Template
AOS-CX 8360 Switch Series	10.06.0001 or later	10.06.0150 or 10.07.0030	-N/A-	-N/A-	-N/A-	UI and Template
AOS-CX 8400 Switch Series	10.06.0001 or later	10.06.0150 or 10.07.0030	-N/A-	-N/A-	-N/A-	Template only



Provisioning and configuring of AOS-CX 6405, 6410, and 8400 switch series is supported only through configuration templates.

Data sheets and technical specifications for the supported switch platforms are available at: <https://www.arubanetworks.com/products/networking/switches/>.

Supported Aruba Mobility Controllers

Aruba Central supports provisioning, management, and monitoring of the following Aruba Mobility Controllers.

Table 8: *Supported Devices and Software Versions*

Supported Device	Latest Validated Software Versions
Aruba 7000 Series Mobility Controllers	8.8.0.0
Aruba 7200 Series Mobility Controllers	8.7.1.0
Aruba 9004 non-LTE Mobility Controllers	8.6.0.7 6.5.4.16
<p>NOTE: Controllers running ArubaOS 6.5.4.8 software image do not support WebSocket connection. You must manually add these controllers to Aruba Central. The minimum software version required for monitoring controller clusters and Mobility Conductor managed networks is ArubaOS 8.2.1.0.</p>	

The following features and enhancements are introduced.

What's New in Aruba Central (on-premises) 2.5.4.3

New Features

The following sections provide an overview of the new features that are added to Aruba Central in this release.

Support for 9004 non-LTE Mobility Controller

Aruba Central (on-premises) supports the Aruba 9004 non-LTE Mobility Controller in discovery and monitoring. After Aruba Central (on-premises) discovers these controllers, you can receive diagnostics, reports, and triggers for these controllers.

For a complete list of supported products, see *Aruba Central (on-premises) Supported Devices Guide*.

What's New in Aruba Central (on-premises) 2.5.4.2

New Features

The following sections provide an overview of the new features that are added to Aruba Central in this release.

Alerts and Events

The **Enable All** and **Disable All** buttons are added to the **Access Point**, **Switch**, **Controller**, and **Central System** tabs under the **Alerts and Events > Config** page of the WebUI. Click **Enable All** to enable all the alerts on a single click. Similarly, click **Disable All** to disable all the alerts.

For more information, see [Configuring Alerts](#).

Bulk Replacement of APs

Aruba Central (on-premises) now allows bulk replacement of Campus APs and Remote APs by using one of the following pages in the WebUI:

- **Manage > Overview > Device Replacement** under **Sites** filter.
- **Manage Sites** under **Maintain > Organization > Network Structure > Sites**.

For more information, see [Replacing APs in Bulk](#).

What's New in Aruba Central (on-premises) 2.5.4.0

Important Notes

It is recommended to upgrade all the Aruba Central (on-premises) nodes to 512 GB for optimum performance and using the 256 GB RAM might result in degraded performance. Note that the 256 GB RAM will not be supported in upcoming releases.

New Features

The following sections provide an overview of the new features that are added to Aruba Central in this release.

AOS-CX 4100i and 6100 Platform Support

Aruba Central (on-premises) now supports configuring and monitoring AOS-CX 6100 Switch Series using UI options and MultiEdit mode. Aruba Central (on-premises) also supports configuring and monitoring AOS-CX 4100i Switch Series using UI options, MultiEdit mode, and templates.

For more information, see [Supported AOS-CX Switch Platforms](#).

AOS-CX Stacking Configuration

In addition to onboarding pre-configured AOS-CX VSF stacks, Aruba Central now supports configuring and managing AOS-CX VSF stacks using UI options and templates.

VSF Stacking UI Configuration

You can now configure an AOS-CX VSF stack using UI group. The following stack-related configurations can be performed using the web UI:

- Creating a stack
- Adding a stack member
- Removing a stack member
- Modifying VSF links
- Changing the secondary member

For more information, see [Configuring AOS-CX VSF Stacks Using UI Groups](#).

VSF Stacking Template Configuration

You can now configure an AOS-CX VSF stack using templates group. The following stack-related configurations can be performed using templates:

- Creating a stack
- Adding a stack member
- Removing a stack member
- Modifying VSF links
- Changing the secondary member

For more information, see, [Configuring AOS-CX VSF Stacks Using Template Groups](#).

AOS-CX UI Configuration

The following new features are available for the AOS-CX UI group and device configuration.

Client Roles

Client roles allow administrators to assign network access to clients. A network administrator can create configuration profiles (roles) and associate them to clients. Client roles allow you to create and manage roles and attributes for the network.

For more information, see [Configuring Client Roles for AOS-CX](#).

Device Fingerprinting

Device fingerprinting allows you to classify the end devices connected to an AOS-CX switch. You can find clients' details such as the type of device, host name, vendor identification, and capability of the device, using device fingerprinting.

In this release, Aruba Central (on-premises) uses device fingerprinting to get only the clients' hostname. To enable Device Fingerprinting and DHCP Option 12 on the switch, run the following commands.

```
(config)# client device-fingerprint profile dfp1
(config)# dhcp option-num 12
```

To apply Device Fingerprinting profile to the interfaces, for example 1/1/1 to 1/1/3, run the following commands.

```
(config)# int 1/1/1-1/1/3
(config-if-1/1/1-1/1/3)# client device-fingerprint apply-profile dfp1
```



Enabling Device Fingerprinting on the AOS-CX switch displays the hostname of the client in the **Client Name** and **Hostname** columns on the **Clients** page.

HTTP Proxy

HTTP proxy enhances security for device management. An IP address can be made a proxy for all HTTP connections. If your network requires a proxy server for Internet access, ensure that you configure the HTTP proxy on the AOS-CX switch to download the image from the cloud server.

For more information, see [Configuring HTTP Proxy on AOS-CX](#).

Managed Mode

When an AOS-CX switch running 10.07 or a later version connects to Aruba Central (on-premises) 2.5.4 or a later version, Aruba Central (on-premises) takes control of modifying the configuration of the AOS-CX switch. A switch cannot be configured using the CLI when the switch is in the Aruba Central (on-premises) Managed mode. Aruba Central (on-premises) becomes the single source of configuration for the switch.

For more information, see [Getting Started with AOS-CX Deployments](#).

Multiple Browser Tab Support and Configuration Drift Warning

Aruba Central (on-premises) allows users to open multiple browser tab sessions of the same Aruba Central (on-premises) instance with a different switch group or device pages simultaneously. For example, you can open the group configuration of a switch in one browser tab and the device-level configuration of a switch in another browser tab.

Aruba Central (on-premises) stores the data from the different browser tabs separately.

However, if you edit the configuration of one AOS-CX switch in the MultiEdit mode in two different browser tab sessions, and try to save the configuration one after the other, the following events occur:

- The configuration that you save first in the editor in any of the two browser tabs is saved on the switch.
- When you try to save the configuration in the editor in the other browser tab, Aruba Central (on-premises) displays a warning that the configuration has been changed outside the current editor.
- If you ignore the warning and continue to save the configuration, Aruba Central (on-premises) overwrites the changes saved earlier with the current changes.

For more information, see [Configuring AOS-CX Switches in UI Groups](#) and [Editing Configuration Using MultiEdit on AOS-CX](#).

Source Interface

Aruba Central (on-premises) allows you to configure a single source interface for a service so that all traffic routed through the AOS-CX switch is sent with the same IP address. You can add the source interface only for Aruba Central (on-premises) and User-based Tunneling services in this release for the AOS-CX switch.

For more information see [Configuring Source Interface for AOS-CX](#).

User-Based Tunneling

User-based tunneling uses GRE to tunnel ingress traffic on a switch interface to a gateway for further processing. User-based tunneling enables a gateway to provide a centralized security policy, using per-user authentication, and access control to ensure consistent access and permissions.

For more information, see [Configuring User-Based Tunneling for AOS-CX](#).

AOS-Switch UI Configuration

The following new features are available for the AOS-Switch UI group and device and configuration.

IP Client Tracker

The IP Client tracker allows you to identify both trusted and untrusted clients that access the system. This feature is supported only on the AOS-Switch 2930F, 2930M, and 3810 switches. This feature is available on AOS-Switch versions 16.10.0008 and later.

For more information, see [Configuring IP Client Tracker on AOS-Switches](#).

Device Identifier for Device Profile

The Device Identifier configuration allows you to configure multiple identifiers for a single device profile. You can create different profiles with predefined rules applicable to a group of devices, directly connected to the switch. This feature is available on AOS-Switch version 16.10.0011 and later. For CDP, this feature is not supported by the AOS-Switch 2530 and 2920 switches.

For more information, see [Configuring Device Profile and Device Identifier on AOS-Switches](#).

Loop Protection – Disable Timer

The **Disable Timer** parameter in the **Loop Protection** tab allows you to access the switch console with non-administrative credentials. This feature allows you to configure a timer to auto-recover ports if the switch detects a loop.

For more information, see [Configuring Loop Protection on AOS-Switch Ports](#).

AI Insights

The following new Switch insights are added in this release:

Availability - Switch

- The **AOS-CX Switch Ports with High Power-over-Ethernet Problems** insight provides information on the switches that have not received required power from PoE devices connected to them.
For more information, see [AOS-CX Switch Ports with High Power-over-Ethernet Problems](#)
- The **AOS-Switch Ports with High Power-over-Ethernet Problems** insight provides information on the switches that have not received required power from PoE devices connected to them.
For more information, see [AOS-Switch Ports with High Power-over-Ethernet Problems](#)

Network Structure Page

Under Organization, the **Network Structure** landing page is added and the existing tabs such as **Groups**, **Sites**, and **Labels**, are added as tiles in this page. You can click a tile to navigate to the respective page.

For more information, see [Network Structure](#).

Group Persona

You can define a persona for devices in a group while creating a group. The persona of a device represents the role that the device plays in a network deployment. Persona and architecture are set at the group level. All devices within a group inherit the same persona from the group settings. You can save the preferred settings to apply the same persona and architecture for subsequent group creations.

For more information, see [Groups](#).

Alerts and Events

The following new alerts are added in this release:

- **Switch Reboot Alert**—Generates an alert when a switch reboots or crashes. This alert is enabled by default and the alert severity is Critical. This alert is applicable only for AOS-Switch.
For more information, see [Switch Alerts](#).

The following AP client events are added in this release:

- Client Accounting Server Timeout
- Client Authentication Server Timeout
- Radius-COA Failure
- Client Match Success
- Client Match Steer Uncontrolled Moves
- Client Match Steer No Move

For more information, see [Supported Client Events for Campus AP and Instant AP Devices](#).

Aruba Central APIs

This release introduces the following new APIs:

WLAN Configuration APIs

Following APIs are introduced in the **Configuration > WLAN Configuration** category:

- **[GET]:**
 - /configuration/full_hotspot/{group_name_or_guid}
 - /configuration/full_hotspot/{group_name_or_guid}/{mode_name}
 - /configuration/full_hotspot/{group_name_or_guid}/template
 - /configuration/full_hotspot/{group_name_or_guid}/{hotspot_name}/{mode_name}
- **[DELETE]:**
 - /configuration/full_hotspot/{group_name_or_guid}/{hotspot_name}/{mode_name}
- **[POST]:**
 - /configuration/full_hotspot/{group_name_or_guid}/{hotspot_name}/{mode_name}
- **[PUT]:**
 - /configuration/full_hotspot/{group_name_or_guid}/{hotspot_name}/{mode_name}

Troubleshooting APIs

Following APIs are introduced in the **Troubleshooting** category:

- **[GET]:**
 - /troubleshooting/v1/running-config-backup/serial/{serial}
 - /troubleshooting/v1/running-config-backup/serial/{serial}/prefix/{prefix}
 - /troubleshooting/v1/running-config-backup/name/{name}
- **[POST]:**
 - /troubleshooting/v1/running-config-backup/serial/{serial}/prefix/{prefix}
 - /troubleshooting/v1/running-config-backup/group_name/{group_name}/prefix/{prefix}

Clients APIs

Following APIs are introduced in the **Monitoring > Clients** category:

- **[GET]:**
 - /monitoring/v2/clients
 - /monitoring/v2/clients/{macaddr}

Authentication & Policy APIs

Following APIs are introduced in the **Authentication & Policy > Client Policy** category:

- **[GET]:**
 - /client_policy
- **[DELETE]:**
 - /client_policy
- **[PUT]:**
 - /client_policy

Following APIs are introduced in the **Authentication & Policy > Client Registration** category:

- **[GET]:**
 - /client_registration

- **[DELETE]:**
 - /client_registration/{mac_address}
- **[POST]:**
 - /client_registration
- **[PATCH]:**
 - /client_registration/{mac_address}

Following APIs are introduced in the **Authentication & Policy > User policy** category:

- **[GET]:**
 - /user_policy
- **[DELETE]:**
 - /user_policy
- **[PUT]:**
 - /user_policy

Service IPMS APIs

Following API is introduced in the **Service IPMS > Aruba ipms** category:

- **[GET]:**
 - /ipms-config/v1/node_list/{node_type}/{node_id}/config/address_pool/{pool_name}/ip_range/
 - /ipms-config/v1/node_list/{node_type}/{node_id}/config/
 - /ipms-config/v1/node_list/{node_type}/{node_id}/config/address_pool/
 - /ipms-config/v1/node_list/{node_type}/{node_id}/config/address_pool/{pool_name}/
 - /ipms-config/v1/node_list/{node_type}/{node_id}/config/address_pool/{pool_name}/ip_range/{range_id}/
 - /ipms-config/v1/node_list/{node_type}/{node_id}/
- **[DELETE]:**
 - /ipms-config/v1/node_list/{node_type}/{node_id}/config/
 - /ipms-config/v1/node_list/{node_type}/{node_id}/config/address_pool/{pool_name}/
 - /ipms-config/v1/node_list/{node_type}/{node_id}/config/address_pool/{pool_name}/ip_range/{range_id}/
- **[POST]:**
 - /ipms-config/v1/node_list/{node_type}/{node_id}/config/address_pool/{pool_name}/
 - /ipms-config/v1/node_list/{node_type}/{node_id}/config/address_pool/{pool_name}/ip_range/{range_id}/
- **[PUT]:**
 - /ipms-config/v1/node_list/{node_type}/{node_id}/config/address_pool/{pool_name}/
 - /ipms-config/v1/node_list/{node_type}/{node_id}/config/address_pool/{pool_name}/ip_range/{range_id}/

AI OPs APIs

Following APIs are introduced in the **AI OPs > Wi-Fi Connectivity at Global** category:

- **[GET]:**
 - /aiops/v1/connectivity/global/stage/{stage}/export
 - /aiops/v1/connectivity/site/{site_id}/stage/{stage}/export
 - /aiops/v1/connectivity/group/{group}/stage/{stage}/export

Following APIs are introduced in the **AI OPs > AI Insights List** category:

- **[GET]:**
 - /aiops/v2/insights/global/list
 - /aiops/v2/insights/site/{site_id}/list
 - /aiops/v2/insights/ap/{ap_serial}/list
 - /aiops/v2/insights/client/{sta_mac}/list
 - /aiops/v2/insights/gateway/{gw_serial}/list
 - /aiops/v2/insights/switch/{sw_serial}/list

Following APIs are introduced in the **AI OPs > AI Insight Details** category:

- **[GET]:**
 - /aiops/v2/insights/global/id/{insight_id}/export
 - /aiops/v2/insights/site/{site_id}/id/{insight_id}/export
 - /aiops/v2/insights/ap/{ap_serial}/id/{insight_id}/export
 - /aiops/v2/insights/client/{sta_mac}/id/{insight_id}/export
 - /aiops/v2/insights/gateway/{gw_serial}/id/{insight_id}/export
 - /aiops/v2/insights/switch/{sw_serial}/id/{insight_id}/export

For more information, see [New APIs](#).

Enhancements

The following sections provide an overview of the enhancements introduced in Aruba Central in this release.

Configuration

The following UI and template configuration enhancements are introduced in this release.

RRM Quiet IE in SSID

The **RRM Quiet IE** in the **Security > Fast Roaming** WLAN SSID configuration UI page allows you to enable or disable the Radio Resource Management IE profile elements advertised by an AP in the SSID profile.

For more information, see [Basic WLAN Security Parameters](#).

Mesh Support for Multiple Radios

Aruba Central now allows you to configure mesh profiles for multiple radios in the **System > Mesh** UI page. Although most mesh deployments require only a single mesh cluster profile, you can configure and apply multiple mesh cluster profiles to an individual AP.

For more information, see [Configuring Mesh for Multiple Radios](#).

Fast Roaming with Mesh

The **Mesh mobility RSSI threshold** in the **Access Points > Mesh** configuration UI page allows you to trigger fast roaming on a mobility mesh point when the RSSI of the parent is lower than the threshold value. For more information, see [Access Points Configuration Parameters](#).

EST support for Radsec and AP1x

Aruba Central now allows EST to support **Radsec**, **AP1X CA**, and **AP1X Client Cert** on the AP in the **Security > Certificate Usage** UI page. The **Radsec use EST Server** allows **Radsec** to use the certificates enrolled using the **EST Profile**.

For more information, see [Mapping IAP Certificates](#) and [Configuring an EST Profile](#)

DHCP Relay Support

The **DHCP Relay** and **Helper Address** in the **System > DHCP** UI page allows the AP to relay the DHCP requests for **Centralized DHCP Scopes**, **Local DHCP Scopes**, and **DHCP For WLANs**.

For more information, see [Configuring a Centralized DHCP Scope](#), [Configuring Local DHCP Scopes](#), and [Configuring DHCP Server for Assigning IP Addresses to IAP Clients](#)

Campus AP or Remote AP Replacement

- You can now replace a Campus AP or a Remote AP with different models on the AP Summary page.
- After the device replacement, the new AP replaces the old AP's VisualRF floor plan if the old AP was associated with a VisualRF floor plan.

For more information, see [Replacing an Access Point](#).

AOS-CX – SNMP Enable

Aruba Central allows you to enable or disable the SNMP service at the global level on AOS-CX switches. You can also select the VRF on which you want to configure SNMP on the switch.

For more information, see [Configuring SNMP on AOS-CX](#).

AOS-CX – Concurrent Authentication

Concurrent authentication is added in the **Ports** table under the **Authentication** parameter.

For more information, see [Configuring Authentication on AOS-CX](#).

AOS-CX – Port Filter

On the **Interfaces > Ports & Link Aggregations** page, in the device view, all access ports are shown by default. The port filter provides options to select **All Uplink Ports** or **All Access Ports**. You can also search for a port using the port name.

For more information, see [Configuring Ports and LAGs on AOS-CX](#).

AOS-Switch – Multiple DNS Server Support

Aruba Central allows you to configure two static IPv4 addresses for the DNS servers for AOS-Switches.

For more information, see [Configuring a Name Server](#).

IAP Local Probe Request Threshold and Min RSSI for Auth Request

To improve the performance of the indoor Wi-Fi clients, this release supports configuring a WLAN SSID with **Local Probe Request Threshold** and **Min RSSI for auth request** advanced settings. Based on your

selection, the local probe request threshold value and the Min RSSI for auth request changes to the recommended value automatically from the AI insight.

For more information, see [Configuring Wireless Network Profiles on IAPs](#).

IAP Beacon Rate in SSID Profile

The **Beacon Rate** for **2.4 GHz** band and **5 GHz** band under **Advanced Settings** in the SSID configuration page is modified. You can only set the maximum transmission rate from the **2.4 GHz** and **5 GHz** drop-down list.

For more information, see [Configuring Wireless Network Profiles on IAPs](#)

IAP Add Named VLAN

Aruba Central supports adding multiple VLAN IDs and VLAN range in the **Add Named VLAN** window in the SSID configuration page.

For more information, see [Configuring Wireless Network Profiles on IAPs](#)

Confirmation Message for Deleting a Site

The delete site action now displays a confirmation message. Deleting a site disassociates all devices that are associated with it. The disassociated devices are moved to the unassigned devices list.

For more information, see the Deleting a Site section in the [Managing Sites](#) page.

UCC Configuration

In the **UCC** configuration page, the **Facetime** protocol row and **Server** column are removed from the table. Additional system default carriers are added to the **DNS Pattern** list of **Wi-Fi Calling** protocol.

For more information, see [Configuring UCC](#).

Monitoring

The following monitoring enhancements are introduced in this release.

LLDP Details support on Campus AP

The **LLDP Neighbor** and **LLDP Port** details on the AP List page and the **LLDP Details** on the AP Summary page are now supported on Campus APs as well.

For more information, see [Network](#) and [Access Points Table](#).

Location and Contact Details on AP Summary Page

The AP Summary page for an AP with firmware version, ArubaOS 8.9.0.0 or later displays the following:

- Physical location of an AP in the Location field.
- Contact of an AP in the Contact field.

For more information, see [Device](#).

Reboot a Campus Access Point or Remote Access Point

The reboot action support is introduced for Campus Access Points and Remote Access Points in the **Details** page and **List** view.

For more information, see [Rebooting an AP in the Details Page](#) and [Rebooting an AP in the List View](#)

Radio Frequency for Campus Access Points and Remote Access Points

The following features are added for monitoring the Campus APs and Remote APs:

- The **Frames - 802.11** graph in the **RF** tab for an AP has **Issues & Transmitted Frames** filter to view the trend of transmitted frames along with retries, errors and drops in frames per second and **Issue %** for percentage of retries, errors, and drops.
- The **Radio Errors** graph has the **Physical Errors** and **MAC Errors** along with **Total Packets** in packets per second.

For more information, see [Access Point > Overview > RF](#).

AOS-CX VSF Stack

This release introduces the following enhancements to the **Switch > LAN > Ports** tab:

The switch stack faceplate now displays the following configuration and connection errors related to the AOS-CX VSF stack. You can monitor and troubleshoot these errors from the **Ports** tab:

- Auto-join eligibility error
- VSF link error
- Cabling error
- Incompatible switch firmware error

For more information, see [Monitoring AOS-CX Switch Stacks](#).

Application Visibility

The following improvements are made to the **Application > Visibility** dashboards:

- The **Application > Visibility** dashboard now includes Site and Client level support. You can now view the applications traffic flow for both the site and client.
- In the **Visibility > Applications** tab, the **Usage** and **Sent** column are removed from the **Applications** table. You can use the filter option in the **Applications** and **Category** column to filter any application and category by its name. Use the sort icon to sort the list in an ascending or descending order.
- In the **Summary** view, the **Visibility** dashboard user interface is enhanced to include a pie chart along with the stacked bars. The new graphs display both the **Applications** and **Websites** usage data, along with the clients traffic flow. You can select or deselect the application/ category check box to show or hide the traffic flow data from the pie chart and stacked bar. By hovering the mouse over the pie chart and stacked bar, you can view the size of the data.

For more information, see [Application Visibility](#).

Global Dashboard

The **Connection Experience** tile in the **Summary** view of **Manage > Overview > WiFi Connectivity** tab is changed to a time series graph. You can hover over the graph to see the connection success percentage for a specific time.

For more information, see [Wi-Fi Connectivity](#).

Clients

The **List** view in the **Clients** section is enhanced with the following features:

- The filter criterion for the **MAC Address** column supports all delimiters when searching for a MAC address. You can search for a MAC address with any delimiter, Aruba Central automatically converts it to a semicolon and displays the corresponding results.

- The  download icon is moved next to the  ellipsis icon in the **Clients** table for quick and easy access. The download icon exports the data in the table to a CSV file.
- In the **List** view, you can hover over the row for a wireless client and select **DISCONNECT FROM AP** to disconnect the client from an AP.

For more details, see [All Clients](#) and [Disconnecting a Wireless Client from an AP](#).

Download Client Live Events

The clients **Live Events** page allows you to download the list of live events to a CSV file for offline analysis. For more information, see [Client Live Events](#).

Download AP Live Events

The AP **Live Events** page allows you to download the list of live events to a CSV file for offline analysis. For more information, see [AP Live Events](#).

Health Bar on the Site Health Dashboard

The **Health Bar** in the **Overview > Site Health** tab displays a short description for the potential issues at the site and the devices connected.

For more information, see [Site Health Dashboard](#) and [The Health Bar](#).

Timezone on the Site Health Dashboard

The **Site Health** dashboard now displays the timezone and local time of the site. For example, IST-11:25 AM. For more information, see [Site Health Dashboard](#).

Timezone on the Site Health Dashboard

The clients graph in the AP **Performance** tab now displays the number of clients connected per radio. For more information, see [Access Point > Overview > Performance](#).

Wired Clients in Data Path -

The AP **Summary** page displays the number of ports that include USB ports available in the AP and the number of wired clients connected to the AP in the data path.

For more information, see [Data Path](#).

Topology Page

In the **Topology** page, the **Show Device Labels** is now renamed to **Show Device Names**.

For more information, see [Monitoring Sites in the Topology Tab](#).

UCC Monitoring

The following improvements are made to the UCC monitoring dashboard:

- The **Summary** bar is removed from the **UCC > List** page and added as a **Call Quality** column in the **Calls** table. You can filter the data by **Good**, **Fair**, **Poor**, or **Unkonwn** calls. The  and  icons are added to the **CDR** column to indicate wireless and wired connections.
- In the **UCC > Summary** page, the default option to view the graph is changed to **Protocol**. The scatter plot graph is removed for the **Health** option. The **per AP** and **per Client** graphs are also removed from this page.

For more information, see [Monitoring UCC in List View](#) and [Monitoring UCC in Summary View](#).

Floor Plan

This release introduces the following enhancements to the **Floor Plan** feature:

- The floor plan user interface for a site has been enhanced and now includes a **Summary** view and **List** view. The summary view in the **Floor Plan** dashboard now features the **All Floors** tile that displays all the available floors in a tile view for a selected site. You can add a new floor using the  add icon and can also search for an AP or floor names using the  search icon. The list view displays all the floors in a **Floor** table.
- The view mode of a floor is also enhanced to provide a better user experience. For a selected floor, you can now view the floor details in the **Floor Details** window by clicking the  icon. To view any device details in the **<Device> Details** window, click any device in the floor plan. You can also view the settings applied to the floor plan by clicking the  **eye** icon.
- The new **Floor Plan** dashboard for the site, allows you to delete or edit a floor plan directly from the summary view and the list view.

For more information, see [About Floorplans](#).

Controller Summary

The **Location** and **Contact** details are added to the **Summary** tab for a controller.

For more information, see [Controller > Overview > Summary](#).

Firmware Upgrade and Compliance

This release introduces the following enhancements to the **Firmware** dashboard:

- Under the **Later Date** radio, the **Select Zone** drop-down menu includes the **Device Local Time** option that allows you to schedule compliance and upgrade based on the local site time.
- The **Set Compliance**, **Upgrade**, and **Upgrade All** option includes a **Install on** drop-down option that allows you to select a Primary or Secondary partition to install the firmware.
- The **Firmware <Device>** table includes a **Group** column that displays the group to which the devices are associated. This information is available only in the global context.
- At the device level when you hover over the **Compliance Status** column, the following information is displayed:
 - version number and compliance configured level for a set compliance
 - date, time (UTC), and firmware version number
 - compliance configured level for a scheduled compliance

For more information, see [Upgrading Device Firmware](#).

Reports

The following enhancements are added to reports.

Uptime for an Offline IAP

In the **Network** report, the - (hyphen) symbol in the **Uptime** column of **APs** table indicates that the corresponding IAP is in offline status.

For more information, see [Report Categories](#).

Wired Client Support in Client and Network Reports

- The explicit details for the wired clients are available in the **Client Inventory**, **Client Usage**, **Client Session**, and **Network** reports.
 - In the **Client Inventory** report, the **Client Count by Connection Type** table displays the client count by wireless and wired connection type.
 - In the **Client Usage** report, you can filter the data in the **Top Ten Clients by Usage** widget by **All**, **Connection Type** (wireless, wired, or remote) or **SSIDs**. The inbound and outbound clients data usage metrics is displayed in the **Client Usage** widget by **Connection Type** (wireless, wired, or remote) and client count data metrics is displayed in the **Client Count** widget by **Connection Type** (wireless, wired, or remote).
 - In the **Network** report, you can filter the data in the **Top Ten Clients by Usage** widget by **All**, **Connection Type** (wireless, wired, or remote) or **SSIDs**. The **Wired Clients** and **Peak & Average Wired Data Usage** widgets are also added. The client count is displayed on the time series graph in the **Wired Clients** widget. The inbound and outbound peak or average data usage metrics is displayed in the **Peak & Average Wired Data Usage** widget.
 - In the **Client Session** report, the **Session Data By Role** and **Clients By Role** widgets display the details by role, connection type (wireless or wired) and SSIDs. You can filter the data in the **Top Ten Clients by Usage** widget by **All**, **Connection Type** (wireless or wired) or **SSIDs**.

For more information, see [Report Categories](#).

RF Health Report

In the **RF Health** report, the **Optional Widgets** section is introduced to include the **RF Details** and **IAP Uplink Usage** details in the CSV format. The **IAP Uplink Usage** information is available only for Instant APs with Advanced license.

For more information, see [Report Categories](#) and [Report Configuration Options](#).

Alerts and Events

The following alert and event enhancements are introduced in this release:

Suppress Alerts

In the **Site** context, while suppressing alert notifications, you can select **Override** or **Append** to either override or append the configured email addresses to receive notifications when an individual or site level alert is generated. You can also override or append the configured default recipient email list to receive alert notifications.

For more information, see [Suppressing Alert Notifications in the Site Dashboard](#) and [Adding Default Recipients](#).

Filter Events

The **Events** table columns enables filtration and search ability at all levels. It also allows free text search to enhance the search capability. You can also copy and paste text on the column headers to improve the search mechanism.

For more information, see [Viewing Events List View](#).

Client Event Filter

Aruba Central allows you to troubleshoot issues related to a wired or wireless client connected to IAPs. The

Events tab in the client context provides a detailed drill-down capability to filter events further to identify a specific issue and perform troubleshooting in both **List** and **Summary** view. It provides an aggregate view of events in different categories to provide a deep insight to the client's health.

For more information, see [Client Events](#).

Troubleshooting Tools

In the **Network Operations** app, use the filter to select a group, label, site, or a device and then, select **Analyze > Tools** to use different troubleshooting tools. The Tools menu option enables users to troubleshoot AP, gateway, and switch issues in the network through various tests available in the **Network Check**, **Device Check**, and **Commands** tabs. The following troubleshooting enhancements are introduced in this release.

VLAN-based Ping Test

Under **Analyze > Tools > Network Check**, you can now perform ping test based on VLAN IDs on IAPs running on firmware version AOS 10.3 and later, to troubleshoot network issues. The **SSID** drop-down is added to enable users to troubleshoot client SSIDs.

For more information, see [Troubleshooting AP Connectivity Issues](#).

Status Indicator in Logs Collection

In the **Analyze > Tools > Logs** tab, the **Status** column now displays a status bar when you upload logs. The status bar displays the **Scheduled**, **In Progress**, **Complete**, or **Failed** statuses as a percentage value, as the logs are uploaded. This helps customers and internal users to understand the status of the log collection.

Live Events – Wired Client Packet Capture

Aruba Central now allows read-write and admin users to launch targeted packet capture on a wired client connected to a gateway or switch. Packet capture can be done at a site level or for a selected client.

For more information, see [Client Live Events](#).

API Gateway

The **API Gateway > Usage** tab is now enhanced to include a **Current usage** status bar that displays the current usage of API calls assigned for a day along with the reset time in local time zone.

For more information, see [Viewing Usage Statistics](#).

System Administration

SCP Protocol for Data Backup

The **SCP** option is added as a **Protocol Type** in the **System Management > Backup and Restore** tab to allow users to take data backup based on the available server.

For more information, see [Backing up and Restoring Aruba Central System Data](#).

Aruba Central APIs

Following are the API changes and enhancements:

Clients APIs

The following enhancements are made in the APIs in the **Monitoring > Clients** category:

- **[GET]:**
 - /monitoring/v1/clients/wireless
 - /monitoring/v1/clients/wired

Topology APIs

The following enhancements are made in the APIs in the **Topology** category:

- **[GET]:**
 - /{site_id}
 - /devices/{device_serial}

For more information, see [Modified API](#).

For more information on configuring Aruba Central (on-premises), refer to the *Aruba Central (on-premises) Installation Guide* to reinstall the software or to set up the Aruba Central server or cluster. To start managing your networks using Aruba Central, complete the steps in this section.

Aruba Central Subscriptions

Ensure that you have a valid Aruba Central subscription key with device and network service subscriptions to deploy your network on cloud.

- If you are an existing Aruba Central customer with a valid subscription key and device licenses, access the Aruba Central UI and complete the provisioning procedures.
- If you are an existing Aruba customer with valid device licenses, but do not have an Aruba Central customer, sign up for an Aruba Central account and log in with your credentials. For more information, see *Aruba Central Help Center*.
- If you are an existing Aruba Central customer with Aruba APs and Aruba Controllers already deployed in the network, you can skip the initial steps and navigate to the configuration procedures.



offers a 90-day evaluation subscription for customers who want to evaluate the Aruba cloud solution for managing their networks. When you sign up for Aruba Central, an evaluation subscription is automatically assigned. To purchase subscriptions, contact the Aruba support team.

Provisioning Workflow

The provisioning workflow for Aruba Central deployments includes the following steps:

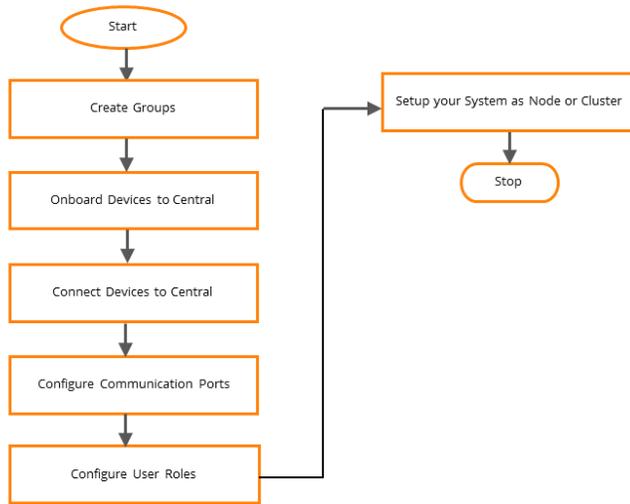


Ensure that you have completed all the steps mentioned in the Setup and Upgrade Guide.

- [Creating a Group](#)
- [Onboarding Devices](#)
- [Assigning Devices to Groups](#)
- [Assigning Labels](#)
- [Assigning Sites](#)
- [Connecting Aruba APs to Aruba Central](#)
- [Connecting Aruba Controllers to Aruba Central](#)
- [Configuring Communication Ports](#)
- [Configuring User Roles](#)
- [System Setup as Node or Cluster](#)

The following figure illustrates the workflow for getting started with Aruba Central (on-premises)

Figure 1 Aruba Central (on-premises) Getting Started Workflow



Scaling Devices for Aruba Central (on-premises)

Aruba Central supports switches, controllers, Instant APs, and Campus APs. Aruba Central can be implemented on multiple nodes. Accordingly, the number of supported devices increase.

Supported Number of Devices - Summary Table

The following table provides a summary of the number of devices supported across multiple nodes

Table 9: Maximum Number of Supported Devices

Node Size	Campus APs (AP and Controller)	Instant AP only	Switches only (AOS-Switch and AOS-CX)	Mixed-Mode
Single Node	2000	2000	1000	1600 APs (Instant AP or Campus AP) and 400 Switches (AOS-Switch or AOS-CX)
Three Node	8000	8000	3000	6000 APs (Instant AP or Campus AP) and 2000 Switches (AOS-Switch or AOS-CX)
Five Node	16000	12000	4000	12000 APs (Instant AP or Campus AP) and 4000 Switches (AOS-Switch or AOS-CX)
Seven Node	25000	16000	10000 (AOS-Switch) / 4000 (AOS-CX)	16000 APs (Instant AP or Campus AP) and 7000 Switches (AOS-Switch) [AOS-CX up to 4000 Switches]

Supported Number of Devices - Detailed Table

The following table details the number of devices that Aruba Central supports across multiple nodes.

Table 10: *Maximum Number of Supported Devices*

Nodes	Maximum Number of Supported Devices	Modes
Single Node	2000	<ul style="list-style-type: none">■ 2000 APs where APs can be either Instant APs, Campus APs, or controllers that manage APs; or a mixed deployment of any of these devices.■ 1000 switches where switches can be AOS-Switches or AOS-CX switches or a mix of the two.■ In a mixed-mode of switches and APs, up to 1600 APs and 400 switches are supported.
Three Node	8000	<ul style="list-style-type: none">■ 8000 APs, where APs can be either Instant APs, Campus APs, or APs along with the controllers that manage APs; or a mix of any of these devices.■ 3000 AOS-Switches or AOS-CX switches or a mix of the two can be deployed in switch-only deployment.■ In a mixed-mode of switches and APs, up to 6000 APs (Instant APs or Campus APs) and 2000 switches (AOS-Switch or AOS-CX) are supported.
Five Node	16000	<ul style="list-style-type: none">■ 16000 Campus APs along with the controllers that manage APs can be deployed.■ 12000 Instant APs can be deployed.■ 4000 AOS-Switches or AOS-CX switches or a mix of the two can be deployed in switch-only deployment.■ In a mixed-mode of switches and APs, up to 12000 (Instant APs or Campus APs) and 4000 (AOS-Switch or AOS-CX) switches are supported.
Seven Node	25000	<ul style="list-style-type: none">■ 25000 Campus APs along with the controllers that manage APs can be deployed.■ 10000 AOS-Switches can be deployed in AOS-Switches only deployment.■ 4000 AOS-CX switches can be deployed in AOS-CX switches only deployment.■ In a mixed-mode of switches and APs, up to 16000 APs (Instant AP or Campus APs), 7000 AOS-Switches and 4000 (AOS-Switch or AOS-CX) switches are supported.

You can check maximum number of supported devices of the Aruba Central setup in the **Account Home > Global Settings > Subscription Assignment** page.

If the device limit is exceeded, the device added to the system is displayed as *Unsubscribed* in the **Account Home > Global Settings > Device Inventory** page.

Limitations

The following features are not supported:

- Live Events on a single-node deployment
- API Streaming on a single-node deployment
- Live Packet Capture on a single-node deployment

- API Gateway on a single-node deployment
- RAPIDS on a single-node deployment
- UCC on a single-node deployment
- High Availability on a single-node deployment
- Adding and replacing node on a single-node deployment
- AI Insights is not supported on a single-node deployment
- AI Insights on single-node and 3-node clusters.

Creating a Group

Aruba Central supports creating groups and assigning devices to groups for the ease of configuration and maintenance. For example, you can create a common group for APs that have similar configuration requirements.

To create a group, complete the following procedure:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click (+) **New Group**. The **Create New Group** pop-up window opens.
4. Click the **Groups** tile.
The Groups page is displayed.
5. Expand a group from which you want to move devices to the selected group. For example, expand the **Unprovisioned Devices** group, select the devices, and then click the  **Move devices** icon.
The Move Devices page is displayed.
6. Enter a name for the group.
By default, enables template-based configuration method for switches and UI-workflow-based configuration method for AP
7. To enable template-based configuration method for all device categories:
 - For Instant APs, select the **IAP** check box.
 - For Switches, ensure that **Switch** check box is selected. The **Switch** check box is enabled by default.
8. To enable UI-based configuration method on all device categories:
 - a. For APs, ensure that the **IAP** checkbox is cleared.
 - b. For switches, clear the **Switch** checkbox.
9. Assign a password. This password enables administrative access to the device interface.
10. Click **Add Group**.



You can also create a group that uses different provisioning methods for switch and IAP device categories. For example, you can create a group with template-based provisioning method for switches and UI-based provisioning method for APs.

For more information, see [Groups](#)

Onboarding Devices

Aruba Central (on-premises) allows you to onboard devices using the offline mode. In this mode, you can manually add devices to the inventory by using one of the following options:

- [Adding Devices Using MAC Address and Serial Number](#)
- [Adding Devices Using a CSV File](#)
- [Adding Devices Using PSK](#)
- [Adding Mobility Controllers](#)

Adding Devices Using MAC Address and Serial Number



Aruba Central (on-premises) supports this method to also add factory default AOS-CX switches.

To add devices:

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.
2. In the **Device Inventory** page, click **Add Devices**.
3. Enter the **Serial Number**, **MAC address**, and **Part Number** of the devices. You can add up to 32 devices.

Adding Devices Using a CSV File

To import devices from a CSV file:

1. Create a CSV file with the device list.
2. Ensure that the CSV file includes column headers for part number, MAC address, serial number, and other optional fields such as firmware version and IP address of the device.
3. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.
4. In the **Device Inventory** page, click **Import Devices Via CSV**.
5. Browse to your local directory, select the CSV file, and then click **Open**.
6. Click **Import**.

Adding Devices Using PSK

Aruba Central (on-premises) supports adding devices using a pre-shared key (PSK). If you want to add APs and switches to Aruba Central (on-premises), you can configure a shared secret key on the DHCP server. When you add the same shared secret key in Aruba Central (on-premises), the devices with the known PSK string are added to the Aruba Central (on-premises) device inventory.

Adding Instant APs Using PSK

To onboard APs using PSK:

1. Configure the following parameters on the DHCP server to which the APs connect.
 - Option 60 with **Aruba InstantAP**
 - Option 43 in the format **<org>:<Aruba-Central IP>:<shared secret>**



Ensure that you provide only the IP address and not the host name.

2. In the Aruba Central (on-premises) UI, go to **Account Home** and under **Global Settings**, click **Device Inventory**.
3. Click **Add/Delete PSK**. The **Add/Delete PSK** window opens.
4. Enter the PSK name and PSK details.
5. Click **Add**.
6. Reboot the Instant APs.
7. Ensure that the Instant APs get the IP address from the DHCP server and connect to Aruba Central (on-premises).

Adding AOS-Switches Using PSK

To onboard AOS-Switches using PSK:

1. Ensure that the switches are running factory default configuration.
2. Configure the following parameters on the DHCP server:
Option 43 in the format **<Group>:<Topfolder>:<folder1>,<Aruba-Central IP>,<shared secret>**
Option 60
3. In the Aruba Central (on-premises) UI, go to **Account Home** and under **Global Settings**, click **Device Inventory**.
4. Click **Add/Delete PSK**. The **Add/Delete PSK** window opens.
5. Enter the PSK name and PSK details.
6. Click **Add**.
7. Reboot the switches.
8. Ensure that the switches get an IP address from the DHCP server, and connect to Aruba Central (on-premises).

Adding AOS-CX switches

Aruba Central (on-premises) supports adding factory default and pre-configured AOS-CX switches.

Adding factory default AOS-CX switches

To add factory default AOS-CX switches:

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.
2. In the **Device Inventory** page, click **Add Devices**.
3. Enter the **Serial Number**, **MAC address**, and **Part Number** of the switches.

Adding pre-configured AOS-CX switches

To add pre-configured AOS-CX switches:

1. Create a backup of the configuration
2. Reset the switch using the `erase all zeroize` command in the CLI.

This initiates ZTP on the switch, enabling the switch to obtain the IP address from the option 43 sent by the DHCP server and then connect to Aruba Central (on-premises).



The `<Group>:<Topfolder>:<folder1>` portion in the option 43 is not used for AOS-CX switches.

Adding Mobility Controllers

Aruba Central (on-premises) offers monitoring service for WLAN networks configured and managed using Aruba Mobility Controllers.

Aruba Central (on-premises) allows you to onboard and monitor controller clusters, the Mobility Conductor setup, and the conductor and local controller setup.

When you add a conductor controller or a Mobility Conductor, Aruba Central (on-premises) discovers all the associated controllers and campus APs, and adds them to the device inventory.



Aruba Central (on-premises) does not support configuring controllers. To configure and deploy controllers, use the ArubaOS WebUI and CLI.

Before You Begin

Before adding controllers to Aruba Central (on-premises), ensure that the controller has the following parameters configured:

- Management Server profile—The Aruba Central (on-premises) server must be configured as a management server on the controller.
- Advanced Monitoring Messages—Enable AMON for communication between the Aruba Central (on-premises) server and controller. When AMON is enabled on the controller over UDP 8211, the controller periodically sends information about user sessions, AP and client association, and other such information required for managing and monitoring controllers on Aruba Central (on-premises).
- Syslog Messages and SNMP Traps—Although AMON is a preferred option for polling data from controllers, to obtain data pertaining to AP lists, you may want to enable SNMP, and configure SNMP traps and syslog server for logging system events.
- Websocket connection—To enable controller firmware upgrade and troubleshooting from Aruba Central (on-premises), ensure that the Aruba Central (on-premises) server URL and IP address are configured on the controllers running ArubaOS 6.5.3.6 or later.
- For more information on configuring controllers, see *ArubaOS User Guide*.



Controllers running ArubaOS 6.5.4.8 version do not support Websocket connection, due to which Aruba Central (on-premises) cannot onboard these controllers.

Configuring SNMP and HTTPS Connection Profiles

To configure connection profiles for adding controllers:

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.
2. Click **Controller Management**. The **Controller Management** pop-up window opens.
3. Under **Connection Profile**, configure the SNMP and HTTPS connection profiles as per your requirement.
4. To add an SNMP connection profile:
 - a. Click **SNMP** and add the following details:
 - **Name**—Name of the connection profile.
 - **SNMP Version**—SNMP version, for example V2 or V3.
 - **Community String**—Community string required for the management of controller.
 - Click **Save**.
5. To add an HTTPS connection profile:
 - a. Click **HTTPS** and add the following details:
 - **Name**—Name of the connection profile.
 - **HTTPS User**—Username for HTTPS authentication.
 - **HTTPS Password** and **Confirm HTTPS Password**—Password for HTTPS authentication.
 - b. Click **Save**.

Adding a Controller

To add controllers, click the **Add MM/Controllers** tab.

1. Click **+** to add a controller.
2. Enter a name for the controller.
3. Enter the IP address of the controller.
4. Select an SNMP or HTTPS profile.
5. Click **Save**.
6. Return to the **Device Inventory** page and verify if your controller is added.



Controllers come up in the **Monitoring** page only if it is licensed. You can choose auto subscription or license each controller manually. For more information on licensing, see [Managing Licenses](#).

Viewing Devices

The devices provisioned in your account are listed under **Global Settings > Device Inventory page**.

Table 1 shows the contents of the Device Inventory page.

Table 11: *Predefined Variables Example*

Parameter	Description
MAC Address	MAC address of the device.

Parameter	Description
Type	Type of the device, for example AP or Switch.
IP address	IP address of the device.
Device Name	Name of the device.
Labels	Name of the label to which the device are assigned.
Model	Hardware model of the device.
Group	Name of the group to which the device is assigned. This column is displayed only for the Aruba Central Standard Enterprise mode users.
Status	Status of the subscription assignment.

Deleting a Device

To delete a device:

1. On the **Global Settings > Device Inventory** page, click **Delete Devices**.
The **Delete Devices** window opens and displays the list of devices provisioned in your network.
2. Select the devices from the list.
3. Click **Delete**.

Assigning Devices to Groups

To assign a device to a group, in the **Account Home** page, under **Global Settings**, click **Device Inventory**:

1. Select the device that you want to assign to a group.
2. Click **Assign Group**. The **Assign Group** pop-up window opens.
3. Select the group to which you want to assign.
4. Click **Assign Device(s)**.

To assign a device to a group from the **Groups** page:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Groups** tile.
The Groups page is displayed.
4. Expand a group from which you want to move devices to the selected group. For example, expand the **Unprovisioned Devices** group, select the devices, and then click the  **Move devices** icon.
The Move Devices page is displayed.
5. Select the **Destination Group** from the drop-down list.

6. Click **Move**.

The selected devices are moved to the destination group. These devices will adopt the destination group configuration.

Assigning Labels

In Aruba Central, assigning Sites and Labels is an optional step. Labels refer to the tags attached to a device provisioned in the network. You can use labels for tagging devices to a specific area in a physical location, to an owner or a specific branch, or a business unit. You can use these labels as filters for monitoring branch and device health, and generating reports.

To assign a label to a device, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Labels** tile.
The **Manage Labels** page is displayed.
4. Locate the label to which you want to assign a device. You can also create a new label by clicking **Add Label** and providing a label name.
5. In the table that lists the labels, you can perform one of the following actions:
 - Click **All Devices** to view all devices.
 - Click **Unassigned** to view all the devices that are not assigned to any labels.
6. Select **Unassigned**. A list of devices that are not assigned to any label is displayed.
7. Select one or several devices from the list of devices.
8. Drag and drop the selected devices to a specific label. A pop-up window opens and prompts you to confirm the label assignment.
9. To confirm the assignment, click **Yes**.

For more information, see [Managing Labels](#).

Assigning Sites

In Aruba Central, assigning Sites and Labels is an optional step. A site in Aruba Central refers to a physical location where a set of devices are installed; for example, campus, branch, or a venue. You can create a branch or campus site; for example Branch A or Campus A, for a specific geographical location and assign devices to it. You can use these sites as filters for viewing your deployment topology, monitoring network and device health.

To assign devices to a site:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Sites** tile.
The **Manage Sites** page is displayed.
4. Under **Manage Sites**, locate the site to which you want to assign a device. You can also add a new site by clicking **(+)New Site** and providing details, such as site name and address.

5. To view devices that are not assigned to any site, click **Unassigned**.
6. Select one or several devices from the list of devices.
7. Drag and drop the devices to the site on the left. A pop-up window opens and prompts you to confirm the site assignment.
8. To confirm the assignment, click **Yes**.

For more information, see [Managing Sites](#).

Connecting Aruba APs to Aruba Central

The Aruba IAPs have the ability to automatically provision themselves and connect to Aruba Central (on-premises) once they are powered on.

To provision IAPs:

1. Connect your IAP to the provisioning network through PSK onboarding.
2. Wait for the device to obtain an IP address through DHCP.
3. Observe the LED indicators. For more information, refer to the *AP Installation Guide*.

When an IAP identifies Aruba Central (on-premises) as its management entity, it connects to Aruba Central (on-premises) and shows up as a connected device in Aruba Central (on-premises).

Connecting Aruba Controllers to Aruba Central

The Aruba Controllers can automatically provision themselves and connect to Aruba Central once they are powered on.

To provision Controllers you must configure SNMP and HTTPS Connection Profiles.

To configure connection profiles for adding controllers:

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.
2. Select **Controllers** and click **Controller Management**. The **Controller Management** pop-up window opens.
3. Under **Connection Profile**, configure the SNMP and HTTPS connection profiles as per your requirement.
4. To add an SNMP connection profile:
 - a. Click **SNMP** and add the following details:
 - **Name**—Name of the connection profile.
 - **SNMP Version**—SNMP version, for example V2 or V3.
 - **Community String**—Community string required for the management of controller.
 - Click **Save**.
5. To add an HTTPS connection profile:
 - a. Click **HTTPS** and add the following details:
 - **Name**—Name of the connection profile.
 - **HTTPS User**—Username for HTTPS authentication.
 - **HTTPS Password** and **Confirm HTTPS Password**—Password for HTTPS authentication.
 - b. Click **Save**.

Adding a Controller

To add controllers, click the **Add MM/Controllers** tab.

1. Click **+** to add a controller.
2. Enter a name for the controller.
3. Enter the IP address of the controller.
4. Select an SNMP or HTTPS profile.
5. Click **Save**.
6. Return to the **Device Inventory** page and verify if your controller is added.



Controllers come up in the **Monitoring** page only if it is licensed. You can choose auto subscription or license each controller manually. For more information on licensing, see [Managing Licenses](#).

Connecting Aruba Switches to Aruba Central

The Aruba switches have the ability to automatically provision themselves and connect to Aruba Central once they are powered on. The switches support zero touch provisioning (ZTP) using which devices obtain the IP address in the option 43 from the DHCP server.

To provision Switches:

1. Connect your switches to the provisioning network.
2. Wait for the device to obtain an IP address through DHCP.
3. Observe the LED indicators. For more information, refer to the *Switch Installation Guide*.
 - If the device has factory default configuration, you must manually add either the serial number, MAC address, or part number of the switch in Aruba Central (on-premises) for the switch to connect to Aruba Central (on-premises).
 - If the device has preconfigured configuration, you must first create a backup of the configuration, then reset the switch using the `erase all zeroize` command in the CLI. This initiates ZTP on the switch, enabling the switch to obtain the IP address from the option 43 sent by the DHCP server and then connect to Aruba Central (on-premises).
 - When a Switch identifies Aruba Central as its management entity, it connects to Aruba Central and shows up as a connected device in Aruba Central.
 - If the Switch is running a software version that is not compatible with Aruba Central, upgrade the Switch to a supported software version and wait for it to connect to Aruba Central.

Configuring Communication Ports

Most of the communication between devices on the remote site and Aruba Central server is carried out through HTTPS (TCP 443). However, verify if the ports listed in [Table 12](#) are open to allow the Aruba Central server and the managed devices to communicate over a network firewall.

Table 12: *Domain Names and Ports for Aruba Central*

Protocol and port	Domain Names and Purpose
Inbound Ports Traffic	

Protocol and port	Domain Names and Purpose
TCP 443	To access and manage Aruba Central (on-premises).
	For HTTPS and websocket between Aruba Central (on-premises) and devices.
UDP 8211, 8285	To receive AMON messages and view data for controllers in the Aruba Central monitoring dashboard.
TCP 22	For management access through SSH and cluster setup.
	For CLI between Aruba Central (on-premises) and devices.
TCP 80	For browser redirect from HTTP to HTTPS.
TCP 2379, 2380, 4433, 6433, and 10250	For communication between Aruba Central nodes in a cluster.
TCP 4343	To access the setup-wizard installation.
TCP 30633	To allow the devices to set up a connection with the OpenFlow controller.
TCP 8888	For HTTP-based firmware image download for CX and PVOS devices.
Outbound Ports Traffic	
TCP 25, 456, or 587	Dependent on the SMTP configuration for alerts, reports, and Aruba Central (on-premises) account registration.
UDP 123	To access ntp.ubuntu.com . NOTE: This is default destination. Users can reconfigure this port.
UDP 161, 162	For SNMP and traps.
TCP 4343	For device bootstrap to controllers.
TCP 22	To access nexus2.airwave.com to support connection.

Protocol and port	Domain Names and Purpose
TCP 443	To access coreupdate.central.arubanetworks.com and allow Aruba Central to check firmware versions for automatic upgrades.
	To access images from the following registries: <ul style="list-style-type: none"> ■ quay.io ■ docker.io ■ docker.com ■ docker.elastic.co <p>NOTE: Quay.io traffic can originate from multiple IP ranges, refer to the article to allow traffic from Quay nodes.</p>
	To access maps.googleapis.com to translate address.
	To access api.mapbox.com to view maps from user's browser.
	To access d1c50u1zbkqmph.cloudfront.net for CDN from user's browser.
	To access https://enterpriselicence.hpe.com for licensing.
	To access help.arubanetworks.com for documentation from user's browser.



The Aruba appliance opens multiple ports. Aruba recommends that you host the Aruba appliance behind a firewall.

Configuring User Roles

A role refers to a logical entity used for determining user access to devices and application services in Aruba Central. Users are always tagged to roles that govern the level of user access to the Aruba Central applications and services.

Aruba Central supports a set of predefined roles with different privileges and access permissions. You can also configure custom roles.

Predefined User Roles

The **Users and Roles** page allows you to configure the following types of users with system-defined roles:

Table 13: *Predefined User Roles*

Application	User Role	Privilege
Account Settings	admin	Administrator for the Account Home page.
	readwrite	Can view and modify settings in the Account Home page and all Global Settings pages.
	readonly	Can view the Account Home page and all Global Settings pages.

Application	User Role	Privilege
Network Operations	admin	Administrator for the Account Home page.
	deny-access	Cannot view the Network Operations application.
	readonly	Can view all pages in the Network Operations application.
	readwrite	Has access to view and modify data using the Aruba Central UI or APIs. However, the user cannot execute APIs to: <ul style="list-style-type: none"> Perform operations in the following pages: <ul style="list-style-type: none"> ● Account Home > Users and Roles ● Network Operations application > Organization > Sites and Labels

Custom Roles

Along with the predefined user roles, Aruba Central also allows you to create custom roles with specific security requirements and access control. However, only users with the administrator role and privileges can create, modify, clone, or delete a custom role in Aruba Central.

With custom roles, you can configure access control at the application level and specify access rights to view or modify specific application services or modules. For example, you can create a custom role that allows access to a specific applications like **Network Management** and assign it to a user.



tenant account users cannot add, edit, or delete roles.

Adding a Custom Role

The following are the permissions that you can associate with a custom role:

- User roles with **Modify** permission can perform add, edit, or delete actions within the specific module.
- User roles with **View Only** permission can only view the specific module.
- User roles with **Block** permission cannot view that particular module.

To add a custom role, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**.
2. Click the **Roles** tab.
3. Click **Add Role**. The **New Role** window is displayed.
4. Specify a name for the role.
5. From the drop-down list, select one of the following:
 - **Account Home**—To manage access to devices and subscriptions in Aruba Central.
 - **Network Operations**—To set permissions at the module level in the **Network Operations** application.
 - **ClearPass Device Insight**—To set permissions at the module level in the **ClearPass Device Insight** application.
6. For Network Management and MSP modules, you can set access rights at the module level.
7. Click **Customize**. Select one of the following options for each module as required:

8. Click **Save**.
9. Assign the role to a user account as required.

Module Permissions

Aruba Central allows you to define user roles with **view** or **modify** permissions. You can also block user access to some modules.

Aruba Central supports setting permissions for the following modules:

Table 14: *Permissions*

Application	Module	Description
Account Home	Devices and Subscription	Allows users to add devices and assign keys and subscriptions to devices.
Network Operations	Group Management	Allows users to create, view, modify, and delete groups and assign devices to groups.
	Devices and Subscription	Allows users to add devices and assign subscriptions to devices.
	Network Management	Allows users to configure, troubleshoot, and monitor Aruba Central-managed networks.
	VisualRF	Allows user to access VisualRF and RF heatmaps.
	Unified Communications	Allows users to access the Unified Communications pages.
	Reports	Allows users to view and create reports.

Viewing User Role Details

To view the details of a user role, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**.
2. Click the **Roles** tab. The **Roles** tab displays the following information:
 - **Role Name**—Name of the user role.
 - **Allowed Applications**—The applications to which the users have access.
 - **Assigned Users**—Number of users assigned to a role.

Editing a User Role

To edit a user role, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**.
2. Click the **Roles** tab.
3. In the **List of Roles** table, select the role and click the edit icon.
4. In the **Edit Role <"Rolename">** window, modify the permissions set for module(s).
5. Click **Save**.

Deleting a User Role

To delete a user role, ensure that the role is not associated to any user and complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**.
2. Click the **Roles** tab.
3. In the **List of Roles** table, select the role and click the delete icon.
4. Confirm role deletion in the **Confirm Action** dialog box.

System Setup as Node or Cluster

Aruba Central can be implemented on multiple nodes. Accordingly, the number of supported devices increases.

You can check the maximum number of supported devices of the Aruba Central set up in the **Account Home > Global Settings > Subscription Assignment** page.

If the device limit is exceeded, the device added to the system is displayed as *Unsubscribed* in the **Account Home > Global Settings > Device Inventory** page.

For more information on verifying the system setup see, [System Management](#).

Verifying Device Configuration Status

Aruba Central provides an audit dashboard for reviewing configuration changes for the devices provisioned in UI and template groups. The **Configuration Audit** menu option under **Manage > Devices** allows you to view the configuration template errors, configuration sync, and device level configuration overrides.

Viewing Configuration Audit Page

To access the **Configuration Audit** page:

- For APs:
 - a. In the **Network Operations** app, use the filter bar to select a group or device.
 - b. Under **Manage > Devices > Access Points**.
 - c. Click the  configuration icon and click **Show Advanced**.
 - d. Click **Configuration Audit**.
- For switches:
 - a. In the **Network Operations** app, use the filter bar to select a group or device
 - b. Under **Manage > Devices > Switches**.
 - c. Click the  configuration icon and click **Show Advanced**.
 - d. Click **Configuration Audit**.

Configuration Synchronization Errors

The devices managed by Aruba Central receive the configuration changes from Aruba Central. Occasionally, an Aruba Central-managed device may fail to receive a configuration change from Aruba Central. Such instances are marked as **Failed changes** in the **Configuration Audit** dashboard. If the condition persists, contact Aruba Technical Assistance.

Local Overrides

In Aruba Central, devices are assigned to groups that serve as the primary configuration elements. Occasionally, based on the network provisioning requirements, the administrators may need to modify the configuration of a specific device in a group. As these modifications override the configuration settings that the device has inherited from the group, Aruba Central marks these as local overrides.

Viewing Status for a Template Group

On selecting a template group, the **Configuration Audit** page displays the options listed in [Table 15](#):

Table 15: Configuration Audit Status for a Template Group

Data Pane Content	Description
Template Errors	<p>Provides details of the number of devices with template errors for the selected template group.</p> <p>Devices deployed in the template group are provisioned using configuration templates. If there are errors in the templates or variable definitions, the configuration push to the devices fails. Aruba Central records such failed instances as template errors and displays these errors on the Configuration Audit page.</p> <p>To view a complete list of errors, click View Template Errors. The Template Errors window allows you to view and resolve the template errors issues if any for the devices in the group.</p>
Configuration Status	<p>Provides details of the number of devices with configuration sync errors for the selected template group.</p> <p>To view the configuration sync errors, click View Details. The Configuration Sync Issues window is displayed with the following tabs:</p> <ul style="list-style-type: none">■ Not In Sync Configuration—Displays the configuration changes that are not synched with the switch.■ Device Running Configuration—Displays the running configuration on the switch. <p>To resolve the configuration sync errors, click Re-Sync Configuration. Aruba Central will attempt to synchronize the configuration with the switch again. Click Yes in the confirmation window. To check whether the configuration was synchronized and pushed to the switch, see the Audit Trail page.</p>
Group & Device Modes	<p>Allows you to view and edit devices that are set to managed or monitored operation mode.</p> <ul style="list-style-type: none">■ Managed Mode Devices—Click the View & Edit link. The Managed Mode Devices window is displayed with the list of devices operating in the managed mode. To change the device operation mode to monitored, click Change to Monitor Mode.■ Monitored Mode Devices—Click the View & Edit link. The Monitored Mode Devices window is displayed. To change the device operation mode to managed, click Change to Managed Mode.

Table 15: Configuration Audit Status for a Template Group

Data Pane Content	Description
Configuration Backup & Restore	Allows you to create a backup of templates and variables applied to the devices in the template group. . <ul style="list-style-type: none"> ■ New Configuration Backup—Allows you to create a new backup of templates and variables applied to the devices in the template group.
All Devices	The All Devices table provides the following device information for the selected group: <ul style="list-style-type: none"> ■ Name—The name of the device. ■ Type—The type of the device. ■ Auto Commit—The status of the auto commit state for all the devices within the group. ■ Config Sync—Indicator showing configuration sync errors. ■ Template Error—Indicator showing configuration template errors for the devices deployed in template groups.

Viewing Status for Devices Assigned to a Template Group

On selecting a device that is provisioned in a template group, the **Configuration Audit** page displays the options listed in [Table 15](#):

Table 16: Configuration Audit Status for Devices in Template Groups

Data Pane Content	Description
Template Applied	Displays the template that is currently applied on the selected device.
Template Errors	Displays the number of template errors for the selected device. To view a complete list of errors, click View Template Errors .
Configuration Status	Displays the configuration sync errors for the selected device. To view the configuration sync errors, click View Details . The Configuration Sync Issues window is displayed with the following tabs: <ul style="list-style-type: none"> ■ Not In Sync Configuration—Displays the configuration changes that are not synched with the switch. ■ Device Running Configuration—Displays the running configuration on the switch. <p>To resolve the configuration sync errors, click Re-Sync Configuration. Aruba Central will attempt to synchronize the configuration with the switch again. Click Yes in the confirmation window. To check whether the configuration was synchronized and pushed to the switch, see the Audit Trail page.</p>
Config Comparison Tool	Allows you to view the difference between the current configuration (Device Running Configuration) and the configuration that is yet to be pushed to the device (Attempted Configuration). To view the running and attempted configuration changes side by side, click View .
Group & Device Modes	Allows you to view and edit devices that are operating in the managed or monitored mode. <ul style="list-style-type: none"> ■ Managed Mode Devices—Click the View & Edit link. The Managed Mode Devices window is displayed with the list of devices operating in the managed mode. To change the device operation mode to monitored, click Change to Monitor Mode.

Table 16: Configuration Audit Status for Devices in Template Groups

Data Pane Content	Description
	<ul style="list-style-type: none">■ Monitored Mode Devices—Click the View & Edit link. The Monitored Mode Devices window is displayed. To change the device operation mode to managed, click Change to Managed Mode.

Viewing Configuration Status for a UI Group

On selecting a UI group, the **Configuration Audit** page displays the options listed in [Table 15](#).

Table 17: Configuration Audit Status for a UI Group

Data Pane Content	Description
Configuration Status	<p>Displays the number of devices with configuration sync errors for the selected UI group.</p> <p>To view the configuration sync errors, click View Details. The Configuration Sync Issues window is displayed with the following tabs:</p> <ul style="list-style-type: none">■ Not In Sync Configuration—Displays the configuration changes that are not synched with the switch.■ Device Running Configuration—Displays the running configuration on the switch. <p>To resolve the configuration sync errors, click Re-Sync Configuration. Aruba Central will attempt to synchronize the configuration with the switch again. Click Yes in the confirmation window. To check whether the configuration was synchronized and pushed to the switch, see the Audit Trail page.</p>
Local Overrides	<p>Displays the number of devices with local overrides. To view a complete list of overrides, click the Manage Local Overrides link. The Local Overrides window is displayed.</p> <ul style="list-style-type: none">■ To preserve the overrides, click Close.■ To remove the overrides, select the group name with local override, click Remove and click OK.
All Devices	<p>The All Devices List table provides the following device information for the selected group:</p> <ul style="list-style-type: none">■ Name—The name of the device.■ Type—The type of the device.■ Auto Commit—The status of the auto commit state for all the devices within the group.■ Config Sync—Indicator showing configuration sync errors.■ Local Override—Indicator showing configuration overrides for the devices deployed in UI groups.

Viewing Configuration Status for Devices Assigned to a UI Group

On selecting a device assigned to a UI group, the **Configuration Audit** page displays the options listed in [Table 15](#).

Table 18: Configuration Audit Status for a Device Assigned to a UI Group

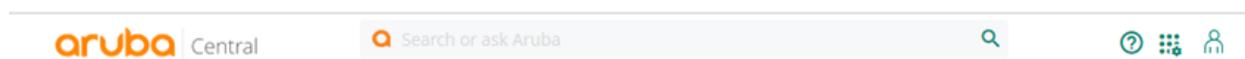
Data Pane Content	Description
Configuration Status	<p>Displays the number of devices with configuration sync errors for the selected device.</p> <p>To view the configuration sync errors, click View Details. The Configuration Sync Issues window is displayed with the following tabs:</p> <ul style="list-style-type: none">■ Not In Sync Configuration—Displays the configuration changes that are not synced with the switch.■ Device Running Configuration—Displays the running configuration on the switch. <p>To resolve the configuration sync errors, click Re-Sync Configuration. Aruba Central will attempt to synchronize the configuration with the switch again. Click Yes in the confirmation window. To check whether the configuration was synchronized and pushed to the switch, see the Audit Trail page.</p>
Local Overrides	<p>Displays the number of local overrides. To view a complete list of overrides, click Manage Local Overrides.</p> <p>The Local Overrides window is displayed. The overrides are grouped based on the features that are configured in the UI and are displayed as drop-down sections. For example, all overrides for IGMP are listed under a separate drop-down with the heading IGMP.</p> <ul style="list-style-type: none">■ To preserve the overrides, click Close.■ To remove the overrides, click Remove, and click OK.

Using the Search Bar

The search bar in the **Network Operations** app enables users to search for clients, devices, and infrastructure connected to the network. The search engine uses Natural Language Processing (NLP) to analyze queries and return relevant search results.

The following figure illustrates the search bar option in Aruba Central.

Figure 2 Search Bar



To start a search in the Aruba Central UI, click the search bar or press / (forward slash) on your computer keyboard.

The search results display cards relevant to the search terms. The **Search Cards** display a monitoring summary of the devices in the **Network Operations** app.

Device Search Terms

The search bar helps you to search all devices monitored by Aruba Central. The search enables you to navigate to the monitoring pages of the devices in the **Network Operation** app.

Using the search bar you can perform the following tasks:

- Hover over a search card to view the monitoring summary for the device.
- Click the client name to open the **Device Details** page.

The cards might vary for each device based on the context. You can click on the search card to navigate to the details page of that device in the app.

You can see the search cards when you search with the device name, IP address, MAC address, site, or label. Following are the examples for APs, switches, and controllers.

Figure 3 Search Card for a Device Name

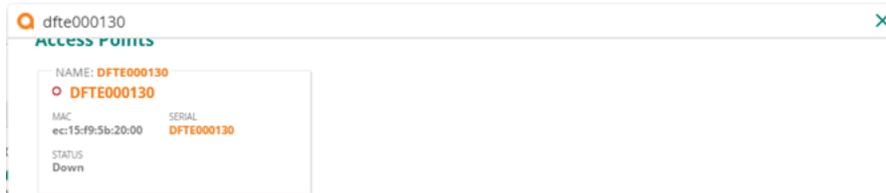


Figure 4 Search Card for a Device Serial

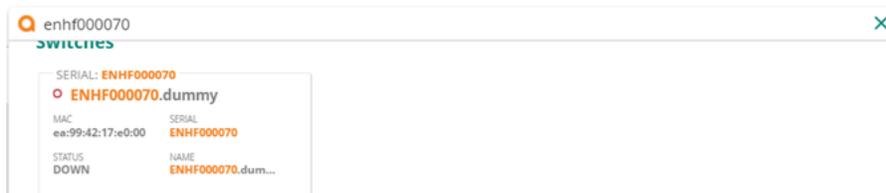
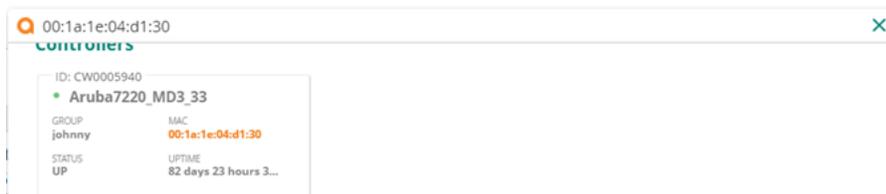
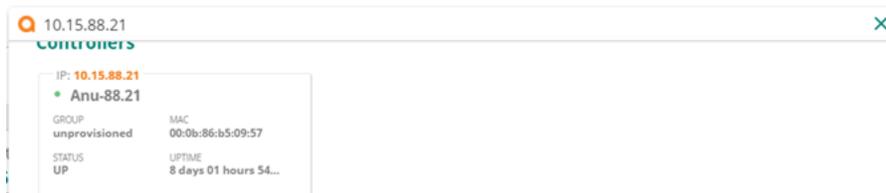


Figure 5 Search Card for a Device MAC Address



Following is an example for the device serial search:

Figure 6 Search Card for a Device IP Address



Client Search Terms

The search bar helps you to search a client's information in the **Network Operation** app.

Using the search bar you can perform the following tasks:

- Hover over a client search card to view the monitoring summary for the client.
- Click the client name to open the **Client Details** page.

You can see the search cards when you search with the client name, IP address, or MAC address. You can see the following details on the search card:

- Client Name
- IP Address
- MAC Address
- Username
- Status

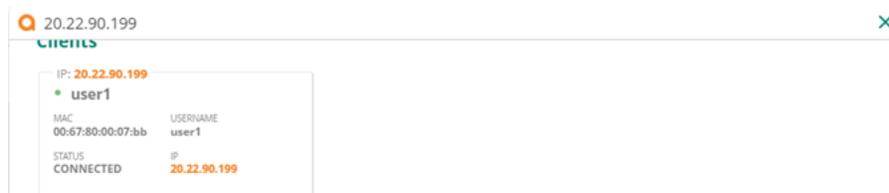
Following is an example for the client name search:

Figure 7 Search Card for Client Name



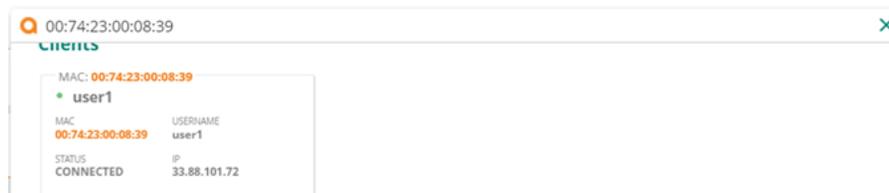
Following is an example for the client IP address search:

Figure 8 Search Card for Client IP Address



Following is an example for the client MAC address search:

Figure 9 Search Card for Client MAC Address



Site Search Terms

The search bar helps you to search a site's information in the **Network Operation** app.

Using the search bar you can perform the following tasks:

- Hover over a client search card to view the monitoring summary for the site.
- Click the client name to open the **Site Details** page.

Following is an example for the site search:

Figure 10 Search Card for a Site

2.5.3-Site-NY

We found the following results:

Access Points

MAC: 44:48:c1:c4:c6:6c 44:48:c1:c4:c6:6c	MAC: 24:f2:7f:c6:4c:7c 24:f2:7f:c6:4c:7c
---	---

Virtual Controllers

MAC: 44:48:c1:c4:c6:6c SetMeUp-C4:C6:6C	MAC: 24:f2:7f:c6:4c:7c IAP-70
--	----------------------------------

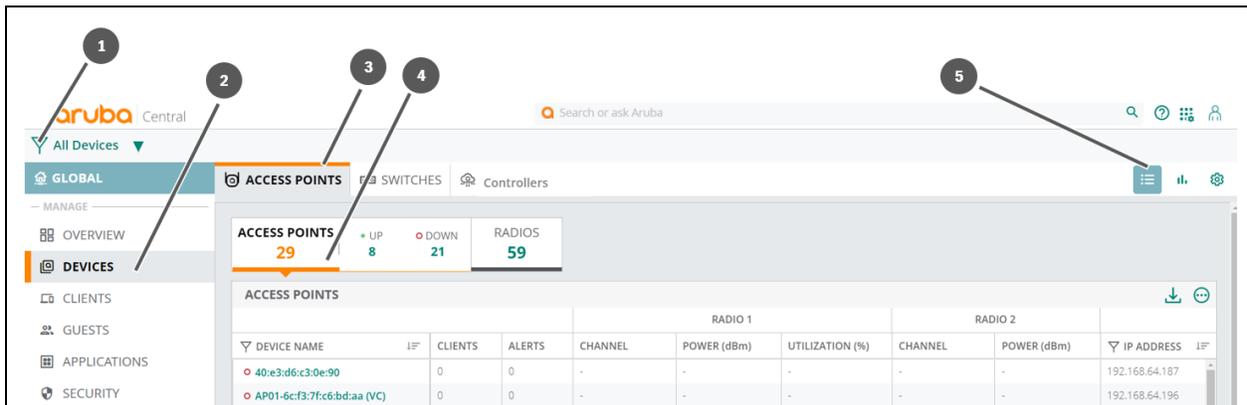
Chapter 5

About the Network Operations App User Interface

The **Network Operations** app is one of the apps in Aruba Central that helps to manage, monitor, and analyze your network. you can manage your respective accounts end-to- end. Here, the customers have complete access to their accounts. You can also provision and manage the accounts.

The following image displays the navigational elements of the **Network Operations** app.

Figure 11 Navigation Elements of the Network Operations App



Callout Number	Description
1	Filter to select an option under Group, Label, Site . For all devices, select Global . A corresponding dashboard is displayed.
2	Item under the left navigation contextual menu. The menu is dependent on the filter selection.
3	First-level tab on the dashboard.
4	Second-level tab on the dashboard.
5	Dashboard content for the selected view and filter. For example, the current dashboard in the image displays the UCC tab under Manage > Applications in the List view for the Global filter.
6	Time range filter. This is displayed for selected dashboards only.
7	List view to display tabular data for the selected filter. This is displayed for selected dashboards only.
8	Summary view to display charts for the selected filter. This is displayed for selected dashboards only.
9	Config view to enable configuration options for the selected filter. This is displayed for selected dashboards only.

Types of Dashboards in the Network Operations App

The **Network Operations** app uses a filter to set the dashboard context for the app. The menu for the left navigation pane changes according to the selected filter value. Selecting any item on the left navigation pane displays a corresponding dashboard. Accordingly, for different values of the filter, the content displayed for the left navigation menu and the dashboard context differs. The following table lists down all the available dashboards and the link to the detailed description of each type of dashboard.

Table 19: *Types of Dashboards*

Link to the Dashboard	Filter Value and Dashboard Description
The Global Dashboard	When the filter is set to Global (for standard enterprise modes) or All Groups (for managed service modes), the dashboard context displayed is for all available devices registered to the specific Aruba Central account. This is called the global dashboard.
The Group Dashboard	When the filter is set to a specific group, the dashboard context displayed is only for the devices that are configured as part of that group. This is called the group dashboard.
The Site Dashboard	When the filter is set to a specific site, the dashboard context displayed is only for the devices that are configured as part of that site. This is called the site dashboard.
The Label Dashboard	When the filter is set to a specific label, the dashboard context displayed is only for the devices that are configured as part of that label. This is called the label dashboard.
The Controller Dashboard	When the filter is set to a controller, the dashboard context displayed is only for that specific controller. This is called the controller dashboard. The controller dashboard enables you to manage and monitor a specific controller.
The Access Point Dashboard	When the filter is set to an access point, the dashboard context displayed is only for that specific access point. This is called the access point dashboard. The access point dashboard enables you to manage and monitor a specific access point.
The Switch Dashboard	When the filter is set to a switch, the dashboard context displayed is only for that specific switch. This is called the switch dashboard. The switch dashboard enables you to manage and monitor a specific switch.
The Client Dashboard	In the Network Operations app, the client dashboard is displayed under Manage > Clients for any filter value.

The dashboard for any item on the left navigation menu can have a combination of the following views:

- 
Summary view— Click the **Summary** icon to display the summary dashboard. The summary dashboard displays a number of charts. For example, for the global dashboard, under **Manage**, the **Overview > Network Health** tab in **Summary** view displays a map of the available sites and their corresponding health. If available, use the time range filter to change the time-lines for the charts.

- **List** view— Click the  **List** icon to display tabular data for a selected dashboard. For example, for the global dashboard under **Manage**, the **Overview > Network Health** tab in **List** view displays a list of the available sites managed by Aruba Central. If available, use the time range filter to change the time-lines for the tabular data.
- **Config** view— Click the  **Config** icon to enable the configuration options for a specific dashboard. For example, for the global dashboard under **Manage**, the **Applications > UCC** tab in **Config** view displays various configuration options for UCC.

Navigating to the Switch, Access Point, or Controller Dashboard

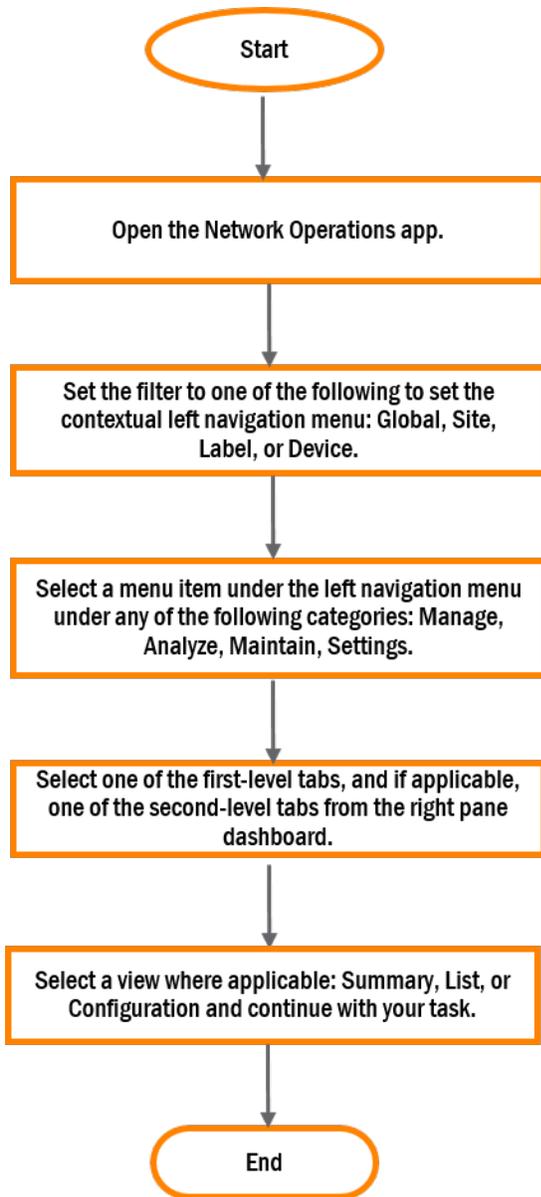
In the **Network Operations** app, you can navigate to a device dashboard for a switch, access point, or controller. The device dashboard enables you to monitor, troubleshoot, or configure a single device. In order to do this, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Group, Label, or Site**.
For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
2. 1. Under **Manage > Devices**, select one of the following options:
 - To view an access point dashboard, click the **Access Points** tab.
 - To view a switch dashboard, click the **Switches** tab.
 - To view a controller dashboard, click the **Controllers** tab.The list of devices is displayed in **List** view.
3. Click a device listed under **Device Name**.
The dashboard context for the specific device is displayed.
To exit the device dashboard, click the back arrow on the filter.

Workflow to Configure, Monitor, or Troubleshoot in the Network Operations App

The following image displays a flowchart to help you navigate the **Network Operations** app to complete any task.

Figure 12 *Navigation Workflow for Network Operations App*



The Global Dashboard

In the **Network Operations** app, the global dashboard is displayed when the filter is set to **Global**. The global dashboard displays information related to all devices registered to that account in Aruba Central.



Some tabs may not be seen in your dashboard view if you are not an administrator for the Aruba Central account.

Table 20: Contents of the Global Dashboard

Left Navigation Menu	First-Level Tabs	Description
Manage > Overview	Network Health	Displays information of the networks sorted by site, including information on network devices and WAN connectivity of individual sites. For more information, see Network Health .
	Summary	Displays details such as the bandwidth usage, client count, top APs by usage, top 5 clients, top AP clusters by usage, top AP clusters by clients, and WLAN network details. By default, the graphs are plotted for a time range of 3 hours. To view the graphs for a different time range, click the Time Range Filter. For more information, see Global—Summary
Manage > Devices	Access Points	Displays the access points information in the following views: <ul style="list-style-type: none"> ■ Summary view: Monitoring APs in Summary View ■ List view: Monitoring APs in List View
	Switches	Displays the switches information in the following views: <ul style="list-style-type: none"> ■ Summary view: Monitoring Switches in Summary View ■ List view: Monitoring Switches in List View
	Controllers	Displays the controller information in the following view: <ul style="list-style-type: none"> ■ Summary view: Controller > Overview > Summary
Manage > Clients	Clients	Displays information about all the clients connected to the devices configured for the group. For more information, see All Clients .
Manage > Applications	Visibility	Provides a summary of client traffic and their data usage to and from applications and websites. Also, analyzes the client traffic flow using the graphs displayed. For more information, see Application Visibility .
	UCC	Monitors voice, video, and application sharing sessions, provides traffic visibility, and allows you to prioritize the required sessions. The app also leverages the functions of the service engine on the cloud platform to provide visual metrics for analytical purposes. For more information, see Unified Communications .
Manage > Security	RAPIDs	Helps to identify and act on interfering devices that can be later considered for investigation, restrictive action, or both. For more information, see RAPIDS .
	Firewall	Monitors traffic coming into and going out of the Aruba Central-managed network and acts as an investigative resource for users to track blocked sessions within the network. For more information, see Configuring Firewall Parameters for Wireless Network Protection .
Analyze > Alerts and Events	Alerts & Events	Displays all types of alerts and events generated for events pertaining to device provisioning, configuration, and user management. For more information, see Alerts & Events .

Left Navigation Menu	First-Level Tabs	Description
Analyze > Audit Trail	Audit Trail	Shows the total number logs generated for all device management, configuration, and user management events triggered in Aruba Central. For more information, see Viewing Audit Trail .
Analyze > Tools	<ul style="list-style-type: none"> ■ Network Check ■ Device Check ■ Commands 	Enables network administrators and users with troubleshooting permission to perform troubleshooting or diagnostics tests on devices and networks managed by Aruba Central. For more information, see Using Troubleshooting Tools .
Analyze > Reports	Reports	Enables you to create various types of reports. You can create recurrent reports or configure the reports to run on demand. For more information, see Reports .
Maintain > Firmware	<ul style="list-style-type: none"> ■ Access Points ■ Switches ■ Controllers 	Provides an overview of the latest supported version of firmware for the device, details of the device, and the option to upgrade the device. For more information, see Upgrading Device Firmware .
Maintain > Organization	Groups	A group in Aruba Central is the primary configuration element that functions as a container for device management, monitoring, and maintenance. Groups enable administrators to manage devices efficiently by using either a UI-based configuration workflow or CLI-based configuration template. For more information, see Managing Groups .
	Sites and Labels	A site refers to a physical location where a set of devices are installed; for example, campus, branch, or venue. Labels are tags attached to a device provisioned in the network. Labels determine the ownership, departments, and functions of the devices. For more information, see Managing Sites and Managing Labels .
	Certificates	Enables administrators to upload a valid certificate signed by a root CA so that devices are validated and authorized to use Aruba Central. For more information, see Managing Certificates .

The Access Point Dashboard

In the **Network Operations** app, the access point dashboard is displayed when the filter is set to an access point. To navigate to an access point dashboard, see [Navigating to the Switch, Access Point, or Controller Dashboard](#).

The following table lists all the available menu items in the **Network Operations** app for the access point dashboard.

Table 21: Contents of the Access Point Dashboard

Left Navigation Menu	First-Level Tabs	Description
Manage > Overview	Summary	The Summary tab displays the AP device details, network information, radio details including the topology of clients connected to each radio, and the health status of the AP in the network. See Access Point > Overview > Summary .
	AI Insights	The AI Insights tab displays information on AP performance issues such as excessive channel changes, excessive reboots, airtime utilization, and memory utilization. See Access Point > Overview > AI Insights .
	Floor Plan	The Floor Plan tab provides information regarding the current location of the Instant AP. See Access Point > Overview > Floor Plan .
	Performance	The Performance tab displays the size of data transmitted through the AP. See Access Point > Overview > Performance .
	RF	The RF tab provides details corresponding to 2.4 GHz, 5 GHz, and 5 GHz Secondary radios of the AP. See Access Point > Overview > RF .
Manage > Device	Access Point Configuration using UI groups	Enables Access Point configuration in the Config view. See Configuring APs . Configuration using UI groups contains the following second-level tabs: <ul style="list-style-type: none"> ■ WLANS—Configure wireless network profiles on Instant APs. See Configuring Wireless Network Profiles on IAPs. ■ Access Points—Configure device parameters on Instant APs. See Configuring Device Parameters. ■ Radios—Configure ARM and RF parameters on Instant APs. See Configuring ARM and RF Parameters on IAPs. ■ Interfaces—Configuring interfaces parameters on Instant APs. See Configuring Uplink Interfaces on IAPs. ■ Security—Configure authentication and security profiles on Instant APs. See Configuring Authentication and Security Profiles on IAPs. ■ VPN—Configure VPN host settings on an Instant AP to enable communication with a controller in a remote location. See Configuring IAPs for VPN Tunnel Creation. ■ Services—Configure AirGroup, location services, Lawful Intercept, OpenDNS, and Firewall services on Instant APs. See Configuring Services. ■ System—Configure system parameters on Instant APs. See Configuring System Parameters for an AP. ■ Configuration Audit—View configuration sync errors and overrides. See Verifying Device Configuration Status.
	Access Point Configuration using template groups	Configuration using template groups contains the following second-level tabs: <ul style="list-style-type: none"> ■ Templates—Configure Access Points using template groups. See Configuring APs Using Templates. ■ Variables—Modify, download, or upload variables associated with devices that you can use in template

Left Navigation Menu	First-Level Tabs	Description
		configuration. See Managing Variable Files . <ul style="list-style-type: none"> ■ Configuration Audit—View configuration sync errors and overrides. See Verifying Device Configuration Status.
Manage > Clients	Clients	The Clients tab displays details of all the clients connected to a specific AP. See Access Point > Clients > Clients .
Manage > Security	VPN	The VPN tab provides information on VPN connections associated with the Virtual Controller along with information on the tunnels and the data usage through each of the tunnels. See Access Point > Security > VPN .
Analyze > Alerts and Events	Alerts & Events	The Alerts & Events tab displays details of the alerts and events generated for the AP. See Access Point > Alerts & Events > Alerts & Events .
Analyze > Audit Trail	Audit Trail	The Audit Trail tab displays the logs for all the device management, configuration, and user management events triggered in Aruba Central. See Viewing Audit Trail .
Analyze > Tools	Commands	The Commands tab allows network administrators and users with troubleshooting permission to perform troubleshooting or diagnostics tests on devices and networks managed by Aruba Central. See Advanced Device Troubleshooting .
Maintain > Firmware	Access Points	The Access Points tab allow the user to view the firmware details for devices provisioned in Aruba Central. See Upgrading Device Firmware .

The Switch Dashboard

In the **Network Operations** app, the switch dashboard is displayed when the filter is set to a switch.

To navigate to a switch dashboard, see [Navigating to the Switch, Access Point, or Controller Dashboard](#).



NOTE

Some tabs may not be seen in your dashboard view if you are not an administrator for the Aruba Central (on-premises) account. Also, some tabs or some fields inside tabs are only applicable either for AOS-Switch or AOS-CX switch series.

Table 22: *Contents of the Switch Dashboard*

Left Navigation Menu	First-Level Tabs	Description
Manage > Overview	Summary	Displays details about a specific switch, including device information, network summary, and port and hardware status. It also displays uplink and usage details. Use the time range filter to change the time period for the displayed information. See Switch > Overview > Summary .

Left Navigation Menu	First-Level Tabs	Description
	Hardware	Displays switch hardware details, including status of power supplies and fans, CPU and memory utilization, and device temperature. See Switch > Overview > Hardware .
	Routing	Displays routing information for the switch, such as, type of route, number of static and connected routes, and distance of the route. See Switch > Overview > Routing . NOTE: The Routing tab is displayed only for AOS-Switches.
Manage > Clients	Clients	Displays details about the wired clients that are connected to the switch. See Switch > Clients > Clients .
	Neighbours	Displays details about the devices neighboring the switch. See Switch > Clients > Neighbours .
Manage > LAN	Ports	Displays details about ports and the LAGs configured in the switch. Also displays information about AOS-CX switch stacks and stack-related errors. See Switch > LAN > Ports . For information about AOS-CX switch stack-related errors, see Monitoring AOS-CX Switch Stacks .
	PoE	Displays details about PoE status, PoE ports, and the power consumption from these ports. See Switch > LAN > PoE .
	VLAN	Displays VLAN information configured on the switch and details about tagged and untagged ports. See Switch > LAN > VLAN .
Manage > VSX	VSX	Displays VSX configuration details between AOS-CX switches and the status of the inter-switch link (ISL). See Switch > VSX . NOTE: The VSX tab is displayed only for AOS-CX switch series.
Manage > Device	AOS-Switch— Configuration using UI groups	Enables AOS-Switch configuration in the AOS-S Config view. See Configuring AOS-Switches in UI Groups . Configuration using UI groups contains the following second-level tabs: <ul style="list-style-type: none"> ■ Switches—Configure and view general switch properties, such as, hostname, IP address, and netmask. See Configuring or Viewing the Switch Properties. ■ Stacks—Create stacks, add members, or view stacking details, such as, stack type, stack id, and topology. See Configuring AOS-Switch Stacks Using UI Groups. ■ Interface: <ul style="list-style-type: none"> ○ Ports—Assign or view port properties, such as, PoE, access policies, and trunk groups. See Configuring Switch Ports on AOS-Switches. ○ PoE—Configure or view PoE settings for each port. See Configuring PoE Settings on AOS-Switch Ports. ○ Trunk Groups—Configure or view trunk groups and their associated

Left Navigation Menu	First-Level Tabs	Description
		<p>properties, such as, members of the trunk group, and type of trunk group. See Configuring Trunk Groups on AOS-Switches in UI Groups.</p> <ul style="list-style-type: none"> ○ VLANs—Configure or view VLAN details and the associated ports and access policies. See Configuring VLANs on AOS-Switches. ○ Spanning Tree—Configure or view spanning tree protocol and its associated properties. See Enabling Spanning Tree Protocol on AOS-Switches in UI Groups. ○ Loop Protection—Configure or view loop protection and its associated properties. See Configuring Loop Protection on AOS-Switch Ports. <ul style="list-style-type: none"> ■ Security: <ul style="list-style-type: none"> ○ Access Policies—Add or view access policies. See Configuring Access Policies on AOS-Switches. ○ DHCP Snooping—Configure or view DHCP snooping, authorized DHCP servers IP addresses, and their associated properties. See Configuring DHCP Snooping on AOS-Switches. ○ Port Rate Limit—View or specify bandwidth to be used for inbound or outbound traffic for each port. See Configuring Port Rate Limit on AOS-Switches in UI Groups. ○ RADIUS—Configure RADIUS (Remote Authentication Dial-In User Service) server settings on AOS-Switches. See Configuring RADIUS Server Settings on AOS-Switches. ○ Downloadable User Role—Enable DUR and configure ClearPass settings to download user roles, policy, and class from the ClearPass Policy Manager server. See Configuring Downloadable User Role on AOS-Switches. ○ Tunneled Node Server—Configure user-based tunnel or port-based tunnel on switches. See Configuring Tunnel Node Server on AOS-Switches. ○ Authentication—Configure and enable 802.1X and MAC authentication on switches. You can also configure authentication order and priority for authentication methods. See Configuring Authentication for AOS-Switches. ■ System: <ul style="list-style-type: none"> ○ Access/DNS—Configure or view the administrator and operator logins. See Configuring System Parameters for AOS-Switches. ○ Time—Configure time synchronization in switches. See Configuring Time Synchronization on AOS-Switches. ○ SNMP—Add or view SNMP v2c and v3 community and its trap destination. See Configuring SNMP on AOS-Switches. ○ CDP—Configure CDP and its associated properties. See Configuring CDP on AOS-Switches. ○ DHCP—Add or view a DHCP pool and its associated properties. See Configuring DHCP on AOS-Switches. ○ IP Client Tracker—Enable AOS-Switches to learn the IP address of all, trusted, or only untrusted clients connected to the switch. See Configuring IP Client Tracker on AOS-Switches.

Left Navigation Menu	First-Level Tabs	Description
		<ul style="list-style-type: none"> ■ Routing—Configure or view a specific routing path to a gateway. See Configuring Routing on AOS-Switches. ■ IGMP—Configure IGMP and its associated properties. See Configuring IGMP on AOS-Switches. ■ QoS—Configure QoS traffic policies on switches to classify and prioritize traffic throughout a network. See Configuring QoS Settings on AOS-Switches. ■ Device Profile—Configure device profile on switches to dynamically detect devices based on certain parameters. See Configuring Device Profile and Device Identifier on AOS-Switches. ■ Configuration Audit—View configuration sync errors and overrides. See Verifying Device Configuration Status.
	AOS-Switch — Configuration using templates	<p>See Using Configuration Templates for AOS-Switch Management. Configuration of AOS-Switches using template groups contains the following second-level tabs:</p> <ul style="list-style-type: none"> ■ Templates—Configure switch using template groups. See Provisioning Devices Using Configuration Templates. ■ Variables—Modify, download, or upload variables associated with devices that you can use in template configuration. See Managing Variable Files. ■ Configuration Audit—View configuration sync errors and overrides. See Verifying Device Configuration Status.
	AOS-Switch Stack — Configuration using templates	<p>Configuration of AOS-Switch stacks using template groups contains the following second-level tabs:</p> <ul style="list-style-type: none"> ■ Templates—Configure switch stack using template groups. See Configuring AOS-Switch Stacks Using Template Groups. ■ Variables—Modify, download, or upload variables associated with devices that you can use in template configuration. See Managing Variable Files. ■ Configuration Audit—View configuration sync errors and overrides. See Verifying Device Configuration Status.
	AOS-CX — Configuration using UI groups	<p>Enables AOS-CX configuration in the AOS-CX Config view. See Configuring AOS-CX Switches in UI Groups. Configuration using UI groups allows you to configure the following features:</p> <ul style="list-style-type: none"> ■ System: <ul style="list-style-type: none"> ○ Properties—Edit system property settings such as contact, location, time zone, and administrator password. You can also select the VRF to be used and add the DNS and NTP servers. See Configuring System Properties on AOS-CX. ○ HTTP Proxy—Edit the HTTP proxy configuration details for the switch. See Configuring HTTP Proxy on AOS-CX. ○ SNMP—Add, edit, or delete SNMP v2 communities, v3 users, and trap notifications. See Configuring SNMP on AOS-CX. ○ Logging—Add, edit, or delete logging servers to view event logs from the AOS-CX switches. Configure FQDN or IP address, log severity level, and the VRF to be used for each of the logging servers. Also configure

Left Navigation Menu	First-Level Tabs	Description
		<p>the global level debug log severity. See Configuring Logging Servers for AOS-CX.</p> <ul style="list-style-type: none"> ○ Administrator—Add, edit, or delete server groups to be used for authentication, authorization, and accounting. You must also configure the protocol required to enable connection to these server groups. See Configuring AAA for AOS-CX. ○ Source Interface—Add, modify, or delete source interface configuration for Central and User-based tunneling interfaces for AOS-CX switches. See Configuring Source Interface for AOS-CX. ○ Stacking—Create stack, add stack members, modify VSF link, change the secondary conductor, delete stack and delete stack members. See Configuring AOS-CX VSF Stacks Using UI Groups. ■ Routing: <ul style="list-style-type: none"> ○ Static Routing—Add, edit, or delete static routes manually and configure destination IP addresses and next hop values, VRF, and the administrative distance. You can add different static routes for different VRFs on the switch. See Configuring Static Routing on AOS-CX. ■ Interfaces: <ul style="list-style-type: none"> ○ Ports & Link Aggregations—View and edit port settings such as description, VLAN mode, speed duplex, routing, and the operational status of the port. Add, edit, or delete LAGs by combining different ports and configuring the speed duplex, VLAN mode, aggregation mode, and the operational status of the LAG. See Configuring Ports and LAGs on AOS-CX. ■ Security: <ul style="list-style-type: none"> ○ Authentication Servers—Add, edit, or view the RADIUS and TACACS servers for authentication. Add settings such as FQDN or IP address of the servers, authentication port number, response timeout, retry count, and the VRF to be used when communicating with the servers. See Configuring Authentication Servers on AOS-CX. ○ Authentication—View or edit details about 802.1X and MAC authentication methods. Configure the precedence order and other parameters such as reauthentication timeout, cached reauthentication timeout, and quiet period. See Configuring Authentication on AOS-CX. ○ Access Control—View or add access policies and rules to permit or deny passage of traffic. See Configuring Access Control on AOS-CX. ○ Dynamic Segmentation—Enable user-based tunneling on the switch to provide a centralized security policy based on user authentication. See Configuring User-Based Tunneling for AOS-CX. ○ Client Roles—Add or delete client roles and associate these roles to clients. See Configuring Client Roles for AOS-CX. ■ Bridging: <ul style="list-style-type: none"> ○ VLANs—Add, edit, delete, or view VLANs, and associated parameters such as type of IP assignment, operational status, IP address of the DHCP relay. See Configuring VLANs on AOS-CX.

Left Navigation Menu	First-Level Tabs	Description
	Configuration using UI groups allows you to configure the following features: <ul style="list-style-type: none"> ■ System: <ul style="list-style-type: none"> ○ Properties— Edit system property settings such as contact, location, time zone, and administrator password. You can also select the VRF to be used and add the DNS and NTP servers. See Configuring System Properties on 	

Left Navigation Menu	First-Level Tabs	Description
	<ul style="list-style-type: none"> AOS-CX. ◦ HTTP Proxy —Edit the HTTP proxy configuration details for the switch. See Configuring HTTP Proxy on AOS-CX. ◦ SNMP —Add, edit, or delete SNMP v2 communities, v3 users, and trap notifications. See Configuring SNMP on AOS-CX. ◦ Login 	

Left Navigation Menu	First-Level Tabs	Description
	<p>g— Add, edit, or delete logging servers to view event logs from the AOS-CX switches. Configure FQDN or IP address, log severity level, and the VRF to be used for each of the logging servers. Also configure the global level debug log severity. See Configuring Logging</p>	

Left Navigation Menu	First-Level Tabs	Description
	<ul style="list-style-type: none"> g Server s for AOS- CX. ◦ Admin istrato r—Add, edit, or delete server groups to be used for authentication, authorization, and accounting. You must also configure the protocol required to enable connection to these server groups. See Configuring AAA for AOS-CX. 	

Left Navigation Menu	First-Level Tabs	Description
	<ul style="list-style-type: none"> ◦ Source Interface— Add, modify, or delete source interface configuration for Central and User-based tunneling interfaces for AOS-CX switches. See Configuring Source Interface for AOS-CX. ◦ Stacking— Create stack, add stack members, modify VSF link, 	

Left Navigation Menu	First-Level Tabs	Description
	<p>change the secondary conductor, delete stack and delete stack members. See Configuring AOS-CX VSF Stacks Using UI Groups.</p> <ul style="list-style-type: none"> ■ Routing: <ul style="list-style-type: none"> ○ Static Routing—Add, edit, or delete static routes manually and configure destination IP addresses and next hop 	

Left Navigation Menu	First-Level Tabs	Description
	<p>values, VRF, and the administrative distance. You can add different static routes for different VRFs on the switch. See Configuring Static Routing on AOS-CX.</p> <ul style="list-style-type: none"> ■ Interface <ul style="list-style-type: none"> S: ○ Ports & Link Aggregations <ul style="list-style-type: none"> —View and edit port settings such as description, VLAN 	

Left Navigation Menu	First-Level Tabs	Description
	<p>mode, speed duplex, routing, and the operational status of the port. Add, edit, or delete LAGs by combining different ports and configuring the speed duplex, VLAN mode, aggregation mode, and the operational status of the LAG. See Configuring Ports and LAGs</p>	

Left Navigation Menu	First-Level Tabs	Description
	<ul style="list-style-type: none"> be used when communicating with the servers. See Configuring Authentication Servers on AOS-CX. o Authentication— View or edit details about 802.1X and MAC authentication methods. Configure the precedence order and other parameters such as reauthentication 	

Left Navigation Menu	First-Level Tabs	Description
	<p>timeout, cached reauthentication on timeout, and quiet period. See Configuring Authentication on AOS-CX.</p> <ul style="list-style-type: none"> ◦ Access Control—View or add access policies and rules to permit or deny passage of traffic. See Configuring Access Control on AOS-CX. ◦ Dynamic Segmentation 	

Left Navigation Menu	First-Level Tabs	Description
	<p>n— Enable user-based tunneling on the switch to provide a centralized security policy based on user authentication. See Configuring User-Based Tunneling for AOS-CX.</p> <ul style="list-style-type: none"> ◦ Client Roles —Add or delete client roles and associate these roles to clients. See Configuring 	

Left Navigation Menu	First-Level Tabs	Description
	<p>Client Roles for AOS-CX.</p> <ul style="list-style-type: none"> ■ Bridging: <ul style="list-style-type: none"> ○ VLANs <ul style="list-style-type: none"> —Add, edit, delete, or view VLANs, and associated parameters such as type of IP assignment, operational status, IP address of the DHCP relay. See Configuring VLANs on AOS-CX. ○ Loop Prevention <ul style="list-style-type: none"> — Enable 	

Left Navigation Menu	First-Level Tabs	Description
	<p>or disable loop protect ion and spanni ng tree protoc ol, and associ ated param eters such as the mode and priorit y. Enable or disable various MSTP mode- related setting s such as BPDU filter, BPDU protect ion, admin edge, and root guard. See Config uring Loop Preven</p>	

Left Navigation Menu	First-Level Tabs	Description
<p>AOS-CX— Configuration using MultiEdit mode</p>	<p>tion on AOS-CX.</p> <p>Enables AOS-CX configuration using the MultiEdit mode in the AOS-CX Config view. View and edit configuration on the AOS-CX switches using the CLI syntax. You can also apply predefined set of configuration settings such as NAE to the switches. See Using MultiEdit View for AOS-CX.</p> <p>Configuration using the MultiEdit mode contains the following options:</p> <ul style="list-style-type: none"> ■ View Config— View configuration of AOS-CX switches and find differences in the configuration across switches. See 	

Left Navigation Menu	First-Level Tabs	Description
	<p>Viewing Configuration Using MultiEdit on AOS-CX.</p> <ul style="list-style-type: none"> <p>■ Edit Config— Edit configuration for one or more AOS-CX switches in the MultiEdit mode. Edit the entire configuration in a familiar looking CLI with syntax checking, colorization, and command completion. See Editing Configuration Using MultiEdit on AOS-CX.</p> <p>■ Express Config— Apply predefined set of configura</p> 	

Left Navigation Menu	First-Level Tabs	Description
	<p>tion settings such as NAE scripts and device profile to a single or multiple switches. See Express Configuration Using MultiEdit on AOS-CX.</p>	
<p>AOS-CX— Configuration using templates</p>	<p>Enables AOS-CX switch configuration in the AOS-CX view. See Using Configuration Templates for AOS-CX Switch Management.</p> <p>Configuration of AOS-CX switches using template groups contains the following second-level tabs:</p> <ul style="list-style-type: none"> ■ Templat es— Configure switch using template groups. See _ 	

Left Navigation Menu	First-Level Tabs	Description
	<p>Creating a Configuration Template.</p> <ul style="list-style-type: none"> ■ Configuration Audit—View configuration sync errors and overrides. See Verifying Device Configuration Status. ■ Configuration Status—View configuration status of AOS-CX switches that are managed through UI groups in Aruba Central (on-premise s). See Using Configuration Status on AOS-CX. 	

Left Navigation Menu	First-Level Tabs	Description
AOS-CX VSF Stack— Configuration		Enables AOS-CX switch stack configuration in the AOS-CX view. See Managing an AOS-CX VSF Stack .
Analyze > Alerts & Events	Alerts & Events	The Alerts & Events tab displays all types of alerts and events generated for events pertaining to device provisioning, configuration, and user management. See Alerts & Events . You can also configure and enable certain categories of switch alerts. See Switch Alerts .
Analyze > Audit Trail	Audit Trail	Displays the details of logs generated for all device management, configuration, and user management events triggered in Aruba Central (on-premises). See Viewing Audit Trail .
Analyze > Tools	Network Check	The Network Check tab allows administrators and users with troubleshooting permission to diagnose issues related to wired network connections. See Troubleshooting Network Issues .
	Device Check	The Device Check tab allows network administrators and users with troubleshooting permission to identify, diagnose, and debug issues on AOS-Switch and AOS-CX switches using predefined tests. See Troubleshooting Device Issues .
	Commands	The Commands tab allows network administrators and user with troubleshooting permission to identify, diagnose, and debug issues on AOS-Switch and AOS-CX switches at an advanced level using commands. See Advanced Device Troubleshooting .
Analyze > Reports	Reports	The Reports tab allows you to create, manage, and view various reports. You can create recurrent reports, generate reports on demand, or schedule reports to run at a later time. See Reports .
Maintain > Firmware	Switches	The Switches tab allows the user to view the firmware details and upgrade the devices provisioned in Aruba Central (on-premises). See Upgrading Device Firmware

The Controller Dashboard

In the **Network Operations** app, the controller dashboard is displayed when the filter is set to a controller. To navigate to a controller dashboard, see

The following table lists all the available menu items in the **Network Operations** app for the controller dashboard.

Table 23: Contents of the Controller Dashboard

Left Navigation Menu	First-Level Tabs	Description
Manage > Overview	Summary	The Summary tab displays the controller device details, client count, usage, top APs, top clients, and health status. See Controller > Overview > Summary .
	Routing	Displays a summary of the IP routes configured on the controller. See Controller > Overview > Routing
Manage > LAN	Summary	Displays information about LAN port and LAN status. See Controller > LAN > Summary .
Manage > Clients	Clients	Displays a list of clients connected to a controller. See All Clients .
Analyze > Alerts and Events	Alerts & Events	The Alerts & Events tab displays details of the alerts and events generated for the controllers. See Controller Alerts
Analyze > Audit Trail	Audit Trail	Displays the total number of logs generated for all device management, configuration, and user management events triggered in Aruba Central (on-premises). See Viewing Audit Trail .
Analyze > Tools	Network Check	Enables network administrators and users with troubleshooting permission to perform troubleshooting or diagnostics tests on devices and networks managed by Aruba Central (on-premises). See Troubleshooting Network Issues .
	Commands	The Commands tab allows network administrators and users with troubleshooting permission to perform troubleshooting or diagnostics tests on devices and networks managed by Aruba Central. See Using Troubleshooting Tools .
Analyze > Reports	Reports	Enables network administrators to create various types of reports. You can create recurrent reports or configure the reports to run on demand. For more information, see Reports .
Maintain > Firmware	List	Provides an overview of the latest supported version of firmware for the device, details of the device, and the option to upgrade the device. For more information, see Upgrading Device Firmware .
	Config	Provides an upgrade status and compliance status for APs that are connected to the selected controller. For more information, see Upgrading Device Firmware .

The Group Dashboard

In the **Network Operations** app, the group dashboard is displayed when the filter is set to a UI or template group. A template group is marked by a superscript **TG** tag. The following table lists all the available menu items in the **Network Operations** app for the group dashboard.



Some tabs may not be seen in your dashboard view if you are not an administrator for the Aruba Central account.

Table 24: Contents of the Group Dashboard

Left Navigation Menu	First-Level Tabs	Description
Manage > Overview	Summary	Displays details such as the bandwidth usage, client count, top APs by usage, top 5 clients, top AP clusters by usage, top AP clusters by clients, and WLAN network details. By default, the graphs are plotted for a time range of 3 hours. To view the graphs for a different time range, click the Time Range filter. For more information, see Global—Summary
Manage > Devices	Access Points	Displays the access points information in the following views: <ul style="list-style-type: none">■ Summary view: Monitoring APs in Summary View■ List view: Monitoring APs in List View■ Config view: Provisioning APs
	Switches	Displays the switches information in the following views: <ul style="list-style-type: none">■ Summary view: Monitoring Switches in Summary View■ List view: Monitoring Switches in List View■ Config view: Getting Started with AOS-Switch Deployments
	Controllers	Displays the controller information in the following view: <ul style="list-style-type: none">■ Summary view: Controller > Overview > Summary
Manage > Clients	Clients	Displays information about all the clients connected to the devices configured for the group. For more information, see All Clients .
Manage > Applications	Visibility	Provides a summary of client traffic and their data usage to and from applications and websites. Also, analyzes the client traffic flow using the graphs displayed. For more information, see Application Visibility .
Manage > Security	RAPIDs	Helps to identify and act on interfering devices that can be later considered for investigation, restrictive action, or both. For more information, see RAPIDS .
Analyze > Alerts and Events	Alerts & Events	Displays all types of alerts and events generated for events pertaining to device provisioning, configuration, and user management. For more information, see Alerts & Events .
Analyze > Audit Trail	Audit Trail	Shows the total number logs generated for all device management, configuration, and user management events triggered in Aruba Central. For more information, see Viewing Audit Trail .
Analyze > Tools	<ul style="list-style-type: none">■ Network Check■ Commands	Enables network administrators and users with troubleshooting permission to perform troubleshooting or diagnostics tests on devices and networks managed by Aruba Central. For more information, see Using Troubleshooting Tools .

Left Navigation Menu	First-Level Tabs	Description
Analyze > Reports	Reports	Enables you to create various types of reports. You can create recurrent reports or configure the reports to run on demand. For more information, see Reports .
Maintain > Firmware	<ul style="list-style-type: none"> ■ Access Points ■ Switches ■ Controllers 	Provides an overview of the latest supported version of firmware for the device, details of the device, and the option to upgrade the device. For more information, see Upgrading Device Firmware .

The Client Dashboard

In the **Network Operations** app, the clients dashboard is displayed when the filter is set to one of the options under **Groups, Labels, Sites, or Global**.

The following table lists all the available menu items in the **Network Operations** app for the clients dashboard.

Table 25: *Contents of the Clients Dashboard*

Left Navigation Menu	First-Level Tabs	Description
Manage > Overview	Summary	Displays the client details about the type of data path that the client uses, the network and connectivity details, and basic client details such as IP address of the client, type of encryption etc. See Client Details .
	Location	Displays the current physical location of the client device on the floor map. See Client Details .
	Sessions	Displays the firewall session details for the client connected to an AP or a Branch Gateway. The Sessions page displays information filtered by the IP address of the client. See Client Details .
Manage > Applications		Displays the client details for passive motoring of the client connected to a wireless network. The Visibility dashboard provides a summary of client traffic and their data usage to and from applications, and websites. See Application Visibility .
Analyze > Events		Displays the details of events generated by the AP and client association. See Alerts & Events

The Site Dashboard

In the **Network Operations** app, the site dashboard is displayed when the filter is set to any of the options under **Sites**. The site dashboard displays information related to all devices configured for that site in Aruba Central.

Table 26: Contents of the Site Dashboard

Left Navigation Menu	First-Level Tabs	Description
Manage > Overview	Site Health	Displays details of wired and wireless devices deployed on the site. This page includes information on client connectivity statistics, change logs, health of devices, and RF health of the site. For more information, see Managing Sites .
	Summary	Displays details such as the bandwidth usage, client count, top APs by usage, top 5 clients, top AP clusters by usage, top AP clusters by clients, and WLAN network details. By default, the graphs are plotted for a time range of 3 hours. To view the graphs for a different time range, click the Time Range filter. For more information, see Global—Summary
	WAN Health	Displays details for the wired, wireless, and controller devices deployed on the site. For more information, see WAN Health—Site .
	Topology	Provides a graphical representation of the site including the network layout, details of the devices deployed, and the health of the WAN uplinks and tunnels. For more information, see Topology Tab.
	Floor Plans	Provides information regarding the current location of the AP. For more information, see Access Point > Overview > Floor Plan .
Manage > Devices	Access Points	Displays the access points information in the following views: <ul style="list-style-type: none"> ■ Summary view: Monitoring APs in Summary View ■ List view: Monitoring APs in List View
	Switches	Displays the switches information in the following views: <ul style="list-style-type: none"> ■ Summary view: Monitoring Switches in Summary View ■ List view: Monitoring Switches in List View
	Controllers	Displays the controller information in the following view: <ul style="list-style-type: none"> ■ Summary view: Controller > Overview > Summary
Manage > Clients	Clients	Displays information about all the clients connected to the devices configured for the group. For more information, see All Clients .
Manage > Applications	Visibility	Provides a summary of client traffic and their data usage to and from applications and websites. Also, analyzes the client traffic flow using the graphs displayed. For more information, see Application Visibility .

Left Navigation Menu	First-Level Tabs	Description
Manage > Security	RAPIDS	Identify and act on interfering devices that can be later considered for investigation, restrictive action, or both. Once the interfering devices are discovered, Aruba Central sends alerts to the network administrators about the possible threat and provides essential information needed to locate and manage the threat. For more information, see RAPIDS .
Analyze > Alerts and Events	Alerts & Events	Displays all types of alerts and events generated for events pertaining to device provisioning, configuration, and user management. For more information, see Alerts & Events .
Analyze > Tools	Network Check Commands	Enables network administrators and users with troubleshooting permission to perform troubleshooting or diagnostics tests on devices and networks managed by Aruba Central. For more information, see Using Troubleshooting Tools .
Analyze > Reports	Reports	Enables you to create various types of reports. You can create recurrent reports or configure the reports to run on demand. For more information, see Reports .

The Label Dashboard

In the **Network Operations** app, the label dashboard is displayed when the filter is set to any of the options under **Labels**. The label dashboard displays information related to all devices configured for that label in Aruba Central.

Table 27: Contents of the Label Dashboard

Left Navigation Menu	First-Level Tabs	Description
Manage > Devices	All Devices	Displays details such as the bandwidth usage, client count, top APs by usage, top 5 clients, top AP clusters by usage, top AP clusters by clients, and WLAN network details. By default, the graphs are plotted for a time range of 3 hours. To view the graphs for a different time range, click the Time Range filter. For more information, see Global—Summary
	Access Points	Displays the access points information in the following views: <ul style="list-style-type: none"> ■ Summary view: Monitoring APs in Summary View ■ List view: Monitoring APs in List View
	Switches	Displays the switches information in the following views: <ul style="list-style-type: none"> ■ Summary view: Monitoring Switches in Summary View ■ List view: Monitoring Switches in List View
	Controllers	Displays the controller information in the following view: <ul style="list-style-type: none"> ■ Summary view: Controller > Overview > Summary

Left Navigation Menu	First-Level Tabs	Description
Manage > Clients	Clients	Displays information about all the clients connected to the devices configured for the group. For more information, see All Clients .
Manage > Applications	UCC	Displays a variety of charts and lists that allow you to assess the quality of calls in the network. For more information, see Unified Communications .
Manage > Security	RAPIDS	Identify and act on interfering devices that can be later considered for investigation, restrictive action, or both. Once the interfering devices are discovered, Aruba Central sends alerts to the network administrators about the possible threat and provides essential information needed to locate and manage the threat. For more information, see RAPIDS .
Analyze > Alerts and Events	Alerts & Events	Displays all types of alerts and events generated for events pertaining to device provisioning, configuration, and user management. For more information, see Alerts & Events .
Analyze > Tools	<ul style="list-style-type: none"> ■ Network Check ■ Device Check ■ Commands 	Enables network administrators and users with troubleshooting permission to perform troubleshooting or diagnostics tests on devices and networks managed by Aruba Central. For more information, see Using Troubleshooting Tools .
Analyze > Reports	Reports	Enables you to create various types of reports. You can create recurrent reports or configure the reports to run on demand. For more information, see Reports .

The Health Bar

The Health Bar provides a snapshot of the overall health of the devices configured as part of the specific dashboard. The applicable dashboards include global, group, site, client, and device dashboards.

The topic discusses the following:

- [Health Bar Dashboard for Global](#)
- [Health Bar Dashboard for Group](#)
- [Health Bar Dashboard for Site](#)
- [Health Bar Dashboard for Access Point](#)
- [Health Bar Dashboard for Switch](#)
- [Health Bar Dashboard for Controller](#)
- [Health Bar Dashboard for Wireless Client](#)
- [Health Bar Dashboard for Wired Client](#)

Viewing the Health Bar Dashboard

To view the Health Bar, perform the following steps:

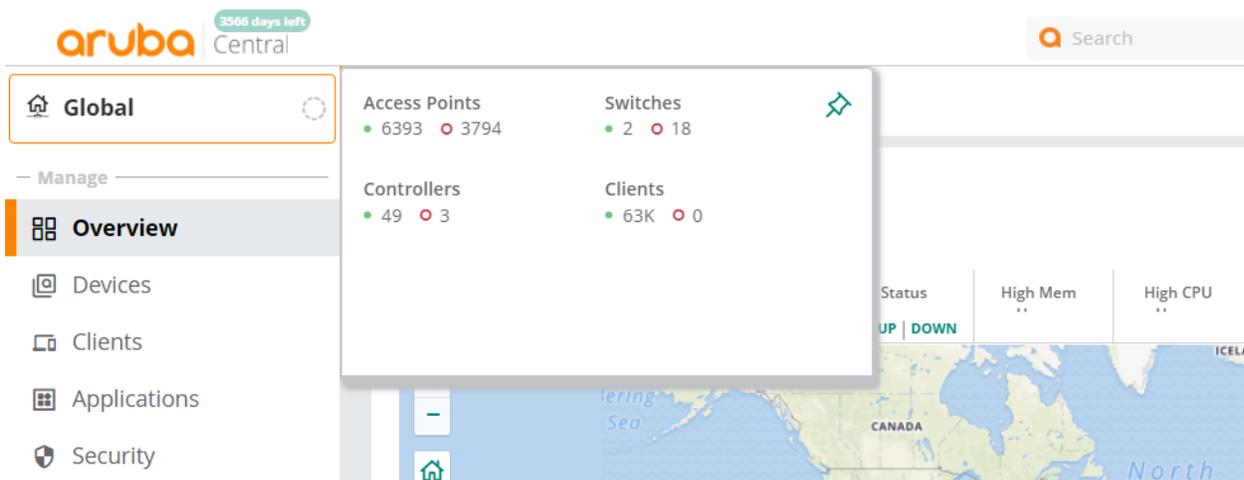
- In the **Network Operations** app, select one of the following options:
 - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
 - To select a device in the filter:
 - Set the filter to **Global**.
 - Under **Manage**, click **Devices**, and then click **Access Points, Switches, or Gateways**.
A list of devices is displayed in the **List** view.
 - Click a device listed under **Device Name**.
The dashboard context for the device is displayed.
 - To select a client:
 - Set the filter to **Global**.
 - Under **Manage**, click **Clients**.
A list of clients is displayed in the **List** view.
 - Click a client listed under **Client Name**.
The dashboard context for the client is displayed.

The Health Bar icon displays the overall health of the network of the selected filter as either online or offline.
- In the selected filter, click the Health Bar icon to expand the Health Bar dashboard.
- Use the  pin icon to pin the Health Bar dashboard to the **Network Operations** app display.

Health Bar Dashboard for Global

The following image shows the health bar for the global dashboard.

Figure 13 Expanded but Unpinned Health Bar in the Global Dashboard



Health Bar Icons

Icon Type	Description
	This icon is specific to Site , Device , and Client dashboard. It indicates that there are no issues in the connection.
	This icon is specific to Site , Device , and Client dashboard. It indicates that there is an issue in the connection.
	This icon is specific to the Global and Group dashboards, and the health is not calculated at these levels.

Device and Clients Status Icons

Icon Type	Description
	<ul style="list-style-type: none"> For devices, indicates the number of devices that are online. For clients, indicates the number of clients that are connected.
	<ul style="list-style-type: none"> For devices, indicates the number of devices that are offline. For clients, indicates the number of failed clients. For AI Insights, indicates the number of insights that are of high priority.
	For AI Insights, indicates the number of insights that are of medium priority.
	For AI Insights, indicates the number of insights that are of low priority.

The following table includes information on the various parameters of the Health Bar displayed for a global dashboard. The health bar in a global dashboard is in the context of all devices.

Parameter	Description
Access Points	<ul style="list-style-type: none"> Displays the number of access points that are online and the number of access points that are offline. The number in green indicates the number of access points that are online. Clicking the number in green redirects you to Manage > Devices > Access Points > Online in List view. The number in red indicates the number of access points that are offline. Clicking the number in red redirects you to Manage > Devices > Access Points > Offline in List view.
Switches	<ul style="list-style-type: none"> Displays the number of switches that are online and the number of switches that are offline. The number in green indicates the number of switches that are online. Clicking the number in green redirects you to Manage > Devices > Switches > Online in List view. The number in red indicates the number of switches that are offline. Clicking the number in red redirects you to Manage > Devices > Switches > Offline in List view.

Parameter	Description
Controllers	<ul style="list-style-type: none"> ■ Displays the number of controllers that are online and the number of controllers that are offline. ■ The number in green indicates the number of controllers that are online. ■ Clicking the number in green redirects you to Manage > Devices > Controllers > Online in List view. ■ The number in red indicates the number of controllers that are offline. ■ Clicking the number in red redirects you to Manage > Devices > Controllers > Offline in List view.
Clients	<ul style="list-style-type: none"> ■ Displays the number of clients that are connected and the number of clients that are failed. ■ The number in green indicates the number of clients that are connected. ■ The number in red indicates the number of clients that are failed. ■ Clicking the numbers redirects you to Manage > Clients > Clients in List view.

Health Bar Dashboard for Group

The following table includes information on the various parameters of the Health Bar displayed for a group dashboard. The health bar in a group dashboard is in the context of all devices configured as part of that group.

Parameter	Description
Access Points	<ul style="list-style-type: none"> ■ Displays the number of access points that are online and the number of access points that are offline. ■ The number in green indicates the number of access points that are online. ■ Clicking the number in green redirects you to Manage > Devices > Access Points > Online in List view. ■ The number in red indicates the number of access points that are offline. ■ Clicking the number in red redirects you to Manage > Devices > Access Points > Offline in List view.
Switches	<ul style="list-style-type: none"> ■ Displays the number of switches that are online and the number of switches that are offline. ■ The number in green indicates the number of switches that are online. ■ Clicking the number in green redirects you to Manage > Devices > Switches > Online in List view. ■ The number in red indicates the number of switches that are offline. ■ Clicking the number in red redirects you to Manage > Devices > Switches > Offline in List view.
Controllers	<ul style="list-style-type: none"> ■ Displays the number of controllers that are online and the number of controllers that are offline. ■ The number in green indicates the number of controllers that are online. ■ Clicking the number in green redirects you to Manage > Devices > Controllers > Online in List view. ■ The number in red indicates the number of controllers that are offline. ■ Clicking the number in red redirects you to Manage > Devices > Controllers > Offline in List view.

Parameter	Description
Clients	<ul style="list-style-type: none"> ■ Displays the number of clients that are connected and the number of clients that are failed. ■ The number in green indicates the number of clients that are connected. ■ The number in red indicates the number of clients that are failed. ■ Clicking the numbers redirects you to Manage > Clients > Clients in List view.

Health Bar Dashboard for Site

The following table includes information on the various parameters of the Health Bar displayed for a site dashboard. The Health Bar in a site dashboard is in the context of all devices configured as part of that site. The values are refreshed every minute. When there is any issue in the connection, short descriptions are displayed for the **Potential Issues** label. If there are multiple criteria issues, only the issue criteria with the highest priority is displayed. The <+x> next to the description indicates that there are more issues. You can hover over the value to view the description of the issue. For more information, see [Site Health Dashboard](#).

Parameter	Description
Access Points	<ul style="list-style-type: none"> ■ Displays the number of access points that are online and the number of access points that are offline. ■ The number in green indicates the number of access points that are online. ■ Clicking the number in green redirects you to Manage > Devices > Access Points > Online in List view. ■ The number in red indicates the number of access points that are offline. ■ Clicking the number in red redirects you to Manage > Devices > Access Points > Offline in List view.
Switches	<ul style="list-style-type: none"> ■ Displays the number of switches that are online and the number of switches that are offline. ■ The number in green indicates the number of switches that are online. ■ Clicking the number in green redirects you to Manage > Devices > Switches > Online in List view. ■ The number in red indicates the number of switches that are offline. ■ Clicking the number in red redirects you to Manage > Devices > Switches > Offline in List view.
Controllers	<ul style="list-style-type: none"> ■ Displays the number of controllers that are online and the number of controllers that are offline. ■ The number in green indicates the number of controllers that are online. ■ Clicking the number in green redirects you to Manage > Devices > Controllers > Online in List view. ■ The number in red indicates the number of controllers that are offline. ■ Clicking the number in red redirects you to Manage > Devices > Controllers > Offline in List view.
Clients	<ul style="list-style-type: none"> ■ Displays the number of clients that are connected and the number of clients that are failed. ■ The number in green indicates the number of clients that are connected. ■ The number in red indicates the number of clients that are failed. ■ Clicking the numbers redirects you to Manage > Clients > Clients in List view.
AI Insights	<ul style="list-style-type: none"> ■ Displays the number of insights categorized by status.

Parameter	Description
	<ul style="list-style-type: none"> ■ The number in red indicates the insights are of high priority. ■ The number in orange indicates the insights are of medium priority. ■ The number in yellow indicates the insights are of low priority. ■ Clicking the numbers redirects you to Manage > Overview > AI Insights at the site context.

Health Bar Dashboard for Access Point

The following table includes information on the various parameters of the Health Bar displayed for an AP. If the AP is not online and running, not all of the following data is available.

Parameter	Description
AP Status	<ul style="list-style-type: none"> ■ Value can be Online Since, Offline, or Operating under Thermal Management. ■ If the value is Online Since, it also displays the time period, in the format of days-hours-minutes, for which the AP has been online and running. ■ When an AP operates under thermal management, the device health is displayed as Poor and the radios are in disabled mode. For more information, see Thermal Shutdown Support in IAP.
Device Health	<ul style="list-style-type: none"> ■ Displays the performance of the AP in terms of the CPU and memory usage. ■ For example, the device health is Good when the CPU usage is less than or equal to 70% and the memory usage is less than or equal to 90%. If the value of the CPU and/or memory usage falls below the threshold, the device health is displayed as Poor. If the AP is down, the value is Offline. If the scenario is not applicable, a "-" sign is displayed. ■ Hover over the Device Health status to get the exact percentage value of the memory and CPU usage.
Radio 2.4 GHz	<ul style="list-style-type: none"> ■ Displays the performance of the AP in terms of the channel utilization and noise floor in the 2.4 GHz channel. ■ For example, the device health is Good when the channel utilization is less than or equal to 70% and the noise floor is less than or equal to -80 dBm. If the value of the channel utilization and noise floor falls below the threshold, the device health is displayed as Poor. If the AP is online, but the radio is down, the value displayed is Disabled. If the scenario is not applicable, a "-" sign is displayed. ■ Hover over the Radio 2.4 GHz status to get the exact value of the channel utilization and noise floor.
Radio 5 GHz	<ul style="list-style-type: none"> ■ Displays the performance of the AP in terms of the channel utilization and noise floor in the 5 GHz channel. ■ For example, the device health is Good when the channel utilization is less than or equal to 70% and the noise floor is less than or equal to -80 dBm. If the value of the channel utilization and noise floor falls below the threshold, the device health is displayed as Poor. If the AP is online, but the radio is down, the value displayed is Disabled. If the scenario is not applicable, a "-" sign is displayed. ■ Hover over the Radio 5 GHz status to get the exact value of the channel utilization and noise floor.

Parameter	Description
Radio 5 GHz (Secondary)	<ul style="list-style-type: none"> Displays the performance of the AP in terms of the channel utilization and noise floor in the 5 GHz (Secondary) channel. For example, the device health is Good when the channel utilization is less than or equal to 70% and the noise floor is less than or equal to -80 dBm. If the value of the channel utilization and noise floor falls below the threshold, the device health is displayed as Poor. If the AP is online, but the radio is down, the value displayed is Disabled. If the scenario is not applicable, a "-" sign is displayed. Hover over the Radio 5 GHz (Secondary) status to get the exact value of the channel utilization and noise floor. <p>NOTE: In the Health Bar dashboard, the Radio 5 GHz (Secondary) data is available only for AP-555 access points and only if the tri-radio mode is enabled. For more information, see About Tri-Radio Mode.</p>
Virtual Controller	Indicates if the AP is connected to a virtual controller. If the AP is connected, clicking on the virtual controller name redirects you to the Manage > Overview > Summary page for the virtual controller.

Health Bar Dashboard for Switch

The following table includes information on the various parameters of the Health Bar displayed for a switch. If the switch is not online and running, not all of the following data is available.

Parameter	Description
Switch Status	Displays the time period for which the switch has been online and running or its offline status.
Device Health	<ul style="list-style-type: none"> Displays the performance of the switch in terms of the CPU and memory usage. For example, the device health is Good when the CPU usage is less than or equal to 70% and the memory usage is less than or equal to 70%. If the value of the CPU and/or memory usage falls below the threshold, the device health is displayed as Poor. Hover over the Device Health status to get the exact percentage value of the memory and CPU usage.
Port - Status	<ul style="list-style-type: none"> Displays the number of ports on the switch that are online and the number of ports that are offline. The number in green indicates the number of switch ports that are online. The number in red indicates the number of switch ports that are offline.
Port - Alerts	<ul style="list-style-type: none"> Displays the total number of open alerts.

Health Bar Dashboard for Controller

The following table includes information on the various parameters of the Health Bar displayed for a controller. If the controller is not online and running, not all of the following data is available.

Parameter	Description
Controller Status	Displays the time period, in the format of days-hours-minutes, for which the controller has been running or its offline status.
LAN	<ul style="list-style-type: none"> ■ Displays the number of LAN ports as online or offline. ■ The number in green indicates the number of LAN ports that are online. ■ The number in red indicates the number of LAN ports that are offline. ■ Clicking the numbers redirects you to Manage > LAN > Summary.
Alerts	<ul style="list-style-type: none"> ■ Displays the total number of open alerts. ■ Clicking the number redirects you to Analyze > Alerts & Events in List view.

Health Bar Dashboard for Wireless Client

The following table includes information on the various parameters of the Health Bar displayed for a wireless client.

Parameter	Description
Client Status	Displays the connection status of the client.
Device Health	Displays the device health of the client.
Signal Quality	Displays the signal quality in dB.
Tx Rx Rate	Displays the transmit and receive rate in Mbps.
Connected To	<ul style="list-style-type: none"> ■ Displays the device to which the wired client is connected. ■ Clicking on the device redirects you to the Manage > Overview > Summary page for that device.
Refresh icon	Refreshes the data on the Health Bar for the client.

Health Bar Dashboard for Wired Client

The following table includes information on the various parameters of the Health Bar displayed for a wired client.

Parameter	Description
Client Status	Displays the connection status of the client.
Connected Port	Displays the port to which the client is connected.
Connected To	<ul style="list-style-type: none"> ■ Displays the device to which the wired client is connected. ■ Clicking on the device redirects you to the Manage > Overview > Summary page for that device.

Parameter	Description
Refresh icon	Refreshes the data on the Health Bar for the client.

Aruba Central includes a unified network operations and assurance platform and an intelligent, machine learning based solution for device discovery, profiling and visibility. Each of these solutions work individually and collectively to support Aruba's APs, Switches, and Controllers. From the **Account Home** page, you can manage network inventory, APIs, user access and so on. Under **Global Settings**, you have the following tiles:

- **Users and Roles**—Aruba Central users can be broadly categorized as system and external users. A role refers to a logical entity used for determining user access to devices and application services in Aruba Central. Users are always tagged to roles that govern the level of user access to the Aruba Central applications and services. For more information on users and roles, see [Managing Users and Roles](#).
- **Key Management**—The **Key Management** menu option in the **Account Home** page allows you to view and track subscriptions key.
- **Device Inventory**—In Aruba Central, you can add devices either in the online or offline mode.
- **License Assignment**—Aruba offers two tiers of device licenses as part of the multi-tier licensing model. The two tiers are Foundation and Advanced Licenses.
- **Audit Trail**—This page shows the total number logs generated for all device management, configuration, and user management events triggered in Aruba Central. For more information, see [Viewing Audit Trail](#).
- **Authentication**—The Single Sign On (SSO) solution simplifies user management by allowing users to access multiple applications and services with a single set of login credentials. If the applications services are offered by different vendors, IT administrators can use the SAML authentication and authorization framework to provide a seamless login experience for their users. For more information, see [SAML SSO](#).
- **API Gateway**—Aruba Central supports a robust set of REST APIs to enable users to build custom applications and integrate the APIs with their applications. The Aruba Central API framework uses OAuth protocol to authenticate and authorize third-party applications, and allows them to obtain secure and limited access to an Aruba Central service. For more information on APIs, refer to the *API Reference Guide*.
- **Webhooks**—Contains the Streaming API and the Webhooks tabs. Streaming APIs allow customers to subscribe to a select set of services instead of polling the NB API to get an aggregated state or statistics of the events. With streaming API, the customers can write value-added applications based on the aggregated context. For more information on streaming APIs, refer to the *API Reference Guide*.

This tile also contains the **Webhook** tab. An application can provide real-time information or notifications to other applications using the Webhook service. You can access the Webhook service through the **Account Home** or API Gateway. Using the Webhook service, you can list, add, or delete Webhooks; get Webhook token; refresh Webhook token; update Webhook settings; do Webhook settings for a specific item; and test for Webhook notification. For more information on webhooks, refer to the *API Reference Guide*.
- **System Management**—This page shows the overall status and performance of the Aruba Central system. For more information, see [System Management](#).

The command-line interface features allows you to install, setup, manage, and troubleshoot Aruba Central (on-premises) deployments. The CLI is accessed through a console or through a Secure Shell (SSH) session from a remote management console or workstation.

Accessing the Aruba Central CLI

The following procedure describes how to access the SSH and start executing CLI commands:

1. From a secure shell (SSH) client, open an SSH connection.
2. Login as an administrator.
3. When prompted, enter the administrator password.
A list of commands is displayed.

For example:

```
login as: copadmin
admin@10.22.150.92 password:
Last login: Wed Aug 7 05:43:22 2019 from 10.20.15.180
```

Syntax

Enter option [0 - <option number>]: <enter option>

For example:

```
1. System
2. File Operations
3. Show
...
0. exit
...
Enter option [ 0 - 9 ]:
```

Common Command Options

The following common options are used to:

- **0 - Exit**—Use this command option to exit the SSH connection.
- **b - Back**—Use this command option to go back to the previous menu.
- **m -Main menu**—Use this command option to go to the main menu.

Password Recovery

The password recovery system helps create a new password for the **copadmin** user. If you have forget the password, login to the console with the user, **coprecovery**, and the following options are displayed to generate the recovery key.

- **Generate Recovery Key**—The recovery key is generated and stored in an encrypted .asc file. You can either copy it or use the SCP command to copy the file. Once the key is copied to the local server, contact customer support to decrypt the recovery key to get a new password.
- **SCP Recovery Key**—The recovery key is generated and an SCP command is used to copy the file to a local server. Once the key is copied to the local server, contact customer support to decrypt the recovery key to get a new password.
- **Activate Recovery secret**—The secret key is provided and verified by the customer support. A reset option is used to rest the password in all nodes.
- **Retrieve "core" Password**—Aruba does not recommend using **core** user access. The customer support will decode the secret file provided by the user to provide access to the core user.

Main Menu Options

When you login to the Aruba Central (on-premises) SSH, the main set of commands are displayed. Using the main menu command options, you can perform various other actions as described in the table.

```
1. System
2. File Operations
3. Show
4. System Configuration
5. Advanced
6. Security
7. Support
8. Temporary Root Shell
9. Search Commands
=====
0. exit
Enter option [ 0 - 9 ]:
```

List of CLI Commands

The following table lists all the commands supported in Aruba Central (on-premises) deployment:

Option Number	Command	Description
1	System	Reboots or resets the system.
1-1	Reboot	Reboots the system.
1-2	Shutdown	Shutowns the system.
1-3	Factory Reset	Resets the system to factory settings.

Option Number	Command	Description
2	File Operations	Uploads a file to the host.
2-1	Upload via (SCP)	Uploads a file to the host over SCP.
2-2	Upload via (SFTP)	Uploads a file to the host over SFTP.
2-3	Upload via (HTTP/HTTPS)	Uploads a file to the host over HTTP or HTTPS
2-4	Download File from COP	Downloads a file that is saved on the host.
2-5	Delete File	Deletes the files that was uploaded by the upload file command.
3	Show	Show commands are used to view or display the settings or parameters configured.
3-1	Version (Detail)	Displays the version (Detail) of the Aruba Central (on-premises) deployment.
3-2	List Files	Displays the total number of files in the pod.
3-3	Backup – Restore Status	Display the backup and restore status of the pod
3-4	Configuration	Display the updated network settings, cluster details, NTP/Timezone information.
3-5	System	Display system information like usage of memory, activate information, and uptime.
3-6	User Sessions	Displays the list of user sessions.
3-7	Show Clock	Displays the date, week, month, time details.
3-8	App status	Pod status of any Aruba Central (on-premises) application.
3-9	Cluster Status	Displays the cluster details for Aruba Central (on-premises)
4	System Configuration	System configuration commands are used to configure system parameters like network setup, cluster setup, timezone setup and also, upgrade the setup or perform a complete factory reset.
4-1	Upgrade	Upgrades the system for either an online customer or an offline customer.
4-2	Network Setup	Sets up a network permanently or temporarily.
4-3	Proxy Setup	Setup proxy configuration for Aruba Central (on-premises)
4-4	Setup Timezone	Sets up a timezone.
4-5	Setup NTP	Sets up an NTP server.
4-6	Node Setup	Sets up a node.
5	Advanced	Advanced commands are used to ping or check connectivity.

Option Number	Command	Description
5-1	Test Connectivity	Tests the connectivity to any URL.
5-2	Nslookup	Performs a DNS lookups for any host names.
5-3	Toggle CDN	Used to enable CDN, disable CDN , or show CDN Status.
6	Security	Security commands are used to reset or update the password.
6-1	Reset Password GUI	Resets the GUI password.
6-2	Reset Password CLI	Resets the CLI password.
6-3	Reset debug apps password	Resets the debug applications password.
7	Support	Support commands are used to collect information that are useful to TAC.
7-1	Support Connection	Starts or stops support connection for remote TAC access.
7-2	Collect All Logs	Collects Aruba Central (on-premises) diagnostic tar for debugging.
7-3	Log Snapshot Operations	Generates and downloads snapshots. It also deletes snapshots and downloads upgrade reports.
7-4	Download COP Setup Logs	Downloads the COP setup logs.
7-5	Restart Applications	Restarts the applications.
7-6	System Operations Lock Management	Restarts a particular application.
8	Temporary Root Shell	Creates a temporary user and allows access to SSH for 2 days at a time.
9	Search	Displays a list of available command options.

System Commands

Enter the command option **1** from the main menu to reboot, shutdown, or reset the system to factory settings.

```

Enter option [ 0 - 9 ]: 1
1. Reboot
2. Shutdown
3. Factory Reset
=====
b. back
m. main menu
0. exit

Enter option [ 0 - 3 ]:

```

Reboot

Enter the command option **1** from the System menu to reboot the system.

```
Enter option [ 0 - 3 ]: 1
Are you sure you want to reboot the node (Y/N):
```

Shutdown

Enter the command option **2** from the System menu to shutdown the system.

```
Enter option [ 0 - 3 ]: 2
Executing shutdown...
Shutdown scheduled. Node will shutdown after 1 minute.
Press [Enter] key to continue...
```

Factory Reset

Enter the command option **3** from the System menu to reset the system to its factory settings. Currently, it is a complete data reset.

```
Enter option [ 0 - 3 ]: 3
Error: Please run the reset command from physical or remote console (ILO)
Press [Enter] key to continue...
```

File Operations Commands

Enter the command option **2** from the main menu to upload a file to the host.

```
Enter option [ 0 - 9 ]: 2
1. Upload via (SCP)
2. Upload via (SFTP)
3. Upload via (HTTP/HTTPS)
4. Download File from COP
5. Delete file
=====
b. back
m. main menu
0. exit

Enter option [ 0 - 5 ]:
```



The **Upload via (HTTP/HTTPS)** option is not available for a FIPS-enabled Aruba Central (on-premises) setup.

Upload via (SCP)

Enter the command option **1** from the File Operations menu to upload a file to the host over SCP.

```
Enter option [ 0 - 4 ]: 1
This will scp a file from the remote server to COP server
Enter remote hostname and path (username@hostname:<filepath>):
auto@10.22.158.92:/home/auto/packages.txt
```

```
Copying auto@10.22.158.92:/home/auto/packages.txt to COP server
FIPS mode initialized
auto@10.22.158.92's password:
packages.txt
100% 3555      4.4MB/s   00:00
Press [Enter] key to continue...
```

Upload via (SFTP)

Enter the command option **2** from the File Operations menu to upload a file to the host over SFTP.

```
Enter option [ 0 - 4 ]: 2
This will scp a file from the remote server to COP server
Enter remote hostname and path (username@hostname:<filepath>):
auto@10.22.158.92:/home/auto/inst_packages.txt

Copying auto@10.22.158.92:/home/auto/inst_packages.txt to COP server
FIPS mode initialized
auto@10.22.158.92's password:
Connected to 10.22.158.92.
Fetching /home/auto/inst_packages.txt to /var/airwave/appliance/localhost/inst_
packages.txt
/home/auto/inst_packages.txt
100% 1583      127.9KB/s   00:00
Press [Enter] key to continue...
```

Upload via (HTTP/HTTPS)

Enter the command option **3** from the File Operations menu to upload a file to the host over HTTP or HTTPS.

```
Enter option [ 0 - 5 ]: 3
This will copy a file from the url to COP server
Enter full url path for file : http://10.22.154.165/a.html
a.html
100%
[=====>]
391.90M  106MB/s   in 3.7s
Upload file successful.
Press [Enter] key to continue...
```

Download File from COP

Enter the command option **3** from the File Operations menu to download a file that is saved on the host.

```
Enter option [ 0 - 4 ]: 3
! Files present under the directory !
cop_setup_logs inst_packages.txt packages.txt sftp.txt
Enter the file name to copy from COP server to the remote server:
packages.txt
This will scp packages.txt from localhost to the remote server
Enter remote hostname and path (username@hostname:<filepath>):
auto@10.22.158.92:/home/auto
```

```

Copying localdisk files to auto@10.22.158.92:/home/auto
FIPS mode initialized
The authenticity of host '10.22.158.92 (10.22.158.92)' can't be established.
RSA key fingerprint is SHA256:e9KqvWRV5YQhrPLoJQMiKFKKwVx7ZWz2T34oF31WvpU.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.22.158.92' (RSA) to the list of known hosts.
auto@10.22.158.92's password:
packages.txt
100% 3555      2.9MB/s   00:00
Press [Enter] key to continue...

```

Delete File

Enter the command option **4** from the File Operations menu to delete the files that was uploaded by the upload file command.

```

Enter option [ 0 - 4 ]: 4
! Files present under the directory !
cop_setup_logs inst_packages.txt packages.txt sftp.txt
Enter file/directory to delete:
packages.txt
Deleting file /var/airwave/appliance/localdisk/packages.txt
Are you sure you want to delete this file(Y/N):
Y
File /var/airwave/appliance/localdisk/packages.txt deleted
Press [Enter] key to continue...

```

Show Commands

Show commands are used to view or display various elements of the Aruba Central (on-premises) deployment like configurations currently performed, user sessions, status, and so on.

Enter the command option **3** from the main menu to view all the show commands supported.

```

Enter option [ 0 - 9 ]: 3
1. Version (Detail)
2. List Files
3. Backup-Restore Status
4. Configuration
5. System
6. User Sessions
7. Clock
8. App Status
9. Cluster Status
=====
b. back
m. main menu
0. exit

Enter option [ 0 - 9 ]:

```

The following section describes the set of commands that can be executed under the Show commands category.

Version (Detail)

Enter command option **1** from the Show commands menu to display the version (Detail).

```
Enter option [ 0 - 9 ]: 1
COP Version: 2.5.5.0
Build: 10.0.0-GA01.139
ISO Installed: Ok
COP Software Installed: Ok
Setup Cluster: Ok
Pulling ILO details. Please wait.
HPE Smart Array P408i-a SR Gen10: "4.11"
iLO 5: "2.18 Jun 22 2020"
System ROM: "U32 v2.34 (04/08/2020)"
Press [Enter] key to continue...
```

List Files

Enter command option **2** from the Show commands menu to display the total number of files.

```
Enter option [ 0 - 9 ]: 2
total 4
drwxr-xr-x 2 root root 4096 Jan  3 16:29 cop_setup_logs
Press [Enter] key to continue...
```

Backup-Restore Status

Enter command option **3** from the Show commands menu to display the backup and restore status.

```
Enter option [ 0 - 9 ]: 3
#####
backup/restore status
#####
{"details": [
  {
    "message": "Postgres backup success",
    "status": "success"
  },
  {
    "message": "Cassandra backup success",
    "status": "success"
  },
  {
    "message": "Elasticsearch backup success",
    "status": "success"
  },
  {
    "message": "Minio backup success",
    "status": "success"
  },
  {
    "message": "Tar creation success",
    "status": "success"
  },
  {
    "message": "Transferring the backup to repository success",
    "status": "success"
  }
],
"endedOn": "Wed, 26 Jun 2019 12:52:29 GMT",
"operation": "Backup",
"startedOn": "Wed, 26 Jun 2019 11:59:43 GMT",
```

```
"status": "Completed"
}
```

Configuration

Enter command option **4** from the Show commands menu to display the updated network settings, AirWave cluster details, and NTP/Timezone information.

```
Enter option [ 0 - 9 ]: 4
1. Network-config/Cluster-info
2. NTP/Timezone Info
Enter option [ 0 - 2 ]:
```

- **Network-config/Cluster-info**—Enter command option **1** from the Configuration menu to view the network configuration and cluster information.

```
Enter option [ 0 - 2 ]: 1
Updated Network Settings
-----
Hostname                : node182-158.arubathena.com
IP Address               : 10.22.158.182
Subnet Mask              : 255.255.255.0
Gateway                 : 10.22.158.2
DNS                     : 10.20.50.10
Secondary DNS           : 10.20.50.25
Timezone                 : UTC
COP Cluster Details
-----
Cluster IP              : 10.22.158.27
Cluster FQDN            : node3vip.arubathena.com
Pod CIDR                 : 172.16.0.0/16
Service CIDR            : 10.3.0.0/23
Router ID                : 27
Time Zone               : UTC
Cluster Node Count      : 3
Cluster Node List       :
NAME                    STATUS  ROLES  AGE   VERSION
10.22.158.181          Ready  master 8h    v1.14.5
10.22.158.182          Ready  master 8h    v1.14.5
10.22.158.77           Ready  master 8h    v1.14.5
```

- **NTP/Timezone Info**—Enter command option **2** from the Configuration menu to view the NTP/Timezone info.

```
Enter option [ 0 - 2 ]: 2
#####
NTP Info
#####
Default NTP server configured is - ntp.ubuntu.com
#####
TimeZone Info
#####
UTC
```

System

Enter command option **5** from the Show commands menu to display system information like usage of memory, system information, and so on.

```
Enter option [ 0 - 9 ]: 5
1. Memory/Hard disk/CPU Usage
3. Uptime
=====
b. back
m. main menu
0. exit
Enter option [ 0 - 2 ]:
```

- **Memory/Hard disk/ CPU Usage**—Enter the command option **1** from the System menu to view the usage of memory, hard disk, and CPU information.

```
Enter option [ 0 - 2 ]: 1
#####
Memory Usage
#####
total          used          free          shared  buff/cache   available
Mem:           251G          113G          111G          990M         26G          137G
Swap:           0B             0B             0B
#####
Harddisk Usage
#####
Filesystem      Size  Used Avail Use% Mounted on
udev            126G   0    126G   0% /dev
tmpfs           26G    17M   26G    1% /run
/dev/sdb4       15G   6.0G   8.3G  42% /
tmpfs           126G   0    126G   0% /dev/shm
tmpfs           5.0M   0    5.0M   0% /run/lock
tmpfs           126G   0    126G   0% /sys/fs/cgroup
/dev/sdb3       465M  109M  328M  25% /boot
/dev/sdb2       241M   512  241M   1% /boot/efi
/dev/sdb5       15G   41M   15G    1% /secondary
/dev/sdb6       1.7T   82G  1.6T   5% /data
tmpfs           26G   0    26G   0% /run/user/1003
tmpfs           26G   0    26G   0% /run/user/1001
tmpfs           26G   0    26G   0% /run/user/1004
#####
CPU Usage
#####
%Cpu(s):  7.0 us,  2.2 sy,  0.0 ni, 90.1 id,  0.4 wa,  0.0 hi,  0.3 si,  0.0 st
Architecture:          x86_64
CPU op-mode(s):        32-bit, 64-bit
Byte Order:             Little Endian
CPU(s):                 80
On-line CPU(s) list:   0-79
Thread(s) per core:    2
Core(s) per socket:    20
Socket(s):              2
NUMA node(s):          2
Vendor ID:              GenuineIntel
CPU family:             6
Model:                  85
Model name:             Intel(R) Xeon(R) Gold 6138 CPU @ 2.00GHz
Stepping:               4
```

```

CPU MHz:          2866.513
CPU max MHz:     3700.0000
CPU min MHz:     1000.0000
BogoMIPS:        4000.00
Virtualization:  VT-x
L1d cache:      32K
L1i cache:      32K
L2 cache:       1024K
L3 cache:       28160K
NUMA node0 CPU(s): 0-19,40-59
NUMA node1 CPU(s): 20-39,60-79
Flags:          fpu vme de pse tsc msr pae mce cx8 apic sep mtrr

```

- **Uptime**—Enter the command option **2** from the System menu to view the uptime duration of a Aruba Central (on-premises) pod.

```

Enter option [ 0 - 2 ]: 2
#####
uptime
#####
06:44:21 up 8:49, 7 users, load average: 17.89, 11.79, 10.51

```

User Sessions

Enter command option **6** from the Show commands menu to display the list of user sessions.

```

Enter option [ 0 - 9 ]: 6
#####
List of user sessions
#####
copadmin pts/0      2020-07-27 05:26 01:17      51432 (10.240.125.20)
inedshell pts/1    2020-07-27 05:02 01:42      3261 (10.20.13.62)
cop_shell pts/2    2020-07-27 05:30 01:10      54299 (10.240.125.20)
copadmin pts/3    2020-07-27 05:54 .          76741 (10.240.126.221)
inedshell pts/4    2020-07-27 06:05 00:39      47373 (10.20.13.113)
inedshell pts/5    2020-07-27 06:11 00:32      36861 (10.20.44.187)
inedshell pts/6    2020-07-27 06:42 00:02      68881 (10.240.130.81)
)

```

Clock

Enter command option **7** from the Show commands menu to display the date, week, month, and time details.

```

Enter option [ 0 - 9 ]: 7
Thu Aug 8 03:33:50 UTC 2019

```

App status

Enter command option **8** from the Show commands menu to provide the pod status of any Aruba Central (on-premises) application. Following example shows the status of the Aruba Central (on-premises) application.

```

Enter option [ 0 - 9 ]: 8
Enter the application name, to list all apps press Enter key:central
Enter the application name, to list all apps press Enter key:central
acp-system      central-grafana-dashboard-7c845956dc-92xgj
1/1      Running
7h42m    172.16.2.94      10.22.158.181    <none>          <none>
1
central      acp-ae-rapids-api-deployment-b8d794d49-4sxck
1/1      Running      0          7h30m    172.16.0.172    10.22.158.182    <none>
<none>
central      acp-ae-rapids-bootstrap-deployment-789f85cbbd-dtjsb
1/1      Running      0          7h38m    172.16.4.131    10.22.158.77    <none>
central      acp-ae-rapids-deployment-588b4989b5-kc58v
1/1      Running      0          7h38m    172.16.0.134    10.22.158.182    <none>
<none>
central      acp-ae-rapids-deployment-588b4989b5-q7mw8
1/1      Running      0          7h38m    172.16.4.130    10.22.158.77    <none>
<non
central      acp-ae-rapids-deployment-588b4989b5-q7mw8
1/1      Running      0          7h38m    172.16.4.130    10.22.158.77    <none>
<none>
central      acp-ae-rapids-deployment-588b4989b5-xx5ks
1/1      Running      0          7h38m    172.16.2.121    10.22.158.181    <none>
central      acp-device-visibility-deployment-5f97648f6f-nxq28
1/1      Running      0          7h42m    172.16.4.102    10.22.158.77    <none>
<none>
central      acp-device-visibility-deployment-5f97648f6f-nxq28
1/1      Running      0          7h42m    172.16.4.102    10.22.158.77    <none>
<none>
central      admin-api-deployment-7d4f4984f7-9wq5h
1/1      Running      0          7h37m    172.16.2.150    10.22.158.181    <none>
<none>

```

Cluster Status

Enter command option **9** from the Show commands menu to display the cluster details for Aruba Central (on-premises).

```

Enter option [ 0 - 9 ]: 9
COP Cluster Details
-----
Cluster IP      : 10.22.158.27
Cluster FQDN    : node3vip.arubathena.com
Pod CIDR       : 172.16.0.0/16
Service CIDR   : 10.3.0.0/23
Router ID      : 27
Time Zone      : UTC
Cluster Node Count : 3
Cluster Node List :
NAME           STATUS   ROLES   AGE   VERSION
10.22.158.181 Ready   master  8h   v1.14.5
10.22.158.182 Ready   master  8h   v1.14.5
10.22.158.77  Ready   master  8h   v1.14.5

```

System Configuration Commands

The System Configuration commands are used to configure system parameters like network setup, cluster setup, timezone setup and also, upgrade the setup or perform a complete factory reset.

Enter command option **4** from the main menu to view all the system configuration commands supported.

```

Enter option [ 0 - 9 ]: 4
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
=====
b. back
m. main menu
0. exit

Enter option [ 0 - 6 ]:

```

The following section describes the set of commands that can be executed under the system configuration category.

Upgrade

Enter command option **1** from the System Configuration commands menu to upgrade the system for either an online user or an offline user.

```

Enter option [ 0 - 6 ]: 1
COP Server Status
-----
Current Version           : 2.5.2.0
Latest Version           : 2.5.2.0
Online Customer          : true
Upgrade Status           : UP_TO_DATE
Upgrade Available        : false
File Transfer Completion Percentage : 0
Upgrade Stage Completion Percentage : 0
-----
Last File Transfer Status :
Last File Transfer Message :
Last File Transfer Time   :
Last Upgrade Status       :
Last Upgrade Message      :
Last Upgrade Time         :
-----
==== COP is in latest version ====

```

Network Setup

Enter command option **2** from the System Configuration commands menu to setup a network permanently or temporarily.

```

Enter option [ 0 - 6 ]: 2
1. Permanent (Network settings)
2. Temporary (Network settings)
=====
b. back
m. main menu
0. exit

Enter option [ 0 - 2 ]:

```

- **Permanent (Network settings)**—Enter command option **1** from the Network Setup commands menu to setup the permanent network settings.

```
Enter option [ 0 - 2 ]: 1

Network Settings

Hostname   : ccs-1n-cophost.arubathena.com
IP Address : 10.22.154.57
Interface  : eno1

Enter Subnet mask : 255.255.255.0
Enter Gateway : 10.22.154.2
Enter DNS : 10.20.50.10

Secondary DNS is optional. Press ENTER to proceed
Enter Secondary DNS : 10.20.50.25

Network settings exist; will be reset to new value
To list timezones, enter 'list'
Enter timezone : UTC

===== Updated Network Settings =====

Hostname           : ccs-1n-cophost.arubathena.com
IP Address         : 10.22.154.57
Subnet Mask       : 255.255.255.0
Gateway           : 10.22.154.2
DNS               : 10.20.50.10
Secondary DNS     : 10.20.50.25
Timezone          : UTC

=====

Press [Enter] key to continue...
```

- **Temporary (Network settings)**—Enter command option **2** from the Network Setup commands menu to setup the temporary network settings.

```
Enter option [ 0 - 2 ]: 2

Network Settings

Hostname   : ccs-1n-cophost.arubathena.com
IP Address : 10.22.154.57
Interface  : eno1

Enter Subnet mask : 255.255.255.0
Enter Gateway : 10.22.154.2
Enter DNS : 10.20.50.10

Secondary DNS is optional. Press ENTER to proceed
Enter Secondary DNS : 10.20.50.25

Network settings exist; will be reset to new value
To list timezones, enter 'list'
Enter timezone : UTC
```

```

===== Updated Network Settings =====
Hostname                : ccs-1n-cophost.arubathena.com
IP Address              : 10.22.154.57
Subnet Mask             : 255.255.255.0
Gateway                 : 10.22.154.2
DNS                     : 10.20.50.10
Secondary DNS           : 10.20.50.25
Timezone                : UTC
=====

Press [Enter] key to continue...

```

Proxy Setup

Enter command option **3** from the System Configuration menu to add, delete, or get proxy URL.

```

Enter option [ 0 - 6 ]: 3
1. Add Proxy
2. Delete Proxy
3. Get Proxy
Enter option [ 0 - 3 ]:

```

- **Add Proxy**—Enter command option **1** from the Proxy Setup commands menu from the Proxy Setup menu to add a proxy URL.

```

Enter option [ 0 - 3 ]: 1
Enter the proxy url:
Enter Port:
Enter username(optional):
Enter password(optional):
Enter option [ 0 - 3 ]: 1
Enter the proxy url: www.techpubs.com
Enter port: 98
Enter username(optional):
Enter password(optional):

```

- **Delete Proxy**—Enter command option **2** from the Proxy Setup commands menu menu to delete a proxy.

```

Enter option [ 0 - 3 ]: 2
Proxy deleted
Press [Enter] key to continue...

```

- **Get Proxy**—Enter command option **3** from the Proxy Setup menu to get the details of a proxy.

```

Enter option [ 0 - 3 ]: 3

"url": "10.22.154.228",
"username": "admin",
"password": "",

```

```
"port": "3128"
```

Setup Timezone

Enter command option **4** from the System Configuration menu to setup a timezone.

```
Enter option [ 0 - 6 ]: 4
To list timezones, enter 'list'
Enter timezone [UTC]: GMT
Setting TimeZone for other nodes in this cluster...
configmap/airwave-config patched (no change)
Press [Enter] key to continue...
```

Setup NTP

Enter command option **5** from the System Configuration menu to setup an NTP.

```
Enter option [ 0 - 6 ]: 5
Enter primary NTP server : 10.22.158.230
Enter secondary NTP server (Optional) :10.22.154.165
Enter tertiary NTP server (Optional):
Is NTP Authentication required (y/n) :
n
Configuring NTP for node : 10.22.154.57
FIPS mode initialized
10.22.158.230 NTP configured on node 10.22.154.57
10.22.154.165 NTP configured on node 10.22.154.57
FIPS mode initialized
FIPS mode initialized
NTP is configured node : 10.22.154.57
Press [Enter] key to continue...
```

All the nodes in a multi-cluster must synchronize to the same NTP server. Run the command `NTP/Timezone info` to verify if all the nodes are synchronized with the same NTP server. To run the `NTP/Timezone info`, enter command option **2** from the `show configuration` menu.

You also have an option to authenticate the NTP server by using the secure key.



NOTE

- If you are using iLO when configuring NTP servers and require the authentication for NTP server, you must either use the WebUI or CLI to copy the NTP server key. The copy and paste operation is not supported on the iLO console. Logon to the CLI with iLO credentials and use the VSP command to get the secure key.
- If `Setup NTP` is executed after the cluster is configured, then the modified details of NTP server is updated to the cluster. If cluster is not configured, then the modified NTP server details is updated only to the node.

Node Setup

Enter command option **6** from the System Configuration menu to setup a node.

```
Enter option [ 0 - 6 ]: 6
```

Advanced Commands

Enter command option **5** from the main menu to check test connectivity and Nslookup.

```
Enter option [ 0 - 9 ]: 5
1. Test Connectivity
2. Nslookup
3. Toggle CDN
4. Configure ILO IP
=====
b. back
m. main menu
0. exit
```

Test Connectivity

Enter command option **1** from the Advanced commands menu to test the connectivity to any URLs.

```
Enter option [ 0 - 4 ]: 1
1. Ping
2. Dependent Servers Reachability
=====
b. back
m. main menu
0. exit

Enter option [ 0 - 2 ]:
```

- **Ping**—Enter command option **1** from the Test Connectivity menu to ping an IP address or hostname.

```
Enter option [ 0 - 2 ]: 1
Enter the IP address or hostname to ping:10.22.154.56
PING 10.22.154.56 (10.22.154.56) 56(84) bytes of data.
64 bytes from 10.22.154.56: icmp_seq=1 ttl=63 time=0.473 ms
64 bytes from 10.22.154.56: icmp_seq=2 ttl=63 time=1.61 ms
64 bytes from 10.22.154.56: icmp_seq=3 ttl=63 time=2.63 ms
64 bytes from 10.22.154.56: icmp_seq=4 ttl=63 time=1.58 ms
64 bytes from 10.22.154.56: icmp_seq=5 ttl=63 time=2.99 ms
```

- **Dependent Servers Reachability**—Enter command option **2** from the Test Connectivity menu to check the reachability of the dependent servers.

```
Enter option [ 0 - 2 ]: 2

Connection to coreupdate (coreupdate.central.arubanetworks.com) successful.

Connecting to coreupdate(coreupdate-prod.central.arubanetworks.com) ...
You are going to access FED system .
Required policy
1 LINE 1
2 LINE 2
3 LINE 3
4 LINE 4
5 LINE 5
```

```
Connection to coreupdate (coreupdate-prod.central.arubanetworks.com) successful.

Connecting to quay(quay.io) ...
You are going to access FED system .
Required policy
1 LINE 1
2 LINE 2
3 LINE 3
4 LINE 4
5 LINE 5

Connection to quay (quay.io) successful.

Connecting to nexus(nexus2.airwave.com) ...
Connection to nexus(nexus2.airwave.com) successful.

----- All dependent HTTP(S) servers are reachable -----

Press [Enter] key to continue...
```

Nslookup

Enter option **2** from the Advanced commands menu to get the DNS lookups for any host names.

```
Enter option [ 0 - 4 ]: 2
Enter the hostname or IP Address for NS Lookup:google.com
../../../../lib/dns/hmac_link.c:349: FIPS mode is 1: MD5 is only supported if the value
is 0.
Please disable either FIPS mode or MD5.
Server:                10.20.50.10
Address:                10.20.50.10#53

Non-authoritative answer:
Name:  google.com
Address: 142.250.76.46
Name:  google.com
Address: 2404:6800:4007:814::200e

Press [Enter] key to continue...
```

Toggle CDN

Enter command option **3** from the Advanced commands menu to enable CDN, disable CDN , or show CDN Status.

```
Enter option [ 0 - 4 ]: 3
1. Enable CDN
2. Disable CDN
3. Show CDN status
=====
b. back
m. main menu
0. exit

Enter option [ 0 - 3 ]:
```

- **Enable CDN**—Enter command option **1** from the Toggle CDN commands menu to enable CDN.

```
Enter option [ 0 - 3 ]: 1
CDN enabled
Press [Enter] key to continue...
```

- **Disable CDN**—Enter command option **2** from the Toggle CDN commands menu to disable CDN.

```
Enter option [ 0 - 3 ]: 2
CDN disabled
Press [Enter] key to continue...
```

- **Show CDN Status**—Enter command option **3** from the Toggle CDN commands menu to show the status of CDN.

```
Enter option [ 0 - 3 ]: 3
{
  "monitoring": "://d1c50ulzbkqmph.cloudfront.net",
  "configuration": "://d1c50ulzbkqmph.cloudfront.net",
  "base": "://d1c50ulzbkqmph.cloudfront.net",
  "enabled": false,
  "guest": "://d1c50ulzbkqmph.cloudfront.net",
  "msp": "://d1c50ulzbkqmph.cloudfront.net"
}
```

Configure ILO IP

Enter command option **4** from the Advanced commands menu to configure the IP address of the ILO.

```
Enter option [ 0 - 4 ]: 4
```

Security Commands

Enter the command option **6** from the main menu to either reset the GUI or CLI password or update the iLO password.

```
Enter option [ 0 - 11 ]: 6
1. Reset Password GUI
2. Reset Password CLI
3. Reset debug apps password
=====
b. back
m. main menu
0. exit

Enter option [ 0 - 3 ]:
```

Reset Password GUI

Enter the command option **1** from the Security Commands menu to reset the GUI password.

```
Enter option [ 0 - 3 ]: 1
Do you want to reset GUI admin user password(y/n) :
```

Reset Password CLI

Enter the command option **2** from the Security commands menu to reset the CLI password.

```
Enter option [ 0 - 3 ]: 2
Do you want to reset copadmin password(y/n) :
```

Reset debug apps password

Enter the command option **3** from the Security commands menu to reset the debug apps password.

```
Enter option [ 0 - 3 ]: 3
Do you want to reset debug apps password(y/n) :
```

Support Commands

Enter the command option **7** from the main menu to start or stop the support connection, collect logs, and restart a particular application.\

```
Enter option [ 0 - 9 ]: 7
1. Support Connection
2. Collect All Logs
3. Log Snapshot Operations
4. Download COP Setup Logs
5. Restart Application
6. System Operations Lock Management
=====
b. back
m. main menu
0. exit

Enter option [ 0 - 6 ]:
```

Support Connection

Enter the command option **1** from the Support commands menu to start, stop, restart the support connection from remote TAC access or check the status of the support connection and upload the support connection file.

```
Enter option [ 0 - 6 ]: 1
1. Start Support Connection
2. Stop Support Connection
3. Restart Support Connection
4. Support Connection Status
5. Upload Support Connection File
6. Add Support User 'copsupport'
7. Delete Support User 'copsupport'
8. Show contents of copsupport.gpg
=====
b. back
```

```
m. main menu
0. exit

Enter option [ 0 - 8 ]: 1
```

- **Start Support Connection**—Enter command option **1** from the Support Connection commands menu to start a support connection.

```
Enter option [ 0 - 8 ]: 1
{
  "support_connection_status": "stopped",
  "active_from": "_",
  "connection": "inactive"
}
Press [Enter] key to continue...
```

- **Stop Support Connection**—Enter command option **2** from the Support Connection commands menu to stop a support connection.

```
Enter option [ 0 - 8 ]: 2
{
  "support_connection_status": "stopped"
}
Press [Enter] key to continue...
```

- **Restart Support Connection**—Enter command option **3** from the Support Connection commands menu to restart a support connection.

```
Enter option [ 0 - 8 ]: 3
{
  "support_connection_status": "stopped"
}
{
  "support_connection_status": "stopped",
  "active_from": "_",
  "connection": "inactive"
}
Press [Enter] key to continue...
```

- **Support Connection Status**—Enter command option **4** from the Support Connection commands menu to check the status of the support connection.

```
Enter option [ 0 - 8 ]: 4
{
  "support_connection_status": "stopped",
  "active_from": "_",
  "connection": "inactive",
  "node": "_"
}
Press [Enter] key to continue...
```

- **Upload Support Connection File**—Enter command option **5** from the Support Connection commands menu to upload the support connection file.

```

Enter option [ 0 - 8 ]: 5
This will scp a file from the remote server to cop server
Enter remote hostname and path (username@hostname:<filepath>):
auto@10.22.158.92:/home/auto/support_connection.tar

Copying auto@10.22.158.92:/home/auto/support_connection.tar to COP server
FIPS mode initialized
auto@10.22.158.92's password:
Connected to 10.22.158.92.
Fetching /home/auto/isupport_connection.tar to
/var/airwave/appliance/localdisk/support_connection.tar
/home/auto/support_connection.tar
100% 1988 127.9MB/s 00:00
Press [Enter] key to continue...

```

- **Add Support User 'copsupport'**—Enter command option **6** from the Support Connection commands menu to add support connection for user, copsupport.

```

Enter option [ 0 - 8 ]: 6

copsupport user account expires on: Mar 10, 2022 8 10:48:17
-----BEGIN PGP MESSAGE-----

hQIMA0wNcZIn82zzAQ//bj0kS7h2s2wMJWX0JlYcfX0531FjWUa2XqHJ5xKk1OP7
jzvVRw+yFAPky5R0DP1RbXnifLHFGGxZx+x40H592agTehIqrI3L5put4Ewi/uK2
RZg9znigDmTe8jKTNWibrN80VBpTz4QXaArD+4yhAJ80JFhFyFij9fwz1dSCwIUj
oej3JpKtDzVNmrZqANje8HeF62Y6WYWXFFn8VrzBPaasIPk1KQU5MZEKXtZyB3zD
nmi3IyM5rF/+uqFniR7vYlQfYXWysB17ToPKvjbo4tvEt5WWwfXeEg+DczdNkdIz
EpxXwgoby958Le0xCgcV8efbRtGCKxrtks37pPMAGJlVc0qtSJ/74DZc/BHD0WrZ
r4euZjWD/F1Eaxq56nMUHal0jzyLVj5w7DP5Rhj9mnCY1+jsy6ZTIbxfDzembUF
LwTbVdjrBq79Ib+RFShMUwFCv9CPGMjMmCJokYpdL82wksdJyOaWwF4Ac1mA19sU
IuyUtwiXb5bZqwCMON3+mVQhaUqtI0Xu4K5K5E8kSje3QOAYuz0ogS9axGkJQUWx
FpthJUF8ZKwH/tHU07K/So5LhahMcIa+qnCxycUC1X9G5R9EhvpGzEEQrUwy59lp
zCz9w4M0ON/QwNh4IVssnZMTW6WLUv0r9fHEjnJAj/toIsRAVbKSAMgzXKNiwc/S
dQEKZuFfFlPufJW4BWIoAn5PeThJQOrNlKxocI+e3H7eUKMZVof38MACs16DJdy+
RCVr14Wie3Ek/i2jXawz9QhBQza5c6BhdnjWqhQ+U9swEB0REnUbTqlaVhTXNvnW
qMGdxD77nPuKKJuTluTONXJLdsF0KA==
=gWUQ
-----END PGP MESSAGE-----
Press [Enter] key to continue...

```

- **Delete Support User 'copsupport'**—Enter command option **7** from the Support Connection commands menu to delete support connection for the user, copsupport.

```

Enter option [ 0 - 8 ]: 7

Are you sure you want to delete support user 'copsupport' (Y/N)y
Removing user `copsupport' ...
Done.
Support user 'copsupport' deleted successfully.
Press [Enter] key to continue...

```

- **Show contents of copsupport.gpg**—Enter command option **8** from the Support Connection commands menu to show the contents of copsupport.gpg file.

```

Enter option [ 0 - 8 ]: 8

-----BEGIN PGP MESSAGE-----

hQIMA0wNcZIn82zzARAAMuLy9Jure2AHc9/oSKXc00EZ9ZW3506r+mvWFk98zrMz
V1IW4wocFj1KhcpfMnMZ00/nBY0oZIBlCK6CpLnaxFAM+T6NLv7Kroz6wqKfVSt8
pjsrmSh3eyfmMK9F1IkU3u2LglB9xUxMFGqjgvqTqcieqgzWFG5LmK1ALUWsUMoE
4PsWTTdVO+gRGkx17hsa7c9US0iVFaeOQJBdfCnOgP3rfqJzoVhbnL3JEnJSZrYs
R/sBIB47LNyW+E0i5ei8mbZ6S3rlWOCexxqFIIdmyw+S52xrDPcACW/oqcnW31ubh
u6jD4JqSgZqavaf+QZKM80/I0r9N0jAXMExCkOT0TQX3mmg5K5pFgo38j5hnifXTN
O+3rAcjRagWhulNq3+1qpdG0esBCYPGdVs5f2mOej+cNBIsfg+RTemejOa71IeVf
R4/NWpMJa0STYk3/qSybEXjLiYxwwwsJILiqjFE5TVKOCaJhoUVyTH/8t9l4zn+/
qASXne52ocPaa4lxI3SxKKGz159cYcQxlXsJh+CS6RudZaAh8m/WktWi2g2SgGhk
UsnJXttG5ruFnbFQPk1DdUSPnSzy4SzaBnwC0fvwkbQNUhTuYJmgQEQe8M9on5su
swhivSLvWYZTg6EYtLrveMRjh/iMbsDqp/yIsKH21jLQf9QA+tBM8yuPTmgAjPPS
dQH6+RPsislhdjkWnH6ZItIwX1WB1DpZaBjJx/PTTG+7Wi5XerA+8v1liJJ0o6X/
yIdMnqlrGrQALRO/xPAXJUc4pQxXIDgHpWTQd3VWlCX5oS12tPIiUAeq5iDds3vS
5KgqEvsKPIeY9BJyMwa+LX2sx175HQ==
=t1Xn
-----END PGP MESSAGE-----
Press [Enter] key to continue...

```

Collect All Logs

Enter the command option **2** from the Support commands menu to collect the log files into a tar.gz file.

```

Enter option [ 0 - 6 ]: 2
cluster_log_collection...
Collect COP logs along with diagnostic information (Y/N):Y

Collecting all logs from Elasticsearch takes around 1-3 hours.
It can be also collected from "Log Snapshot Operations" by selecting all as cate

                                                                    gory.

Do you want to collect logs from Elasticsearch(Y/N):Y

Collecting COP diagnostic information may take 2-5 minutes

COP diagnostic information dumped and will be zipped to logs as well
Starting Elasticsearch snapshot for all logs...
Logs are being collected from 10.22.156.209 now @Tue Feb 8 11:15:25 UTC 2022
tar: /var/log/snmp: Cannot open: No such file or directory
tar: Error is not recoverable: exiting now
0
kubect1 exec [POD] [COMMAND] is DEPRECATED and will be removed in a future version.
Use kubect1 kubect1 exec [POD] -- [COMMAND] instead.
mv: cannot stat 'cop-156-209.arubathena.com_log_collection_2022-02-08_11-15-25_
UTC.tar.gz': No such file or directory
log_compression...
The following archive(tar.gz) contains all the log information to help debugging the
problem:
cop-156-209.arubathena.com_log_collection_2022-02-08_11-14-18_UTC.tar.gz
Please share it with COP customer support team.
cp: cannot stat '/home/copadmin/log_collection': No such file or directory
Press [Enter] key to continue...

```

Log Snapshot Operations

Enter the command option **3** from the Support commands menu to generate and download snapshots for a category or node, generate logs for various pods, delete snapshots, and download upgrade reports.

```
Enter option [ 0 - 6 ]: 3
1. Generate Snapshots for a Category
2. Generate System Operation Logs
3. Generate Pod Logs
4. Generate Node Snapshot
5. Download Logs/Snapshots
6. Delete Logs/Snapshots
7. Download Upgrade Reports
=====
b. back
m. main menu
0. exit

Enter option [ 0 - 7 ]:
```

- **Generate Snapshots for a Category**—Enter command option **1** from the Log Snapshot Operations commands menu to collect log snapshots of specific categories (kube, nginx, alert, infra, syslog, and system).

```
Enter option [ 0 - 7 ]: 1

Enter a category to create the snapshot [kube nginx alert infra syslog system
all]... alert
Enter the time range for snapshot creation [3h, 1d, 1w, 1M, 3M]... 1w
{ "status": "Accepted", "snapshotId": "alert-snap-7d-1644406412" }
Press [Enter] key to continue...
```

- **Generate System Operation Logs**—Enter command option **2** from the Log Snapshot Operations commands menu to collect system operation logs.

```
Enter option [ 0 - 7 ]: 2

Enter a category to create the snapshot [upgrade backuprestore migration]...
migration
% Total      % Received % Xferd  Average Speed   Time    Time       Time  Current
           Dload  Upload  Total      Spent    Left     Speed
100 105 100 105  0    0  652    0  --:--:--  --:--:--  --:--:--  660
{ "status": "Accepted", "snapshotId": "migration-plain-1m-1644910302", "category":
"migration" }
Press [Enter] key to continue...
```

- **Generate Pod Logs**—Enter command option **3** from the Log Snapshot Operations commands menu to collect pod logs.

```
Enter option [ 0 - 7 ]: 3

Enter a pod name to generate logs... postgres-cluster-0
{ "status": "Accepted", "snapshotId": "postgres-cluster-0-1m-1644410009",
```

```
"category": "pod" }
Press [Enter] key to continue...
```

- **Generate Node Snapshot**—Enter command option **4** from the Log Snapshot Operations commands menu to collect log snapshots for specific nodes.

```
Enter option [ 0 - 7 ]: 4

Enter node to generate logs [10.22.154.57]... 10.22.154.57
{ "status": "Accepted", "snapshotId": "10.22.154.57-snap-1m-1644410130" }
Press [Enter] key to continue...
```

- **Download Logs/Snapshots**—Enter command option **5** from the Log Snapshot Operations commands menu to download the log snapshot file.

```
Enter option [ 0 - 7 ]: 5

List of available snapshots and their status
-----
create time          snapshot name          status
-----
2022-02-08 11:12:35, "all-snap-7d-1644318755": "in_progress"
-----

Select a name to be downloaded (without quotes)...
```

- **Delete Logs/Snapshots**—Enter command option **6** from the Log Snapshot Operations commands menu to delete log snapshots.

```
Enter option [ 0 - 7 ]: 6

List of available snapshots and their status
-----
create time          snapshot name          status
-----
2022-02-08 11:12:35, "all-snap-7d-1644318755": "in_progress"
-----

Select a name to be deleted (without quotes)...
```

- **Download Upgrade Reports**—Enter command option **7** from the Log Snapshot Operations commands menu to download upgrade reports.

```
Enter option [ 0 - 7 ]: 7

Added `minio` successfully.
mc: Configuration written to `/home/copadmin/.mc/config.json`. Please update your
access credentials.
mc: Successfully created `/home/copadmin/.mc/share`.
mc: Initialized share uploads `/home/copadmin/.mc/share/uploads.json` file.
```

```
mc: Initialized share downloads `/home/copadmin/.mc/share/downloads.json` file.
mc: <ERROR> Unable to validate source minio/deployment/
Press [Enter] key to continue...
```

Download COP Setup Logs

Enter the command option **4** from the Support commands menu to download the Aruba Central (on-premises) setup logs.

```
Enter option [ 0 - 6 ]: 4
#####
SCP would be used to copy the logs to a remote host
#####
Enter remote hostname and path (username@hostname:<filepath>):
```

Restart Application

Enter the command option **5** from the Support commands menu to restart applications.

```
Enter option [ 0 - 6 ]: 5
Enter an application name to restart:
```

System Operations Lock Management

Enter the command option **6** from the Support commands menu to manage the system operations lock management.

```
Enter option [ 0 - 6 ]: 6
1. Lock status
2. Release Lock
3. Update Lock Setting
=====
b. back
m. main menu
0. exit

Enter option [ 0 - 3 ]:
```

- **Lock status**—Enter command option **1** from the System Operations Lock Management commands menu to lock the status of the system operation.

```
Enter option [ 0 - 3 ]: 1

No system operation is active currently
Press [Enter] key to continue...
```

- **Release Lock**—Enter command option **2** from the System Operations Lock Management commands menu to release the lock of the system operation.

```
Enter option [ 0 - 3 ]: 2
1. Upgrade
2. Backup
3. Restore
4. Migration
5. Add node
6. Replace node
7. Reboot node
=====
b. back
m. main menu
0. exit

Enter option [ 0 - 7 ]:
```

- **Update Lock Setting**—Enter command option **3** from the System Operations Lock Management commands menu to update the lock settings of the system operation.

```
1. on
2. off
=====
b. back
m. main menu
0. exit

Enter option [ 0 - 2 ]: 1

Do you really want to update system operation lock settings?(y/n):
```

Temporary Root Shell Commands

Enter command option **8** from the main menu to create a temporary user, **cop_shell** with a random password and the system encrypts this password. Provide this key to the customer support. The customer support will then be able to access the Aruba Central (on-premises) SSH using the username, **cop_shell** for 2 days from the date of creation.

Use this option to get access to the Shell for a limited period of time for checking pods, collecting logs, or for executing other CLI commands. This is useful if you want to troubleshoot or debug an issue.

```
Enter option [ 0 - 9 ]: 8
This will reset the previous COP root shell's pwd. proceed? (y/n): Y
No changes made.
Press [Enter] key to continue...
```



After the expiry, you can repeat the same process to extend the temporary root access by another 2 days.

Search Commands

Enter option **8** from the main menu to view a list of available command options.

```
Enter option [ 0 - 9 ]: 8
```

```

Enter the text to get the list of available command options (case insensitive) :
cluster
1) Show -> Configuration -> Network-config/Cluster-info
2) Show -> Cluster Status
Use number to select a command and execute it, enter (stop) to quit: 1

Updated Network Settings
-----
Hostname           : cop-156-209.arubathena.com
IP Address         : 10.22.156.209
Subnet Mask        : 255.255.255.0
Gateway            : 10.22.156.2
DNS                : 10.20.50.10
Secondary DNS      : 10.20.50.25
Timezone           : UTC

COP Cluster Details
-----
Cluster IP         : 10.22.156.192
Cluster FQDN       : copvip-156-192.arubathena.com
Pod CIDR           : 172.16.0.0/16
Service CIDR       : 10.3.0.0/23
Router ID          : 192

Time Zone          : UTC

Cluster Node Count : 1
Cluster Node List  :
NAME               STATUS   ROLES    AGE   VERSION
10.22.156.209     Ready   conductor 35d   v1.18.6

Press [Enter] key to continue...

```

Network Structure

The **Network Structure** page shows tiles view for groups, sites, labels, install manager, and certificates sections. You can click on a tile to navigate to the respective page in Aruba Central.

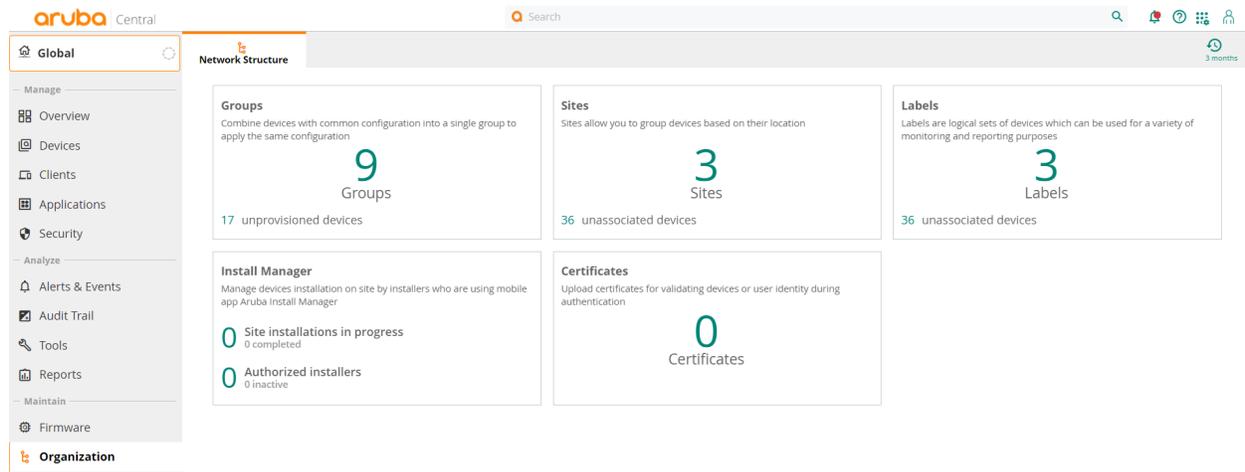
Viewing the Network Structure Page

To view the **Network Structure** page, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
3. Select the **Network Structure** tab.

The **Network Structure** page is displayed.

Figure 14 Network Structure Page



The **Network Structure** page displays tiles view for the following sections:

- **Groups**—Displays the number of groups and number of unprovisioned devices. Click on the tile to navigate to the [Groups](#) page.
- **Sites**—Displays the number of sites and number of unassociated devices. Click on the tile to navigate to the [Managing Sites](#) page.
- **Labels**—Displays the number of labels and number of unassociated devices. Click on the tile to navigate to the [Managing Labels](#) page.
- **Install Manager**—Displays the number of site installations that are either in progress or completed, and the number of authorized installers. Click on the tile to navigate to the Install Manager page.
- **Certificates**—Displays the number of certificates available to upload. Click on the tile to navigate to the [Managing Certificates](#) page.

Aruba Central (on-premises) simplifies the configuration workflow for managed devices by allowing administrators to combine a set of devices into groups. A group in Aruba Central is the primary configuration element that functions as a container for device management, monitoring, and maintenance. Groups enable administrators to manage devices efficiently by using either a UI-based configuration workflow or CLI-based configuration template.

Groups provide the following functions and benefits:

- Ability to provision multiple devices in a single group. For example, a group can consist of multiple AP Virtual Controllers (VCs). These VCs can share common configuration settings and push the configuration updates to member APs in their respective AP clusters. For example, you can apply a common security policy for the devices deployed in a specific geographical location.
- Ability to provision different types of devices in a group. For example, a group can consist of APs and Switches.
- Ability to create a configuration base and add devices as necessary. When you assign a new device to a group, it inherits the configuration that is currently applied to the group.
- Ability to create a clone of an existing group. If you want to build a new group based on an existing group, you can create a clone of the group and customize it as per your network requirements.

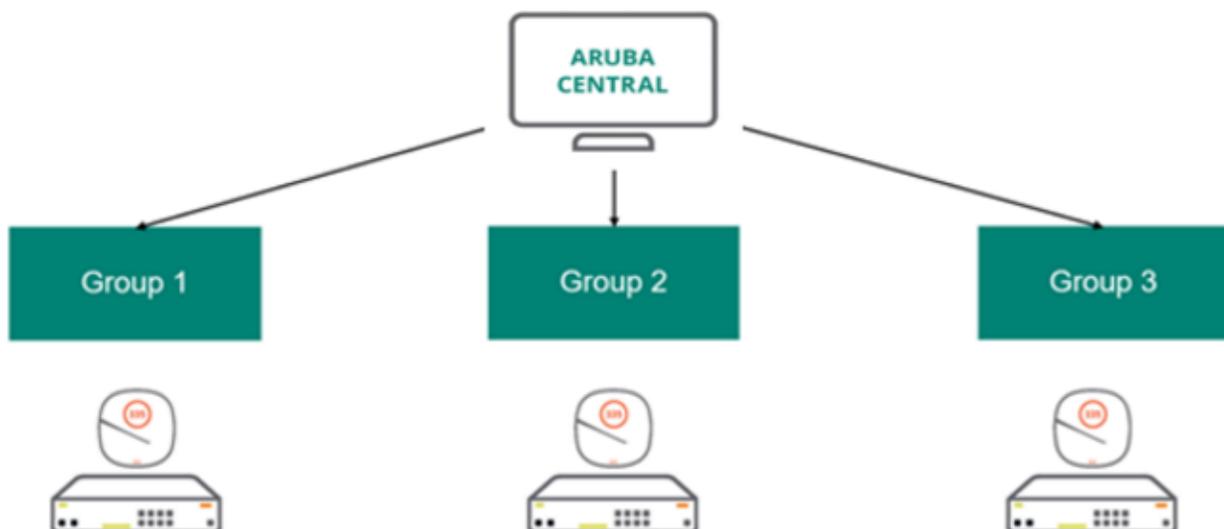


A device can be part of only one group at any given time.

Groups in Aruba Central are mutually exclusive (independent) and do not follow a hierarchical model.

The following figure illustrates a generic group deployment scenario in Aruba Central:

Figure 15 *Group Deployment*



Group Operations

The following list shows the most common tasks performed at a group level:

- Configuration— Add, modify, or delete configuration parameters for devices in a group
- User Management—Control user access to device groups and group operations based the type of user role
- Device Status and Health Monitoring—View device health and performance for devices in a specific group.
- Report Generation—Run reports per group.
- Alerts and Notifications—View and configure notification settings per group.
- Firmware Upgrades—Enforce firmware compliance across all devices in a group.

Group Configuration Modes

Aruba Central allows network administrators to manage device configuration using either UI workflows or configuration templates:

- UI-based configuration method—For device groups that use UI-based workflows, Aruba Central provides a set of UI menu options. You can use these UI menu options to configure devices in a group. You can also secure the UI-based device groups with a password and thus restrict user access.
- Template-based configuration method—For device groups that use a template-based workflow, Aruba Central allows you to manage devices using configuration templates. A device configuration template includes a set of CLI commands and variable definitions that can be applied to all other devices deployed in a group.
- If your site or store has different types of devices, such as the Instant APs, Switches, and Controllers, and you want to manage these devices using different configuration methods, that is, either using the UI or template-based workflows, you can create a single group and define a configuration method to use for each type of device. This allows you to use a single group for both UI and template based configuration and eliminates the need for creating separate groups for each configuration method.
- For example, you can create a group with the name **Group1** and within this group, you can enable template-based configuration method for switches and UI-based configuration method for APs and Controllers. Aruba Central identifies both these groups under a single name (**Group1**). If a device type in the group is marked for template-based configuration method, the group name is prefixed with **TG** prefix is added (**TG Group1**). You can use **Group1** as the group ID for workflows such as user management, monitoring, reports, and audit trail.
- When you add APs, Controllers, and switches to a group, Aruba Central groups these devices based on the configuration method you chose for the device type, and displays relevant workflows when you try to access the respective configuration menu.

For information on how to create a group, see [Creating a Group](#).

Default Groups and Unprovisioned Devices

The **default** group is a system-defined group to which Aruba Central assigns all new devices with factory default configuration. When a new device with factory default configuration connects to Aruba Central, it is automatically added to the **default** group.

If a device has customized configuration and connects to Aruba Central, Aruba Central marks the device as **Unprovisioned**. If you want to preserve the device configuration, you can create a new group and assign this device to the newly created group. If you want to overwrite the configuration, you can move the unprovisioned device to an existing group.



The unprovisioned state does not apply to Aruba Switches as only the factory-default switches can join Aruba Central.

Best Practices and Recommendations

Use the following best practices and recommendations for deploying devices in groups:

- Determine the configuration method (UI or template-based) to use based on your deployment, configuration, and device management requirements.
- If there are multiple sites with similar characteristics—for example, with the same device management and configuration requirements—assign the devices deployed in these sites to a single group.
- Apply device-level or cluster-level configuration changes if necessary.
- Use groups cloning feature if you need to create a group with an existing group configuration settings.
- If the user access to a particular site must be restricted, create separate groups for each site.

Groups

The **Groups** page allows you to create, edit, or delete a group, view the list of groups provisioned in Aruba Central, and assign devices to groups.

This section describes the following topics:

- [Group Persona](#)
- [Creating a Group Persona with ArubaOS8 Architecture](#)
- [Creating a Group](#)
- [Assigning Devices to Groups](#)
- [Creating a New Group by Importing Configuration from a Device](#)
- [Viewing Groups and Associated Devices](#)
- [Cloning a Group](#)
- [Moving Devices between Groups](#)
- [Configuring Device Groups](#)
- [Deleting a Group](#)

Creating a Group

Aruba Central (on-premises) allows you to manage configuration for different types of devices, such as Aruba APs, controllers, and switches in your inventory. These devices can be configured using either UI workflows or configuration templates. You can define your preferred configuration method when creating a group.

After you assign devices to group and when you access configuration containers, Aruba Central (on-premises) automatically displays relevant configuration options based on the configuration method you defined for the device group.

For more information, see [Creating a Group Persona with ArubaOS8 Architecture](#)

Assigning Devices to Groups

To assign a device to a group, in the **Account Home** page, under **Global Settings**, click **Device Inventory**:

1. Select the device that you want to assign to a group.
2. Click **Assign Group**. The **Assign Group** pop-up window opens.
3. Select the group to which you want to assign.
4. Click **Assign Device(s)**.

To assign a device to a group from the **Groups** page:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Groups** tile.
The Groups page is displayed.
4. Expand a group from which you want to move devices to the selected group. For example, expand the **Unprovisioned Devices** group, select the devices, and then click the  **Move devices** icon.
The Move Devices page is displayed.
5. Select the **Destination Group** from the drop-down list.
6. Click **Move**.
The selected devices are moved to the destination group. These devices will adopt the destination group configuration.

Viewing Groups and Associated Devices

To view the groups dashboard:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Groups** tile.
The Groups page is displayed.
The groups table lists all the groups and displays the following information:
 - **Group Name**—Name of the group.
 - **Devices**—Number of devices assigned to a group.
 - **All Connected Devices**—Total number of devices provisioned in Aruba Central (on-premises).
The devices table on right side of the page shows all the devices provisioned in Aruba Central (on-premises).
 - **Unassigned Devices**—Total number of devices that are yet to be assigned. The devices table on the right shows the devices are not assigned any group.
4. To view the devices assigned to a group, select the group from the table on the left. The devices table displays the following information:
 - **Device Name**—Name of the device.
 - **Type**—Type of the device such as AP, Switch, or Controller.

- **Serial Number**—Serial number of the device.
- **MAC Address**—MAC address of the device.

Creating a New Group by Importing Configuration from a Device

You can create a new group by importing configuration from a device. The import configuration is supported only for IAPs with ArubaOS 8 architecture. You can create a new group for IAPs with ArubaOS 8 architecture by importing configuration from an IAP. You can add more devices later by editing the group.

To import configuration from an existing device to a new group, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Groups** tile.
The Groups page is displayed.
4. Expand a group which has IAP devices.
5. Select the IAP with ArubaOS 8 architecture.
6. Click the  **Import Group** icon.
The Import Configuration pop-up window is displayed.
7. Enter a name for the group.
8. Click **Add**.
A group is created with the configuration imported from a device.

Cloning a Group

Cloning a group will clone the same architecture and persona from the source group.

To clone a group, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Groups** tile.
The Groups page is displayed.
4. To create a clone of an existing group, hover over the group in the groups table and click the  **Clone Group** icon.
The Clone Group page is displayed.
5. Enter a name for the cloned group.
6. Click **Clone**.
A new group is created from the source group settings.

When you clone a group, Aruba Central (on-premises) also copies the configuration templates applied to the devices in the group.

Moving Devices between Groups

This feature allows the user to move the Mobility Conductor and all the associated devices like the standby Mobility Conductor, Managed Devices, and access points to a different group. When you move the Mobility Conductor to a new group, the associated devices will automatically move to the same new group. Similarly, when you move the managed device, all the managed devices in that cluster and the corresponding APs will move automatically to the destined group.

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Groups** tile.
The Groups page is displayed.
4. Expand a group from which you want to move devices to the selected group. For example, expand the **Unprovisioned Devices** group, select the devices, and then click the  **Move devices** icon.
The Move Devices page is displayed.
5. Select the **Destination Group** from the drop-down list. Based on the device, the following actions are performed automatically:
 - a. If you have selected a Mobility Conductor to move to a different group, all the associated devices like the standby Mobility Conductor, clusters and access points will automatically move to the destined group.
 - b. If you have selected a managed device to move to a different group, all the managed devices in that cluster and the corresponding APs will move automatically to the destined group.
6. Click **Move**.
The selected devices are moved to the destination group. These devices will adopt the destination group configuration.
7. You can verify the device or group move information by navigating to **Analyze > Audit Trail** page.



The sites and labels page should also display the updated group information.

Configuring Device Groups

For information on provisioning devices in groups, see the following topics:

- [Provisioning Devices Using UI-based Workflows](#)
- [Provisioning Devices Using Configuration Templates](#)

Deleting a Group



When you delete a group, Aruba Central (on-premises) removes all configuration, templates, and variable definitions associated with the group. Before deleting a group, ensure that there are no devices attached to the group.

To delete a group:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Groups** tile.
The Groups page is displayed.
4. From the list of groups, hover over the group in the groups table and click the  **Delete Group** icon.
The Delete Group confirmation window is displayed.
5. Click **Yes** to confirm.
The group is deleted.

Group Persona

A persona of a device represents the role that the device plays in a network deployment. Creating persona for devices helps in customizing configuration workflows, automating parts of configurations, showing the default configuration, showing relevant settings for the device. Persona configuration also helps in customizing the monitoring screens and troubleshooting workflows appropriate for the device.

Creating a Persona

Persona can be created when creating a group. Persona and architecture can be set at the group level. All devices within a group inherit the same persona from the group settings.

While creating a group, the architecture and persona settings of the current group can be marked as preferred settings for adding subsequent groups. For subsequent groups, you can either automatically apply the preferred settings or manually select settings for the new group.

Persona for Access Points

Access Points can have the following persona:

- **Campus/Branch**—In this persona, AP provides WLAN functionality.

Persona for Controllers

Controllers can have the following persona:

- **Branch**—In this persona, controllers provide Aruba Instant OS SD-Branch (LAN + WAN) functionality.

Architecture

The following architecture is supported for creating groups:

- **ArubaOS 8**—Instant AP-based deployment, including 6.x/8.x IAP, IAP-VPN, or 8.x SD-Branch deployments.

Creating a Group Persona with ArubaOS8 Architecture

To manage device configuration using configuration containers in Aruba Central, you can create a group and assign devices. During the group creation, you can assign a device persona and select an architecture for the group.

Adding a Group

To add a group and assign a persona and ArubaOS 8 architecture, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Groups** tile.
The Groups page is displayed.
4. Click (+) **Add Group** on the **Groups** table.
The Add Group page is displayed.
5. Enter a name for the group.
The group name can be a maximum of 32 single byte ASCII characters if you use the UI to create the names. However, if you are using an NB API, the character limit increases to 128. A group name supports all special characters excluding the ">" character. System-defined group names such as "default", "unprovisioned", and "global" are not allowed in group names.



By default, Aruba Central enables the UI-based configuration. The template-based configuration is displayed only when you select devices in the **Add group** page. Use the toggle button to enable the **Configure using templates**.

6. Select device types that will be part of this group. A group can contain following devices:
 - Access points
 - Controllers
 - SwitchesFor detailed device combinations, refer to the **Device Combinations** table.
7. Click **Next**.
By default the ArubaOS 8 architecture is applied for access points and controllers.
8. Select the check box for **Make these the preferred group settings** optionally to save the architecture and persona settings of the current group for subsequent group creations.
9. Click **Add**.
A group with persona configuration is created.



You can also create a group that uses different provisioning methods for switch, IAP, device categories. For example, you can create a group with template-based provisioning method for switches and UI-based provisioning method for Instant APs.

Device Combinations

The following table lists the valid combinations for a group persona with ArubaOS 8 architecture.

Table 28: Device Combinations for a Group Persona

Device Type	Architecture	AP Network Role	Controller Network Role	Switches	Monitoring Only
APs	ArubaOS 8	Campus/Branch	N/A	N/A	N/A
Controllers	ArubaOS 8	N/A	Branch	N/A	N/A
Switches	No architecture	N/A	N/A	<ul style="list-style-type: none"> ■ AOS-CX only ■ AOS-S only ■ Both AOS-CX and AOS-S 	Monitoring only for AOS-S (not applicable for AOS-CX only switch types)
<ul style="list-style-type: none"> ■ APs ■ Controllers 	ArubaOS 8	Campus/Branch	Branch	N/A	N/A
<ul style="list-style-type: none"> ■ APs ■ Switches 	ArubaOS 8	Campus/Branch	N/A	<ul style="list-style-type: none"> ■ AOS-CX only ■ AOS-S only ■ Both AOS-CX and AOS-S 	Monitoring only for AOS-S (not applicable for AOS-CX only switch types)
<ul style="list-style-type: none"> ■ APs ■ Controllers ■ Switch 	ArubaOS 8	Campus/Branch	Branch	<ul style="list-style-type: none"> ■ AOS-CX only ■ AOS-S only ■ Both AOS-CX and AOS-S 	Monitoring only for AOS-S (not applicable for AOS-CX only switch types)

Editing a Group

You can edit a group to add a new device type to the group. The group architecture and persona cannot be changed through group edit. You can mark the settings of an edited group as preferred settings for subsequent group creations.

To edit a group, complete the following steps:

1. From the **Network Operations** app, filter **All Groups**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Groups** tile.
The Groups page is displayed.

4. To edit an existing group, hover over the group in the groups table and click the  **Edit Group** icon.
The Edit Group page is displayed.
5. Add a new device type and its persona.
6. For valid edit operations, refer to the **Editing a Group** table.
7. Select check box for **Make these the preferred group settings** optionally to save the architecture and persona settings of the current group for subsequent group creations.
8. Click **Save**.
The group edit changes are saved.

The following table lists the behavior for various edit operations:

Table 29: Editing a Group

Original State		Action	Edit Group Behaviour
Architecture	Devices and Persona		
ArubaOS 8	AP - Campus/Branch No Controllers	<ul style="list-style-type: none"> ■ Add Controller ■ Add Switches 	Allowed Controller persona - Branch Switch types: AOS-CX only or AOS-S only or Both AOS-CX and AOS-S
ArubaOS 8	No AP Controllers - Branch	<ul style="list-style-type: none"> ■ Add AP ■ Add Switches 	Allowed AP persona - Campus/Branch Switch types: AOS-CX only or AOS-S only or Both AOS-CX and AOS-S
No architecture	No Access Points No Controllers Switches - AOS-CX only or AOS-S only or Both AOS-CX and AOS-S	<ul style="list-style-type: none"> ■ Add AP ■ Add Controllers 	Allowed AP persona - Campus/Branch Controllers persona - Branch

Creating Groups for Switches

You can create a group with switches only in it or you can also add a switch to an existing group containing other devices such as APs and gateways. A switch group will not have any architecture.

Adding a Switch Group

To add a switch group, complete the following steps:

1. From the **Network Operations** app, filter **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Groups** tile.
The Groups page is displayed.
4. Click (+) **Add Group** on the **Groups** table.
The Add Group page is displayed.

5. Enter a name for the group.

The group name can be a maximum of 32 single byte ASCII characters if you use the UI to create the names. However, if you are using an NB API, the character limit increases to 128. A group name supports all special characters excluding the ">" character. System-defined group names such as "default", "unprovisioned", and "global" are not allowed in group names.



By default, Aruba Central enables the UI-based configuration. The template-based configuration is displayed only when you select devices in the **Add group** page. Use the toggle button to enable the **Configure using templates**.

6. From the **Group will contain** section, select the switch check box.
7. Click **Next**.
8. Select the type of switches used in this group:
 - AOS-CX only
 - AOS-S only
 - Both AOS-CX and AOS-S

You can select the 'Monitoring only for AOS-S' option for the AOS-S switches.
9. Select the check box for **Make these the preferred group settings** optionally to save the architecture and persona settings of the current group for subsequent group creations.
10. Click **Add**.

A group for the selected switch type is created.

To add a switch type to an existing group, see [Creating a Group Persona with ArubaOS8 Architecture](#)

Assigning Devices to Groups

In Aruba Central, devices are assigned to groups for configuration, monitoring, and management purposes. A group in Aruba Central is a primary configuration element that acts like a container. In other words, groups are a subset of one or several devices that share common configuration settings. Aruba Central supports assigning devices to groups for the ease of configuration and maintenance. For example, you can create a common group for Branch Gateways or Instant APs that have similar configuration requirements.

Assigning Instant APs to Groups

The Instant AP groups may consist of the configuration elements:

- Instant AP Cluster—Consists of a master Instant AP and a set of slave Instant APs in the same VLAN.
- Virtual Controller—A virtual controller provides an interface for entire cluster. The slave Instant APs and master Instant APs function together to provide a virtual interface.
- Master Instant AP and Slave Instant AP—In a typical Instant AP deployment scenario, the first Instant AP that comes up is elected as the master Instant AP. All other Instant APs joining the cluster function as the slave Instant APs. When a master Instant AP is elected, the slave Instant APs download the configuration changes.

The following table describes the group assignment criteria for Instant APs:

Table 30: Instant AP Group Assignment

APs with Default Configuration	APs with Non-Default Configuration
<p>If an Instant AP with factory default configuration joins Aruba Central, it is automatically assigned to the default group or to an existing group with similar configuration settings.</p> <p>The administrators can perform any of the following actions:</p> <ul style="list-style-type: none">Manually assign them to a pre-provisioned group.Create a new group.	<p>If an Instant AP with non-default or custom configuration joins Aruba Central, it is automatically assigned to an unprovisioned group.</p> <p>The administrators can perform any of the following actions:</p> <ul style="list-style-type: none">Create a new group for the device and preserve device configuration.Move the device to an existing group and override the device configuration.

To manually assign Instant AP(s) to a group, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Groups** tile.
The Groups page is displayed.
4. To view a list of unassigned devices, expand **Unprovisioned Devices**.
A list of unassigned devices is displayed.
5. From the list of devices, select Instant AP(s) to assign.
6. Click the  **Move devices** icon.
The Move Devices page is displayed.
7. Select the **Destination Group** from the drop-down list.
8. Click **Move**.
The selected devices are moved to the destination group. These devices will adopt the destination group configuration.

Assigning Switches to Groups

Aruba Central allows switches to join groups only if the switches are running factory default configuration. Switches with factory default configuration are automatically assigned to the **default** group. Administrators can either move the switch to an existing group or create a new group.

Aruba Central does not support UI-based configuration workflows for Aruba 5400R Switch Series and switch stacks. Aruba recommends that you assign these devices to template groups and provision them using configuration templates.



Aruba Central does not support moving Aruba 5400R Switch Series from the template group to a UI group. If Aruba 5400R Switch Series is pre-assigned to a UI group, the device is moved to an unprovisioned group after it joins Aruba Central.

To manually assign switch(s) to a group, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Groups** tile.
The Groups page is displayed.
4. To view a list of unassigned devices, expand **Unprovisioned Devices**.
A list of unassigned devices is displayed.
5. From the list of devices, select the switch(s) to assign.
6. Click the  **Move devices** icon.
The Move Devices page is displayed.
7. Select the **Destination Group** from the drop-down list.
8. Click **Move**.
The selected devices are moved to the destination group. These devices will adopt the destination group configuration.

Assigning Controllers to Groups

Aruba Central allows controllers to join groups and the controllers with factory default configuration are automatically assigned to the **default** group. Administrators can either move the controller to an existing group or create a new group.

To manually assign controller(s) to a group, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Groups** tile.
The Groups page is displayed.
4. To view a list of unassigned devices, expand **Unprovisioned Devices**.
A list of unassigned devices is displayed.
5. From the list of devices, select the controller(s) to assign.
6. Click the  **Move devices** icon.
The Move Devices page is displayed.
7. Select the **Destination Group** from the drop-down list.
8. Click **Move**.
The selected devices are moved to the destination group. These devices will adopt the destination group configuration.

Provisioning Devices Using UI-based Workflows

This section describes the important points to consider when assigning devices to UI groups:

- [Provisioning APs using UI-based Configuration Method](#)
- [Provisioning Switches Using UI-based Configuration Method](#)

Provisioning APs using UI-based Configuration Method

An AP device group may consist of any of the following:

- **AP Cluster**—Consists of a conductor AP and member APs in the same VLAN.
- **VC**—A virtual controller. VC provides an interface for the entire cluster. The member APs and conductor APs function together to provide a virtual interface.
- **Conductor AP and Member AP**—In a typical AP deployment scenario, the first AP that comes up is elected as the conductor AP. All other APs joining the cluster function as the member APs. When a conductor AP is configured, the member APs download the configuration changes. The conductor AP may change as necessary from one device to another without impacting network performance.

Aruba Central (on-premises) allows configuration operations at the following levels for a device group with APs.

- **Per group configuration**—Aruba Central (on-premises) allows you to maintain unique configuration settings for each group. However, these settings are applied to all devices within that group. For example, all VCs within a group can have common SSID settings.
- **Per VC Configuration**—Any changes that need to be applied at the AP cluster level can be configured on a VC within a group. For example, VCs within a group can have different VLAN configuration for the SSIDs.
- **Per Device Configuration**—Although devices are assigned to a group, the users can maintain device-specific configuration such as radio, power, or uplink settings for an individual AP within a group.

When the APs that are not pre-provisioned to any group join Aruba Central (on-premises), they are assigned to groups based on their current configuration.

Table 31: *Instant AP Provisioning*

APs with Default Configuration	APs with Non-Default Configuration
<p>If an AP with factory default configuration joins Aruba Central (on-premises), it is automatically assigned to the default group or an existing group with similar configuration settings.</p> <p>The administrators can perform any of the following actions:</p> <ul style="list-style-type: none">■ Manually assign them to an existing group.■ Groups.	<p>If an AP with non-default or custom configuration joins Aruba Central (on-premises), it is automatically assigned to an unprovisioned group.</p> <p>The administrators can perform any of the following actions:</p> <ul style="list-style-type: none">■ Groups for the device and preserve device configuration.■ Move the device to an existing group and override the device configuration.

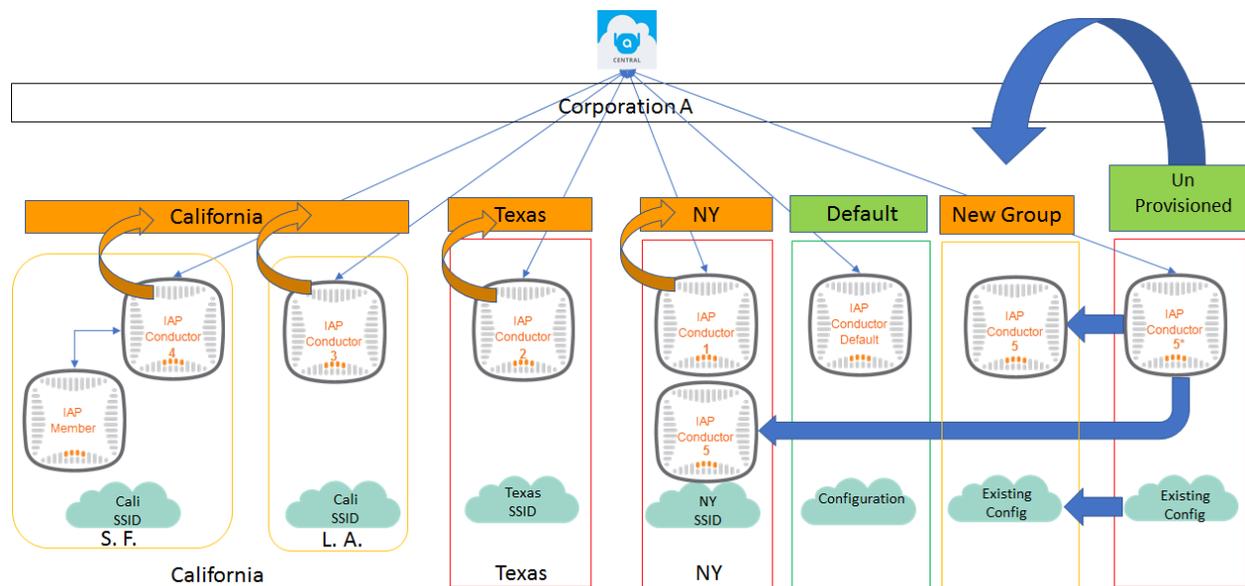


Ensure that the conductor AP and member APs are assigned to the same group. You must convert the member AP to a standalone AP in order to move the member AP to another group independently

In the following illustration, APs from three different geographical locations are grouped under California, Texas, and New York states. Each state has unique SSIDs and can support devices from multiple locations in a state. As shown in [Figure 16](#), the California group has devices from different locations and has the same SSID, while devices in the other states/groups have different SSIDs.

When a device with the factory default configuration connects to Aruba Central (on-premises), it is automatically assigned to the default group. If the device has a custom configuration, it is marked as unprovisioned. If you want to preserve the custom configuration, create a new group for the device. If you want to overwrite the custom configuration, you can assign the device to an existing group.

Figure 16 AP provisioning



Provisioning Switches Using UI-based Configuration Method

Aruba Central (on-premises) allows switches to join UI groups only if the switches are running factory default configuration. Aruba Central (on-premises) assigns switches with a factory default configuration to the **default** group.

The administrators can either move the switch to an existing group or create a new group.

Aruba Central (on-premises) does not support UI-based configuration workflows for Aruba 5400R Switch Series and switch stacks. Aruba recommends that you assign these devices to template groups and provision them using configuration templates



Aruba Central (on-premises) does not support moving Aruba 5400R Switch Series from the template group to a UI group. If Aruba 5400R Switch Series is pre-assigned to a UI group, the device is moved to an unprovisioned group after it joins Aruba Central (on-premises).

Aruba Central (on-premises) allows the following configuration operations at the following levels for switches in a UI group:

- **Per group configuration**— Aruba Central (on-premises) allows you to maintain unique configuration settings for each group. However, these settings are applied to all devices within that group. For example, all switches within a group can have common VLAN settings.

- **Per Device Configuration**—Although the Switches inherit group configuration, the users can maintain device-specific configuration, for example, ports or DHCP pools.

Provisioning Devices Using Configuration Templates

Aruba Central (on-premises) allows you to provision devices using UI-based or template-based configuration method. If you have groups with template-based configuration enabled, you can create a template with a common set of CLI scripts, configuration commands, and variables. Using templates, you can apply CLI-based configuration parameters to multiple devices in a group.

If the template-based configuration method is enabled for a group, the UI configuration wizards for the devices in that group are disabled.

Creating a Group with Template-Based Configuration Method

To create a template group:

1. From the **Network Operations** app, filter **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Groups** tile.
The Groups page is displayed.
4. Click (+) **Add Group** on the **Groups** table.
The Add Group page is displayed.
5. Enter the name of the group.

The group name can be a maximum of 32 single byte ASCII characters if you use the UI to create the names. However, if you are using an NB API, the character limit increases to 128. A group name supports all special characters excluding the ">" character. System-defined group names such as "default", "unprovisioned", and "global" are not allowed in group names.



By default, Aruba Central enables the UI-based configuration. The template-based configuration is displayed only when you select devices in the **Add group** page. Use the toggle button to enable the **Configure using templates**.

6. Select the device type for which you want to create a template group:
 - Access points
 - Controllers
 - Switches
7. Click **Next**.
By default the ArubaOS 8 architecture is applied for access points and controllers.
8. Select the switch type for the group.
9. Select the check box for **Make these the preferred group settings** optionally to save the architecture and persona settings of the current group for subsequent group creations.
10. Click **Add**.



If the group is set as a template group, a configuration template is required for managing device configuration.

Provisioning Devices Using Configuration Templates and Variable Definitions

For information on configuration template, see the following topics:

- [Configuring APs Using Templates](#)
- [Using Configuration Templates for AOS-Switch Management](#)
- [Using Configuration Templates for AOS-CX Switch Management](#)
- [Managing Variable Files](#)

Configuring APs Using Templates

Templates in Aruba Central (on-premises) refer to a set of configuration commands that can be used by the administrators for provisioning devices in a group. Configuration templates enable administrators to apply a set of configuration parameters simultaneously to multiple devices in a group and thus automate access point (AP) deployments.



To minimize configuration errors and troubleshoot device-specific configuration issues, Aruba recommends that the device administrators familiarize themselves with the CLI configuration commands available on Aruba APs.

For template-based provisioning, APs must be assigned to a group with template-based configuration method enabled.

To create a template for the APs in a template group, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the template group under **Groups**.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure APs in a template group are displayed.
4. In the **Templates** table, click **+** to add a new template.
The Add Template window is displayed.
5. Under **Basic Info**, enter the following information:
 - a. **Template Name**—Enter the template name.
 - b. **Model**—Set the model parameter to **ALL**.
 - c. **Version**—Set the model parameter to **ALL**.
6. Under **Template**, add the CLI script content.
7. Check the following guidelines before adding content to the template:
 - Ensure that the command text indentation matches the indentation in the running configuration.
 - The template allows multiple **per-ap-settings** blocks. The template must include the **per-ap-settings %_sys_lan_mac%** variable. The **per-ap-settings** block uses the variables for each AP. The general VC configuration uses variables for conductor AP to generate the final configuration from the provided template. Hence, Aruba recommends that you upload all variables for all devices in a cluster and change values as required for individual AP variables.
 - You can obtain the list of variables for **per-ap-settings** by using the `show amp-audit` command. The following example shows the list of variables for **per-ap-settings**.

```
(Instant AP)# show amp-audit | begin per-ap
per-ap-settings 70:3a:0e:cc:ee:60
hostname EE:60-335-24
rf-zone bj-qa
ip-address 10.65.127.24 255.255.255.0 10.65.127.1 10.65.6.15 ""
swarm-mode standalone
wifi0-mode access
wifi1-mode access
g-channel 6+ 21
a-channel 140 26
uplink-vlan 0
g-external-antenna 0
a-external-antenna 0
ap1x-peap-user peap22 282eaf1077b8d898b91ec41b5da19895
```

The commands in the template are case-sensitive.

IF ELSE ENDIF conditions are supported in the template. If the template text includes the if condition, % sign is required at the beginning and the end of the text. For example, %if guest%.

The following example shows the template text with the IF ELSE ENDIF condition.

```
wlan ssid-profile %ssid_name%
%if disable_ssid=true%
disable-ssid
%endif%
%if ssid_security=wpa2%
opmode wpa2-aes
%else%
opmode opensystem
%endif%
```

Templates also support nesting of the IF ELSE END IF condition blocks.

The following example shows how to nest such blocks:

```
%if condition1=true%
routing-profile
route 10.10.0.0 255.255.255.0 10.10.0.255
%if condition2=true%
routing-profile
route 10.20.0.0 255.255.255.0 10.20.0.255
%else%
routing-profile
route 10.30.0.0 255.255.255.0 10.30.0.255
%endif%
%else%
routing-profile
route 10.40.0.0 255.255.255.0 10.40.0.255
%if condition3=true%
routing-profile
route 10.50.0.0 255.255.255.0 10.50.0.255
%else%
routing-profile
route 10.60.0.0 255.255.255.0 10.60.0.255
%endif%
%endif%
```

For profile configuration CLI text, for example, vlan, interface, access-list, ssid and so on, the first command must start with no white space. The subsequent local commands in given profile must start with at least one initial space (' ') or indented as shown in the following examples:

Example 1

```
vlan 1
  name "vlan1"
  no untagged 1-24
  ip address dhcp-bootp
  exit
```

Example 2

```
%if vlan_id1%
vlan %vlan_id1%
%if vlan_id1=1%
ip address dhcp-bootp
%endif%
no untagged %_sys_vlan_1_untag_command%
exit
%endif%
```

To comment out a line in the template text, use the pound sign (#). Any template text preceded by # is ignored when processing the template.

To allow or restrict APs from joining the Instant Access Point (IAP) cluster, Aruba Central uses the **_sys_allowed_ap_** system-defined variable. Use this variable only when allowed APs configuration is enabled. For example, **_sys_allowed_ap_**: "a_mac, b_mac, c_mac". Use this variable only once in the template.

8. Click **OK**.

Using Configuration Templates for AOS-Switch Management

Templates in Aruba Central (on-premises) refer to a set of configuration commands that can be used by the administrators for provisioning devices in a group. Configuration templates enable administrators to apply a set of configuration parameters simultaneously to multiple switches in a group and thus automate switch deployments.



To minimize configuration errors and troubleshoot device-specific configuration issues, Aruba recommends that the device administrators familiarize themselves with the CLI configuration commands available on AOS-Switch.

For template-based provisioning, switches must be assigned to a template group.

Creating a Group for Template-Based Configuration

Unlike UI groups, template groups have minimal UI options and use the CLI commands to provision a device. Template groups allow you to automate switch deployments. For template-based provisioning, switches must be assigned to a group with template-based configuration method enabled.

To manage devices using configuration templates, you can create a template group and assign devices.

For more information, see [Creating a Group](#) and [Assigning Devices to Groups](#).

Creating a Configuration Template

To create a configuration template for switches:

1. In the **Network Operations** app, set the filter to a template group.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Switches**.
3. Click the **Config** icon.
The tabs to configure switches using templates is displayed.
4. Click the **Templates** tab. The Templates page is displayed.
5. Click **+** to add a new template. The **Add Template** window is displayed.
6. In the **Basic Info** tab, enter a name for the template in the **Template Name** field.
7. In the **Device Type** drop-down, select **Aruba Switch**.
8. Select the switch model and software version. You can specify any of the following combinations:
 - **ALL** for both **Model** and **Version**—To apply the template to all switch models and all supported switch software versions.
 - **ALL** for **Model** and a software version for **Version**—To apply the template to all switch models running the selected software version.
 - **ALL** for **Version** and a switch model for **Model**—To apply the template to a switch model and all software versions supported by the selected switch model.
 - A switch model and a software version—To apply the template to a specific switch model and the software version. The template created for a switch model and a software version takes precedence over the template that is created for all platforms and versions.
9. Select the manufacturing part number of the switch in the **Part Number** drop-down.



NOTE

-
- The **Part Number** drop-down is displayed only if you select a switch model in the **Model** drop-down.
 - If you select a specific switch model and part number, you can apply the template to a standalone switch and not to a stack.
 - If you select **All** in the **Model** drop-down, or if you select a switch model and **All** in the **Part Number** drop-down, you can apply a template to both a standalone switch and stack.
-

10. Click **Next**. The Template tab is displayed.
11. Build a new template or import configuration information from a switch that is already provisioned in the template group.
 - To build a new template, add the switch command information in the **Template** text box. Ensure that the template text adheres to the guidelines listed in the [Important Points to Note](#).
 - To import configuration text from a switch that is already provisioned in the template group:
 - a. Click **Import Configuration As Template**.
 - b. From the search box, select the switch from which you want to import the configuration. The imported configuration is displayed in the **Template** text box.
 - c. If required, modify the configuration parameters. Ensure that the template text adheres to the guidelines listed in the [Important Points to Note](#).



- Importing configuration from an existing device in the template group allows you to quickly create a basic template. However, before applying the template to other switches in the group, ensure that the template text is variabilized as per your deployment requirements. For more information on variable definitions, see [Managing Variable Files](#).
- All switch templates must include a password command to set a password for the device. The template cannot be saved without adding a password command. If the configuration that is pushed from Aruba Central (on-premises) to the device does not contain a password command, the configuration push is aborted for the device and a log is added to the audit trail. For example, if you add the password command in a condition block and the condition evaluates to false, the configuration that is pushed will not contain the password command. For more information, see [Managing Password in Configuration Templates](#).

For more information about using password commands, see the Configuring Username and Password Security chapter in the *ArubaOS-Switch Access Security Guide*.

- d. To view the variables present in the imported configuration template, click **Show Variables List**. The Variables in Template column is displayed.

For more information on variables, see [Managing Variable Files](#).

- e. To download the variables as a CSV or plain text file, click the download icon and select one of the following options:

- **Download .CSV**
- **Download plain text (.txt)**

12. Click **Save**. After you apply the configuration template, switches reboot and reconnect to Aruba Central (on-premises) with the new configuration.

Important Points to Note

Note the following points when adding configuration text to a template:

- The CLI syntax in the switch template must be accurate. Aruba recommends that you validate the configuration syntax on the switch before adding it to the template text.
- Ensure that the command text indentation matches the indentation in the running configuration.
- The commands in the template are case-sensitive.

The following example illustrates the case discrepancies that the users must avoid in templates and variable definitions.

```
trunk E1-E4 trk1 trunk
interface Trk1
  dhcp-snooping trust
  exit

trunk E1-E4 trk1 trunk
switch-interconnect trk1

trunk E5-E6 trk2 trunk
vlan 5
  name "VLAN5"
```

```

untagged Trk2
tagged Trk1
isolate-list Trk1
ip igmp forcedfastleave Trk1
ip igmp blocked Trk1
ip igmp forward Trk1
forbid Trk1

loop-protect Trk2

trunk E1-E4 trk1 trunk
trunk E4-E5 trk2 trunk
spanning-tree Trk1 priority 4
spanning-tree Trk2 admin-edge-port

trunk A2-A4 trk1 trunk
igmp fastlearn Trk1

trunk E4-E5 trk2 trunk
ip source-binding 2 4.5.6.7 b05ada-96a4a0 Trk2

[no] ip source-binding trap OutOfResources

snmp-server mib hpSwitchAuthMIB ..

snmp-server mib hpicfMACsec unsecured-access ..

[no] lldp config <P-PORT-LIST> dot1TlvEnable ..

[no] lldp config <P-PORT-LIST> medTlvEnable ..

no lldp config <P-PORT-LIST> medPortLocation..

[no] lldp config <P-PORT-LIST> dot3TlvEnable ..

[no] lldp config <P-PORT-LIST> basicTlvEnable ..

[no] lldp config <P-PORT-LIST> ipAddrEnable <lldp-ip>

trunk-load-balance L4-based
trunk-load-balance L3-based

```

See also: [Managing Variable Files](#).

Best Practices

Aruba recommends you to follow the below steps to use configuration templates in managing switches:

1. Configure the switch.
2. Add the switch to Aruba Central (on-premises).
3. Create the template, You can use **Import template** option to import an existing template created for switches.
4. Modify the template based on the user requirement. For example, addition or removal of variables.
5. Save the edited template.

Managing Variable Files

Aruba Central (on-premises) allows you to configure multiple devices in bulk using templates. However, in some cases, the configuration parameters may vary per device. To address this, Aruba Central (on-premises)

identifies some customizable CLI parameters as variables and allows you to modify the definitions for these variables as per your requirements.

You can download a sample file with variables for a template group or for the devices deployed in a template group, update the variable definitions, upload the file with the customized definitions, and apply these configuration changes in bulk.

Downloading Sample Variables File

The sample variables file includes a set of sample variables that the users can customize. You can download the sample variables file in the JSON or CSV format.

To download a sample variables file:

1. In the **Network Operations** app, set the filter to one of the template group under **Groups**.
2. Under **Manage**, click **Devices > Switches**.
3. Click the **Config** icon.
4. Click **Variables**.
5. Select one of the following formats to download the sample variables file:
 - JSON—shows the file in JSON format.
 - CSV—Shows the variables in different columns.
6. Click **Download Sample Variables File**. The sample variables file is saved to your local directory.

Modifying a Variable File

The CSV file includes the following columns for which the variable definitions are mandatory:

- **_sys_serial**—For serial number of the device
- **_sys_lan_mac**—For MAC address of the device
- **modified**—To indicate the modification status of the device. The value for this column is set to **N** in the sample variables file. When you edit a variable definition, set the **modified** column to **Y** to allow Aruba Central to parse the modified definition.

Predefined Variables for Aruba Switches

The system defined variables in the sample variables files are indicated with **_sys** prefix.

[Table 32](#) lists the predefined variables for switches.

Table 32: *Predefined Variables Example*

Variable Name	Description	Variable Value
_sys_gateway	Populates gateway IP address.	10.22.159.1
_sys_hostname	Maintains unique host name.	HP-2920-48G-POEP
_sys_ip_address	Indicates the IP address of the device.	10.22.159.201
_sys_module_command	Populates module lines	module 1 type j9729a
_sys_netmask	Netmask of the device.	255.255.255.0

Variable Name	Description	Variable Value
_sys_oobm_command	Represents Out of Band Management (OOBM) block.	oobm ip address dhcp-bootp exit
_sys_snmpv3_engineid	Populates engine ID.	00:00:00:0b:00:00:5c:b9:01:22:4c:00
_sys_stack_command	Represents stack block	stacking member 1 type "J9729A" mac-address 5cb901-224c00 exit
_sys_template_header	Represents the first two lines of the configuration file. Ensure that this variable is the first line in the template.	; J9729A Configuration Editor; Created on release #WB.16.03.0003+ ; Ver #0f:3f.f3.b8.ee.34.79.3c.29.eb.9f.fc.f3.ff.37.ef:91
_sys_use_dhcp	Indicates DHCP status (true or false) of VLAN 1	0
_sys_vlan_1_untag_command	Indicates untagged ports of VLAN 1	1-28,A1-A2
_sys_vlan_1_tag_command	Indicates tagged ports of VLAN 1	28-48



The **_sys_template_header_** and **_sys_snmpv3_engineid** are mandatory variables that must have the values populated, irrespective of their use in the template. If there is no value set for these variables, Aruba Central re-imports the values for these mandatory variables when it processes the running configuration of the device.

Predefined Variables for APs

For APs, the sample variables file includes the **_sys_allowed_ap** variable for which you can specify a value to allow new APs to join the AP cluster.

Important Points to Note

The following conditions apply to the variable files:

- The variable names must be on the left side of condition and its value must be defined on the right side. For example, %if var=100% is supported and %if 100=var% is not supported.
- The < or <= or > or >= operators should have only numeric integer value on the right side. The variables used in these 4 operations are compared as integer after flooring. For example, if any float value is set as %if dpi_value > 2.8%, it is converted as %if dpi_value > 2 for comparison.
- The variable names should not include white space, and the **&** and **%** special characters. The variable names must match regular expression [a-zA-Z0-9_]. If the variables values with **%** are defined, ensure that the variable is surrounded by space. For example, *wlan ssid-profile %ssid_name%*.
- The first character of the variable name must be an alphabet. Numeric values are not accepted.
- The values defined for the variable must not include spaces. If quotes are required, they must be included as part of the variable value. For example, if the intended variable name is *wlan ssid-profile*

"emp ssid", then the recommended format for the syntax is "wlan ssid-profile %ssid_name%" and variable as "ssid_name": "\"emp ssid\"".

- If the configuration text has the percentage sign % in it—for example, "url "/portal/scope.cust-5001098/Splash%20Profile%201/capture"—Aruba Central treats it as a variable when you save the template. To allow the use of percentage % as an escape character, use \ in the variable definition as shown in the following example:

- **Template text**

```
wlan external-captive-portal "Splash Profile 1_#guest#_"
server naw1.cloudguest.central.arubanetworks.com
port 443
url %url%
```

- **Variable**

```
"url": "\"/portal/scope.cust-5001098/Splash%20Profile%201/capture\""
```

- Aruba Central supports adding multiple lines of variables in AP configuration templates. If you want to add multiple lines of variables, you must add the HAS_MULTILINE_VARIABLE directive at the beginning of the template.

- **Example**

```
#define HAS_MULTILINE_VARIABLE 1
%if allowed_aps%
%allowed_aps%
%endif%
```

- **Variable**

```
"allowed_aps": "allowed-ap 24:de:c6:cb:76:4e\n allowed-ap ac:a3:1e:c5:db:d8\n
allowed-ap 84:d4:7e:c4:8f:2c"
```



For APs, you can configure a variable file with a set of values defined for a conductor AP in the network. When the variable file is uploaded, the configuration changes are applied to all AP devices in the cluster.

Examples

The following example shows the contents of a variable file in the JSON format for APs:

```
{
  "CK0036968": {
    "_sys_serial": "CK0036968",
    "ssid": "s1",
    "_sys_lan_mac": "ac:a3:1e:c5:db:7a",
    "vc_name": "test_config_CK0036968",
```

```

"org": "Uber_org_test",
"vc_dns_ip": "22.22.22.22",
"zonename": "Uber_1",
"uplinkvlan": "0",
"swarmmode": "cluster",
"md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
"hostname": "Uber_1"
},
"CJ0219729": {
  "_sys_serial": "CJ0219729",
  "ssid": "s1",
  "_sys_lan_mac": "ac:a3:1e:cb:04:92",
  "vc_name": "test_config_CK0036968",
  "org": "Uber_org_test",
  "vc_dns_ip": "22.22.22.22",
  "zonename": "Uber_1",
  "uplinkvlan": "0",
  "swarmmode": "cluster",
  "hostname": "Uber_2"
},
"CK0112486": {
  "_sys_serial": "CK0112486",
  "ssid": "s1",
  "_sys_lan_mac": "ac:a3:1e:c8:29:76",
  "vc_name": "test_config_CK0036968",
  "org": "Uber_org_test",
  "vc_dns_ip": "22.22.22.22",
  "zonename": "Uber_1",
  "uplinkvlan": "0",
  "swarmmode": "cluster",
  "md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
  "hostname": "Uber_3"
},
"CT0779001": {
  "_sys_serial": "CT0779001",
  "ssid": "s1",
  "_sys_lan_mac": "84:d4:7e:c5:c6:b0",
  "vc_name": "test_config_CK0036968",
  "org": "Uber_org_test",
  "vc_dns_ip": "22.22.22.22",
  "zonename": "Uber_1",
  "uplinkvlan": "0",
  "swarmmode": "cluster",
  "md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
  "hostname": "Uber_4"
},
"CM0640401": {
  "_sys_serial": "CM0640401",
  "ssid": "s1",
  "_sys_lan_mac": "84:d4:7e:c4:8f:2c",
  "vc_name": "test_config_CK0036968",
  "org": "Uber_org_test",
  "vc_dns_ip": "22.22.22.22",
  "zonename": "Uber_1",
  "uplinkvlan": "0",
  "swarmmode": "cluster",
  "md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
  "hostname": "Uber_6"
},
"CK0037015": {
  "_sys_serial": "CK0037015",
  "ssid": "s1",

```

```

_sys_lan_mac": "ac:a3:1e:c5:db:d8",
_vc_name": "test_config_CK0036968",
_org": "Uber_org_test",
_vc_dns_ip": "22.22.22.22",
_zonename": "Uber_1",
_uplinkvlan": "0",
_swarmmode": "cluster",
_md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
_hostname": "Uber_7"
},
"CK0324517": {
_sys_serial": "CK0324517",
_ssid": "s1",
_sys_lan_mac": "f0:5c:19:c0:71:24",
_vc_name": "test_config_CK0036968",
_org": "Uber_org_test",
_vc_dns_ip": "22.22.22.22",
_zonename": "Uber_1",
_uplinkvlan": "0",
_swarmmode": "cluster",
_md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
_hostname": "Uber_8"
}
}
}

```

Figure 17 shows a sample variables file in the CSV format:

Figure 17 Variables File in the CSV Format

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z				
1	_sys_serial	_sys_lan_mac	_sys_modified	_sys_gateway	_sys_host	_sys_ip	_ai	_sys_mod	_sys_netn	_sys_oobr	_sys_snmj	_sys_stacl	_sys_temj	_sys_use	_sys_vlan	_sys_vlan	att_gateway	att_mgmt	att_mgmt	backup_ai	backup_ra	backup_vj	corp_acc	custom_ai	custom_ai	custom_ai	custom_ai		
2	5G62GYW	70:10:6f:9:N	10.22.183	Aruba-Sta	10.22.183	***		255.255.25.2	oobm		00:00:00:0	stacking	;	0	***	1/1-1/24.1	TRUE	10.22.181.	181	***	***	***	***	***	***	***	***	***	
3	CN69HKW	94:18:82:4:N																											
4	CN69HKW	e0:07:1b:c:N	10.22.182	Aruba293	10.22.182	***		255.255.25.***		00:00:00:0	vsf	;	0	***	1/1-1/22.1/24-1/28.2/1-2/23.2/25-2/28														
5																													
6																													
7																													

Uploading Variable Files

To upload a variable file, complete the following steps:

1. Ensure that the **_sys_serial** and **_sys_lan_mac** variables are defined with the serial number and MAC address of the devices, respectively.
2. In the **Network Operations** app, set the filter to one of the template groups under **Groups**.
3. Under **Manage**, click **Devices > Switches**.
4. Click the **Config** icon.
5. Click **Variables**.
6. Click **Upload Variables File** and select the variable file to upload.
7. Click **Open**. The contents of the variable file is displayed in the **Variables** table.
8. To search for a variable, specify a search term and click **Search** icon.
9. To download variable file with device-specific definitions, click the download icon in the **Variables** table

Modifying Variables

To modify variables without downloading a variable file, modifying the variable file, and uploading the customized variable file:

1. In the **Network Operations** app, set the filter to one of the template groups under **Groups**.
2. Under **Manage**, click **Devices > Switches**.
3. Click the **Config** icon.
4. Click **Variables**.
5. Select a device and variable.
6. Modify the value and click **Add to Modifications**.
7. Click **Save**.

Alternatively, to modify a single variable without downloading a variable file, modifying the variable file, and uploading the customized variable file:

1. In the **Network Operations** app, set the filter to one of the template groups under **Groups**.
2. Under **Manage**, click **Devices > Switches**.
3. Click the **Config** icon.
4. Hover over a desired variable and click **Edit**.
5. Modify the value and click **Save**.
6. Click **Save**.

This section describes how to configure WLAN SSIDs, radio profiles, DHCP profiles, VPN routes, security and firewall settings, uplink interfaces, logging servers on access points (APs).

APs offer an enterprise-grade networking solution with a simple setup. The WLAN solution with APs supports simplified deployment, configuration, and management of Wi-Fi networks.

APs run the ArubaOS and Aruba Instant software that virtualizes ArubaMobility Controller capabilities on 802.11 APs and offers a feature-rich enterprise-grade Wi-Fi solution.

In an Instant deployment scenario, only the first AP or the conductor AP that is connected to a provisioning network is configured. All other Instant APs in the same VLAN join the conductor AP inherit the configuration changes. The IAP clusters are configured through a common interface called Virtual Controller. A Virtual Controller represents the combined intelligence of the IAPs in a cluster.

For more information on APs, see the following topics:

- [Configuring APs](#)
- [Monitoring APs](#)

Configuring APs

This section describes how to configure WLAN SSIDs, radio profiles, DHCP profiles, VPN routes, security and firewall settings, uplink interfaces, and logging servers on access points (APs).

For more information on AP configuration, see the following topics:

- [Configuring Device Parameters](#)
- [Configuring Network Profiles on Instant APs](#)
- [Configuring Time-Based Services for Wireless Network Profiles](#)
- [Configuring ARM and RF Parameters on IAPs](#)
- [Configuring IDS Parameters on APs](#)
- [Configuring Authentication and Security Profiles on IAPs](#)
- [Configuring IAPs for VPN Services](#)
- [Configuring DHCP Pools and Client IP Assignment Modes on IAPs](#)
- [Configuring Services](#)
- [Configuring Uplink Interfaces on IAPs](#)
- [Configuring Enterprise Domains](#)
- [Configuring Syslog and TFTP Servers for Logging Events](#)
- [Mapping IAP Certificates](#)

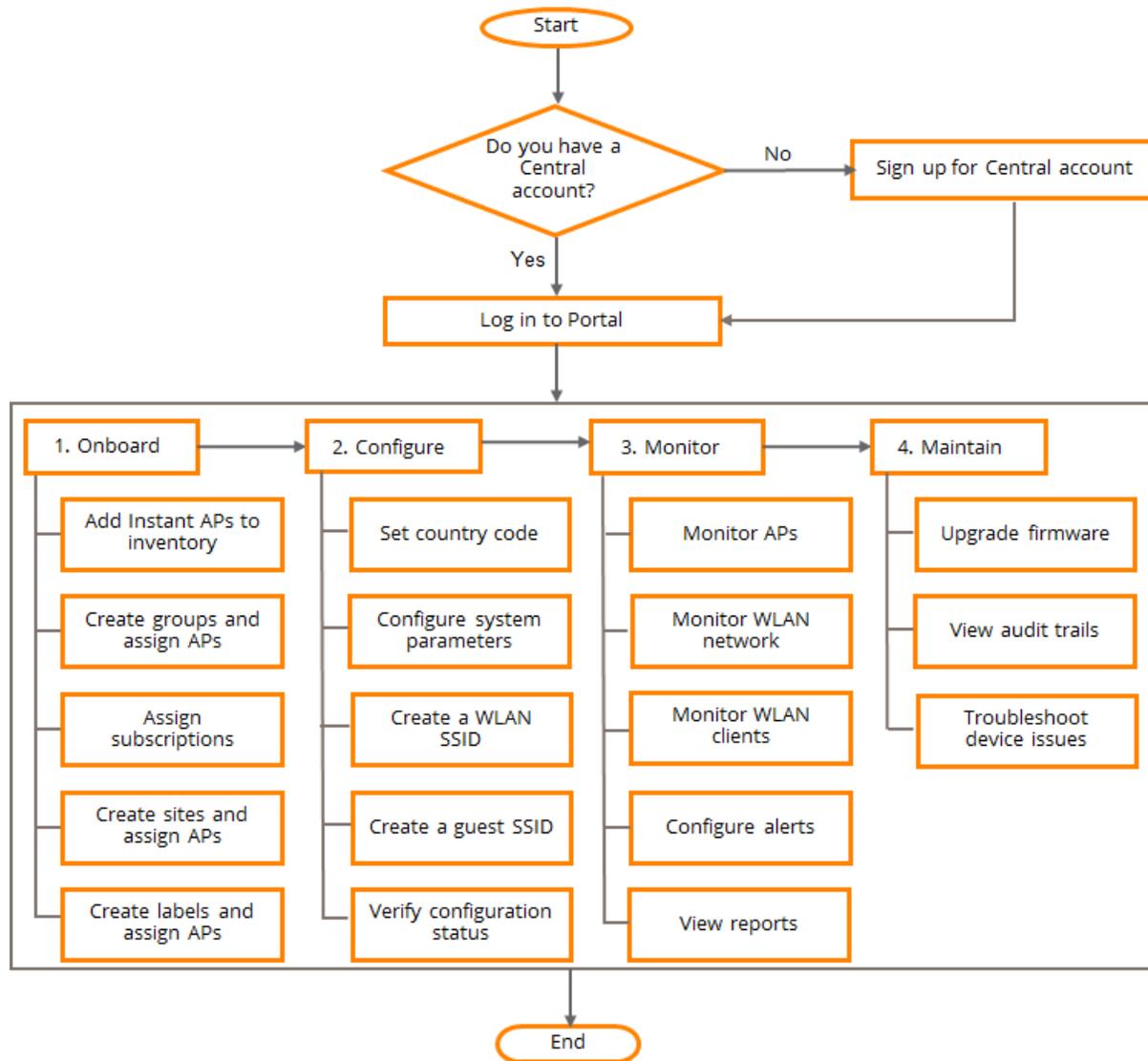
Provisioning APs

The following figure illustrates the procedure for bringing up access points (APs) and configuring a basic WLAN setup. To view a detailed description of the tasks, click the task link in the flowchart.



When you click a task in the flowchart, the linked topic opens in a pop-up window. After you browse through the topic, click outside the pop-up window to return to this page.

Figure 18 *Getting Started—APs*



Configuring APs Using Templates

Templates in Aruba Central (on-premises) refer to a set of configuration commands that can be used by the administrators for provisioning devices in a group. Configuration templates enable administrators to apply a set of configuration parameters simultaneously to multiple devices in a group and thus automate access point (AP) deployments.



To minimize configuration errors and troubleshoot device-specific configuration issues, Aruba recommends that the device administrators familiarize themselves with the CLI configuration commands available on Aruba APs.

For template-based provisioning, APs must be assigned to a group with template-based configuration method enabled.

To create a template for the APs in a template group, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the template group under **Groups**.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure APs in a template group are displayed.
4. In the **Templates** table, click **+** to add a new template.
The Add Template window is displayed.
5. Under **Basic Info**, enter the following information:
 - a. **Template Name**—Enter the template name.
 - b. **Model**—Set the model parameter to **ALL**.
 - c. **Version**—Set the model parameter to **ALL**.
6. Under **Template**, add the CLI script content.
7. Check the following guidelines before adding content to the template:
 - Ensure that the command text indentation matches the indentation in the running configuration.
 - The template allows multiple **per-ap-settings** blocks. The template must include the **per-ap-settings %_sys_lan_mac%** variable. The **per-ap-settings** block uses the variables for each AP. The general VC configuration uses variables for conductor AP to generate the final configuration from the provided template. Hence, Aruba recommends that you upload all variables for all devices in a cluster and change values as required for individual AP variables.
 - You can obtain the list of variables for **per-ap-settings** by using the `show amp-audit` command.
The following example shows the list of variables for **per-ap-settings**.

```
(Instant AP)# show amp-audit | begin per-ap
per-ap-settings 70:3a:0e:cc:ee:60
hostname EE:60-335-24
rf-zone bj-qa
ip-address 10.65.127.24 255.255.255.0 10.65.127.1 10.65.6.15 ""
swarm-mode standalone
wifi0-mode access
wifil-mode access
g-channel 6+ 21
a-channel 140 26
uplink-vlan 0
g-external-antenna 0
a-external-antenna 0
apl-x-peap-user peap22 282eaf1077b8d898b91ec41b5da19895
```

The commands in the template are case-sensitive.

IF ELSE ENDIF conditions are supported in the template. If the template text includes the if condition, % sign is required at the beginning and the end of the text. For example, %if guest%.

The following example shows the template text with the IF ELSE ENDIF condition.

```
wlan ssid-profile %ssid_name%
%if disable_ssid=true%
disable-ssid
%endif%
%if ssid_security=wpa2%
opmode wpa2-aes
%else%
opmode opensystem
%endif%
```

Templates also support nesting of the IF ELSE END IF condition blocks.

The following example shows how to nest such blocks:

```
%if condition1=true%
routing-profile
  route 10.10.0.0 255.255.255.0 10.10.0.255
%if condition2=true%
routing-profile
  route 10.20.0.0 255.255.255.0 10.20.0.255
%else%
routing-profile
  route 10.30.0.0 255.255.255.0 10.30.0.255
%endif%
%else%
routing-profile
  route 10.40.0.0 255.255.255.0 10.40.0.255
%if condition3=true%
routing-profile
  route 10.50.0.0 255.255.255.0 10.50.0.255
%else%
routing-profile
  route 10.60.0.0 255.255.255.0 10.60.0.255
%endif%
%endif%
```

For profile configuration CLI text, for example, vlan, interface, access-list, ssid and so on, the first command must start with no white space. The subsequent local commands in given profile must start with at least one initial space (' ') or indented as shown in the following examples:

Example 1

```
vlan 1
  name "vlan1"
  no untagged 1-24
  ip address dhcp-bootp
  exit
```

Example 2

```
%if vlan_id1%
vlan %vlan_id1%
%if vlan_id1=1%
ip address dhcp-bootp
%endif%
no untagged %_sys_vlan_1_untag_command%
```

```
exit
#endif%
```

To comment out a line in the template text, use the pound sign (#). Any template text preceded by # is ignored when processing the template.

To allow or restrict APs from joining the Instant Access Point (IAP) cluster, Aruba Central uses the **_sys_allowed_ap_** system-defined variable. Use this variable only when allowed APs configuration is enabled. For example, **_sys_allowed_ap: "a_mac, b_mac, c_mac"**. Use this variable only once in the template.

8. Click **OK**.

Viewing APs Configuration Tabs

Aruba Central (on-premises) now constantly displays the default tabs under the **Show Advanced** and **Hide Advanced** options in the **Devices > Access Points** page. When you click the **Show Advanced** or **Hide Advanced** option, a set of default configuration tabs are displayed. The respective default tabs under these two options are still displayed when you navigate out of the page, and visit the same page next time.

Following are the default tabs displayed when you navigate to **Devices > Access Points** page and click the **Config** icon:

- WLANs
- Access Points
- Radios

When you click the **Show Advanced** option, the following tabs are displayed:

- WLANs
- Access Points
- Radios
- Interfaces
- Security
- VPN
- Services
- System
- Configuration Audit

To view the default tabs, click **Hide Advanced**.

Configuring Device Parameters

To configure device parameters on an access point (AP), complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select an AP group in the filter:
 - a. Set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.

- To select an AP in the filter:
 - a. Set the filter to **Global** or a group containing at least one AP.
 - b. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
 - c. Click an AP listed under **Device Name**.
The dashboard context for the AP is displayed.
 - d. Under **Manage**, click **Devices > Access Point**.
- 2. Click the **Config** icon.
The tabs to configure the APs are displayed.
- 3. Click the **Access Points** tab.
The Access Points page is displayed.
- 4. To edit an AP, select an AP in the **Access Points** table, and then click the edit icon.
- 5. Configure the parameters described below:

Table 33: Access Points Configuration Parameters

UI	Parameters	Description
Basic Info	Name	Configures a name for the IAP. For IAPs running 8.7.0.0 or later versions, you can enter up to 128 ASCII or non-ASCII characters. For IAPs running 8.6.0.0 or earlier versions, you can enter up to 32 ASCII or non-ASCII characters.
	AP Zone	Configures the IAP zone. For IAPs running firmware versions 6.5.4.7 or later, and 8.3.0.0 or later, you can configure multiple AP zones by adding zone names as comma separated values. Aruba recommends that you do not configure zones in both SSID and in the Per AP settings of an IAP. If the same zones are configured in SSID and Per AP settings, APs may broadcast the SSIDs, but if the SSIDs and Per AP settings have different zones configured, it may lead to a configuration error. For more information on AP zones, see <i>Aruba Instant User Guide</i> .
	RF Zone	Allows you to create an RF zone for the AP. With RF zone, you can configure different power transmission settings for APs in different zones or sections of a deployment site. For example, you can configure power transmission settings to make Wi-Fi available only for the devices in specific areas of a store. You can also configure separate RF zones for the 2.4 GHz and 5 GHz radio bands for the IAPs in a cluster. For more information, see Configuring Radio Parameters . Aruba recommends that you configure RF zone for either individual AP or for the cluster. Any discrepancy in the RF zone names may lead to configuration errors.
	Swarm Mode	Allows you to set one of the following operation modes: <ul style="list-style-type: none"> ■ Cluster—Allows an IAP to operate in the cluster mode. When an Instant AP operates in the cluster mode, it can form a cluster with other virtual controller Instant APs in the same VLAN. ■ Standalone—Allows an IAP to operate in the standalone mode. When an Instant AP operates in the standalone mode, it cannot join

UI	Parameters	Description
		<p>a cluster of Instant APs even if the Instant AP is in the same VLAN.</p> <ul style="list-style-type: none"> ■ Single-AP—Allows an Instant AP to operate in the single AP mode. It is a type of Standalone AP deployment with additional security rules to prevent local access to AP management. In the single AP mode, the management access of the AP is exclusively reserved to the remote management platform and is facilitated through a secure tunnel between the AP and the management platform. The Local WebUI and SSH access to the AP through the uplink port is disabled. Additionally, the AP will not send or receive management frames such as mobility packets, roaming packets, and hierarchy beacons through the uplink port. <p>NOTE: After changing the AP operation mode, ensure that you reboot the IAP.</p>
	LACP Mode	<p>Allows you to set one of the following LACP modes:</p> <ul style="list-style-type: none"> ■ Active—Allows you to enable the LACP on an IAP. In this mode, both the ethernet ports on the Instant AP forms a static LAG. ■ Passive—Allows you to set the LACP on an IAP in a passive mode. ■ Disabled—Allows you to disable the LACP on an IAP.
	Preferred Conductor	<p>Turn on the toggle switch to provision the IAP as a conductor IAP. After provisioning the IAP as a conductor IAP, ensure that you reboot the AP.</p>
	IP Address for Access Point	<p>Select one of the following options:</p> <ul style="list-style-type: none"> ■ Get IP Address from DHCP server—Allows IP to get an IP address from the DHCP server. By default, the IAPs obtain IP address from a DHCP server. ■ Static—You can also assign a static IP address to the IAP. To specify a static IP address for the IAP, complete the following steps: <ul style="list-style-type: none"> ■ Enter the new IP address for the IAP in the IP Address text-box. ■ Enter the subnet mask of the network in the Netmask text-box. ■ Enter the IP address of the DNS server in the DNS Server text-box. ■ Enter the domain name in the Domain Name text-box. <p>You can configure up to two DNS servers separated by a comma. If the first DNS server goes down, the second DNS server takes control of resolving the domain name.</p>

UI	Parameters	Description
Radio	Dual 5G Mode	Select the Dual 5G Mode check-box to enable the dual 5G mode. In the Dual 5G Mode , the Mode remains as Access and is non-editable. The Dual 5G Mode is only supported on AP-344 and AP-345 running on Aruba InstantOS 8.3.0.0. For more information, see Configuring Dual 5 GHz Radio Bands on an IAP .
	Split Radio	Select the Split Radio check-box to allow the radios of the IAP to operate in the tri-radio mode. The Split Radio is only supported on AP-555 running on Aruba InstantOS 8.5.0.0. For more information, see About Tri-Radio Mode .
	Enable Radio	Select the Enable Radio check-box under 2.4GHz Band and 5 GHz Band to enable and disable the radio.
	Mode	From the Mode drop-down list, select any of the following options: <ul style="list-style-type: none"> ■ Access—In this mode, the IAP serves clients, while also monitoring for rogue IAPs in the background. ■ Monitor—In this mode, the IAP acts as a dedicated monitor, scanning all channels for rogue IAPs and clients. ■ Spectrum—In this mode, the IAP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference, whether from the neighboring IAPs or from non-Wi-Fi devices such as microwaves and cordless phones. <p>To get accurate monitoring details and statistics, it is highly recommended to reboot the IAPs once the IAPs are toggled from the 2.4 or 5 GHz mode to dual 5 GHz radio mode or vice-versa.</p> <p>The access, spectrum, and monitor mode of the radios of an access point is available for Foundation and Advanced licenses for APs.</p>
	Adaptive radio management assigned	You can configure a radio profile on an Instant AP either manually or by configuring the Adaptive radio management assigned option. Adaptive Radio Management (ARM) feature is enabled on Aruba Central by default. It automatically assigns appropriate channel and power settings for the IAPs.
	Administrator assigned	You can also assign an administrator by using the Administrator assigned option and selecting the number of channels in the Channel drop-down list. In the Transmit Power field, enter the signal strength measured in dBm.
	External Antenna	Antenna Gain
Antenna Polarization Type		From the Antenna Polarization Type drop-down list, select any of the following: <ul style="list-style-type: none"> ■ co-polarization—Select this option for the polarization of both the transmitting and receiving antenna to be same. ■ cross-polarization—Select this option for the polarization of both the transmitting and receiving antenna to be different. <p>The integrated antenna of the wireless bridge sends a radio signal that is polarized in a particular direction. The receive sensitivity of the antenna is also higher for radio signals that have the same polarization. To maximize the performance of the wireless link, both antennas must be set to the same polarization direction.</p>

UI	Parameters	Description
Installation Type	Installation Type	<p>Configure the Installation Type of the Instant AP. The Installation Type drop-down consists of the following options:</p> <ul style="list-style-type: none"> ■ Default—Select this option to change the installation type to the default mode. ■ Indoor—Select this option to change the installation type to the indoor mode. ■ Outdoor—Select this option to change the installation type to the outdoor mode. <p>The options in the Installation Type drop-down are listed based on the Instant AP model.</p>
Uplink	Uplink Management VLAN	<p>The uplink traffic on Instant AP is carried out through a management VLAN. However, you can configure a non-native VLAN as an uplink management VLAN. After an Instant AP is provisioned with the uplink management VLAN, all management traffic sent from the Instant AP is tagged to the management VLAN.</p> <p>To configure a non-native uplink VLAN, click Uplink and specify the VLAN in Uplink Management VLAN.</p>
	Eth0 Mode	<p>Allows you to change the Eth0 bridging mode in your wired network. The Eth0 Mode drop-down consists of the following options:</p> <ul style="list-style-type: none"> ■ Uplink—Select this option to change the Eth0 bridging mode to the uplink port. ■ Downlink—Select this option to change the Eth0 bridging mode to the downlink port.
	Eth1 Mode	<p>Allows you to change the Eth1 bridging mode in your wired network. The Eth1 Mode drop-down consists of the following options:</p> <ul style="list-style-type: none"> ■ Default—Select this option to change the Eth1 bridging mode to the default port. ■ Uplink—Select this option to change the Eth1 bridging mode to the uplink port. ■ Downlink—Select this option to change the Eth1 bridging mode to the downlink port.
	USB Port	<p>Enable the USB port if you do not want to use the cellular uplink or 3G/4G modem in your current network setup.</p>
	PEAP User	<p>Create the PEAP user credentials for certificate based authentication. Enter the user name, password, and retype password in the Username, Password, and Retype Password field for creating the PEAP user.</p>

UI	Parameters	Description
Mesh	Mesh enable	Select the Mesh enable check-box to allow mesh access points to form mesh network. The mesh feature ensures reliability and redundancy by allowing the network to continue operating even when an Instant AP is non-functional or if the device fails to connect to the network. For more information, see Aruba Mesh Network and Mesh IAP .
	Clusterless mesh name	Enter the name of mesh access points that do not belong to any cluster. The Clusterless mesh name field is disabled when the Mesh enable option is enabled.
	Clusterless mesh key	Enter the key of the mesh access points that do not belong to any cluster. The Clusterless mesh key field is disabled when the Mesh enable option is enabled.
	Retype	Re-enter the clusterless mesh key. The Retype is disabled when the Mesh enable option is enabled.
	Mesh mobility RSSI threshold	Fast roaming is triggered on a mobility mesh point when the RSSI of the parent is lower than the threshold value. Enter the threshold value either in number between 10—50, high, or low.

6. Click **Save Settings** and then reboot the AP.

Setting Country Code

The initial Wi-Fi setup of an Instant Access Point (IAP) requires you to specify the country code for the country in which the IAP operates. This configuration sets the regulatory domain for the radio frequencies that the IAP uses. The available 20 MHz, 40 MHz, or 80 MHz channels are dependent on the specified country code.

Country Code Configuration in Aruba Central (on-premises) from UI

If you provision a new IAP without the country code, Aruba Central (on-premises) exhibits the following behavior:

Table 34: IAP Provisioned To Aruba Central

Country Code Configured at IAP	Country Code Configured in Group	Behavior
No	Yes	The country code of the group is pushed to the newly added IAP.
No	No	Aruba Central (on-premises) displays the Country Code not set. Config not updated message in Audit Trail . A notification is also displayed at the bottom of the main window to set the country code of the new IAP. To set the country code, perform the following actions: 1. Click Set Country Code now link on the notifications pane. The Set Country Code pop up is displayed.

Country Code Configured at IAP	Country Code Configured in Group	Behavior
		2. In the Device(s) without country code table, click the edit icon. 3. Specify a country code from the Country Code drop-down list. 4. Click Save .



If an IAP has a country code and joins Aruba Central (on-premises) using ZTP configuration, then the country code of the IAP is retained. In this case, Aruba Central (on-premises) will not push the group country code.

Setting Country Code at a Group Level

To set the country code of the IAP at the group level, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The default tabs to configure the virtual controller are displayed.
4. Click **Show Advanced** to view advanced configuration options.
5. Click the **System** tab.
The System details page is displayed.
6. Expand the **General** accordion.
7. In the **Set Country code for group** drop-down list, select the country code for the IAP.
8. Click **Save Settings** and then reboot the IAP.



- By default, the value corresponding to the **Set Country code for group** field is empty. This indicates that any IAP with different country codes can be a part of the group.
- When the **Set Country code for group** field is set, the field cannot revert to the default value. When the country code of the group is changed, the country code of the already connected IAP also will be updated.

Setting Country Code at a Device Level

To set the country code of the IAP at the device level, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. In the **Virtual Controller** column, click the virtual controller link to navigate to the **Access Points > List** view of the virtual controller.



When you click the virtual controller link in the **Virtual Controller** column, the dashboard context for the virtual controller is displayed.

4. Click the **Config** icon.
The default tabs to configure the virtual controller are displayed.
5. Click **Show Advanced** to view advanced configuration options.
6. Click the **System** tab.
The System details page is displayed.
7. Expand the **General** accordion.
8. In the **Virtual Controller** table, select a virtual controller and then click the edit icon.
9. In the **Edit IP Address** window, select the country code from the **Country Code** drop-down list.
10. Click **Ok**.
11. Click **Save Settings** and then reboot the IAP.



-
- By default, the value corresponding to the **Country code** is the country code set at the group level which can be then modified at the device level from the drop-down list. The country code of the IAP will always be the most recently set country code at the group level or device level.
 - If there is a discrepancy in the country code configuration, Aruba Central (on-premises) displays it as an override in the **Configuration Audit** page.
-

Country Code Configuration at Group Level from API

Aruba Central (on-premises) provides an option to set and get the country code at group level through the APIs in **API Gateway**.

To set or get the country code at group level through API, complete the following steps:

1. In the **Account Home** page, click **API Gateway**.
The API Gateway page is displayed.
2. Click the **Authorized Apps & Tokens** tab and generate a token key.



The token key is valid only for 2 hours from the time it was generated.

3. Download and copy the generated token.
4. In the **All Published APIs** window, click the url link listed under the **Documentation** column.
The Central Network Management APIs page is displayed.
5. On the left navigation pane, select **Configuration** from the **URL** drop-down list.
6. Paste the token key in the **Token** field and press enter.
7. Click **NB UI Group Configuration**.
The following options are displayed:
 - **Set country code at group level ([PUT]/configuration/v1/country)**—This API allows to set country code for multiple groups at once. Aruba Central (on-premises) currently allows country codes of up to 50 IAP device groups to be configured simultaneously. To set the country codes of multiple groups, enter the group names and country code as inputs corresponding to the **groups**

and **country** labels respectively in the script { "groups": ["string"], "country": "string" } within the **set_group_config_country_code** text box.

- **Get country code set for group([GET]/configuration/v1/{group}/country)**—This API allows to retrieve the country code set for a specific IAP group. To get the country code information of the IAP group, enter the name of the group for which the country code is being queried corresponding to the **country** label in the script { "country": "string"} within the **group** text box.



The APIs for setting and retrieving country code information are not available for the IAP devices deployed in template groups.

The following are the response messages displayed in the **Set country code at group level** and **Get country code set for group** sections:

Table 35: *Response Messages*

Set country code at group level	Get country code set for group
<ul style="list-style-type: none"> ■ 201 - Successful operation ■ 400 - Bad Request ■ 401 - Unauthorized access, authentication required ■ 403 - Forbidden, do not have write access for group ■ 413 - Request-size limit exceeded ■ 417 - Request-size limit exceeded ■ 429 - API Rate limit exceeded ■ 500 - Internal Server Error ■ 503 - Service unavailable, configuration update in progress 	<ul style="list-style-type: none"> ■ 400 - Bad Request ■ 401 - Unauthorized access authentication required ■ 403 - Forbidden, do not have read access for group ■ 413 - Request-size limit exceeded ■ 417 - Request-size limit exceeded ■ 429 - API Rate limit exceeded ■ 500 - Internal Server Error ■ 503 - Service unavailable, configuration update in progress

For further details on APIs, see <https://app1-apigw.central.arubanetworks.com/swagger/central>.

Configuring Systems

This section describes how to configure the General, Administrator, Time-Based Services, DHCP, Layer-3 Mobility, Enterprise Domains, Logging, SNMP, WISPr, Proxy, and Named VLAN Mapping parameters on an Instant Access Point (IAP).

- [Configuring System Parameters for an AP](#)
- [Configuring Users Accounts for the IAP Management Interface](#)
- [Configuring Mesh for Multiple Radios](#)
- [Configuring Time-Based Services for Wireless Network Profiles](#)
- [Configuring DHCP Pools and Client IP Assignment Modes on IAPs](#)
- [Mobility and Client Management](#)
- [Configuring Enterprise Domains](#)
- [Configuring Syslog and TFTP Servers for Logging Events](#)
- [Configuring SNMP Parameters](#)
- [Supported Authentication Methods](#)
- [Configuring HTTP Proxy on an IAP](#)
- [Configuring VLAN Name and VLAN ID](#)

Configuring VLAN Name and VLAN ID

Aruba Central (on-premises) allows you to map VLAN name to a VLAN ID for the ease of identifying the existing VLANs.

To map a VLAN name to a VLAN ID, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
The System page is displayed.
6. Click the **Named VLAN Mapping** accordion.
7. Click the + icon in the **VLAN Name to VLAN ID Mapping** pane.
The **VLAN Name to VLAN ID Mapping** window is displayed.
8. In the **VLAN Name to VLAN ID Mapping** window, enter the **VLAN Name** and **VLAN ID**.
9. Click **OK**.
The **VLAN Name to VLAN ID Mapping** table in the **Named VLAN Mapping** section lists all the mapped VLAN.

You can find the **Named VLAN Mapping** feature applied in the following fields of corresponding UI pages of Aruba Central (on-premises):

- The **VLAN ID** field in the **VLANs** tab, when for when **Custom** for **Instant AP Assigned** and **Static** for **External DHCP server assigned** is selected during WLAN SSID creation. For more information, see

[Creating a Wireless Network Profile.](#)

- The **VLAN ID** field in the **VLANs** tab, when **Custom** for **Instant AP Assigned** and **Static** for **External DHCP server assigned** is selected during wired port profile creation. For more information, see [Configuring Wired Port Profiles on Instant APs.](#)
- The **Access rules** page in the **Interfaces > Access** tab and the **WLANs > Access** tab, when you add rules for selected roles. Select **VLAN Assignment** as the rule type in the **Access rules** page to find the mapped VLAN name in the **VLAN ID** field.



You can also map VLAN ID to a VLAN name when you customize the **Client VLAN Assignment** configuration in **VLANs** tab during network profile creation. For more information, see [VLANs Parameters.](#)

Points to Remember

- The maximum number of **Named VLAN ID Mapping** allowed in Aruba Central (on-premises) is 32.
- VLAN mapping cannot be performed if the VLAN name does not exist.
- The VLAN mapping record is deleted from the **VLAN Name to VLAN ID Mapping** table when the VLAN name is deleted.
- You can only map a single VLAN id to a VLAN name.
- The VLAN name field is not case-sensitive.

Configuring External Antenna

If the Instant Access Point (IAP) has external antenna connectors, you need to configure the transmit power of the system. The configuration must ensure that the system's EIRP is in compliance with the limit specified by the regulatory authority of the country in which the IAP is deployed. You can also measure or calculate additional attenuation between the device and antenna before configuring the antenna gain. To know, if the IAP device supports external antenna connectors, see the *Installation Guide* that is shipped along with the IAP device.

EIRP and Antenna Gain

The following formula can be used to calculate the EIRP limit related RF power based on selected antennas (Antenna Gain) and feeder (Coaxial Cable Loss):

$$\text{EIRP} = \text{Tx RF Power (dBm)} + \text{GA (dB)} - \text{FL (dB)}$$

The following table describes this formula:

Table 36: *Formula Variable Definitions*

Formula Element	Description
EIRP	Limit specific for each country of deployment.
Tx RF Power	RF power measured at RF connector of the unit.
GA	Antenna gain
FL	Feeder loss

Configuring Antenna Gain

To configure antenna gain for IAPs with external connectors, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select an AP group in the filter:
 - a. Set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
 - To select an AP in the filter:
 - a. Set the filter to **Global** or a group containing at least one AP.
 - b. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
 - c. Click an AP listed under **Device Name**.
The dashboard context for the AP is displayed.
 - d. Under **Manage**, click **Devices > Access Point**.
2. Click the **Config** icon.
The tabs to configure the APs are displayed.
3. Click the **Access Points** tab.
The Access Points page is displayed.
4. To edit an AP, select an AP in the **Access Points** table, and then click the edit icon.
5. Click the **External Antenna** tab.
6. Enter the **Antenna Gain** values in dBi for the **2.4 GHz Antenna Gain** and the **5 GHz Antenna Gain**.
7. From the **Antenna Polarization Type** drop-down list, select any of the following:
 - **co-polarization**—Select this option for the polarization of both the transmitting and receiving antenna to be same.
 - **cross-polarization**—Select this option for the polarization of both the transmitting and receiving antenna to be different.
8. Click **Save Settings**.



After configuring the external antenna parameters, ensure that you reboot the IAP.

Configuring ARM Features

To configure the ARM features, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of access points is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the access points are displayed.

4. Click the **Radios** tab.
The Radios details page is displayed.
5. Under **RF > Adaptive Radio Management (ARM)**, the **Client Control** section displays the following components:
 - **Band Steering Mode**
 - **Airtime Fairness Mode**
 - **ClientMatch**
 - **ClientMatch Calculating Interval**
 - **ClientMatch Neighbor Matching**
 - **ClientMatch Threshold**
 - **ClientMatch Key**
 - **Spectrum Load Balancing Mode**
6. For **Band Steering Mode**, configure the following parameters.

Table 37: *Band Steering Mode Configuration Parameters*

Data pane item	Description
Prefer 5 GHz	Enables band steering in the 5 GHz mode. On selecting this, the IAP steers the client to the 5 GHz band (if the client is 5 GHz capable), but allows the client connection on the 2.4 GHz band if the client persistently attempts for 2.4 GHz association.
Force 5 GHz	Enforces 5 GHz band steering mode on the IAPs.
Balance Bands	Allows the IAP to balance the clients across the two radios to best utilize the available 2.4 GHz bandwidth. This feature takes into account the fact that the 5 GHz band has more channels than the 2.4 GHz band, and that the 5 GHz channels operate in 40 MHz, while the 2.5 GHz band operates in 20 MHz.
Disable	Allows the clients to select the band to use.

7. For **Airtime Fairness Mode**, specify any of the following values.

Table 38: *Airtime Fairness Mode Configuration Parameters*

Data Pane Item	Description
Default Access	Allows access based on client requests. When Airtime Fairness Mode is set to Default Access option, per user and per SSID bandwidth limits are not enforced.
Fair Access	Allocates air time evenly across all the clients.
Preferred Access	Sets a preference where 802.11n clients are assigned more air time than 802.11a/11g. The 802.11a/11g clients get more airtime than 802.11b. The ratio is 16:4:1.

8. For **ClientMatch**, configure the following parameters.

Table 39: Client Match Configuration Parameters

Data Pane Item	Description
Client Match	Turn on the toggle switch to enable the Client Match feature on APs. When enabled, client count is balanced among all the channels in the same band. When Client Match is enabled, ensure that the Scanning option is enabled. For more information, see AP Control Configuration Parameters . NOTE: When Client Match is disabled, channels can be changed even when the clients are active on a BSSID. The Client Match option is disabled by default.
ClientMatch Calculating Interval	Configures a value for the calculating interval of Client Match . The interval is specified in seconds and the default value is 3 seconds. You can specify a value within the range of 1-600.
ClientMatch Neighbor Matching	Configures the calculating interval of Client Match . This number takes into account the least similarity percentage to be considered as in the same virtual RF neighborhood of Client Match . You can specify a percentage value within the range of 20-100. The default value is 60%.
ClientMatch Threshold	Configures a Client Match threshold value. This threshold is the maximum difference allowed in the number of associated clients between channels, radios, or channel + radios. When the client load on an AP reaches or exceeds the threshold in comparison, Client Match is enabled on that AP. You can specify a value within range of 1-20. The default value is 5.
ClientMatch Key	Enables the Client Match feature to work across different standalone IAPs in the same management VLAN. All such standalone IAPs must be set with the same Client Match key. Client Match uses the wired layer 2 protocol to synchronize information exchanged between IAPs. Users have an option to configure the Client Match keys. IAPs verify if the frames that they broadcast contain a common Client Match key. IAPs that receive these frames verify if the sender belongs to the same network or if the sender and receiver both have the same Client Match key. You can specify a value within the range of 1-2147483646.
Spectrum Load Balancing Mode	Enables the Spectrum Load Balancing mode to determine the balancing strategy for Client Match . The following options are available: <ul style="list-style-type: none"> ■ Channel—Balances client count based on each channel. ■ Radio—Balances client count based on each radio. ■ Channel + Radio—Balances client count based on each channel and each radio.

9. Click **Access Point Control**, and configure the following parameters.

Table 40: AP Control Configuration Parameters

Data pane item	Description
Customize Valid Channels	Allows you to select a custom list of valid 20 MHz and 40 MHz channels for 2.4 GHz and 5 GHz bands. By default, the AP uses valid channels as defined by the Country Code (regulatory domain). On selecting Customize Valid Channels , a list of valid channels for both 2.4 GHz and 5 GHz are displayed. The valid channel customization feature is disabled by default.

Data pane item	Description
	The valid channels automatically show in the Static Channel Assignment pane
Min Transmit Power	Allows you to configure a minimum transmission power within a range of 3 to 33 dBm in 3 dBm increments. If the minimum transmission EIRP setting configured on an AP is not supported by the AP model, this value is reduced to the highest supported power setting. The default value for minimum transmit power is 18 dBm.
Max Transmit Power	Allows you to configure the maximum transmission power within a range of 3 to 33 dBm in 3 dBm increments. If the maximum transmission EIRP configured on an AP is not supported by the local regulatory requirements or AP model, the value is reduced to the highest supported power settings.
Client Aware	Allows ARM to control channel assignments for the IAPs with active clients. When the Client Match mode is disabled, an IAP may change to a more optimal channel, which disrupts current client traffic. The Client Aware option is enabled by default.
Scanning	Allows the IAP to dynamically scan all 802.11 channels within its 802.11 regulatory domain at regular intervals. This scanning report includes WLAN coverage, interference, and intrusion detection data. For Client Match configuration, ensure that Scanning is enabled.
Wide Channel Bands	Allows the administrators to configure 40 MHz channels in the 2.4 GHz and 5 GHz bands. 40 MHz channels are two 20 MHz adjacent channels that are bonded together. The 40 MHz channel effectively doubles the frequency bandwidth available for data transmission. For high performance, you can select 5 GHz. If the AP density is low, enable in the 2.4 GHz band.
80 MHz Support	Enables or disables the use of 80 MHz channels on APs. This feature allows ARM to assign 80 MHz channels on APs with 5 GHz radios, which support a very high throughput. This setting is enabled by default. Only the APs that support 802.11ac can be configured with 80 MHz channels.

- Click **Channel Control**, and configure the following parameters.

Table 41: *Channel Control Configuration Parameters*

Data pane item	Description
Backoff Time	Allows you to configure the time within a range of 10 to 3600 seconds, when an IAP backs off after requesting a new channel or power. It can increase the time window of channel interference check, and the time window of power check. The default value for minimum back off time is 240 seconds.
Free Channel Index	Allows you to check the difference in threshold in the channel interference index between the new channel and the existing channel. An IAP only moves to a new channel if the new channel has a lower interference index value than the current channel. This parameter specifies the required difference between the two interference index values before the IAP moves to the new channel. The lower this value, the more likely the IAP moves to the new channel. It has a default value of 25.

Data pane item	Description
Ideal Coverage Index	Allows you to specify the ideal coverage index in the range of 2 to 20, which an IAP tries to achieve on its channel. The denser the IAP deployment, the lower this value should be. It has a default value of 10.
Channel Quality Aware Arm Disable	Allows ARM to ignore the internally calculated channel quality metric and initiates channel changes based on thresholds defined in the profile. ARM chooses the channel based on the calculated interference index value. The option Channel Quality Aware Arm Disable is disabled by default.
Channel Quality Threshold	Allows you to specify the channel quality percentage within a range of 0 to 100, below which ARM initiates a channel change. It has a default value of 70%.
Channel Quality Wait Time	Specifies the time that the channel quality is below the channel quality threshold value to initiate a channel change. It has a range of 1 to 3600 seconds, with a default value of 120 seconds. If current channel quality is below the specified channel quality threshold for this wait time period, ARM initiates a channel change.

- Click **Error Rate**, and configure the following parameters.

Table 42: *Error Rate Configuration Parameters*

Data Pane Item	Description
Error Rate Threshold	Configures the minimum percentage of errors in the channel that triggers a channel change. It has a range of 0 to 100 % with a default value of 70%.
Error Rate Wait Time	Configures the time that the error rate has to be at least equal to the error rate threshold to trigger a channel change. The error rate must be equal to or more than the error rate threshold to trigger a channel change. It has a range of 1 to 3600 seconds, with a default value of 90 seconds.

- Click **Save Settings**.

Configuring Radio Parameters

To configure RF parameters for the 2.4 GHz and 5 GHz radio bands on an Instant Access Point (IAP), complete the following steps:

- In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
- Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
- Click the **Config** icon.
The tabs to configure the APs are displayed.

4. Click the **Radios** tab.
The Radios details page is displayed.
5. Expand the **Radio** accordion in the **RF** dashboard.
6. Under **2.4 GHz band** and **5 GHz band**, configure the following parameters by clicking the **+** sign.

Table 43: Radio Configuration Parameters

Data Pane Item	Description
Zone	<p>Allows you to configure a zone per radio band for IAPs in a cluster. You can also configure an RF zone per IAP.</p> <p>NOTE: Aruba recommends that you configure RF zone for either individual AP or for the cluster. Any discrepancy in the RF zone names may lead to configuration errors.</p>
Legacy Only	<p>Turn on the Legacy Only toggle switch. When enabled, the IAP runs the radio in the non-802.11n mode. This option is disabled by default.</p>
802.11d / 802.11h	<p>Turn on the 802.11d / 802.11h toggle switch. When enabled, the radios advertise their 802.11d (Country Information) and 802.11h (Transmit Power Control) capabilities. This option is disabled by default.</p>
Beacon Interval	<p>Configures the beacon period for the IAP in milliseconds. This indicates how often the 802.11 beacon management frames are transmitted by the AP. You can specify a value within the range of 60–500. The default value is 100 milliseconds.</p>
Interference Immunity Level	<p>Configures the immunity level to improve performance in high-interference environments. The default immunity level is 2.</p> <ul style="list-style-type: none"> ■ Level 0—No ANI adaptation. ■ Level 1—Noise immunity only. This level enables power-based packet detection by controlling the amount of power increase that makes a radio aware that it has received a packet. ■ Level 2—Noise and spur immunity. This level also controls the detection of OFDM packets, and is the default setting for the Noise Immunity feature. ■ Level 3—Level 2 settings and weak OFDM immunity. This level minimizes false detects on the radio due to interference, but may also reduce radio sensitivity. This level is recommended for environments with a high-level of interference related to 2.4 GHz appliances such as cordless phones. ■ Level 4—Level 3 settings, and FIR immunity. At this level, the AP adjusts its sensitivity to in-band power, which can improve performance in environments with high and constant levels of noise interference. ■ Level 5—The AP completely disables PHY error reporting, improving performance by eliminating the time the IAP spends on PHY processing. Increasing the immunity level makes the AP lose a small amount of range.
Channel Switch Announcement Count	<p>Configures the number of channel switching announcements to be sent before switching to a new channel. This allows the associated clients to recover gracefully from a channel change.</p>

Table 43: Radio Configuration Parameters

Data Pane Item	Description
Background Spectrum Monitoring	Turn on the Background Spectrum Monitoring toggle switch. When enabled, the APs in the access mode continue with their normal access service to clients, while performing additional function of monitoring RF interference (from both neighboring APs and non Wi-Fi sources such as, microwaves and cordless phones) on the channel they are currently serving the clients.
Customize ARM Power Range	Configures a minimum (Min Power) and maximum (Max Power) power range value for the 2.4 GHz and 5 GHz band frequencies. The default value is 3 dBm. Unlike the configuration in the ARM profile, the transmit power of all radios in the Radio profile do not share the same configuration.
Enable 11ac	Turn on the Enable 11ac toggle switch. When enabled, VHT is enabled on the 802.11ac devices for the 5 GHz radio band. If VHT is enabled for the 5 GHz radio profile on an IAP, it is automatically enabled for all SSIDs configured on an IAP. By default, VHT is enabled on all SSIDs. NOTE: If you want the 802.11ac IAPs to function as 802.11n IAPs, clear this check box to disable VHT on these devices.
Smart antenna	Turn on the Smart antenna toggle switch to combine an antenna array with a digital signal-processing capability to transmit and receive in an adaptive, spatially sensitive manner.
ARM/WIDS Override	When ARM/WIDS Override is disabled, the Instant AP will always process frames for WIDS. WIDS is an application that detects the attacks on a wireless network or wireless system. purposes even when it is heavily loaded with client traffic. When ARM/WIDS Override is enabled, the Instant AP will stop processing frames for WIDS.

7. Click **Save Settings**.

Configuring Dual 5 GHz Radio Bands on an IAP

Aruba Central (on-premises) provides an option to retrieve the radio numbers of Instant Access Point (IAP) through the APIs. It also provides an option to filter IAP details using radio numbers in the IAP monitoring dashboard.



For regular IAPs with non-dual band, Central automatically assigns **Radio 1** to 2.4 GHz band and **Radio 0** to 5 GHz band respectively.

To retrieve the radio numbers through API, complete the following steps:

1. In the **Account Home** page, click **API Gateway**.
The API Gateway page is displayed.
2. Click the **APIs** tab.



The token key is valid only for 2 hours from the time it was generated.

3. In the **All Published APIs** window, click the url link listed under the **Documentation** column.
The Central Network Management APIs page is displayed.

4. On the left navigation pane, select **Monitoring** from the **URL** drop-down list.
5. Click **API Reference > AP**.

The following APIs allow you to retrieve the radio number for the total number of clients connected:

Table 44: APIs to Get Radio Number in APs

API	Description
[GET]/monitoring/v1/aps/{serial}/neighbouring_clients	Allows you to filter data of neighbouring clients for a specific radio number in a given time period. When there is no radio number entered in the radio_number field, the API filters the data of neighbouring clients for both radio 0 and radio 1. It is mandatory to provide the serial number of the AP to get the data of neighboring clients for a specific radio number.
[GET]/monitoring/v1/aps/rf_summary	Retrieves information on RF summary such as channel utilization and noise floor in positive, errors, drops for a given time period. This API can also be used to filter RF health statistics for a specific radio number in a given time period. When there is no radio number entered in the radio_number field, the API filters the RF health statistics for both radio 0 and radio 1. It is mandatory to provide the serial number of the AP to get the RF health statistics for a specific radio number.
[GET]/monitoring/v1/aps/bandwidth_usage	This API can also be used to filter out bandwidth usage data for a specific radio number in a given time period. When there is no radio number entered in the radio_number field, the API filters the bandwidth usage for both radio 0 and radio 1. It is mandatory to provide the serial number of the AP to get the bandwidth usage for a specific radio number.

6. On the left navigation pane, click **API Reference > Client**.

The following APIs allow you to retrieve the radio number for the total number of clients connected:

Table 45: APIs to Get Radio Number in Connected Clients

API	Description
[GET]/monitoring/v1/clients/count	This API is used to filter out the data for connected clients for a specific radio number of AP in a given time period. When there is no radio number entered in the radio_number field, the API filters the clients count for both radio 0 and radio 1. It is mandatory to provide the serial number of the AP to get the total count of clients for a specific radio number.

For further details on APIs, see <https://app1-apigw.central.arubanetworks.com/swagger/central>.

Support for Dual 5 GHz AP

Aruba Central (on-premises) supports automatic opmode selection for dual 5 GHz AP. When the opmode is set to automatic, AirMatch determines whether to convert a radio in an AP to 5 GHz operation instead of the 2.4 GHz and 5 GHz dual band operation. Automatic is the default dual 5G mode where Airmatch detects what is an optimal mode for the radios – dual band or dual 5G and updates the running opmode without requiring an AP reboot between the mode changes.

Manual setting of dual band and dual 5G is possible and the manual setting overrides the automatic mode and explicitly enables or disables the dual 5G mode. In this scenario, the AP immediately switches to the specified mode without a reboot and AirMatch maintains the specified channel and power assignments in the specified mode.



Automatic mode is not supported on AP-344. By default, AP-344 assumes the automatic mode to be the same as dual 5G disabled and operates in the dual band mode. To switch AP-344 to dual 5G mode, explicitly enable the dual 5G mode.

The following procedure describes how to configure automatic opmode selection for dual 5 GHz AP:

1. In the **Network Operations** app, select one of the following options:
 - To select an AP group in the filter:
 - a. Set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
 - To select an AP in the filter:
 - a. Set the filter to **Global** or a group containing at least one AP.
 - b. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
 - c. Click an AP listed under **Device Name**.
The dashboard context for the AP is displayed.
 - d. Under **Manage**, click **Devices > Access Point**.
2. Click the **Config** icon.
The tabs to configure the APs are displayed.
3. Click the **Access Points** tab.
The Access Points page is displayed.
4. To edit an AP, select an AP in the **Access Points** table, and then click the edit icon.
5. Click the **Radio** tab.
6. Set **Dual 5G Mode** to **Automatic**.
7. Optionally, specify the manual channel by setting **Channel Assignment** to **Manual**.
8. Optionally, specify the transmit power by setting **Transmit Power Assignment** to **Manual**.
9. Click **Save Settings**.

Configuring Intelligent Power Monitoring

The Intelligent Power Monitoring (IPM) feature actively measures the power utilization of an access point (AP) and dynamically adapts to the power resources. IPM allows you to define the features that must be disabled to save power, allowing the APs to operate at a lower power consumption without hampering the performance of the related features. This feature constantly monitors the AP power consumption and adjusts the power saving IPM features within the power budget.

IPM dynamically limits the power requirement of an AP as per the available power resources. IPM applies a sequence of power reduction steps as defined by the priority definition until the AP functions within the power budget. This happens dynamically as IPM constantly monitors the AP power consumption and applies the next power reduction step in the priority list if the AP exceeds the power threshold. To manage

this prioritization, you can create IPM policies to define a set of power reduction steps and associate them with a priority. The IPM policies, when applied to the AP, are based on IPM priorities, where the IPM policy can be configured to disable or reduce certain features in a specific sequence to reduce the AP power consumption below the power budget. IPM priority settings are defined by integer values, where the lower values have the highest priority and are implemented first.



The Intelligent Power Monitoring feature is available only on APs running Aruba Instant OS 8.6.0.3.

To configure Intelligent Power Monitoring, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
The System page is displayed.
6. Click the **IPM** accordion.
7. Select the **IPM Activation** check box to enable IPM.
8. Click the + icon in the **IPM Power Reduction Steps With Priorities** pane.
The **IPM Power Reduction Steps With Priorities** window is displayed.
9. In the **IPM Step Priority** field, enter a value from 1 to 16 to define IPM priority.
10. From the **IPM Step** drop-down list, select a setting as described in the following table:

Table 46: Intelligent Power Monitoring Step Parameters

Parameters	Description
cpu_throttle_25	Reduces CPU frequency to 25% of normal.
cpu_throttle_50	Reduces CPU frequency to 50% of normal.
cpu_throttle_75	Reduces CPU frequency to 75% of normal.
disable_alt_eth	Disables the second Ethernet port.
disable_pse	Disables Power Sourcing Equipment (PSE).
disable_usb	Disables USB.
radio_2ghz_chain_1	Reduces 2 GHz chains to 1x1.
radio_2ghz_chain_2	Reduces 2 GHz chains to 2x2.
radio_2ghz_chain_3	Reduces 2 GHz chains to 3x3.

Parameters	Description
radio_2ghz_power_3dB	Reduces 2 GHz radio power by 3 dB from the maximum value.
radio_2ghz_power_6dB	Reduces 2 GHz radio power by 6 dB from the maximum value.
radio_5ghz_chain_1	Reduces 5 GHz chains to 1x1.
radio_5ghz_chain_2	Reduces 5 GHz chains to 2x2.
radio_5ghz_chain_3	Reduces 5 GHz chains to 3x3.
radio_5ghz_power_3dB	Reduces 5 GHz radio power by 3 dB from the maximum value.
radio_5ghz_power_6dB	Reduces 5 GHz radio power by 6 dB from the maximum value.

11. Click **OK**.

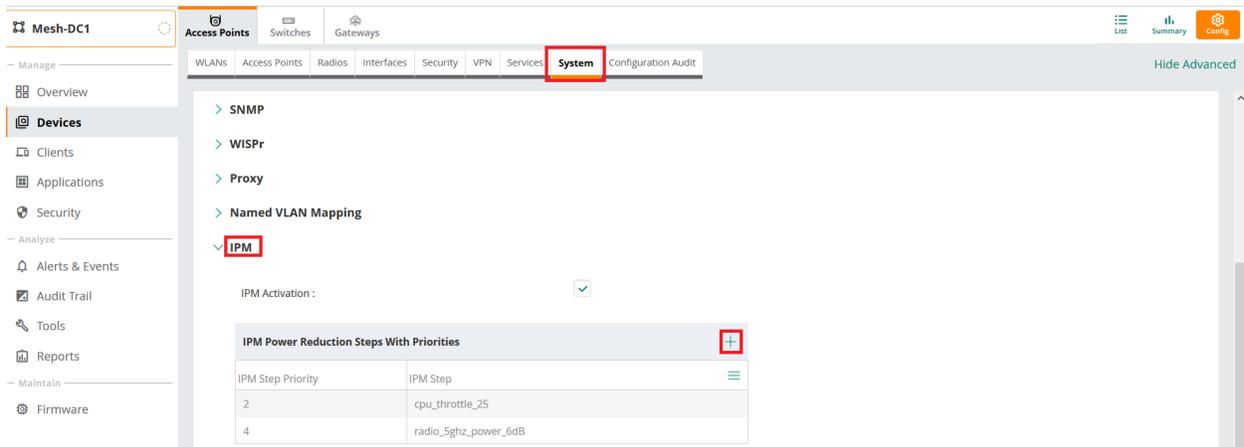
The **IPM Power Reduction Steps With Priorities** table in the **IPM** section lists all the IPM settings.

12. Click **Save Settings**.

13. Reboot the IAP for changes to take effect.

The following figure shows the IPM steps and priorities listed in the **IPM Power Reduction Steps With Priorities** table:

Figure 19 IPM Steps and Priorities



Setting a low-priority value for a power reduction step reduces the power level sooner than setting a high-priority value for a power reduction step. However, if the power reduction step is of the same type but different level, the smallest reduction should be allocated the lowest priority value so that the power reduction step takes place earlier. For example, the **cpu_throttle_25** or **radio_2ghz_power_3dB** parameter should have a lower priority level than the **cpu_throttle_50** or **radio_2ghz_power_6dB**, respectively, so that Intelligent Power Monitoring reduces the CPU throttle or power usage based on the priority list.



Points to Remember

- By default, Intelligent Power Monitoring is disabled.
- When enabled, IPM enables all IAP functionality initially. IPM then proceeds to shut down or restrict functionality if the power usage of the AP goes beyond the power budget of the IAP.

Configuring System Parameters for an AP

To configure system parameters for an access point (AP), complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
The System page is displayed.
6. Click the **General** accordion and configure the following parameters:

Table 47: System Parameters

Data Pane Item	Description
Virtual Controller	<p>This parameter configuration is only applicable for APs that operate in a cluster deployment environment.</p> <p>To configure the virtual controller name and IP address, click edit icon and update the name and IP address. The IP address serves as a static IP address for the multi-AP network. When configured, this IP address is automatically provisioned on a shadow interface on the AP that takes the role of a virtual controller. The AP sends three ARP messages with the static IP address and its MAC address to update the network ARP cache.</p> <ul style="list-style-type: none">■ Name—Name of the virtual controller.■ IP address—IPv4 address configured for the virtual controller. The IPv4 address uses the 0.0.0.0 notation.■ IPv6 address—IPv6 address configured for the virtual controller. You can configure IPv6 address for the virtual controller only if the Configuring System Parameters for an AP feature is enabled. <p>IPv6 is the latest version of IP that is suitable for large-scale IP networks. IPv6 supports a 128-bit address to allow 2¹²⁸, or approximately 3.4×10³⁸ addresses while IPv4 supports only 2³² addresses.</p> <p>The IP address of the IPv6 host is always represented as eight groups of four hexadecimal digits separated by colons. For example <code>2001:0db8:0a0b:12f0:0000:0000:0000:0001</code>. However, the IPv6 notation can be abbreviated to compress one or more groups of zeroes or to compress leading or trailing zeroes; for example <code>2001:db8:a0b:12f0::0:1</code>.</p>
Set Country code for group	<p>To configure a country code for the AP at the group level, select the country code from the Set Country code for group drop-down list. By default, no country code is configured for the AP device groups.</p>

Table 47: System Parameters

Data Pane Item	Description
	When a country code is configured for the group, it takes precedence over the country code setting configured at the device level.
Timezone	To configure a time zone, select a time zone from the Timezone drop-down list. If the selected timezone supports DST, the UI displays the "The selected country observes Daylight Savings Time" message.
Preferred Band	Assign a preferred band by selecting an appropriate option from the Preferred Band drop-down list. Reboot the AP after modifying the radio profile for changes to take effect.
NTP Server	<p>To facilitate communication between various elements in a network, time synchronization between the elements and across the network is critical. Time synchronization allows you to:</p> <ul style="list-style-type: none"> ■ Trace and track security gaps, network usage, and troubleshoot network issues. ■ Validate certificates. ■ Map an event on one network element to a corresponding event on another. ■ Maintain accurate time for billing services and similar. ■ NTP helps obtain the precise time from a server and regulate the local time in each network element. Connectivity to a valid NTP server is required to synchronize the AP clock to set the correct time. If NTP server is not configured in the AP network, an AP reboot may lead to variation in time data. <p>By default, the AP tries to connect to pool.ntp.org to synchronize time. The NTP server can also be provisioned through the DHCP option 42. If the NTP server is configured, it takes precedence over the DHCP option 42 provisioned value. The NTP server provisioned through the DHCP option 42 is used if no server is configured. The default server pool.ntp.org is used if no NTP server is configured or provisioned through DHCP option 42.</p> <p>To configure an NTP server, enter the IP address or the URL of the NTP server and reboot the AP to apply the configuration changes.</p>
Virtual Controller Netmask Virtual Controller Virtual Controller DNS Virtual Controller VLAN	<p>This parameter configuration is only applicable for APs that operate in a cluster deployment environment.</p> <p>The IP configured for the virtual controller can be in the same subnet as AP or can be in a different subnet. Ensure that you configure the virtual controller VLAN, controller, and subnet mask details only if the virtual controller IP is in a different subnet.</p> <p>Ensure that virtual controller VLAN is not the same as native VLAN of the AP.</p>
DHCP Option 82 XML	<p>The DHCP Option 82 XML is not applicable for cloud APs.</p> <p>DHCP Option 82 XML can be customized to cater to the requirements of any ISP using the conductor AP. To facilitate customization using a XML definition, multiple parameters for Circuit ID and Remote ID options of DHCP Option 82 XML are introduced.</p> <p>The XML file is used as the input and is validated against an XSD file in the conductor AP. The format in the XML file is parsed and stored in the DHCP relay which is used to insert Option 82 related values in the DHCP request packets sent from the client to the server.</p> <p>From the drop-down list, select one of the following XML files:</p> <ul style="list-style-type: none"> ■ default_dhcpopt82_1.xml ■ default_dhcpopt82_2.xml <p>For more information, see Configuring DHCP Scopes on IAPs.</p>

Table 47: System Parameters

Data Pane Item	Description
Dynamic CPU Utilization	<p>APs perform various functions such as wired and wireless client connectivity and traffic flows, wireless security, network management, and location tracking. If an AP is overloaded, prioritize the platform resources across different functions. Typically, the APs manage resources automatically in real time. However, under special circumstances, if dynamic resource management needs to be enforced or disabled altogether, the dynamic CPU management feature settings can be modified. To configure dynamic CPU management, select any of the following options from Dynamic CPU Utilization.</p> <ul style="list-style-type: none"> ■ Automatic—When selected, the CPU management is enabled or disabled automatically during run-time. This decision is based on real time load calculations taking into account all different functions that the CPU needs to perform. This is the default and recommended option. ■ Always Disabled in all APs—When selected, this setting disables CPU management on all APs, typically for small networks. This setting protects user experience. ■ Always Enabled in all APs—When selected, the client and network management functions are protected. This setting helps in large networks with high client density.
Auto-Join Mode	<p>When enabled, APs can automatically discover the virtual controller and join the network. The Auto-Join Mode feature is enabled by default.</p>
APs allowed for Auto-Join Mode	<p>Displays the number of APs allowed for Auto-Join Mode.</p> <ul style="list-style-type: none"> ■ Click View Allowed APs to view the details of AP allowed for Auto-Join mode. ■ Click Hide Allowed APs to hide the details of AP allowed for Auto-Join mode. <p>When Auto-Join Mode is enabled, the APs are automatically discovered and are allowed to join the cluster. When the Auto-Join Mode is disabled on the AP, the list of allowed APs on Aruba Central may not be synchronized or up-to-date. In such cases, you can manually add a list of APs that can join the AP cluster in the Aruba Central UI.</p> <p>To manually add the list of allowed AP devices, complete the following steps:</p> <ol style="list-style-type: none"> 1. Under View Allowed APs, click + in the Allowed APs pane. 2. In the Add Allowed AP window, enter the MAC address of the AP in the MAC Address field. 3. Click Save.
Allow IPv6 Management	<p>Enables IPv6 address configuration for the virtual controller. You can configure an IPv6 address for a virtual controller IP only when Allow IPv6 Management feature is enabled.</p>
Uplink switch native VLAN	<p>Allows you to specify a VLAN ID, to prevent the AP from sending tagged frames for clients connected on the SSID that uses the same VLAN as the native VLAN of the switch.</p> <p>By default, the AP considers the native VLAN of the upstream switch, to which it is connected, as the VLAN ID 1.</p>
Terminal Access	<p>When enabled, the users can access the AP CLI through SSH.</p>
Login Session Timeout	<p>Allows you to set a timeout for login session.</p>

Table 47: System Parameters

Data Pane Item	Description
Console Access	When enabled, the users can access AP through the console port.
WebUI Access	If an AP is connected to Aruba Central, you can use this option to disable AP Web UI access and any communication via HTTPS or SSH. If you enable this feature, you can manage the AP only from Aruba Central.
Telnet Server	When enabled, the users can start a Telnet session with the AP CLI.
LED Display	Enables or disables the LED display for all APs in a cluster. The LED display is always enabled during the AP reboot.
Extended SSID	Extended SSID is enabled by default in the factory default settings of APs. This disables mesh in the factory default settings. NOTE: For AP devices that support Aruba InstantOS 8.4.0.0 firmware versions and above, you can configure up to 14 SSIDs. By enabling Extended SSID , you can create up to 16 networks.
Advanced Zone	Turn on the Advanced Zone toggle switch to enable the advance zone. When the advanced-zone feature is enabled and a zone is already configured with 16 SSIDs, ensure to remove the zone from two WLAN SSID profiles if you want to disable extended SSID.
Deny Inter User Bridging	If you have security and traffic management policies defined in upstream devices, you can disable bridging traffic between two clients connected to the same AP on the same VLAN. When inter-user bridging is denied, the clients can connect to the Internet but cannot communicate with each other, and the bridging traffic between the clients is sent to the upstream device to make the forwarding decision. To disable inter-user bridging, turn off the Deny Inter User Bridging toggle switch.
Deny Local Routing	If you have security and traffic management policies defined in upstream devices, you can disable routing traffic between two clients connected to the same AP on different VLANs. When local routing is disabled, the clients can connect to the Internet but cannot communicate with each other, and the routing traffic between the clients is sent to the upstream device to make the forwarding decision. To disable local routing, move the slider to the right.
Dynamic RADIUS Proxy	If your network has separate RADIUS authentication servers (local and centralized servers) for user authentication, you may want to enable Dynamic RADIUS proxy to route traffic to a specific RADIUS server. When Dynamic RADIUS proxy is enabled, the IP address of the virtual controller is used for communication with external RADIUS servers. To enable Dynamic RADIUS Proxy , you must configure an IP address for the Virtual Controller and set it as a NAS client in the RADIUS server profile.
Dynamic TACACS Proxy	If you want to route traffic to different TACACS servers, enable Dynamic TACACS Proxy . When enabled, the AP cluster uses the IP address of the Virtual Controller for communication with external TACACS servers. If an IP address is not configured for the Virtual Controller, the IP address of the bridge interface is used for communication between the AP and TACACS servers. However, if a VPN tunnel exists between the Instant AP and TACACS server, the IP address of the tunnel interface is used.
Cluster Security	This parameter is required to be set only for APs that operate in a cluster deployment environment.

Table 47: System Parameters

Data Pane Item	Description
	<p>Enables or disables the cluster security feature. When enabled, the control plane communication between the AP cluster nodes is secured. The Disallow Non-DTLS Members toggle switch appears. Turn on the toggle switch to allow member APs to join a DTLS enabled cluster.</p> <p>For secure communication between the cluster nodes, the Internet connection must be available, or at least a local NTP server must be configured.</p> <p>After enabling or disabling cluster security, ensure that the configuration is synchronized across all devices in the cluster, and then reboot the cluster.</p> <p>The Disallow Non-DTLS Members feature is only supported in AP devices supporting Aruba InstantOS 8.4.0.0 firmware versions and above.</p>
Low Assurance PKI	<p>Turn on the toggle switch to allow low assurance devices that use non-TPM chip, in the network.</p> <p>To enable the cluster security feature, turn on the Low Assurance PKI toggle switch. For more information on <i>Low Assurance PKI</i>, refer to <i>Cluster Security</i> section in <i>Aruba Instant User Guide</i>.</p> <p>The Low Assurance PKI toggle switch is supported in AP devices running Aruba InstantOS 6.5.3.0 firmware versions and later.</p>
URL Visibility	<p>Turn on the toggle switch to enable URL data logging for client HTTP and HTTPS sessions and allows APs to extract URL information and periodically log them on ALE for DPI and application analytics.</p>

7. Click **Save Settings**.

Enabling 802.1X Authentication on Uplink Ports of an AP

If your network requires all wired devices to authenticate using **PEAP** or **TLS** protocol, you must enable 802.1X authentication type on uplink ports of an access points (AP), so that the APs are granted access only after completing the authentication as a valid client.

To enable 802.1X authentication on uplink ports using **PEAP** or **TLS** protocol, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Interfaces** tab.
The Interfaces page is displayed.
6. Click the **Uplink** accordion.
7. Expand the **AP1X** section.
 - To set **PEAP** based authentication, select **PEAP** in the **AP1X Type** drop-down list.



If you select **PEAP** protocol, ensure that the **PEAP User** is configured on the uplink port by selecting an AP group and navigating to **Uplink** section in the **Access Points** tab.

- To set **TLS** based authentication:
 - a. Select **TLS** in the **AP1X Type** drop-down list.
 - b. Select **User** in the **Certificate Type** drop-down list.
- 8. Select the **Validate Server** check-box to validate the server credentials using server certificate. Ensure that the server certificates for validating server credentials are available in the IAP database.
- 9. Click **Save Settings**.

Configuring HTTP Proxy on an IAP

If your network requires a proxy server for Internet access, ensure that you configure the HTTP proxy on the Instant Access Point (IAP) to download the image from the cloud server. After setting up the HTTP proxy settings, the IAP connects to the Activate server, Aruba Central (on-premises), or OpenDNS server through a secure HTTP connection. You can also exempt certain applications from using the HTTP proxy (configured on an IAP) by providing their host name or IP address under **Exception**. Aruba Central allows the user to configure HTTP proxy on an IAP.

To configure HTTP proxy on IAP through Aruba Central (on-premises), complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
The System page is displayed.
6. Click the **Proxy** accordion and specify the following:
 - a. Enter the HTTP proxy server IP address in the **Server** text-box.
 - b. Enter the port number in the **Port** text-box.
7. Click **Save Settings**.



Aruba Central (on-premises) displays the **Username**, **Password**, and **Retype Password** fields under **System > Proxy** for IAPs running ArubaInstantOS 8.3.0.0. The IAPs running ArubaInstantOS 8.3.0.0 firmware require user credentials for proxy server authentication.

Configuring Network Profiles on Instant APs

This section describes the following procedures:

- [Configuring Wireless Network Profiles on IAPs](#)
- [Configuring Wireless Networks for Guest Users on IAPs](#)
- [Configuring Wired Port Profiles on Instant APs](#)
- [Editing a Wireless Network Profile](#)
- [Deleting a Network Profile](#)

Configuring Wireless Network Profiles on IAPs

You can configure up to 14 SSIDs. By enabling **Extended SSID** in the **System > General** accordion, you can create up to 16 networks.



If more than 16 SSIDs are assigned to a zone and the extended zone option is disabled, an error message is displayed.

This section describes the following topics:

- [Creating a Wireless Network Profile](#)
- [Configuring VLAN Settings for Wireless Network](#)
- [Configuring Security Settings for Wireless Network](#)
- [Configuring ACLs for User Access to a Wireless Network](#)
- [Viewing Wireless SSID Summary](#)

Creating a Wireless Network Profile

To configure WLAN settings, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click the **WLANs** tab.
The WLANs details page is displayed.
5. In the **WLANs** tab, click **+Add SSID**.
The Create a New Network pane is displayed.
6. In **General** tab, enter a name that is used to identify the network in the **Name (SSID)** text-box.

- Under **Advanced Settings**, configure the following parameters:

Table 48: *Advanced Settings Parameters*

Parameter	Description
Broadcast/Multicast	
Broadcast filtering	<p>Select any of the following values:</p> <ul style="list-style-type: none"> ■ All—The IAP drops all broadcast and multicast frames except DHCP and ARP, IGMP group queries, and IPv6 neighbor discovery protocols. ■ ARP—The IAP drops broadcast and multicast frames except DHCP and ARP, IGMP group queries, and IPv6 neighbor discovery protocols. Additionally, it converts ARP requests to unicast and sends frames directly to the associated clients. By default, the IAP is configured to ARP mode. ■ Unicast ARP Only—This option enables Instant AP to convert ARP requests to unicast frames thereby sending them to the associated clients. ■ Disabled—The IAP forwards all the broadcast and multicast traffic is forwarded to the wireless interfaces.
DTIM Interval	<p>The DTIM Interval indicates the DTIM period in beacons, which can be configured for every WLAN SSID profile. The DTIM interval determines how often the IAP delivers the buffered broadcast and multicast frames to the associated clients in the power save mode. Range is 1 to 10 beacons. The default value is 1, which means the client checks for buffered data on the IAP at every beacon. You can also configure a higher DTIM value for power saving.</p>
Multicast Transmission Optimization	<p>Select the check-box if you want the IAP to select the optimal rate for sending broadcast and multicast frames based on the lowest of unicast rates across all associated clients. When this option is enabled, multicast traffic can be sent up to a rate of 24 Mbps. The default rate for sending frames for 2.4 GHz is 1 Mbps and that for 5 GHz is 6 Mbps. This option is disabled by default.</p>
Dynamic Multicast Optimization (DMO)	<p>Select the check-box to allow IAP to convert multicast streams into unicast streams over the wireless link. Enabling DMO enhances the quality and reliability of streaming video, while preserving the bandwidth available to the non-video clients. When you enable DMO on multicast SSID profiles, ensure that the DMO feature is enabled on all SSIDs configured in the same VLAN.</p>
DMO channel utilization threshold	<p>Specify a value to set a threshold for DMO channel utilization. With DMO, the IAP converts multicast streams into unicast streams as long as the channel utilization does not exceed this threshold. The default value is 90% and the maximum threshold value is 100%. When the threshold is reached or exceeds the maximum value, the IAP sends multicast traffic over the wireless link. This option will be enabled only when Dynamic Multicast Optimization is enabled.</p>
Beacon Rate	
2.4 GHz	<p>If the 2.4 GHz band is configured on an AP, specify the transmission rates from the 2.4 GHz drop-down list. By default, the transmission rate is set as 1 Mbps. The minimum transmission rate supported is 1 Mbps and the maximum transmission rate supported is 54 Mbps.</p>

Parameter	Description
5 GHz	If the 5 GHz band is configured on an AP, specify the transmission rates from the 5 GHz drop-down list. By default, the transmission rate is set to 6 Mbps. The minimum transmission rate supported is 6 Mbps and the maximum transmission rate supported is 54 Mbps.
Zone	
Zone	Specify the zone for the SSID. If a zone is configured in the SSID, only the IAP in that zone broadcasts this SSID. If there are no IAPs in the zone, SSID is broadcast. If the IAP cluster has devices running IAP firmware versions 6.5.4.7 or later, and 8.3.0.0 or later, you can configure multiple AP zones by adding zone names as comma separated values. Aruba recommends that you do not configure zones in both SSID and in the device specific settings of an IAP. If the same zones are configured in SSID and Per AP settings, APs may broadcast the SSIDs, but if the SSIDs and Per AP settings have different zones configured, it may lead to a configuration error. For more information on AP zones, see <i>Aruba Instant User Guide</i> .
Bandwidth Control	
Airtime	Select this to specify an aggregate amount of airtime that all clients in this network can use for sending and receiving data. Specify the airtime percentage.
Downstream	Enter the downstream rates within a range of 1 to 65,535 Kbps for the SSID users. If the assignment is specific for each user, select the Per User check-box. The bandwidth limit set in this method is implemented at the device level and not cluster level.
Upstream	Enter the upstream rates within a range of 1 to 65,535 Kbps for the SSID users. If the assignment is specific for each user, select the Per user check-box. The bandwidth limit set in this method is implemented at the device level and not cluster level.
Each Radio	Select this to specify an aggregate amount of throughput that each radio is allowed to provide for the connected clients. The value ranges from 1 through 65535.
Enable 11n	When this option is selected, there is no disabling of High-Throughput (HT) on 802.11n devices for the 5 GHz radio band. If HT is enabled for the 5 GHz radio profile on an IAP, it is automatically enabled for all SSIDs configured on an IAP. By default, HT is enabled on all SSIDs. If you want the 802.11ac IAPs to function as 802.11n IAPs, clear this check-box to disable VHT on these devices.
Enable 11ac	When this option is selected, VHT is enabled on the 802.11ac devices for the 5 GHz radio band. If VHT is enabled for the 5 GHz radio profile on an IAP, it is automatically enabled for all SSIDs configured on an IAP. By default, VHT is enabled on all SSIDs. If you want the 802.11ac IAPs to function as 802.11n IAPs, clear this check-box to disable VHT on these devices.
Enable 11ax	When this option is selected, VHT is enabled on the 802.11ax devices. If VHT is enabled for a radio profile on an IAP, it is automatically enabled for all SSIDs configured on an IAP. By default, VHT is enabled on all SSIDs.
WiFi Multimedia	

Parameter	Description
Background Wifi Multimedia Share	Allocates bandwidth for background traffic such as file downloads or print jobs. Specify the appropriate DSCP mapping values within a range of 0–63 for the background traffic in the corresponding DSCP mapping text-box. Enter up to 8 values with no white space and no duplicate single DSCP mapping value.
Best Effort Wifi Multimedia Share	Allocates bandwidth or best effort traffic such as traffic from legacy devices or traffic from applications or devices that do not support QoS. Specify the appropriate DSCP mapping values within a range of 0–63 for the best effort traffic in the corresponding DSCP mapping text-box.
Video Wifi Multimedia Share	Allocates bandwidth for video traffic generated from video streaming. Specify the appropriate DSCP mapping values within a range of 0–63 for the video traffic in the corresponding DSCP mapping text-box.
Voice Wifi Multimedia Share	Allocates bandwidth for voice traffic generated from the incoming and outgoing voice communication. Specify the appropriate DSCP mapping values within a range of 0–63 for the voice traffic in the corresponding DSCP mapping text-box. In a non-WMM or hybrid environment, where some clients are not WMM-capable, you can allocate higher values for Best Effort Wifi Multimedia Share and Voice Wifi Multimedia Share to allocate a higher bandwidth to clients transmitting best effort and voice traffic.
Traffic Specification (TSPEC)	Select this check-box to set if you want the TSPEC for the wireless network. The term TSPEC is used in wireless networks supporting the IEEE 802.11e Quality of Service standard. It defines a series of parameters, characteristics and Quality of Service expectations of a traffic flow.
TSPEC Bandwidth	Enter the bandwidth for the TSPEC.
Spectralink Voice Protocol (SVP)	Select this check-box to opt for SVP protocol.
WiFi Multimedia Power Save (U-APSD)	Select this check-box to enable WiFi Multimedia Power Save (U-APSD). The U-APSD is a power saving mechanism that is an optional part of the IEEE amendment 802.11e, QoS.
Miscellaneous	
Band	Select a value to specify the band at which the network transmits radio signals in the Band drop-down list. You can set the band to 2.4 GHz , 5 GHz , or All . The All option is selected by default.
Content Filtering	Select this check-box to route all DNS requests for the non-corporate domains to OpenDNS on this network.
Primary Usage	Based on the type of network profile, select one of the following options:

Parameter	Description
	<p>Mixed Traffic—Select this option to create an employee or guest network profile. The employee network is used by the employees in an organization and it supports passphrase-based or 802.1X-based authentication methods. Employees can access the protected data of an enterprise through the employee network after successful authentication. The guest network is created for guests, visitors, contractors, and any non-employee users who use the enterprise Wi-Fi network. The VC assigns the IP address for the guest clients. Captive portal or passphrase-based authentication methods can be set for this wireless network. Typically, a guest network is an unencrypted network. However, you can specify the encryption settings when configuring a guest network.</p> <p>Voice Only—Select this option to configure a network profile for devices that provide only voice services such as handsets or applications that require voice traffic prioritization.</p> <p>When a client is associated with the voice network, all data traffic is marked and placed into the high priority queue in QoS.</p>
Inactivity timeout	Specify an interval for session timeout. If a client session is inactive for the specified duration, the session expires and the users are required to log in again. You can specify a value within the range of 60–3600 seconds. The default value is 1000 seconds.
Hide SSID	Select this check-box if you do not want the SSID to be visible to users.
Disable Network	Select this check-box if you want to disable the SSID. When selected, the SSID is disabled, but is not removed from the network. By default, all SSIDs are enabled.
Max clients threshold	Specify the maximum number of clients that can be configured for each BSSID on a WLAN. You can specify a value within the range of 0–255. The default value is 64.
Local Probe Request Threshold	<p>Select either automatic or manual to set the Local Probe Request Threshold.</p> <p>automatic: The local probe request threshold value changes to the recommended value provided by the AI insights to improve the performance for the indoor Wi-Fi clients. Threshold values are evaluated weekly, and new recommendations will be updated automatically. To revert the applied AI insight recommended values, select manual and specify the threshold value.</p> <p>manual: Specify a threshold value to limit the number of incoming probe requests. When a client sends a broadcast probe request frame to search for all available SSIDs, this option controls system response for this network profile and ignores probe requests, if required.</p>
Min RSSI for auth request	<p>Select either automatic or manual to set the minimum RSSI for authentication request.</p> <p>automatic: The minimum RSSI for authentication request value changes to the recommended value provided by the AI insights to improve the performance for the indoor Wi-Fi clients. Threshold values are evaluated weekly, and new recommendations will be updated automatically. To revert the applied AI insight recommended values, select manual and specify the threshold value.</p> <p>manual: Enter the minimum RSSI threshold for authentication requests. You can specify an RSSI value within the range of 0–100 dB.</p>
Deauth inactive clients	Select this option to allow the IAP to send a de-authentication frame to the inactive client and the clear client entry.
Can be used without uplink	Select this check-box if you do not want the SSID profile to use the uplink.

Parameter	Description
Deny inter user bridging	Disables bridging traffic between two clients connected to the same SSID on the same VLAN. When this option is enabled, the clients can connect to the Internet, but cannot communicate with each other, and the bridging traffic between the clients is sent to the upstream device to make the forwarding decision.
Enable SSID when	Select an option from the drop-down list and specify the time period.
Disable SSID when	Select an option from the drop-down list and specify the time period.
Deny Intra VLAN Traffic	Disables intra VLAN traffic to enable the client isolation and disable all peer-to-peer communication. Client isolation disables inter-client communication by allowing only client to controller traffic from clients to flow in the network. All other traffic from the client that is not destined to the controller or configured servers will not be forwarded by the Instant AP. This feature enhances the security of the network and protects it from vulnerabilities. For more information, see Configuring Client Isolation .
Management Frame Protection	Turn on the Management Frames Protection toggle switch to provide high network security by maintaining data confidentiality of management frames. The Management Frame Protection (MFP) establishes encryption keys between the client and Instant AP using 802.11i framework. For more information, see Management Frames Protection .
Fine Timing Measurement (802.11mc) Responder Mode	Turn on the toggle switch to enable the fine timing measurement (802.11mc) responder mode.
Time Range Profiles	
Time Range Profiles	Ensure that the NTP server connection is active. Select a time range profile from the Time Range Profiles list and apply a status form the drop-down list. Click + New Time Range Profile to create a new time range profile. For more information, see Configuring Time-Based Services for Wireless Network Profiles .

Configuring VLAN Settings for Wireless Network

To configure VLANs settings for an SSID, complete the following steps:

1. In the **VLANs** tab, select any of the following options for **Client IP Assignment: Instant AP assigned**—When selected, the client obtains the IP address from the VC. **External DHCP server assigned**—When selected, the client obtains the IP address from the network.

- Based on the type of client IP assignment mode selected, configure the following parameters:

Table 49: VLANs Parameters

Parameter	Description
Instant AP assigned	<p>When this option is selected, the client obtains the IP address from the virtual controller. The virtual controller creates a private subnet and VLAN on the IAP for the wireless clients. The network address translation for all client traffic that goes out of this interface is carried out at the source. This setup eliminates the need for complex VLAN and IP address management for a multi-site wireless network. For more information on DHCP scopes and server configuration, see Configuring DHCP Pools and Client IP Assignment Modes on IAPs.</p> <p>If this option is selected, specify any of the following options in Client VLAN Assignment:</p> <ul style="list-style-type: none"> ■ Internal VLAN—Assigns IP address to the client in the same subnet as the IAPs. By default, the client VLAN is assigned to the native VLAN on the wired network. ■ Custom—Allows you to customize the client VLAN assignment to a specific VLAN, or a range of VLANs. When this option is selected, select the scope from the VLAN ID drop-down list.
External DHCP server assigned	<p>When this option is selected, specify any of the following options in Client VLAN Assignment:</p> <ul style="list-style-type: none"> ■ Static—In VLAN ID, specify a VLAN ID for a single VLAN(s). If a large number of clients need to be in the same subnet, you can select this option to configure VLAN pooling. VLAN pooling allows random assignment of VLANs from a pool of VLANs to each client connecting to the SSID. <p>To show or hide the Named VLANs, click Show Named VLANs. Click the Show Named VLANs, to view the Named VLAN table. To add a new Named VLAN, complete the following steps:</p> <ol style="list-style-type: none"> Click +Add Named VLAN. The Add Named VLAN window is displayed. Enter the VLAN Name and VLAN details, and then click OK. <ul style="list-style-type: none"> ■ Dynamic—Assigns the VLANs dynamically from a DHCP server. To add a new VLAN assignment rule, complete the following steps: <ol style="list-style-type: none"> Click + Add Rule in the VLAN Assignment Rules window. The New VLAN Assignment Rule page is displayed. Enter the Attribute, Operator, String, and VLAN details, and then click OK. <p>To delete a VLAN assignment rule, select a rule in the VLAN Assignment Rules window, and then click the delete icon.</p> <p>To show or hide the Named VLANs, click Show Named VLANs. Click the Show Named VLANs, to view the Named VLAN table. To add a new Named VLAN, complete the following steps:</p> <ul style="list-style-type: none"> ■ Click + Add Named VLAN. The Add Named VLAN window is displayed. ■ Enter the VLAN Name and VLAN details, and then click OK. <p>To delete, select a Named VLAN in the Named VLAN table, and then click the delete icon.</p> <ul style="list-style-type: none"> ■ Native VLAN—Assigns the client VLAN is assigned to the native VLAN. <p>From Aruba Central (on-premises) 2.5.4, the Add Named VLAN window supports adding multiple VLAN IDs and VLAN range.</p>

- Click **Next**.

Configuring Security Settings for Wireless Network

To configure security settings for mixed traffic or voice network, complete the following steps:

1. In the **Security** tab, specify any one of the following options in the **Security Level**:
 - **Enterprise**—On selecting **Enterprise** security level, the authentication options applicable to the network are displayed.
 - **Personal**—On selecting **Personal** security level, the authentication options applicable to the personalized network are displayed.
 - **Captive Portal**—On selecting **Captive Portal** security level, the authentication options applicable to the captive portal is displayed. For more information on captive portal, see [Configuring Wireless Networks for Guest Users on IAPs](#).
 - **Open**—On selecting **Open** security level, the authentication options applicable to an open network are displayed.



The default security setting for a network profile is **Personal**.

2. Based on the security level specified, configure the following basic parameters:

Table 50: Basic WLAN Security Parameters

Data Pane Item	Description
Key Management	<p>For Enterprise security level, select an encryption key from Key Management drop-down list:</p> <ul style="list-style-type: none"> ■ WPA-2 Enterprise—Select this option to use WPA-2 security. The WPA-2 Enterprise requires user authentication and requires the use of a RADIUS server for authentication. ■ WPA Enterprise—Select this option to use both WPA Enterprise. ■ Both (WPA-2 & WPA)—Select this option to use both WPA-2 and WPA security. ■ Dynamic- WEP with 802.1X—If you do not want to use a session key from the RADIUS Server to derive pairwise unicast keys, turn on the Use Session Key for LEAP toggle switch. This is required for old printers that use dynamic WEP through LEAP authentication. The Use Session Key for LEAP feature is Disabled by default. ■ WPA-3 Enterprise(CNSA)—Select this option to use WPA-3 security employing CNSA encryption. ■ WPA-3 Enterprise(CCM 128)—Select this option to use WPA-3 security employing CCM encryption operation mode limited to encrypting 128 bits of plain text. ■ WPA-3 Enterprise(GCM 256)—Select this option to use WPA-3 security employing GCM encryption operation mode limited to encrypting 256 bits of plain text. <p>When WPA-2 Enterprise and Both (WPA2-WPA) encryption types are selected and if 802.1x authentication method is configured, OKC is enabled by default. If OKC is enabled, a cached PMK is used when the client roams to a new AP. This allows faster roaming of clients without the need for a complete 802.1x authentication. OKC roaming can be configured only for the Enterprise security level.</p>
	<p>For Personal security level, select an encryption key from Key Management drop-down list.</p>

Data Pane Item	Description
	<p>For WPA-2 Personal, WPA Personal, Both (WPA-2&WPA), and WPA-3 Personal keys, specify the following parameters:</p> <ul style="list-style-type: none"> ■ Passphrase Format—Select a passphrase format. The options available are 8-63 alphanumeric characters and 64 hexadecimal characters. ■ Passphrase—Enter a passphrase in ■ Retype—Retype the passphrase to confirm. <p>For Static WEP, specify the following parameters:</p> <ul style="list-style-type: none"> ■ WEP Key Size—Select an appropriate value for WEP key size from the drop-down list. Select an appropriate value from the Tx Key drop-down list. ■ WEP Key—Enter an appropriate WEP key. ■ Retype WEP Key—Retype the WEP key to confirm. <p>For MPSK-AES, select a primary server from the drop-down list. For MPSK-LOCAL, select a Mpsk Local server from the drop-down list.</p> <hr/> <p>For Captive Portal security level, select an encryption key from Key Management. For WPA-2 Personal, WPA Personal, Both (WPA-2&WPA), and WPA-3 Personal keys, specify the following parameters:</p> <ul style="list-style-type: none"> ■ Passphrase Format—Select a passphrase format. The options available are 8-63 alphanumeric characters and 64 hexadecimal characters. ■ Passphrase—Enter a passphrase in ■ Retype—Retype the passphrase to confirm. <p>For Static WEP, specify the following parameters:</p> <ul style="list-style-type: none"> ■ WEP Key Size—Select an appropriate value for WEP key size from the drop-down list. Select an appropriate value from the Tx Key drop-down list. ■ WEP Key—Enter an appropriate WEP key. ■ Retype WEP Key—Retype the WEP key to confirm. <p>For information on configuring captive portal, see Configuring Wireless Networks for Guest Users on IAPs.</p> <hr/> <p>For Open security level, the Key Management includes Open and Enhanced Open options.</p>
EAP offload	<p>This option is applicable to Enterprise security levels only. To terminate the EAP portion of 802.1X authentication on the Instant AP instead of the RADIUS server, turn on the EAP offload toggle switch. Enabling EAP offload can reduce network traffic to the external RADIUS server by terminating the authorization protocol on the Instant AP. By default, for 802.1X authorization, the client conducts an EAP exchange with the RADIUS server, and the Instant AP acts as a relay for this exchange. When EAP Offload is enabled, the Instant AP by itself acts as an authentication server and terminates the outer layers of the EAP protocol, only relaying the innermost layer to the external RADIUS server. It can also reduce the number of exchange packets between the Instant AP and the authentication server.</p> <p>Instant supports the configuration of primary and backup authentication servers in an EAP termination-enabled SSID.</p> <p>If you are using LDAP for authentication, ensure that Instant AP termination is configured to support EAP.</p>
Authentication Server	<p>Configure the following parameters:</p> <ul style="list-style-type: none"> ■ MAC Authentication—Turn on the MAC Authentication toggle switch to allow MAC address based authentication for Personal, Captive Portal, and Open security levels.

Data Pane Item	Description
	<ul style="list-style-type: none"> ■ Primary Server—Set a primary authentication server. The Primary Server option appears only for Enterprise security level, internal and external captive portal types. Select one of the following options from the drop-down list: ■ Internal Server—To use an internal server, select Internal Server and add the clients that are required to authenticate with the internal RADIUS Server. Click Users to add the users. ■ To add a new server, click +. For information on configuring external servers, see Configuring External Authentication Servers for APs. ■ Aruba Central allows you to configure an external RADIUS server, TACACS or LDAP server, and External Captive Portal for user authentication. ■ Secondary Server—To add another server for authentication, configure another authentication server. ■ Authentication Survivability—If an external server is configured for authentication, you can enable authentication survivability. Specify a value in hours for Cache Timeout to set the duration after which the authenticated credentials in the cache expires. When the cache expires, the clients are required to authenticate again. You can specify a value within range of 1 to 99 hours. By default, authentication survivability is disabled. ■ Load Balancing—Turn on the toggle switch to enable, if you are using two RADIUS authentication servers, to balance the load across these servers. For more information on the dynamic load balancing mechanism, see Configuring External Authentication Servers for APs.
Users	Click Users to add the users. The registered users of Employee type will be able to access the users of Enterprise network. To add a new user, click + Add User and enter the new user in the Add User pane. The Primary Server option appears only for Enterprise security level, Internal Captive Portal , and External Captive Portal .

- Based on the security level specified, specify the following parameters in the **Advanced Settings** section:

Table 51: *Advanced WLAN Security Parameters*

Data pane item	Description
Use Session Key for LEAP	Turn on the toggle switch to use the session key for Lightweight Extensible Authentication Protocol. This option is available only for Enterprise level.
Opportunistic Key Caching (OKC)	Turn on the Opportunistic key caching (OKC) toggle switch to reduce the time needed for authentication. When OKC is used, multiple APs can share Pairwise Master Keys (PMKs) among themselves, and the station can roam to a new access points that has not visited before and reuse a PMK that was established with the current AP. OKC allows the station to roam quickly to an access point it has never authenticated to, without having to perform pre-authentication. OKC is available specifically on WPA2 SSIDs only.

Data pane item	Description
MAC Authentication for Enterprise Networks	<p>To enable MAC address based authentication for Personal and Open security levels, turn on the toggle switch to enable MAC Authentication. For Enterprise security level, the following options are available:</p> <ul style="list-style-type: none"> ■ Perform MAC authentication before 802.1X—Select this to use 802.1X authentication only when the MAC authentication is successful. ■ MAC Authentication Fail-Through—On selecting this, the 802.1X authentication is attempted when the MAC authentication fails. ■ If MAC Authentication is enabled, configure the following parameters: ■ Delimiter Character—Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the IAP uses the delimiter in the MAC authentication request. For example, if you specify the colon as a delimiter, MAC addresses in the xx:xx:xx:xx:xx:xx format are used. If the delimiter is not specified, the MAC address in the xxxxxxxxxxxx format is used. This option is available only when MAC authentication is enabled. ■ Uppercase Support—Turn on the toggle switch to allow the IAP to use uppercase letters in MAC address string for MAC authentication. This option is available only if MAC authentication is enabled.
Reauth Interval	<p>Specify a value for Reauth Interval. When set to a value greater than zero, APs periodically re-authenticate all associated and authenticated clients.</p> <p>If the re-authentication interval is configured:</p> <p>On an SSID performing L2 authentication (MAC or 802.1X authentication): When re-authentication fails, the clients are disconnected. If the SSID is performing only MAC authentication and has a pre-authentication role assigned to the client, the client will get a post-authentication role only after a successful re-authentication. If re-authentication fails, the client retains the pre-authentication role.</p> <p>On an SSID performing both L2 and L3 authentication (MAC with captive portal authentication): When re-authentication succeeds, the client retains the role that is already assigned. If re-authentication fails, a pre-authentication role is assigned to the client.</p> <p>On an SSID performing only L3 authentication (captive portal authentication): When re-authentication succeeds, a pre-authentication role is assigned to the client that is in a post-authentication role. Due to this, the clients are required to go through captive portal to regain access.</p>
Denylisting	<p>By default, this option is disabled. To enable denylisting of the clients with a specific number of authentication failures, select Denylisting and specify a value for Max Authentication Failures. The users who fail to authenticate the number of times specified in Max Authentication Failures field are dynamically denylisted. By default, the Denylisting option is disabled.</p>
Enforce DHCP	<p>Enforces WLAN SSID on IAP clients. When DHCP is enforced:</p> <p>A layer-2 user entry is created when a client associates with an IAP.</p> <p>The client DHCP state and IP address are tracked.</p> <p>When the client obtains an IP address from DHCP, the DHCP state changes to complete.</p> <p>If the DHCP state is complete, a layer-3 user entry is created.</p> <p>When a client roams between the IAPs, the DHCP state and the client IP address is synchronized with the new IAP.</p>

Data pane item	Description
WPA3 Transition	Enable this option to allow transition from WPA3 to WPA2 and vice versa. The WPA3 Transition appears only when WPA3 is selected in the Key Management for Personal , Captive Portal , and Open level.
Legacy Support	Enable this option to allow backward compatibility of encryption modes in networks. The Legacy Support appears only when WPA3 is selected in the Key Management for Personal , Captive Portal , and Open level.
Use IP for Calling Station ID	<p>Enable this option to configure client IP address as calling station ID. When this option is enabled, the following options are displayed:</p> <ul style="list-style-type: none"> ■ Called Station ID Type—Select any of the following options for configuring called station ID: <ul style="list-style-type: none"> ○ Access Point Group—Uses the VC ID as the called station ID. ○ Access Point Name—Uses the host name of the IAP as the called station ID. ○ VLAN ID—Uses the VLAN ID of as the called station ID. ○ IP Address—Uses the IP address of the IAP as the called station ID. ○ MAC address—Uses the MAC address of the IAP as the called station ID. ■ Called Station ID Include SSID—Appends the SSID name to the called station ID. <p>NOTE: The Called Station ID Type detail can be configured even if the Use IP for Calling Station ID is set to disabled.</p> <ul style="list-style-type: none"> ■ Called Station ID Delimiter—Sets delimiter at the end of the called station ID. ■ Max Authentication Failures—Sets a value for the maximum allowed authentication failures.
Delimiter Character	Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the IAP uses the delimiter in the MAC authentication request. For example, if you specify the colon as a delimiter, MAC addresses in the xx:xx:xx:xx:xx:xx format are used. If the delimiter is not specified, the MAC address in the xxxxxxxxxxxx format is used. This option is available only when MAC authentication is enabled.
Uppercase Support	Select this option to allow the IAP to use uppercase letters in MAC address string for MAC authentication. This option is available only if MAC authentication is enabled.
Fast Roaming	<p>Enable the following fast roaming features as per your requirement:</p> <ul style="list-style-type: none"> ■ 802.11k—Turn on the 802.11k toggle switch to enable 802.11k roaming. The 802.11k protocol enables IAPs and clients to dynamically measure the available radio resources. When 802.11k is enabled, IAPs and clients send neighbor reports, beacon reports, and link measurement reports to each other. ■ 802.11v—Turn on the 802.11v toggle switch to enable 802.11v based BSS transition. The 802.11v standard defines mechanisms for wireless network management enhancements and BSS transition management. It allows the client devices to exchange information about the network topology and RF environment. The BSS transition management mechanism enables an AP to request a voice client to transition to a specific AP, or suggest a set of preferred APs to a voice client, due to network load balancing or BSS termination. It also helps the voice client identify the best AP to transition to as they roam. ■ RRM Quiet IE—Configures a radio resource management IE profile elements advertised by an AP.

4. Click **Next**.

Configuring ACLs for User Access to a Wireless Network

You can configure up to 64 access rules for a wireless network profile. To configure access rules for a network, complete the following steps:

1. In the **Access** tab, turn on the **Downloadable Role** toggle switch to allow downloading of pre-existing user roles. For more information, see [Configuring Downloadable Roles](#).



-
- The **Downloadable Role** feature is optional.
 - The **Downloadable Role** feature is available only for networks that include APs that run a minimum of Aruba Instant 8.4.0.0 firmware version with a minimum of ClearPass server version 6.7.8.
 - At least one radius server must be configured to apply the **Downloadable Role** feature. For more information on configuring radius server, see [Authentication Servers for IAPs](#)
-

2. Click the action corresponding to the server. The **Edit Server** page is displayed.

Viewing Wireless SSID Summary

In the **Summary** tab, the **Network Summary** page displays all the settings configured in the **General**, **VLANs**, **Security**, and **Access** tabs.

Click **Save Settings** to complete the network profile creation and save the settings.

Configuring Wireless Networks for Guest Users on IAPs

Instant Access Points (IAPs) support the captive portal authentication method in which a webpage is presented to the guest users, when they try to access the Internet in hotels, conference centers, or Wi-Fi hotspots. The webpage also prompts the guest users to authenticate or accept the usage policy and terms. Captive portals are used at Wi-Fi hotspots and can be used to control wired access as well.

The captive portal solution for an IAP cluster consists of the following:

- The captive portal web login page hosted by an internal or external server.
- The RADIUS authentication or user authentication against internal database of the AP.
- The SSID broadcast by the IAP.

The IAP administrators can create a wired or WLAN guest network based on captive portal authentication for guests, visitors, contractors, and any non-employee users who can use the enterprise Wi-Fi network. Administrators can also create guest accounts and customize the captive portal page with organization-specific logo, terms, and usage policy. With captive portal authentication and guest profiles, the devices associating with the guest SSID are assigned an initial role and are assigned IP addresses. When a guest user tries to access a URL through HTTP or HTTPS, the captive portal webpage prompts the user to authenticate with a user name and password.

Splash Page Profiles

Instant APs support the following types of splash page profiles:

- **Internal Captive portal**—Select this splash page to use an internal server for hosting the captive portal service. Internal captive portal supports the following types of authentication:

- **Internal Authenticated**—When **Internal Authenticated** is enabled, a guest user who is pre-provisioned in the user database has to provide the authentication details.
- **Internal Acknowledged**—When **Internal Acknowledged** is enabled, a guest user has to accept the terms and conditions to access the Internet.
- **External Captive portal**—Select this splash page to use an external portal on the cloud or on a server outside the enterprise network for authentication.
- **Cloud Guest**—Select this splash page to use the cloud guest profile configured through the **Guest Management** tab.
- **None**—Select to disable the captive portal authentication.

To create splash page profiles, see the following sections:

- [Creating a Wireless Network Profile for Guest Users](#)
- [Configuring Wireless Networks for Guest Users on IAPs](#)
- [Configuring an External Captive Portal Splash Page Profile](#)
- [Associating a Cloud Guest Splash Page Profile to a Guest SSID](#)
- [Associating a Cloud Guest Splash Page Profile to a Guest SSID](#)
- [Configuring ACLs for Guest User Access](#)
- [Configuring Captive Portal Roles for an SSID](#)
- [Disabling Captive Portal Authentication](#)

Creating a Wireless Network Profile for Guest Users

To create an SSID for guest users, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one AP. The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of access points is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the access points are displayed.
4. Click the **WLANS** tab.
The WLANS details page is displayed.
5. In the **WLANS** page, click **+ Add SSID**.
The **Create a New Network** pane is displayed.
6. Under **General**, enter a network name in the **Name (SSID)** text-box.
7. If configuring a wireless guest profile, set the required WLAN configuration parameters described in [Table 1](#).
8. Click **Next**.
The VLANS details are displayed.
9. Under **VLANS**, select any of the following options for **Client IP Assignment**:

Table 52: VLANs Assignment

Parameter	Description
<p>Instant AP assigned</p>	<p>When this option is selected, the client obtains the IP address from the virtual controller. The virtual controller creates a private subnet and VLAN on the IAP for the wireless clients. The network address translation for all client traffic that goes out of this interface is carried out at the source. This setup eliminates the need for complex VLAN and IP address management for a multi-site wireless network. For more information on DHCP scopes and server configuration, see Configuring DHCP Pools and Client IP Assignment Modes on IAPs.</p> <p>If this option is selected, specify any of the following options in Client VLAN Assignment:</p> <ul style="list-style-type: none"> ■ Internal VLAN—Assigns IP address to the client in the same subnet as the IAPs. By default, the client VLAN is assigned to the native VLAN on the wired network. ■ Custom—Allows you to customize the client VLAN assignment to a specific VLAN, or a range of VLANs. When this option is selected, select the scope from the VLAN ID drop-down list.
<p>External DHCP server assigned</p>	<p>When this option is selected, specify any of the following options in Client VLAN Assignment:</p> <ul style="list-style-type: none"> ■ Static—In VLAN ID, specify a VLAN ID for a single VLAN(s). If a large number of clients need to be in the same subnet, you can select this option to configure VLAN pooling. VLAN pooling allows random assignment of VLANs from a pool of VLANs to each client connecting to the SSID. To show or hide the Named VLANs, click Show Named VLANs. Click Show Named VLANs to view the Named VLAN table. To add a new Named VLAN, complete the following steps: <ol style="list-style-type: none"> 1. Click +Add Named VLAN. The Add Named VLAN window is displayed. 2. Enter the VLAN Name and VLAN details, and then click OK. ■ Dynamic—Assigns the VLANs dynamically from a DHCP server. To add a new VLAN assignment rule, complete the following steps: <ol style="list-style-type: none"> 1. Click +Add Rule in the VLAN Assignment Rules window. The New VLAN Assignment Rule page is displayed. 2. Enter the Attribute, Operator, String, and VLAN details, and then click OK. <p>To delete a VLAN assignment rule, select a rule in the VLAN Assignment Rules window, and then click the delete icon.</p> <p>To show or hide the Named VLANs, click Show Named VLANs. Click Show Named VLANs to view the Named VLAN table. To add a new Named VLAN, complete the following steps:</p> <ol style="list-style-type: none"> 1. Click +Add Named VLAN. The Add Named VLAN window is displayed. 2. Enter the VLAN Name and VLAN details, and then click OK. <p>To delete, select a Named VLAN in the Named VLAN table, and then click the delete icon.</p>

Parameter	Description
	<ul style="list-style-type: none"> ■ Native VLAN—Assigns the client VLAN is assigned to the native VLAN. For more information, see Configuring VLAN Assignment Rule.

Configuring an Internal Captive Portal Splash Page Profile

To configure an internal captive portal profile, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of access points is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the access points are displayed.
4. Click the **WLANS** tab.
The WLANS details page is displayed.
5. In the **Wireless SSIDs** table, select a guest SSID, and then click the edit icon.
6. Under **Security** tab, in the **Security Level**, select **Captive Portal** and configure the following parameters:

Table 53: *Internal Captive Portal Configuration Parameters*

Parameter	Description
Captive Portal Type	Select Internal from the drop-down list.
Captive Portal Location	Select Acknowledged or Authenticated from the drop-down list.
Customize Captive Portal	<p>Under Splash Page, when Customize Captive Portal is clicked, use the editor to specify text and colors for the initial page that is displayed to the users connecting to the network. The initial page asks for user credentials or email, depending on the splash page type (Authenticated or Acknowledged) for which you are customizing the splash page design.</p> <p>Complete the following steps to customize the splash page design.</p> <ul style="list-style-type: none"> ■ Top banner title—Enter a title for the banner. ■ Header fill color—Specify a background color for the header. ■ Welcome text—To change the welcome text, click the first square box in the splash page, enter the required text in the Welcome text box, and click OK. Ensure that the welcome text does not exceed 127 characters. ■ Policy text—To change the policy text, click the second square in the splash page, enter the required text in the Policy text box, and click OK. Ensure that the policy text does not exceed 255 characters. ■ Page fill color—To change the color of the splash page, click the Splash page rectangle and select the required color from the color palette. ■ Redirect URL—To redirect users to another URL, specify a URL in Redirect URL.

Table 53: Internal Captive Portal Configuration Parameters

Parameter	Description
	<ul style="list-style-type: none"> ▪ Logo image—To upload a custom logo, click Choose File to upload. Ensure that the image file size does not exceed 16 KB. To delete an image, click Delete Logo. <p>To preview the captive portal page, click preview_splash_page.</p> <p>To configure a captive portal proxy server or global proxy server to match your browser configuration, enter the IP address and port number in the Captive-portal proxy server IP and Captive Portal Proxy Server Port fields.</p>
Encryption	<p>By default, this field is disabled. Turn on the toggle switch to enable and configure the following encryption parameters:</p> <ul style="list-style-type: none"> ▪ Key Management—Specify an encryption and authentication key. ▪ Passphrase format—Specify a passphrase format. ▪ Passphrase—Enter a passphrase. ▪ Retype—Retype the passphrase to confirm.
Key Management	Select Open or Enhanced Open from the drop-down list.
Advanced Settings	
Captive Portal Proxy Server IP	Specify the IP address of the Captive Portal proxy server.
Captive Portal Proxy Server Port	Specify the port number of the Captive Portal proxy server.
MAC Authentication	<p>Configure the following parameters:</p> <ul style="list-style-type: none"> ▪ MAC Authentication—To enable MAC address based authentication for Personal and Open security levels, turn on the MAC Authentication toggle switch. ▪ Secondary Server—To add another server for authentication, configure another authentication server. ▪ Load Balancing—Turn on the toggle switch to enable, if you are using two RADIUS authentication servers, to balance the load across these servers. For more information on the dynamic load balancing mechanism, see Configuring DHCP Server for Assigning IP Addresses to IAP Clients. <p>To use an internal server, select Internal Server and add the clients that are required to authenticate with the internal RADIUS Server. Click Users to add the users.</p> <p>To add a new server, click +. For information on configuring external servers, see Configuring External Authentication Servers for APs.</p>
Reauth Interval	Specify a value for Reauth Interval . When set to a value greater than zero, APs periodically re-authenticate all associated and authenticated clients.
Accounting	Select an accounting mode for posting accounting information at the specified Accounting interval . When the accounting mode is set to Authentication , the accounting starts only after client authentication is successful and stops when the client logs out of the network. If the accounting mode is set to Association , the accounting starts when the client associates to the network successfully and stops when the client disconnects. This is applicable for WLAN SSIDs only.

Table 53: *Internal Captive Portal Configuration Parameters*

Parameter	Description
Denylisting	If you are configuring a wireless network profile, turn on the Denylisting toggle switch to denylist clients with a specific number of authentication failures. This is applicable for WLAN SSIDs only.
Max Authentication Failures	If you are configuring a wireless network profile, turn on the Denylisting toggle switch to denylist clients with a specific number of authentication failures. This is applicable for WLAN SSIDs only.
Enforce DHCP	If you are configuring a wireless network profile, turn on the Denylisting toggle switch to denylist clients with a specific number of authentication failures. This is applicable for WLAN SSIDs only.
WPA3 Transition	If you are configuring a wireless network profile, turn on the Denylisting toggle switch to denylist clients with a specific number of authentication failures. This is applicable for WLAN SSIDs only.
Called Station ID Include SSID	If you are configuring a wireless network profile, turn on the Denylisting toggle switch to denylist clients with a specific number of authentication failures. This is applicable for WLAN SSIDs only.
Uppercase Support	If you are configuring a wireless network profile, turn on the Denylisting toggle switch to denylist clients with a specific number of authentication failures. This is applicable for WLAN SSIDs only.
Disable if uplink type is	To exclude uplink(s), expand Disable if uplink type is , and turn on the toggle switch for the uplink type(s). For example, Ethernet, Wi-Fi, and 3G/4G .

1. Click **Save Settings**.

Configuring an External Captive Portal Splash Page Profile

You can configure external captive portal profiles and associate these profiles to a user role or SSID. You can create a set of captive portal profiles and associate these profiles with an SSID or a wired profile. You can configure up to eight external captive portal profiles.

When the captive portal profile is associated to an SSID, it is used before user authentication. If the profile is associated to a role, it is used only after the user authentication. When a captive portal profile is applied to an SSID or wired profile, the users connecting to the SSID or wired network are assigned a role with the captive portal rule. The guest user role allows only DNS and DHCP traffic between the client and network, and directs all HTTP or HTTPS requests to the captive portal unless explicitly permitted.

To configure an external captive portal profile, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click the **WLANs** tab.
The WLANs details page is displayed.

5. In the **Wireless SSIDs** table, select a guest SSID, and then click the edit icon.
6. Under **Security** tab, in the **Security Level**, select **Captive Portal**.
7. Select the **Splash Page** type as **External**.
8. If required, configure a captive portal proxy server or a global proxy server to match your browser configuration by specifying the IP address and port number in the **Captive Portal Proxy Server IP** and **Captive Portal Proxy Server Port** fields.
9. Select a captive portal profile. To add a new profile, click **+** and configure the following parameters:

Table 54: External Captive Portal Profile Configuration Parameters

Data Pane Item	Description
Name	Enter a name for the profile.
Type	Select any one of the following types of authentication: <ul style="list-style-type: none"> ■ Radius Authentication—Select this option to enable user authentication against a RADIUS server. ■ Authentication Text—Select this option to specify an authentication text. The specified text will be returned by the external server after a successful user authentication.
IP or Hostname	Enter the IP address or the host name of the external splash page server.
URL	Enter the URL of the external captive portal server.
Port	Enter the port number that is used for communicating with the external captive portal server.
Use HTTPS	Select this to enforce clients to use HTTPS to communicate with the captive portal server. This option is available only if RADIUS Authentication is selected.
Captive Portal Failure	This field allows you to configure Internet access for the guest users when the external captive portal server is not available. Select Deny Internet to prevent guest users from using the network, or Allow Internet to access the network.
Server Offload	Select the check box to enable the server offload feature. The server offload feature ensures that the non-browser client applications are not unnecessarily redirected to the external captive portal server, thereby reducing the load on the external captive portal server.
Prevent Frame Overlay	Select this check box to prevent the overlay of frames. When enabled, the frames display only those pages that are in the same domain as the main page.
Automatic URL Allowlisting	On enabling this for the external captive portal authentication, the URLs that are allowed for the unauthenticated users to access are automatically allowlisted.
Auth Text	If the External Authentication splash page is selected, specify the authentication text that is returned by the external server after successful authentication. This option is available only if Authentication Text is selected.
Redirect URL	Specify a redirect URL if you want to redirect the users to another URL.

10. Click **Save**.
11. On the external captive portal splash page configuration page, specify encryption settings if required.
12. Specify the following authentication parameters under **Advanced Settings**:

- **MAC Authentication**—To enable MAC address based authentication for **Personal** and **Open** security levels, turn on the **MAC Authentication** toggle switch.
 - **Primary Server**—Sets a primary authentication server.
 - To use an internal server, select **Internal server** and add the clients that are required to authenticate with the internal RADIUS Server. Click **Users** to add the users.
 - To add a new server, click **+**. For information on configuring external servers, see [Configuring External Authentication Servers for APs](#).
 - **Secondary Server**—To add another server for authentication, configure another authentication server.
 - **Load Balancing**—Turn on the toggle switch to enable, if you are using two RADIUS authentication servers, to balance the load across these servers.
13. If required, under **Walled Garden**, create a list of domains that are denylisted and also a allowlist of websites that the users connected to this splash page profile can access.
 14. To exclude uplink, select an uplink type.
 15. If MAC authentication is enabled, you can configure the following parameters:
 - **Delimiter Character**—Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the IAP uses the delimiter in the MAC authentication request. For example, if you specify the colon as a delimiter, MAC addresses in the xx:xx:xx:xx:xx:xx format are used. If the delimiter is not specified, the MAC address in the xxxxxxxxxxxx format is used. This option is available only when MAC authentication is enabled.
 - **Uppercase Support**—Turn on the toggle switch to enable to allow the IAP to use uppercase letters in MAC address string for MAC authentication. This option is available only if MAC authentication is enabled.
 16. Configure the **Reauth Interval**. Specify a value for **Reauth Interval**. When set to a value greater than zero, IAPs periodically re-authenticate all associated and authenticated clients.
 17. If required, enable denylisting. Set a threshold for denylisting clients based on the number of failed authentication attempts.
 18. Click **Save Settings**.

Associating a Cloud Guest Splash Page Profile to a Guest SSID

To use the Cloud Guest splash page profile for the guest SSID, ensure that the Cloud Guest splash Page profile is configured through the **Guest Access** app.

To associate a Cloud Guest splash page profile to a guest SSID, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click the **WLANS** tab.
The WLANS details page is displayed.
5. Under **WLANS** tab, in the **Wireless SSIDs** table, select a guest SSID and click the edit icon.

6. Click the **Security** tab.
 - a. Under **Splash Page**, select **Cloud Guest** from the **Captive Portal Type** drop-down list.
 - b. Select the splash page profile name from the **Guest Captive Portal Profile** list, and then click **Next**.
 - c. To enable encryption, turn on the **Encryption** toggle switch and configure the following encryption parameters:
 - d. **Key Management**—Specify an encryption and authentication key.
 - e. **Passphrase format**—Specify a passphrase format.
 - f. **Passphrase**—Enter a passphrase.
 - g. **Retype**—Retype the passphrase to confirm.
 - h. To exclude uplink, expand **Disable if uplink type is** and select an uplink type. For example, **Ethernet, Wi-Fi**, and **3G/4G**.
 - i. Click **Next**.
7. Click **Save Settings**.

Configuring ACLs for Guest User Access

To configure access rules for a guest network, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click the **WLANS** tab.
The WLANS details page is displayed.
5. Under **WLANS** tab, in the **Wireless SSIDs** table, select a guest SSID and click the edit icon.
6. Click the **Access** tab.
7. Under **Access rules**, select any of the following types of access control:
 - **Unrestricted**—Select this to set unrestricted access to the network.
 - **Network Based**—Select **Network Based** to set common rules for all users in a network. By default, **Allow any to all destinations** access rule is enabled. This rule allows traffic to all destinations. To define an access rule, complete the following steps:
 - Click **+** and select appropriate options for **Rule Type**, **Service**, **Action**, **Destination**, and **Options** fields.
 - Click **Save**.
 - **Role Based**—Select **Role Based** to enable access based on user roles.

For role-based access control, complete the following steps:

1. To create a user role:
 - a. Click **+Add Role** in **Role** pane.
 - b. Enter a name for the new role and click **OK**.
2. To create access rules for a specific user role:

- a. Click **+Add Rule** in **Access Rules for Selected Roles**, and select appropriate options for **Rule Type, Service, Action, Destination**, and **Options** fields.
- b. Click **Save**.
3. To create a role assignment rule:
 - a. Under **Role Assignment Rules**, click **+Add Role Assignment**. The **New Role Assignment Rule** pane is displayed.
 - b. Select appropriate options in **Attribute, Operator, String**, and **Role** fields.
 - c. Click **Save**.
4. To assign pre-authentication role, select the **Assign Pre-Authentication Role** check-box and select a pre-authentication role from the drop-down list.
5. Click **Save Settings**.

Configuring Captive Portal Roles for an SSID

You can configure an access rule to enforce captive portal authentication for SSIDs with 802.1X authentication enabled. You can configure rules to provide access to an external captive portal, internal captive portal, so that some of the clients using this SSID can derive the captive portal role.

The following conditions apply to the 802.1X and captive portal authentication configuration:

- If captive portal settings are not configured for a user role, the captive portal settings configured for an SSID are applied to the client's profile.
- If captive portal settings are not configured for a SSID, the captive portal settings configured for a user role are applied to the client's profile.
- If captive portal settings are configured for both SSID and user role, the captive portal settings configured for a user role are applied to the profile of the client.

To create a captive portal role for the **Internal** and **External** splash page types:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click the **WLANS** tab.
The WLANS details page is displayed.
5. Under **WLANS** tab, in the **Wireless SSIDs** table, select a guest SSID and click the edit icon.
6. Click the **Access** tab.
7. Under **Access rules**, select **Role Based**.
8. Click **+Add Rule** in **Access Rules for Selected Roles**.
9. In the **Add Rules** window, specify the following parameters.

Table 55: Access Rule Configuration Parameters

Data Pane Item	Description
Rule Type	Select Captive Portal from the drop-down list.
Splash Page Type	Select a splash page type from the drop-down list.
Internal	<p>If Internal is selected as Splash Page Type drop-down list, complete the following steps:</p> <ul style="list-style-type: none"> ■ Top banner title—Enter a title for the banner. To preview the page with the new banner title, click Preview splash page. ■ Header fill color—Specify a background color for the header. ■ Welcome text—To change the welcome text, click the first square box in the splash page, enter the required text in the Welcome text box, and click OK. Ensure that the welcome text does not exceed 127 characters. ■ Policy text—To change the policy text, click the second square in the splash page, enter the required text in the Policy text box, and click OK. Ensure that the policy text does not exceed 255 characters. ■ Page fill color—To change the color of the splash page, click the Splash page rectangle and select the required color from the color palette. ■ Redirect URL—To redirect users to another URL, specify a URL in Redirect URL. ■ Logo image—To upload a custom logo, click Choose File to upload. Ensure that the image file size does not exceed 16 KB. To delete an image, click Delete Logo. <p>To preview the captive portal page, click preview_splash_page.</p>
External	<p>If External is selected as Splash Page Type drop-down list, complete the following steps:</p> <ul style="list-style-type: none"> ■ Captive Portal Profile—Select a profile from the drop-down list. To create a profile, click the + icon and enter the following information in the External Captive Portal window. ■ Name ■ Authentication Type—From the drop-down list, select either RADIUS Authentication (to enable user authentication against a RADIUS server) or Authentication Text (to specify the authentication text to returned by the external server after a successful user authentication). ■ IP OR Hostname—Enter the IP address or the hostname of the external splash page server. ■ URL—Enter the URL for the external splash page server. ■ Port—Enter the port number for communicating with the external splash page server. ■ Captive Portal Failure—This field allows you to configure Internet access for the guest clients when the external captive portal server is not available. From the drop-down list, select Deny Internet to prevent clients from using the network, or Allow Internet to allow the guest clients to access Internet when the external captive portal server is not available. ■ Automatic URL Allowlisting—Turn on the toggle switch to enable or disable automatic allowlisting of URLs. On selecting this for the external captive portal authentication, the URLs allowed for the unauthenticated users to access are automatically allowlisted. The automatic URL allowlisting is disabled by default.

Table 55: Access Rule Configuration Parameters

Data Pane Item	Description
	<ul style="list-style-type: none">■ Server offload—Turn on the toggle switch to offload the server.■ Prevent Frame Overlay—Turn on the toggle switch to prevent frame overlay.■ Use VC IP in Redirect URL—Turn on the toggle switch to use the virtual controller IP address as a redirect URL.■ Auth TEXT—Indicates the authentication text returned by the external server after a successful user authentication.■ Redirect URL—Specify a redirect URL to redirect the users to another URL. <p>To edit a profile, click the edit icon and modify the parameters in the External Captive Portal window.</p>

10. Click **Save**. The enforce captive portal rule is created and listed as an access rule.
11. Click **Save Settings**.

The client can connect to this SSID after authenticating with user name and password. After the user logs in successfully, the captive portal role is assigned to the client.

Disabling Captive Portal Authentication

To disable captive portal authentication, perform the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click the **WLANS** tab.
The WLANS details page is displayed.
5. In the **Wireless SSIDs** table, select a guest SSID, and then click the edit icon.
6. Under **Security** tab, in the **Security Level**, select **Captive Portal**.
7. Under **Splash Page**, select **None** from the **Captive Portal Type** drop-down list.
8. Click **Save Settings**.

Configuring Client Isolation

Aruba Central (on-premises) supports the **Client Isolation** feature isolates clients from one another and disables all peer-to-peer communication within the network. Client isolation disables inter-client communication by allowing only client to gateway traffic from clients to flow in the network. All other traffic from the client that is not destined to the gateway or configured servers will not be forwarded by the Instant Access Point (IAP).

This feature enhances the security of the network and protects it from vulnerabilities. **Client Isolation** can only be configured through the CLI. When **Client Isolation** is configured, the IAP learns the IP, subnet mask, MAC, and other essential information of the gateway and the DNS server. A subnet table of trusted destinations is then populated with this information. Wired servers used in the network should be manually

configured into this subnet table to serve clients. The destination MAC of data packets sent by the client is validated against this subnet table and only the data packets destined to the trusted addresses in the subnet table are forwarded by the I AP. All other data packets are dropped.



Client Isolation feature is supported only in IPv4 networks. This feature does not support **AirGroup** and affects **Chromecast** and **Airplay** services.

Enabling Client Isolation Feature for Wireless Networks in Aruba Central (on-premises)

To enable the Client Isolation feature, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click the **WLANS** tab.
The WLANS details page is displayed.
5. In the **WLANS** page, click **+Add SSID**.
The Create a New Network page is displayed.
6. Click **Advanced Settings** and expand **Miscellaneous**.
7. Turn on the **Deny Intra VLAN Traffic** toggle switch.
8. Click **Next**.

Management Frames Protection

Aruba Central (on-premises) supports the Management Frame Protection (MFP) feature in networks that include Aruba Instant 8.5.0.0 firmware version and later. This feature protects networks against forged management frames spoofed from other devices that might otherwise disrupt a valid user session.

The MFP increases the security by providing data confidentiality of management frames. MFP uses 802.11i framework that establishes encryption keys between the client and Instant AP.

Enabling Management Frames Protection Feature for Wireless Networks in Aruba Central (on-premises)

To enable the MFP feature, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click the **WLANS** tab.
The WLANS details page is displayed.

5. In the **WLANs** page, click **+Add SSID**. To modify an existing SSID, select a wireless SSID from the **Wireless SSIDs** table and then click the edit icon.
6. In the **General** tab, click **Advanced Settings**.
7. Expand **Miscellaneous**.
8. Turn on the **Management Frames Protection** toggle switch to enable the MFP feature.
9. Click **Next**.
10. Click **Save Settings**.



The MFP configuration is a per-SSID configuration. The MFP feature can be enabled only on WPA2-PSK and WPA2-Enterprise SSIDs. The 802.11r fast roaming option will not take effect when the MFP is enabled.

Configuring Wired Networks for Guest Users on IAPs

Instant Access Points (IAPs) support the captive portal authentication method in which a webpage is presented to the guest users, when they try to access the Internet in hotels, conference centres, or Wi-Fi hotspots. The webpage also prompts the guest users to authenticate or accept the usage policy and terms. Captive portals are used at Wi-Fi hotspots and can be used to control wired access as well.

The captive portal solution for an IAP cluster consists of the following:

- The captive portal web login page hosted by an internal or external server.
- The RADIUS authentication or user authentication against internal database of the AP.
- The SSID broadcast by the IAP.

The IAP administrators can create a wired or WLAN guest network based on captive portal authentication for guests, visitors, contractors, and any non-employee users who can use the enterprise Wi-Fi network. Administrators can also create guest accounts and customize the captive portal page with organization-specific logo, terms, and usage policy. With captive portal authentication and guest profiles, the devices associating with the guest SSID are assigned an initial role and are assigned IP addresses. When a guest user tries to access a URL through HTTP or HTTPS, the captive portal webpage prompts the user to authenticate with a user name and password.

Splash Page Profiles

IAPs support the following types of splash page profiles:

- **Internal Captive portal**—Select this splash page to use an internal server for hosting the captive portal service. Internal captive portal supports the following types of authentication:
 - **Internal Authenticated**—When **Internal Authenticated** is enabled, a guest user who is pre-provisioned in the user database has to provide the authentication details.
 - **Internal Acknowledged**—When **Internal Acknowledged** is enabled, a guest user has to accept the terms and conditions to access the Internet.
- **External Captive portal**—Select this splash page to use an external portal on the cloud or on a server outside the enterprise network for authentication.
- **Cloud Guest**—Select this splash page to use the cloud guest profile configured through the **Guest Management** tab.
- **None**—Select to disable the captive portal authentication.

For information on how to create splash page profiles, see the following sections:

- [Creating a Wired Network Profile for Guest Users](#)
- [Configuring an Internal Captive Portal Splash Page Profile](#)
- [Configuring an External Captive Portal Splash Page Profile](#)
- [Disabling Captive Portal Authentication](#)

Creating a Wired Network Profile for Guest Users

To create a wired SSID for guest access, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Interfaces** tab.
The Interfaces page is displayed.
6. Click the **Wired** accordion.
7. To create a new wired SSID profile, click **+Add Port Profile**.
The **Create a New Network** pane is displayed.
8. Under **General**, enter the following information:
 - a. **Name**—Enter a name.
 - b. **ports**—Select port(s) from the drop-down list.
9. Click **Next** to configure the **VLANS** settings.
The VLANS details are displayed.
10. In the **VLANS** tab, select a type of mode from the **Mode** drop-down list.
11. Select any of the following options for **Client IP Assignment**:

Table 56: *VLANS Parameters*

Parameter	Description
Instant AP assigned	Select this option to allow the Virtual Controller to assign IP addresses to the wired clients. When the Virtual Controller assignment is used, the source IP address is translated for all client traffic that goes through this interface. The Virtual Controller can also assign a guest VLAN to a wired client. If this option is selected, specify any of the following options in Client VLAN Assignment : <ul style="list-style-type: none"> ■ Default—When the client VLAN must be assigned to the native VLAN on the network. ■ Custom—To customize the client VLAN assignment to a specific VLAN, or a range of VLANs.
External DHCP server assigned	Select this option to allow the clients to receive an IP address from the network to which the Virtual Controller is connected. On selecting this option, the New button to create a VLAN is displayed. Create a new VLAN if required.

Configuring an Internal Captive Portal Splash Page Profile

To configure internal captive portal profile, complete the following steps:

1. Open the guest SSID to edit and configure the following parameters in the **Ports > Security** page.

Table 57: Internal Captive Portal Configuration Parameters

Parameter	Description
Captive Portal Type	<p>Select any of the following from the drop-down list:</p> <ul style="list-style-type: none"> ■ Internal - Authenticated—When Internal Authenticated is selected, the guest users are required to authenticate in the captive portal page to access the Internet. The guest users who are required to authenticate must already be added to the user database. ■ Internal - Acknowledged—When Internal Acknowledged is selected, the guest users are required to accept the terms and conditions to access the Internet. ■ External—When External is selected, the guest users are required to enter the proxy server details such as IP address and captive portal proxy server port details. Also enter the details in Walled Garden, and Advanced section. ■ Cloud Guest—When Cloud Guest is selected, the guest users are required to select the Guest Captive Portal Profile. ■ None—Select this option if you do not want to set any splash page.
Captive Portal Location	Select Acknowledged or Authenticated from the drop-down list.
Splash Page Properties	<p>Policy text for which you are customizing the splash page design. Perform the following steps to customize the splash page design.</p> <ul style="list-style-type: none"> ■ Top Banner Title—Enter a title for the banner. To preview the page with the new banner title, click Preview Splash Page. ■ Header fill color—Specify a background color for the header. ■ Welcome Text—To change the welcome text, click the first square box in the splash page, enter the required text in the Welcome Text box, and click OK. Ensure that the welcome text does not exceed 127 characters. ■ Policy Text—To change the policy text, click the second square in the splash page, enter the required text in the Policy Text box, and click OK. Ensure that the policy text does not exceed 255 characters. ■ Page Fill Color—To change the color of the splash page, click the Splash page rectangle and select the required color from the color palette. ■ Redirect URL—To redirect users to another URL, specify a URL in Redirect URL. ■ Logo Image—To upload a custom logo, click Upload, browse the image file, and click upload image. Ensure that the image file size does not exceed 16 KB. To delete an image, click Delete. <p>To preview the captive portal page, click Preview splash page. To configure a captive portal proxy server or global proxy server to match your browser configuration, enter the IP address and port number in the Captive-portal proxy server IP and Captive Portal Proxy Server Port fields.</p>
Encryption	By default, this field is disabled. Turn on the toggle switch to enable and configure the following encryption parameters:

Table 57: Internal Captive Portal Configuration Parameters

Parameter	Description
	<ul style="list-style-type: none"> ■ Key Management—Specify an encryption and authentication key. ■ Passphrase format—Specify a passphrase format. ■ Passphrase—Enter a passphrase and retype to confirm.
Authentication	<p>Configure the following parameters:</p> <ul style="list-style-type: none"> ■ MAC Authentication—To enable MAC address based authentication for Personal and Open security levels, turn on the MAC Authentication toggle switch. ■ Secondary Server—To add another server for authentication, configure another authentication server. ■ Load Balancing—Turn on the toggle switch to enable, if you are using two RADIUS authentication servers, to balance the load across these servers. For more information on the dynamic load balancing mechanism, see Configuring DHCP Server for Assigning IP Addresses to IAP Clients. <p>To use an internal server, select Internal Server and add the clients that are required to authenticate with the internal RADIUS Server. Click Users to add the users.</p> <p>To add a new server, click +. For information on configuring external servers, see Configuring External Authentication Servers for APs.</p>
Users	Create and manage users in the captive portal network. Only registered users of type Guest Employee will be able to access this network.
Advanced Settings > MAC Authentication	To enable MAC address based authentication for Personal and Open security levels, turn on the MAC Authentication toggle switch.
Advanced Settings > Reauth Interval	Specify a value for Reauth Interval . When set to a value greater than zero, APs periodically re-authenticate all associated and authenticated clients.
Advanced Settings > Denylisting	If you are configuring a wireless network profile, turn on the Denylisting toggle switch to denylist clients with a specific number of authentication failures. This is applicable for WLAN SSIDs only.
Advanced Settings > Disable If Uplink Type Is	To exclude uplink, select an uplink type.

2. Click **Save Settings**.

Configuring an External Captive Portal Splash Page Profile

You can configure external captive portal profiles and associate these profiles to a user role or SSID. You can create a set of captive portal profiles in the **Security > External Captive Portal** data pane and associate these profiles with an SSID or a wired profile. You can also create a new captive portal profile under the **Security** tab of the WLAN wizard or a Wired Network pane. You can configure up to eight external captive portal profiles.

When the captive portal profile is associated to an SSID, it is used before user authentication. If the profile is associated to a role, it is used only after the user authentication. When a captive portal profile is applied to an SSID or wired profile, the users connecting to the SSID or wired network are assigned a role with the

captive portal rule. The guest user role allows only DNS and DHCP traffic between the client and network, and directs all HTTP or HTTPS requests to the captive portal unless explicitly permitted.

To configure an external captive portal profile, complete the following steps:

1. Under **WLANS** tab, in the **Wireless SSIDs** table, select a guest SSID and click the edit icon. The **Create a New Network** pane is displayed.
2. Under **Security** tab, in the **Security Level**, select **Captive Portal** and configure the following parameters under **Splash Page**:
3. Select the Splash Page type as **External**.
4. If required, configure a captive portal proxy server or a global proxy server to match your browser configuration by specifying the IP address and port number in the **Captive Portal Proxy Server IP** and **Captive Portal Proxy Server Port** fields.
5. Select a captive portal profile. To add a new profile, click **+** and configure the following parameters:

Table 58: *External Captive Portal Profile Configuration Parameters*

Data Pane Item	Description
Name	Enter a name for the profile.
Type	Select any one of the following types of authentication: <ul style="list-style-type: none"> ■ Radius Authentication—Select this option to enable user authentication against a RADIUS server. ■ Authentication Text—Select this option to specify an authentication text. The specified text will be returned by the external server after a successful user authentication.
IP or Hostname	Enter the IP address or the host name of the external splash page server.
URL	Enter the URL of the external captive portal server.
Port	Enter the port number that is used for communicating with the external captive portal server.
Use HTTPS	Select this to enforce clients to use HTTPS to communicate with the captive portal server. This option is available only if RADIUS Authentication is selected.
Captive Portal Failure	This field allows you to configure Internet access for the guest users when the external captive portal server is not available. Select Deny Internet to prevent guest users from using the network, or Allow Internet to access the network.
Server Offload	Select the check box to enable the server offload feature. The server offload feature ensures that the non-browser client applications are not unnecessarily redirected to the external captive portal server, thereby reducing the load on the external captive portal server.
Prevent Frame Overlay	Select this check box to prevent the overlay of frames. When enabled, the frames display only those pages that are in the same domain as the main page.
Automatic URL Allowlisting	On enabling this for the external captive portal authentication, the URLs that are allowed for the unauthenticated users to access are automatically allowlisted.

Data Pane Item	Description
Auth Text	If the External Authentication Splash page is selected, specify the authentication text that is returned by the external server after successful authentication. This option is available only if Authentication Text is selected.
Redirect URL	Specify a redirect URL if you want to redirect the users to another URL.

6. Click **Save**.
7. On the external captive portal splash page configuration page, specify encryption settings if required.
8. Specify the following authentication parameters in **Advanced Settings**:
 - **MAC Authentication**—To enable MAC address based authentication for **Personal** and **Open** security levels, turn on the **MAC Authentication** toggle switch.
 - **Primary Server**—Sets a primary authentication server.
 - To use an internal server, select **Internal server** and add the clients that are required to authenticate with the internal RADIUS Server. Click **Users** to add the users.
 - To add a new server, click **+**. For information on configuring external servers, see [Configuring External Authentication Servers for APs](#).
 - **Secondary Server**—To add another server for authentication, configure another authentication server.
 - **Load Balancing**—Turn on the toggle switch to enable, if you are using two RADIUS authentication servers, to balance the load across these servers.
9. If required, under **Walled Garden**, create a list of domains that are denylisted and also an allowlist of websites that the users connected to this splash page profile can access.
10. To exclude uplink, select an uplink type.
11. If MAC authentication is enabled, you can configure the following parameters:
 - **Delimiter Character**—Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the IAP uses the delimiter in the MAC authentication request. For example, if you specify the colon as a delimiter, MAC addresses in the xx:xx:xx:xx:xx:xx format are used. If the delimiter is not specified, the MAC address in the xxxxxxxxxxxx format is used. This option is available only when MAC authentication is enabled.
 - **Uppercase Support**—Turn on the toggle switch to enable, to allow the IAP to use uppercase letters in MAC address string for MAC authentication. This option is available only if MAC authentication is enabled.
12. Configure the **Reauth Interval**. Specify a value for **Reauth Interval**. When set to a value greater than zero, IAPs periodically re-authenticate all associated and authenticated clients.
13. If required, enable denylisting. Set a threshold for denylisting clients based on the number of failed authentication attempts.
14. Click **Save Settings**.

Configuring ACLs for Guest User Access

To configure access rules for a guest network, complete the following steps:

1. Under **WLANS** tab, in the **Wireless SSIDs** table, select a guest SSID and click the edit icon. The Create a New Network pane is displayed.
2. Click the **Access** tab.

3. Under **Access**, select any of the following types of access control:
 - **Unrestricted**—Select this to set unrestricted access to the network.
 - **Network Based**—Select **Network Based** to set common rules for all users in a network. By default, **Allow any to all destinations** access rule is enabled. This rule allows traffic to all destinations. To define an access rule, complete the following steps:
 - a. Click **+** and select appropriate options for **Rule Type**, **Service**, **Action**, **Destination**, and **Options** fields.
 - b. Click **Save**.
 - **Role Based**—Select **Role Based** to enable access based on user roles.
For role-based access control:
 1. Create a user role:
 - a. Click **New** in **Role** pane.
 - b. Enter a name for the new role and click **OK**
 2. Create access rules for a specific user role:
 - a. Click **+** and select appropriate options for **Rule Type**, **Service**, **Action**, **Destination**, and **Options** fields.
 - b. Click **Save**.
 3. Create a role assignment rule.
 - a. Under **Role Assignment Rule**, click **New**. The **New Role Assignment Rule** pane is displayed.
 - b. Select appropriate options in **Attribute**, **Operator**, **String**, and **Role** fields.
 - c. Click **Save**.
4. Click **Save Settings**.

Disabling Captive Portal Authentication

To disable captive portal authentication, complete the following steps:

1. Under **WLANS** tab, in the **Wireless SSIDs** table, select a guest SSID and click the edit icon.
The **Create a New Network** pane is displayed.
2. Click the **Security** tab.
3. Under **Security**, select **None** for **Splash Page Type**.
4. Click **Save Settings**.

Configuring Wired Port Profiles on Instant APs

If the wired clients must be supported on the Instant Access Points (IAPs), configure wired port profiles and assign these profiles to the ports of an IAP.

The wired ports of an IAP allow third-party devices such as VoIP phones or printers (which support only wired port connections) to connect to the wireless network. You can also configure an ACL for additional security on the Ethernet downlink.

To configure wired port profiles on IAP, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.

3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Interfaces** tab.
The Interfaces page is displayed.
6. Click the **Wired** accordion.
7. To create a new wired port profile, click **+Add Port Profile**.
The Create a New Network pane is displayed.

Complete the configuration for each of the tabs in the **Create a New Network** page as described in the below sections:

Configuring General Network Profile Settings

To configure general network profile settings, complete the following steps in the **General** tab:

1. Under **General**, enter the following information:
 - a. **Name**—Enter a name.
 - b. **ports**—Select port(s) from the drop-down list.
2. Under **Advanced Settings** section, configure the following parameters:
 - a. **Speed/Duplex**—Select the appropriate value from the Speed and Duplex drop-down list. Contact your network administrator if you need to assign speed and duplex parameters.
 - b. **Port Bonding**—Turn on the **Port Bonding** toggle switch to enable port bonding.
 - c. **Power over Ethernet**—Turn on the **Power over Ethernet** toggle switch to enable PoE.
 - d. **Admin Status**—The **Admin Status** indicates if the port is up or down.
 - e. **Content Filtering**—Turn on the **Content Filtering** toggle switch to ensure that all DNS requests to non-corporate domains on this wired port network are sent to OpenDNS.
 - f. **Uplink**—Turn on the toggle switch to configure uplink on this wired port profile. If the **Uplink** toggle switch is turned on and this network profile is assigned to a specific port, the port is enabled as an uplink port.
 - g. **Spanning Tree**—Turn on the toggle switch to enable STP on the wired port profile. STP ensures that there are no loops in any bridged Ethernet network and operates on all downlink ports, regardless of forwarding mode. STP does not operate on uplink ports and is supported only on IAPs with three or more ports. By default, STP is disabled on wired port profiles.
 - h. **Inactivity Timeout**—Enter the time duration after which an inactive user needs to be disabled from the network. The user must undergo the authentication process to re-join the network.
 - i. **802.3az**—Turn on the toggle switch to enable, to support 802.3az Energy Efficient Ethernet (EEE) standard on the device. This option allows the device to consume less power during periods of low data activity. This setting can be enabled for provisioned APs or AP groups through the wired port network. If this feature is enabled for an AP group, APs in the group that do not support 802.3.az ignore this setting. This option is available for IAPs that support a minimum of Aruba Instant 8.4.0.0 firmware version.
 - j. **Deny Intra VLAN Traffic**—Turn on the toggle switch to disable intra VLAN traffic. It enables the client isolation and disable all peer-to-peer communication. Client isolation disables inter-client communication by allowing only client to gateway traffic from clients to flow in the network. All other traffic from the client that is not destined to the gateway or configured servers will not be forwarded by the Instant AP. This feature enhances the security of the network and protects it from vulnerabilities.

3. Click **Next**.

The **VLANs** details page is displayed.

Configuring VLAN Network Profile Settings

To configure VLAN settings, complete the following steps in the **VLANs** tab:

1. **Mode**—Specify any of the following modes:
 - **Access**—Select this mode to allow the port to carry a single VLAN specified as the native VLAN. If the **Access** mode is selected, perform one of the following options:
 - If the **Client IP Assignment** is set to **Virtual Controller Assigned**, proceed to step 6.
 - If the **Client IP Assignment** is set to **Network Assigned**, specify a value for **Access VLAN** to indicate the VLAN carried by the port in the **Access** mode.
 - **Trunk**—Select this mode to allow the port to carry packets for multiple VLANs specified as allowed VLANs. If the **Trunk** mode is selected:
 - Specify the **Allowed VLAN**, enter a list of comma separated digits or ranges, for example 1, 2, 5, or 1-4, or all. The Allowed VLAN refers to the VLANs carried by the port in Access mode.
 - If the **Client IP Assignment** is set to **Network Assigned**, specify a value for **Native VLAN**. A VLAN that does not have a VLAN ID tag in the frames is referred to as Native VLAN. You can specify a value within the range of 1-4093.
2. **Client IP Assignment**—specify any of the following values:
 - **Instant AP Assigned**—Select this option to allow the virtual controller to assign IP addresses to the wired clients. When the virtual controller assignment is used, the source IP address is translated for all client traffic that goes through this interface. The virtual controller can also assign a guest VLAN to a wired client. In the **Client VLAN Assignment** section, select **Default** when the client VLAN must be assigned to the native VLAN on the network. Select **Custom** to customize the client VLAN assignment to a specific VLAN, or a range of VLANs. Click the **Show Named VLANs** section to view all the named VLANs mapped to VLAN ID. Click **+Add Named VLAN** and enter the VLAN Name and VLAN ID that is required to be mapped. Clicking **OK** populates the named VLAN in the VLAN Name to VLAN ID Mapping table.
 - **External DHCP server Assigned**—Select this option to allow the clients to receive an IP address from the network to which the Virtual Controller is connected. On selecting this option, the **New** button to create a VLAN is displayed. Create a new VLAN if required.
3. Click **Next**.

The Security details page is displayed.

Configuring Security Settings

To configure security-specific settings, complete the following steps in the **Security** tab:

1. On the **Security** pane, select the following security options as per your requirement:
 - **802.1X Authentication**—Set the toggle button to enable **802.1X Authentication**. Configure the basic parameters such as the authentication server, and MAC Authentication Fail-Through. Select any of the following options for authentication server:
 - **New**—On selecting this option, an external RADIUS server must be configured to authenticate the users. For information on configuring an external server, see [Configuring External Authentication Servers for APs](#).
 - **Internal Server**—If an internal server is selected, add the clients that are required to authenticate with the internal RADIUS server. Click the **Users** link to add the users.

- **Load Balancing**—Set the toggle button to enable, if you are using two RADIUS authentication servers, so that the load across the two RADIUS servers is balanced. For more information on the dynamic load balancing mechanism, see [Dynamic Load Balancing between Authentication Servers](#).
 - **MAC Authentication**—To enable MAC authentication, enable the toggle button. The MAC authentication is disabled by default.
 - **Captive Portal**—Set the toggle button to enable captive portal authentication. For more information on configuring security on captive portal, see [Configuring Wired Networks for Guest Users on IAPs](#).
 - **Open**—Set the toggle button to enable, to set security for open network.
2. Enable the **Port Type Trusted** option to connect uplink and downlink to a trusted port only.
 3. In the **Primary Server** field, perform one of the following steps:
 - **Internal Server**—To use an internal server, select Internal Server and add the clients that are required to authenticate with the internal RADIUS Server. Click **Users** to add the users. To add a new server, click +. For information on configuring external servers, see [Configuring External Authentication Servers for APs](#).
 - **Secondary Server**—To add another server for authentication, configure another authentication server.
 - **Authentication Survivability**—If an external server is configured for authentication, you can enable authentication survivability. Specify a value in hours for Cache Timeout to set the duration after which the authenticated credentials in the cache expires. When the cache expires, the clients are required to authenticate again. You can specify a value within range of 1 to 99 hours. and the default value is 24 hours. By default, authentication survivability is disabled.
 - **Load Balancing**—Set the toggle button to enable, if you are using two RADIUS authentication servers, to balance the load across these servers. For more information on the dynamic load balancing mechanism, see [Dynamic Load Balancing between Authentication Servers](#).
 4. **MAC Authentication Fail-Thru**—Set the toggle button to enable, to attempt 802.1X authentication is attempted when the MAC authentication fails.
 5. Under the **Advance Settings** section, configure the following options:
 - **Use IP for Calling Station ID**—Set the toggle button to enable, to configure client IP address as calling station ID.
 - **Called Station ID Type**—Select one of the following options:
 - **Access Point Group**—Uses the VC ID as the called station ID.
 - **Access Point Name**—Uses the host name of the IAP as the called station ID.
 - **VLAN ID**—Uses the VLAN ID of as the called station ID.
 - **IP Address**—Uses the IP address of the IAP as the called station ID.
 - **MAC address**—Uses the MAC address of the IAP as the called station ID.



The **Called Station ID Type** detail can be configured even if the **Use IP for Calling Station ID** is set to disabled.

- **Reauth Interval**—Specify the interval at which all associated and authenticated clients must be re-authenticated.
6. Click **Next**.
The **Access** pane is displayed.

Configuring Access Settings

To configure access-specific settings, complete the following steps:

1. In the **Access** tab, turn on the **Downloadable Role** toggle switch to allow downloading of pre-existing user roles. For more information, see [Configuring Downloadable Roles](#).



NOTE

- The **Downloadable Role** feature is optional. The **Downloadable Role** feature is available only for networks that include APs that run a minimum of Aruba Instant 8.4.0.0 firmware version with a minimum of ClearPass server version 6.7.8.
- At least one radius server must be configured to apply the **Downloadable Role** feature. For more information on configuring radius server, see [Authentication Servers for IAPs](#)

2. Click the action corresponding to the server.
The **Edit Server** page is displayed.



NOTE

The **Edit Server** page displays the radius server name. The **Name** field is non-editable.

3. Enter the CPPM username along with the CPPM authentication credentials for the radius server.
4. Click **Ok**.
5. Under Access Rules, configure the following access rule parameters:
 - a. Select any of the following types of access control:
 - **Role-based**—Allows the users to obtain access based on the roles assigned to them.
 - **Unrestricted**—Allows the users to obtain unrestricted access on the port.
 - **Network-based**—Allows the users to be authenticated based on access rules specified for a network.
 - b. If the **Role-based** access control is selected:
Under **Role**, select an existing role for which you want to apply the access rules, or click **New** and add the required role. To add a new access rule, click **Add Rule** under **Access Rules For Selected Roles**.



NOTE

The default role with the same name as the network is automatically defined for each network. The default roles cannot be modified or deleted.

Configure role assignment rules. To add a new role assignment rule, click **New** under **Role Assignment Rules**. Under **New Role Assignment Rule**:

- a. Select an attribute.
 - b. Specify an operator condition.
 - c. Select a role.
 - d. Click **Save**.
6. Click **Finish** to create the wired port profile successfully.

Configuring Network Port Profile Assignment

To map the wired port profile to ethernet ports, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Interfaces** tab.
The Interfaces page is displayed.
6. Click the **Wired** accordion.
The Wired Port Profiles page is displayed.
7. In the **Port Profiles Assignments** section, assign wired port profiles to Ethernet ports:
 - a. Select a profile from the **Ethernet 0/0** drop down list.
 - b. Select the profile from the **Ethernet 0/1** drop down list.
 - c. If the IAP supports Ethernet 2, Ethernet 3 and Ethernet 4 ports, assign profiles to these ports by selecting a profile from the **Ethernet 0/2**, **Ethernet 0/3**, and **Ethernet 0/4** drop-down list respectively.
8. Click **Save Settings**.

Viewing Wired Port Profile Summary

In the **Summary** tab, the **Network Summary** page displays all the settings configured in the **General**, **VLANs**, **Security**, and **Access** tabs.

Click **Save Settings** to complete the network profile creation and save the settings.

Configuring Downloadable Roles

Aruba Central (on-premises) allows you to download pre-existing user roles when you create network profiles.



The **Downloadable Role** feature is available only for networks that include access points (APs) that run a minimum of Aruba Instant 8.4.0.0 firmware version with a minimum of ClearPass server version 6.7.8.

Aruba Instant and ClearPass Policy Manager include support for centralized policy definition and distribution.

When ClearPass Policy Manager successfully authenticates a user, the user is assigned a role by ClearPass Policy Manager. If the role is not defined on the IAP, the role attributes can also be downloaded automatically. In order to provide highly granular per-user level access, user roles can be created when a user has been successfully authenticated. During the configuration of a policy enforcement profile in ClearPass Policy Manager, the administrator can define a role that should be assigned to the user after successful authentication. In RADIUS authentication, when ClearPass Policy Manager successfully authenticates a user, the user is assigned a role by ClearPass Policy Manager.

If the role is not defined on the IAP, the role attributes can also be downloaded automatically. This feature supports roles obtained by the following authentication methods:

- 802.1X (WLAN and wired users)
- MAC authentication
- Captive Portal

This section describes the following topics:

- [ClearPass Policy Manager Certificate Validation for Downloadable Role](#)
- [Enabling Downloadable Role Feature for Wireless Networks in Aruba Central](#)
- [Enabling Downloadable Role Feature for Wired Networks in Aruba Central](#)

ClearPass Policy Manager Certificate Validation for Downloadable Role

When a ClearPass Policy Manager server is configured as the domain for RADIUS authentication for downloading user roles, in order to validate the ClearPass Policy Manager customized CA, IAPs are required to publish the root CA for the HTTPS server to the well-known URL (**http://<clearpass-fqdn>/wellknown/aruba/clearpass/https-root.pem**). The IAP must ensure that an FQDN is defined in the above URL for the RADIUS server and then attempt to fetch the trust anchor by using the RADIUS FQDN. Upon configuring the domain of the ClearPass Policy Manager server for RADIUS authentication along with a username and password, the IAP tries to retrieve the CA from the above well-known URL and store it in flash memory. However, if there is more than one ClearPass Policy Manager server configured for authentication, the CA must be uploaded manually.

Enabling Downloadable Role Feature for Wireless Networks in Aruba Central

To enable the **Downloadable Role** feature, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of access points is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the access points are displayed.
4. Click the **WLANS** tab.
The WLANS details page is displayed.
5. In the **WLANS** tab, click **+ Add SSID**.
To modify an existing SSID, select a wireless SSID from the **Wireless SSIDs** table and then click the edit icon.
6. In the **Security** tab, select the **RADIUS** server in **Primary Server** field.



At least one radius server must be configured to apply the Downloadable User Roles feature. For more information on configuring radius server, see [Authentication Servers for IAPs](#)

7. Click **Next**.
8. The **Access** tab is displayed.
9. Turn on the **Downloadable Role** toggle switch to allow downloading of pre-existing user roles. The **CPPM Settings** table with **Name**, **CPPM Username**, and **Actions** columns related to the radius servers are displayed.



-
- The **Downloadable Role** feature is available only for networks that include APs that run a minimum of Aruba InstantOS 8.4.0.0 firmware version with a minimum of ClearPass server version 6.7.8.
 - At least one radius server must be configured to apply the **Downloadable Role** feature. For more information on configuring radius server, see [Authentication Servers for IAPs](#)
-

10. Click the action corresponding to the radius server listed in the **CPM Settings** table. The **Edit Server** page is displayed.



The **Edit Server** page displays the name of the radius server name. The **Name** field is non-editable.

11. Enter the following details:
 - a. **CPM Username**—Enter the ClearPass Policy Manager admin username.
 - b. **Password**—Enter the password.
 - c. **Retype**—Retype the password.
12. Click **OK**.

Enabling Downloadable Role Feature for Wired Networks in Aruba Central

To enable the **Downloadable Role** feature, perform the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one AP. The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**. A list of access points is displayed in the **List** view.
3. Click the **Config** icon. The tabs to configure the access points are displayed.
4. Click **Show Advanced**, and click the **Interfaces** tab. The Interfaces details page is displayed.
5. Click the **Wired** accordion.
6. Under **Wired**, click **+ Add Port Profile**. To modify an existing profile, select the network that you want to edit in the **Wired Port Profiles** pane, and then click the edit icon.
7. In the **Security** tab, select the **RADIUS** server in **Primary Server** field.



At least one radius server must be configured to apply the **Downloadable Role** feature. For more information on configuring radius server, see [Authentication Servers for IAPs](#)

8. Click **Next**.
9. The **Access** tab is displayed.
10. Enable the **Downloadable Role** option to allow downloading of pre-existing user roles. The **CPM Settings** table with **Name**, **CPM Username**, and **Actions** columns related to the radius servers are displayed.



-
- The **Downloadable Role** feature is available only for networks that include APs that run a minimum of Aruba InstantOS 8.4.0.0 firmware version with a minimum of ClearPass server version 6.7.8.
 - At least one radius server must be configured to apply the **Downloadable Role** feature. For more information on configuring radius server, see [Authentication Servers for IAPs](#)
-

11. Click the action corresponding to the radius server listed in the **CPM Settings** table. The **Edit Server** page with the radius server name is displayed.



The **Edit Server** page displays the radius server name. The **Name** field is non-editable.

12. Enter the following details:
 - **CPM Username**—Enter the ClearPass Policy Manager admin username.
 - **Password**—Enter the password.
 - **Retype**—Retype the password.
13. Click **OK**.

Editing a Wireless Network Profile

To edit a network profile, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one AP. The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**. A list of access points is displayed in the **List** view.
3. Click the **Config** icon. The tabs to configure the access points are displayed.
4. Click the **WLANs** tab. The WLANs details page is displayed.
5. In the **Wireless SSIDs** table, select the network that you want to edit, and then click the edit icon under the **Actions** column.
6. Modify the profile and click **Save Settings**.



You can directly edit the SSID name under the **Display Name** column of the **Wireless SSIDs** table. Double-click the relevant SSID that you want to rename, and type the new name. Press Enter to complete the process

Editing a Wired Port Profile

To edit a network profile, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one AP.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the **Config** icon.

The tabs to configure access points are displayed.

4. Click **Show Advanced**, and click the **Interfaces** tab.
The Interfaces details page is displayed.
5. Click the **Wired** accordion.
6. In the **Wired Port Profiles** pane, select the network that you want to edit, and then click the edit icon under the **Actions** column.
7. Modify the profile and click **Save Settings**.

Deleting a Network Profile

To delete a network profile, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of access points is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the access points are displayed.
4. Click the **WLANs** tab.
The WLANs details page is displayed.
5. In the **Wireless SSIDs** table, select the network that you want to delete, and then click the delete icon under the **Actions** column.
6. Click **Yes** in the confirmation dialog box.

Aruba Mesh Network and Mesh IAP

Mesh Network Overview

The mesh solution effectively expands and configures network coverage for outdoor and indoor enterprises in a wireless environment. The mesh network automatically reconfigures broken or blocked paths when traffic traverses across mesh Instant Access Point (IAP). This feature provides increased reliability by allowing the network to continue operating even when an IAP is non-functional or if the device fails to connect to the network.



A mesh network requires at least one valid wired or 3G uplink connection. The mesh network must be provisioned by plugging into the wired network for the first time.

Mesh IAPs

The IAPs that are configured for mesh can either operate as mesh portals or as mesh points based on the uplink type.

IAP as Mesh Portal

Any provisioned IAP that has a valid wired or 3G uplink connection functions as a mesh portal. A mesh portal acts as a gateway between the wireless mesh network and the enterprise wired LAN. The mesh roles are automatically assigned based on the IAP configuration. The mesh portal can also act as a virtual controller.



The mesh portal reboots after 5 minutes, when it loses its uplink connectivity to a wired network.

IAP as Mesh Point

The IAP without an ethernet link functions as a mesh point. The mesh point establishes an all-wireless path to the mesh portal and provides traditional WLAN services such as client connectivity, IDS capabilities, user role association, and QoS for LAN-to-mesh communication to the clients, and performs mesh backhaul or network connectivity. The mesh points authenticate to the mesh portal and establish a secured link using AES encryption.



-
- A mesh point also supports LAN bridging by connecting any wired device to the downlink port of the mesh point. In the case of single ethernet port platforms such as Instant AP-105, you can convert the Eth0 uplink port to a downlink port by enabling Eth0 Bridging.
 - Redundancy is observed in a mesh network when two Instant APs have valid uplink connections, and most mesh points try to mesh directly with one of the two portals.
-

There can be a maximum of eight mesh points per mesh portal in a mesh network. When mesh IAPs boot up, they detect the environment to locate and associate with their nearest neighbor. The mesh IAPs determine the best path to the mesh portal ensuring a reliable network connectivity.



In a dual-radio, the 2.4 GHz radio is always used for client traffic, and the 5 GHz radio is always used for both mesh-backhaul and client traffic.

Automatic Mesh Role Assignment

Aruba Central (on-premises) supports enhanced role detection during IAP boot-up and IAP running time. When a mesh point discovers that the Ethernet 0 port link is up, it sends loop detection packets to check the availability of Ethernet 0 link. If the Ethernet 0 link is available, the mesh point reboots as a mesh portal. Else, the mesh point does not reboot.

Mesh Role Detection during System Boot-Up

If the ethernet link is down during Instant AP boot-up, the IAP acts as a mesh point. If the Ethernet link is up, the IAP continues to detect if the network is reachable in the following scenarios:

- In a static IP address scenario, the IAP acts as a mesh portal if it successfully pings the controller. Otherwise, it acts as a mesh point.
- In case of DHCP, the IAP acts as a mesh portal when it obtains the IP address successfully. Otherwise, it acts as a mesh point.
- In case of IPv6, IAPs do not support the static IP address but only support DHCP for detection of network reachability.



If the IAP has a 3G or 4G USB modem plugged, it always acts as a mesh portal. If the IAP is set to Ethernet 0 bridging, it always acts as a mesh point

Mesh Role Detection during System Running Time

The mesh point uses the Loop Protection for Secure Jack Port feature to detect the loop when the ethernet is up. If the loop is detected, the Instant AP reboots. Otherwise, the Instant AP does not reboot and the mesh role continues to act as a mesh point.

Setting up Instant Mesh Network

To provision Instant APs as mesh Instant APs, complete the following steps:

1. Connect the Instant APs to a wired switch.
2. Ensure that the virtual controller key is synchronized and the country code is configured.
3. Ensure that a valid SSID is configured on the Instant AP.
4. If the Instant AP has a factory default SSID (SetMeUp or Instant SSID), delete the SSID.
5. If an Extended SSID is enabled on the virtual controller, disable **Extended SSID** in the **System > General** accordion and reboot the Instant AP cluster.
6. Disconnect the Instant APs that you want to deploy as mesh points from the switch, and place the Instant APs at a remote location. The Instant APs come up without any wired uplink connection and function as mesh points. The Instant APs with valid uplink connections function as mesh portals.

Configuring Wired Bridging on Eth0 for Mesh Point

Aruba Central (on-premises) supports wired bridging on the Eth0 port of an Instant AP. You can configure wired bridging, if the Instant AP is configured to function as a mesh point.

To configure support for wired bridging on the Eth0 port of an Instant AP from Aruba Central (on-premises) UI, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select an AP group in the filter:
 - a. Set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
 - To select an AP in the filter:
 - a. Set the filter to **Global** or a group containing at least one AP.
 - b. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
 - c. Click an AP listed under **Device Name**.
The dashboard context for the AP is displayed.
 - d. Under **Manage**, click **Devices > Access Point**.
2. Click the **Config** icon.
The tabs to configure the APs are displayed.
3. Click the **Access Points** tab.
The Access Points table is displayed.
4. To edit an AP, select an AP in the **Access Points** table, and then click the edit icon.
5. Click the **Uplink** tab.

6. To configure a non-native uplink VLAN, specify the management VLAN number in the **Uplink Management VLAN** text-box.
7. From the **Eth0 Mode** drop-down list, select any of the following:
 - **Uplink**—Select this option to change the Eth0 bridging mode to the uplink port.
 - **Downlink**—Select this option to change the Eth0 bridging mode to the downlink port.
8. Click **Save Settings**.



After configuring the support for wired bridging on the Eth0 port of an Instant AP, ensure that you reboot the Instant AP.

Mesh Cluster Function

Aruba Central (on-premises) introduces the mesh cluster function for easy deployments of Instant APs. You can configure the ID, password, and also provision Instant APs to a specific mesh cluster.

In a cluster-based scenario, you can configure unlimited mesh profiles in a network. When an Instant AP boots up, it attempts to find a mesh cluster configuration. The Instant AP fetches a pre-existing mesh cluster configuration, if any. Otherwise, it uses the default mesh configuration in which the SSID, password, and cluster name are generated by the virtual controller key.



Instant APs that belong to the same mesh network can establish mesh links with each other. The Instant APs can establish a mesh link in a standalone scenario also. However, the network role election does not take place in a standalone environment. Users can set the same mesh cluster configuration to establish mesh links with other networks. For more information on mesh cluster configuration, refer to the *Mesh Instant AP Configuration* chapter of *Aruba Instant User Guide*.

Configuring Mesh for Multiple Radios

Mesh clusters are grouped and defined by a mesh cluster profile, which provides the framework of the mesh network. The mesh cluster profile contains the MSSID, authentication methods, security credentials, and cluster priority required for mesh points to associate with their neighbors and join the cluster. Associated mesh points store this information in flash memory. Although most mesh deployments require only a single mesh cluster profile, you can configure and apply multiple mesh cluster profiles to an individual AP.

To configure a mesh for multiple radios, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
The System page is displayed.
6. Click the **Mesh** accordion.
7. Select the radio band to deploy mesh network from the **Mesh Band** drop-down list.

8. Click + in the **Mesh** table.
The **Mesh** pane is displayed.
9. Configure the following parameters:

Table 59: Mesh Configuration Parameters

Data pane item	Description
Name	Name for the mesh cluster profile. Range: 8-32 characters
Key	Configures a WPA2 PSK or passphrase as the cluster key. Range: 8-64 characters
Priority	Configures the priority of the mesh cluster profile. If more than two mesh cluster profiles are configured, mesh points use this number to identify primary and backup profiles. The lower the number, the higher the priority. Range: 1–15
Opmode	Configures the operation mode. Select WPA2 PSK or WPA3 SAE from the drop-down list.

10. Click **OK**.
11. Click **Save Settings**.

Configuring ARM and RF Parameters on IAPs

This section provides the following information:

- [ARM Overview](#)
- [Configuring ARM Features](#)
- [Configuring Radio Parameters](#)

ARM Overview

ARM is a radio frequency management technology that optimizes WLAN performance even in the networks with highest traffic by dynamically and intelligently choosing the best 802.11 channel and transmitting power for each Instant Access Point (IAP) in its current RF environment. ARM works with all standard clients, across all operating systems, while remaining in compliance with the IEEE 802.11 standards. It does not require any proprietary client software to achieve its performance goals. ARM ensures low-latency roaming, consistently high performance, and maximum client compatibility in a multi-channel environment. By ensuring the fair distribution of available Wi-Fi bandwidth to mobile devices, ARM ensures that data, voice, and video applications have sufficient network resources at all times. ARM allows mixed 802.11 a, b, g, n, and ac client types to inter operate at the highest performance levels.

When ARM is enabled, an IAP dynamically scans all 802.11 channels within its 802.11 regulatory domain at regular intervals and sends reports on WLAN coverage, interference, and intrusion detection to the virtual controller. ARM computes coverage and interference metrics for each valid channel, chooses the best performing channel, and transmit power settings for each IAP RF environment. Each IAP gathers other metrics on its ARM-assigned channel to provide a snapshot of the current RF health state.

IAPs support the following ARM features:

- Channel or Power Assignment—Assigns channel and power settings for all the IAPs in the network according to changes in the RF environment.
- Voice Aware Scanning—Improves voice quality by preventing an IAP from scanning for other channels in the RF spectrum during a voice call and by allowing an IAP to resume scanning when there are no active voice calls.
- Load Aware Scanning—Dynamically adjusts the scanning behavior to maintain uninterrupted data transfer on resource intensive systems when the network traffic exceeds a predefined threshold.
- Band Steering—Assigns the dual-band capable clients to the 5 GHz band on dual-band IAPs thereby reducing co-channel interference and increasing the available bandwidth for dual-band clients.
- Client Match—Continually monitors the RF neighborhood of the client to support the ongoing band steering and load balancing of channels, and enhanced IAP reassignment for roaming mobile clients.



When Client Match is enabled on 802.11n capable IAPs, the Client Match feature overrides any settings configured for the legacy band steering, station hand-off assist or load balancing features. The 802.11ac capable IAPs do not support the legacy band steering, station hand off or load balancing settings, so these IAPs must be managed using Client Match.

- Airtime Fairness—Provides equal access to all clients on the wireless medium, regardless of client type, capability, or operating system to deliver uniform performance to all clients.

For more information on ARM features supported by the APs, see the *Aruba Instant User Guide*.

Configuring ARM Features

To configure the ARM features, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of access points is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the access points are displayed.
4. Click the **Radios** tab.
The Radios details page is displayed.
5. Under **RF > Adaptive Radio Management (ARM)**, the **Client Control** section displays the following components:
 - **Band Steering Mode**
 - **Airtime Fairness Mode**
 - **ClientMatch**
 - **ClientMatch Calculating Interval**
 - **ClientMatch Neighbor Matching**
 - **ClientMatch Threshold**
 - **ClientMatch Key**
 - **Spectrum Load Balancing Mode**
6. For **Band Steering Mode**, configure the following parameters.

Table 60: *Band Steering Mode Configuration Parameters*

Data pane item	Description
Prefer 5 GHz	Enables band steering in the 5 GHz mode. On selecting this, the IAP steers the client to the 5 GHz band (if the client is 5 GHz capable), but allows the client connection on the 2.4 GHz band if the client persistently attempts for 2.4 GHz association.
Force 5 GHz	Enforces 5 GHz band steering mode on the IAPs.
Balance Bands	Allows the IAP to balance the clients across the two radios to best utilize the available 2.4 GHz bandwidth. This feature takes into account the fact that the 5 GHz band has more channels than the 2.4 GHz band, and that the 5 GHz channels operate in 40 MHz, while the 2.5 GHz band operates in 20 MHz.
Disable	Allows the clients to select the band to use.

7. For **Airtime Fairness Mode**, specify any of the following values.

Table 61: *Airtime Fairness Mode Configuration Parameters*

Data Pane Item	Description
Default Access	Allows access based on client requests. When Airtime Fairness Mode is set to Default Access option, per user and per SSID bandwidth limits are not enforced.
Fair Access	Allocates air time evenly across all the clients.
Preferred Access	Sets a preference where 802.11n clients are assigned more air time than 802.11a/11g. The 802.11a/11g clients get more airtime than 802.11b. The ratio is 16:4:1.

8. For **ClientMatch**, configure the following parameters.

Table 62: *Client Match Configuration Parameters*

Data Pane Item	Description
Client Match	<p>Turn on the toggle switch to enable the Client Match feature on APs. When enabled, client count is balanced among all the channels in the same band. When Client Match is enabled, ensure that the Scanning option is enabled. For more information, see AP Control Configuration Parameters.</p> <p>NOTE: When Client Match is disabled, channels can be changed even when the clients are active on a BSSID. The Client Match option is disabled by default.</p>

Data Pane Item	Description
ClientMatch Calculating Interval	Configures a value for the calculating interval of Client Match . The interval is specified in seconds and the default value is 3 seconds. You can specify a value within the range of 1-600.
ClientMatch Neighbor Matching	Configures the calculating interval of Client Match . This number takes into account the least similarity percentage to be considered as in the same virtual RF neighborhood of Client Match . You can specify a percentage value within the range of 20-100. The default value is 60%.
ClientMatch Threshold	Configures a Client Match threshold value. This threshold is the maximum difference allowed in the number of associated clients between channels, radios, or channel + radios. When the client load on an AP reaches or exceeds the threshold in comparison, Client Match is enabled on that AP. You can specify a value within range of 1-20. The default value is 5.
ClientMatch Key	Enables the Client Match feature to work across different standalone IAPs in the same management VLAN. All such standalone IAPs must be set with the same Client Match key. Client Match uses the wired layer 2 protocol to synchronize information exchanged between IAPs. Users have an option to configure the Client Match keys. IAPs verify if the frames that they broadcast contain a common Client Match key. IAPs that receive these frames verify if the sender belongs to the same network or if the sender and receiver both have the same Client Match key. You can specify a value within the range of 1-2147483646.
Spectrum Load Balancing Mode	Enables the Spectrum Load Balancing mode to determine the balancing strategy for Client Match . The following options are available: <ul style="list-style-type: none"> ■ Channel—Balances client count based on each channel. ■ Radio—Balances client count based on each radio. ■ Channel + Radio—Balances client count based on each channel and each radio.

- Click **Access Point Control**, and configure the following parameters.

Table 63: AP Control Configuration Parameters

Data pane item	Description
Customize Valid Channels	Allows you to select a custom list of valid 20 MHz and 40 MHz channels for 2.4 GHz and 5 GHz bands. By default, the AP uses valid channels as defined by the Country Code (regulatory domain). On selecting Customize Valid Channels , a list of valid channels for both 2.4 GHz and 5 GHz are displayed. The valid channel customization feature is disabled by default. The valid channels automatically show in the Static Channel Assignment pane
Min Transmit Power	Allows you to configure a minimum transmission power within a range of 3 to 33 dBm in 3 dBm increments. If the minimum transmission EIRP setting configured on an AP is not supported by the AP model, this value is reduced to the highest supported power setting. The default value for minimum transmit power is 18 dBm.

Data pane item	Description
Max Transmit Power	Allows you to configure the maximum transmission power within a range of 3 to 33 dBm in 3 dBm increments. If the maximum transmission EIRP configured on an AP is not supported by the local regulatory requirements or AP model, the value is reduced to the highest supported power settings.
Client Aware	Allows ARM to control channel assignments for the IAPs with active clients. When the Client Match mode is disabled, an IAP may change to a more optimal channel, which disrupts current client traffic. The Client Aware option is enabled by default.
Scanning	Allows the IAP to dynamically scan all 802.11 channels within its 802.11 regulatory domain at regular intervals. This scanning report includes WLAN coverage, interference, and intrusion detection data. For Client Match configuration, ensure that Scanning is enabled.
Wide Channel Bands	Allows the administrators to configure 40 MHz channels in the 2.4 GHz and 5 GHz bands. 40 MHz channels are two 20 MHz adjacent channels that are bonded together. The 40 MHz channel effectively doubles the frequency bandwidth available for data transmission. For high performance, you can select 5 GHz. If the AP density is low, enable in the 2.4 GHz band.
80 MHz Support	Enables or disables the use of 80 MHz channels on APs. This feature allows ARM to assign 80 MHz channels on APs with 5 GHz radios, which support a very high throughput. This setting is enabled by default. Only the APs that support 802.11ac can be configured with 80 MHz channels.

- Click **Channel Control**, and configure the following parameters.

Table 64: Channel Control Configuration Parameters

Data pane item	Description
Backoff Time	Allows you to configure the time within a range of 10 to 3600 seconds, when an IAP backs off after requesting a new channel or power. It can increase the time window of channel interference check, and the time window of power check. The default value for minimum back off time is 240 seconds.
Free Channel Index	Allows you to check the difference in threshold in the channel interference index between the new channel and the existing channel. An IAP only moves to a new channel if the new channel has a lower interference index value than the current channel. This parameter specifies the required difference between the two interference index values before the IAP moves to the new channel. The lower this value, the more likely the IAP moves to the new channel. It has a default value of 25.
Ideal Coverage Index	Allows you to specify the ideal coverage index in the range of 2 to 20, which an IAP tries to achieve on its channel. The denser the IAP deployment, the lower this value should be. It has a default value of 10.

Data pane item	Description
Channel Quality Aware Arm Disable	Allows ARM to ignore the internally calculated channel quality metric and initiates channel changes based on thresholds defined in the profile. ARM chooses the channel based on the calculated interference index value. The option Channel Quality Aware Arm Disable is disabled by default.
Channel Quality Threshold	Allows you to specify the channel quality percentage within a range of 0 to 100, below which ARM initiates a channel change. It has a default value of 70%.
Channel Quality Wait Time	Specifies the time that the channel quality is below the channel quality threshold value to initiate a channel change. It has a range of 1 to 3600 seconds, with a default value of 120 seconds. If current channel quality is below the specified channel quality threshold for this wait time period, ARM initiates a channel change.

- Click **Error Rate**, and configure the following parameters.

Table 65: *Error Rate Configuration Parameters*

Data Pane Item	Description
Error Rate Threshold	Configures the minimum percentage of errors in the channel that triggers a channel change. It has a range of 0 to 100 % with a default value of 70%.
Error Rate Wait Time	Configures the time that the error rate has to be at least equal to the error rate threshold to trigger a channel change. The error rate must be equal to or more than the error rate threshold to trigger a channel change. It has a range of 1 to 3600 seconds, with a default value of 90 seconds.

- Click **Save Settings**.

Configuring Radio Parameters

To configure RF parameters for the 2.4 GHz and 5 GHz radio bands on an Instant Access Point (IAP), complete the following steps:

- In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
- Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
- Click the **Config** icon.
The tabs to configure the APs are displayed.
- Click the **Radios** tab.
The Radios details page is displayed.

5. Expand the **Radio** accordion in the **RF** dashboard.
6. Under **2.4 GHz band** and **5 GHz band**, configure the following parameters by clicking the **+** sign.

Table 66: *Radio Configuration Parameters*

Data Pane Item	Description
Zone	<p>Allows you to configure a zone per radio band for IAPs in a cluster. You can also configure an RF zone per IAP.</p> <p>NOTE: Aruba recommends that you configure RF zone for either individual AP or for the cluster. Any discrepancy in the RF zone names may lead to configuration errors.</p>
Legacy Only	Turn on the Legacy Only toggle switch. When enabled, the IAP runs the radio in the non-802.11n mode. This option is disabled by default.
802.11d / 802.11h	Turn on the 802.11d / 802.11h toggle switch. When enabled, the radios advertise their 802.11d (Country Information) and 802.11h (Transmit Power Control) capabilities. This option is disabled by default.
Beacon Interval	Configures the beacon period for the IAP in milliseconds. This indicates how often the 802.11 beacon management frames are transmitted by the AP. You can specify a value within the range of 60–500. The default value is 100 milliseconds.
Interference Immunity Level	<p>Configures the immunity level to improve performance in high-interference environments. The default immunity level is 2.</p> <ul style="list-style-type: none"> ■ Level 0—No ANI adaptation. ■ Level 1—Noise immunity only. This level enables power-based packet detection by controlling the amount of power increase that makes a radio aware that it has received a packet. ■ Level 2—Noise and spur immunity. This level also controls the detection of OFDM packets, and is the default setting for the Noise Immunity feature. ■ Level 3—Level 2 settings and weak OFDM immunity. This level minimizes false detects on the radio due to interference, but may also reduce radio sensitivity. This level is recommended for environments with a high-level of interference related to 2.4 GHz appliances such as cordless phones. ■ Level 4—Level 3 settings, and FIR immunity. At this level, the AP adjusts its sensitivity to in-band power, which can improve performance in environments with high and constant levels of noise interference. ■ Level 5—The AP completely disables PHY error reporting, improving performance by eliminating the time the IAP spends on PHY processing. Increasing the immunity level makes the AP lose a small amount of range.
Channel Switch Announcement Count	Configures the number of channel switching announcements to be sent before switching to a new channel. This allows the associated clients to recover gracefully from a channel change.
Background Spectrum Monitoring	Turn on the Background Spectrum Monitoring toggle switch. When enabled, the APs in the access mode continue with their normal access service to clients, while performing additional function of monitoring RF interference (from both neighboring APs and non Wi-Fi sources such as, microwaves and cordless phones) on the channel they are currently serving the clients.

Table 66: Radio Configuration Parameters

Data Pane Item	Description
Customize ARM Power Range	Configures a minimum (Min Power) and maximum (Max Power) power range value for the 2.4 GHz and 5 GHz band frequencies. The default value is 3 dBm. Unlike the configuration in the ARM profile, the transmit power of all radios in the Radio profile do not share the same configuration.
Enable 11ac	Turn on the Enable 11ac toggle switch. When enabled, VHT is enabled on the 802.11ac devices for the 5 GHz radio band. If VHT is enabled for the 5 GHz radio profile on an IAP, it is automatically enabled for all SSIDs configured on an IAP. By default, VHT is enabled on all SSIDs. NOTE: If you want the 802.11ac IAPs to function as 802.11n IAPs, clear this check box to disable VHT on these devices.
Smart antenna	Turn on the Smart antenna toggle switch to combine an antenna array with a digital signal-processing capability to transmit and receive in an adaptive, spatially sensitive manner.
ARM/WIDS Override	When ARM/WIDS Override is disabled, the Instant AP will always process frames for WIDS. WIDS is an application that detects the attacks on a wireless network or wireless system. purposes even when it is heavily loaded with client traffic. When ARM/WIDS Override is enabled, the Instant AP will stop processing frames for WIDS.

7. Click **Save Settings**.

Configuring IDS Parameters on APs

Aruba Central supports the IDS feature that monitors the network for the presence of unauthorized access points (APs). It also logs information about the unauthorized APs and clients, and generates reports based on the logged information.

Rogue APs

The IDS feature in the Aruba Central network enables you to detect rogue APs, interfering APs, and other devices that can potentially disrupt network operations. A rogue AP is an unauthorized AP plugged into the wired side of the network. An interfering AP is an AP seen in the RF environment, but it is not connected to the wired network. While the interfering AP can potentially cause RF interference, it is not considered a direct security threat, because it is not connected to the wired network. However, an interfering AP may be reclassified as a rogue AP.

The built-in IDS scans for APs that are not controlled by the VC. These are listed and classified as either Interfering or Rogue, depending on whether they are on a foreign network or your network.

Configuring Wireless Intrusion Detection and Protection Policies

To configure a Wireless Intrusion Detection and Protection policy:

1. In the **Network Operations** app, set the filter to a group that contains at least one AP.
2. The dashboard context for the group is displayed.
3. Under **Manage**, click **Devices > Access Points**.
4. Click the **Config** icon. The tabs to configure access points is displayed.

5. Click **Show Advanced**.
6. Click **Security**. The **Security** details page is displayed.
7. Click the **Wireless IDS/IPS** accordion. The following three sections are displayed:
 - **Detection**
 - **Protection**
 - **Firewall Settings**

You can configure the following options in the above mentioned sections:

- **Infrastructure Detection Policies**—Specifies the policy for detecting wireless attacks on APs.
- **Client Detection Policies**—Specifies the policy for detecting wireless attacks on clients.
- **Infrastructure Protection Policies**—Specifies the policy for protecting APs from wireless attacks.
- **Client Protection Policies**—Specifies the policy for protecting clients from wireless attacks.
- **Firewall Policies**—Specifies the policies to set a firewall for a secured network access.
- **Containment Methods**—Prevents unauthorized stations from connecting to your Aruba Central network.

Each of these options contains several default levels that enable different sets of policies. An administrator can customize enable or disable these options accordingly.

Detection

The detection levels can be configured using the **Detection** section. The following levels of detection can be configured in the WIP Detection page:

- **High**
- **Medium**
- **Low**
- **Off**
- **Custom**

The following table describes the detection policies enabled in the Infrastructure Detection field.

Table 67: *Infrastructure Detection Policies*

Detection level	Detection policy
Off	All detection policies are disabled.
Low	<ul style="list-style-type: none"> ■ Detect Windows Bridge—Enables detection of Windows station bridging. ■ Signature Deassociation Broadcast—Configures signature matching for the deassociation broadcast frame type. ■ Signature Deauthentication Broadcast—Configures signature matching for the deauthentication broadcast frame type. ■ Detect AP Spoofing—Enables AP Spoofing detection.
Medium	<ul style="list-style-type: none"> ■ Detect Windows Bridge—Enables detection of Windows station bridging. ■ Signature Deassociation Broadcast—Configures signature matching for the deassociation broadcast frame type.

Table 67: Infrastructure Detection Policies

Detection level	Detection policy
	<ul style="list-style-type: none"> ■ Signature Deauthentication Broadcast—Configures signature matching for the deauthentication broadcast frame type. ■ Detect AP Spoofing—Enables AP Spoofing detection. ■ Detect adhoc using VALID SSID—Enables detection of adhoc networks. ■ Detect malformed large duration—Enables detection of unusually large durations in frames.
High	<ul style="list-style-type: none"> ■ Detect Windows Bridge—Enables detection of Windows station bridging. ■ Signature Deassociation Broadcast—Configures signature matching for the deassociation broadcast frame type. ■ Signature Deauthentication Broadcast—Configures signature matching for the deauthentication broadcast frame type. ■ Detect AP Spoofing—Enables AP Spoofing detection. ■ Detect adhoc using VALID SSID—Enables detection of adhoc networks. ■ Detect malformed large duration—Enables detection of unusually large durations in frames. ■ Detect Overflow EAPOL key—Enables detection of overflow EAPOL key requests. ■ Detect Invalid Address Combination—Enables detection of invalid address combinations. ■ Detect AP Impersonation—Enables detection of AP impersonation. In AP impersonation attacks, the attacker sets up an AP that assumes the BSSID and ESSID of a valid AP. AP impersonation attacks can be done for man-in-the-middle attacks, a rogue AP attempting to bypass detection, or a honeypot attack. ■ Detect AP Flood—Enables detection of flooding with fake IAP beacons to confuse the legitimate users and to increase the amount of processing needed on client operating systems. ■ Detect Beacon Wrong Channel—Enables detection of beacons advertising the incorrect channel. ■ Detect ht Greenfield—Enables detection of high throughput devices advertising greenfield preamble capability. ■ Detect Overflow IE—Enables detection of overflow Information Elements (IE). ■ Detect RTS Rate Anomaly—Enables detection of rate anomalies. ■ Detect Malformed HT IE—Enables detection of malformed HT Information Elements (IE). ■ Detect CTS Rate Anomaly—Enables detection of CTS rate anomaly. ■ Detect Malformed Frame Auth—Enables detection of malformed authentication frames. ■ Detect invalid MAC OUI—Enables checking of the first three bytes of a MAC address, known as the organizationally unique identifier (OUI), assigned by the IEEE to known manufacturers. Often clients using a spoofed MAC address do not use a valid OUI and instead use a randomly generated MAC address. Enabling MAC OUI check triggers an alarm to be triggered if an unrecognized MAC address is in use. ■ Detect Malformed Association Request—Enables detection of malformed association requests. ■ Detect Bad WEP—Enables detection of WEP initialization vectors that are known to be weak and/or repeating. A primary means of cracking WEP keys is to capture 802.11 frames over an extended period of time and search for implementations that are still used by many legacy devices. ■ Detect Wireless Bridge—Enables detection of wireless bridging.

Table 67: Infrastructure Detection Policies

Detection level	Detection policy
	<ul style="list-style-type: none"> ■ Detect HT 40 MHz intolerance—Enables detection of 802.11n 40 MHz intolerance setting when the stations and APs advertise 40 MHz intolerance. ■ Detect Valid SSID Misuse—Enables detection of interfering or neighbor APs using valid or protected SSIDs. ■ Detect Adhoc Network—Enables detection of adhoc networks. ■ Detect Client Flood—Enables detection of client flood attack.
Custom	Allows you to select custom detection policies. To select, click the check box of respective detection policy.

The following table describes the detection policies enabled in the Client Detection field.

Table 68: Client Detection Policies

Detection level	Detection policy
Off	All detection policies are disabled.
Low	<p>Detect Valid Client Misassociation—Enables detection of misassociation between a valid client and an unsafe AP. This setting can detect the following misassociation types:</p> <ul style="list-style-type: none"> ■ Misassociation to rogue AP ■ Misassociation to external AP ■ Misassociation to honeypot AP ■ Misassociation to adhoc AP ■ Misassociation to Hosted AP
Medium	<ul style="list-style-type: none"> ■ Detect Valid Client Misassociation—Enables detection of misassociation between a valid client and an unsafe AP. This setting can detect the following misassociation types: <ul style="list-style-type: none"> ○ Misassociation to rogue AP ○ Misassociation to external AP ○ Misassociation to honeypot AP ○ Misassociation to adhoc AP ○ Misassociation to Hosted AP ■ Detect Hotspotter Attack—Enables detection of hotspot attacks. ■ Detect Power Save DOS Attack—Enables detection of Power Save DoS attack. ■ Detect Omerta Attack—Enables detection of Omerta attack. ■ Detect Disconnect Station—Enables a station disconnection attack. In a station disconnection, attacker spoofs the MAC address of either an active client or an active AP. The attacker then sends deauthenticate frames to the target device, causing it to lose its active association. ■ Detect unencrypted Valid —Enables detection of unencrypted valid clients. ■ Detect Block ACK Attack—Enables detection of attempts to reset traffic receive windows using the forged Block ACK Add messages. ■ Detect FATA-Jack—Enables detection of fatjack attacks.
High	<ul style="list-style-type: none"> ■ Detect Valid Client Misassociation—Enables detection of misassociation between a valid

Detection level	Detection policy
	<p>client and an unsafe AP. This setting can detect the following misassociation types:</p> <ul style="list-style-type: none"> ○ Misassociation to rogue AP ○ Misassociation to external AP ○ Misassociation to honeypot AP ○ Misassociation to adhoc AP ○ Misassociation to Hosted AP <ul style="list-style-type: none"> ■ Detect Hotspotter Attack—Enables detection of hotspot attacks. ■ Detect Power Save DOS Attack—Enables detection of Power Save DoS attack. ■ Detect Omerta Attack—Enables detection of Omerta attack. ■ Detect Disconnect Station—Enables a station disconnection attack. In a station disconnection, attacker spoofs the MAC address of either an active client or an active AP. The attacker then sends deauthenticate frames to the target device, causing it to lose its active association. ■ Detect unencrypted Valid —Enables detection of unencrypted valid clients. ■ Detect Block ACK Attack—Enables detection of attempts to reset traffic receive windows using the forged Block ACK Add messages. ■ Detect FATA-Jack—Enables detection of fatjack attacks. ■ Detect Rate Anomalies—Enables detection of rate anomalies. ■ Detect ChopChop Attack—Enables detection of ChopChop attack. ■ Detect EAP Rate Anomaly—Enables Extensible Authentication Protocol (EAP) handshake analysis to detect an abnormal number of authentication procedures on a channel and generate an alarm when this condition is detected. ■ Detect TKIP Replay Attack—Enables detection of TKIP replay attack. ■ Signature-Air Jack—Enables signature matching for the Air Jack frame type. ■ Signature-ASLEAP—Enables signature matching for the ASLEAP frame type.
Custom	Allows you to select custom detection policies. To select, click the check box of respective detection policy.

Protection

The following levels of detection can be configured in the WIP Protection page:

- **Off**
- **Low**
- **High**
- **Custom**

The following table describes the protection policies that are enabled in the Infrastructure Protection field.

Table 69: *Infrastructure Protection Policies*

Protection level	Protection policy
Off	All protection policies are disabled
Low	<ul style="list-style-type: none"> ■ Protect SSID—Enforces policy where the valid/protected SSIDs are used only by valid APs.

Protection level	Protection policy
	<p>An offending AP is contained by preventing clients from associating to it.</p> <ul style="list-style-type: none"> ■ Rogue Containment—Controls Rogue APs. When rogue APs are detected, they are not automatically disabled. This option automatically disables a rogue AP by preventing clients from associating to it.
High	<ul style="list-style-type: none"> ■ Protect SSID—Enforces policy where the valid/protected SSIDs are used only by valid APs. An offending AP is contained by preventing clients from associating to it. ■ Rogue Containment—Controls Rogue APs. When rogue APs are detected, they are not automatically disabled. This option automatically disables a rogue AP by preventing clients from associating to it. ■ Protect AP Impersonation—Enables protection from AP impersonation attacks. When AP impersonation is detected, both the legitimate and impersonating AP are disabled using a Denial of Service (DoS). ■ Protect from Adhoc Networks—Enables protection from adhoc networks. When adhoc networks are detected, they are disabled using a denial of service attack.
Custom	Allows you to select custom detection policies. To select, click the check box of respective protection policy.

The following table describes the detection policies that are enabled in the Client Protection field.

Table 70: *Client Protection Policies*

Protection level	Protection policy
Off	All protection policies are disabled
Low	Protect Valid Station —Enables protection of valid stations. When enabled valid stations are not allowed to connect to an invalid AP.
High	<ul style="list-style-type: none"> ■ Protect Valid Station—Enables protection of valid stations. When enabled valid stations are not allowed to connect to an invalid AP. ■ Protect Windows Bridge—Enables protection of a Windows station bridging.
Custom	Allows you to select custom detection policies. To select, click the check box of respective protection policy.

Containment Methods

You can enable wired and wireless containment measures to prevent unauthorized stations from connecting to your Aruba Central network.

Aruba Central supports the following types of containment mechanisms:

- **Wired containment** — When enabled, APs generate ARP packets on the wired network to contain wireless attacks.
- **Wireless containment** — When enabled, the system attempts to disconnect all clients that are connected or attempting to connect to the identified AP.

- **None** — Disables all the containment mechanisms.
- **Deauthenticate only** — With deauthentication containment, the AP or client is contained by disrupting the client association on the wireless interface.
- **Tarpit containment** — With tarpit containment, the AP is contained by luring clients that are attempting to associate with it to a tarpit. The tarpit can be on the same channel or a different channel as the AP being contained.
- **Tarpit all stations**—Enables wireless containment by tarpit for all stations.



The FCC and some third parties have alleged that under certain circumstances, the use of containment functionality violates 47 U.S.C. §333. Before using any containment functionality, ensure that your intended use is allowed under the applicable rules, regulations, and policies. Aruba is not liable for any claims, sanctions, or other direct, indirect, special, consequential or incidental damages related to your use of containment functionality.

Protection Against Wired Attacks

In the **Protection Against Wired Attacks** section, enable the following options:

- **Drop Bad ARP**—Drops the fake ARP packets.
- **Fix Malformed DHCP**—Fixes the malformed DHCP packets.
- **ARP Poison Check**—Triggers an alert on ARP poisoning caused by the rogue APs.

Firewall Settings

To configure firewall settings by specifying the policies for a secured network access, see [Enabling ALG Protocols on IAPs on page 305](#) and [Configuring Firewall Parameters for Wireless Network Protection](#).



-
- For all subnets, a deny rule is created by default as the last rule. If at least one rule is configured, the deny all rule is applied to the upstream traffic by default.
 - Management access to the Instant AP is allowed irrespective of the inbound firewall rule.
 - The inbound firewall is not applied to traffic coming through the GRE tunnel.
-

Configuring Time-Based Services for Wireless Network Profiles

Aruba Central (on-premises) allows you to configure the availability of a WLAN SSID at a particular time of the day. You can now create a time range profile and assign it to a WLAN SSID, so that you can enable or disable access to the SSID and thus control user access to the network during a specific time period.

Instant Access Points (IAPs) support the configuration of both absolute and periodic time range profiles. You can configure an absolute time range profile to execute during a specific time frame, or create a periodic profile to execute at regular intervals based on the periodicity specified in the configuration.

This section describes the following topics:

- [Creating a Time Range Profile](#)
- [Associating a Time Range Profile to an SSID](#)
- [Associating a Time Range Profile to ACL](#)

Before You Begin

Before you configure time-based services, ensure that the NTP server connection is active.

Creating a Time Range Profile

To create a time range profile, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
The System page is displayed.
6. Click the **Time-Based Services** accordion.
7. Click + in the **Time Based Profiles** table.
The **New Profile** window for creating a time range profile is displayed.
8. Configure the parameters that are listed in the following table:

Table 71: Time Range Profile Configuration Parameters

Parameter	Description
Name	Specify a name for the time range profile.
Type	Select the type of time range profile: <ul style="list-style-type: none">■ Periodic—Allows you configure a specific periodicity and recurrence pattern for a time range profile.■ Absolute—Allows you to configure an absolute day and time range.
Repeat	Specify the frequency for the periodic time range profile: <ul style="list-style-type: none">■ Daily—Enables daily recurrence.■ Weekly—Allows you define a specific time range with specific start and end days in a week.
Day Range	<p>Absolute For an absolute time range profile, this field allows you to specify the start day and end day, both in mm/dd/yyyy format. You can also use the calendar to specify the start and end days.</p> <p>Periodic For a periodic time range profile, the following Day Range options are available:</p> <ul style="list-style-type: none">■ For daily recurrence—If the Repeat option is set to Daily, this field allows you to select the following time ranges:<ul style="list-style-type: none">○ Monday—Sunday (All Days)○ Monday—Friday (Weekdays)○ Saturday—Sunday (Weekend) <p>For example, if you set the Repeat option to Daily and then select Monday—Friday (Weekday) for Day Range, and Start Time as 1 and End time as 2, the applied time range will be Monday to Friday from 1 am to 2 am; that is, on Monday at 3 am, the profile will not be applied or disabled.</p> <ul style="list-style-type: none">■ For weekly occurrence—If the Repeat option is set to Weekly, this field

Table 71: Time Range Profile Configuration Parameters

Parameter	Description
	allows you to select the start and end days of a week and time range. For example, if you set Start Day as Monday and End Day as Friday, and Start Time as 1 and End Time as 2, the applied time range profile is Monday 1 am to Friday 2 am every week; that is, on Monday at 3 am, the profile will be applied or enabled.
Start Time	Select the start time for the time range profile from the Hours and Minutes drop-down lists, respectively.
End Time	Select the end time for the time range profile from the Hours and Minutes drop-down lists, respectively.
Visualization Graph for Time	The Visualization graph (approximated to the hour) provides a visual display of the selected time range (Day Range, Start Time, and End Time) for periodic profiles.

Associating a Time Range Profile to an SSID

To apply a time range profile to an SSID, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click the **WLANS** tab.
The WLANS details page is displayed.
5. In the **Wireless SSIDs** table, select a network profile for which you want to apply the time range profile, and then click the edit icon. You can also add a time range profile when configuring an SSID.
6. In **General**, click **Time Range Profiles** under **Advanced Settings**.
7. In the **Time Range Profiles** section, enter the following information:
 - Select a time range profile from the **Time Range Profile** list.
 - Select a value from the **Status** drop-down list.
 - When a time range profile is enabled on SSID, the SSID is made available to the users for the configured time range. For example, if the specified time range is 12:00 to 13:00, the SSID becomes available only between 12 PM to 1 PM on a given day.
 - If a time range is disabled, the SSID becomes unavailable for the configured time range. For example, if configured time-range is 14:00 to 17:00, the SSID is made unavailable from 2 PM to 5 PM on a given day.

Associating a Time Range Profile to ACL

Aruba Central allows you to configure time-based services for specific ACL. To apply a time range profile to an access rule, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.

2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
The Security page is displayed.
6. In the **Roles** accordion, click the edit icon listed for access rules under **Access Rules For Selected Roles** to which you want to apply the time range profile.
The Access Rules page is displayed.
7. In the **Options** section, select the **Time Range** check-box and select the time range profile from the drop-down list.
 - When a time range profile is associated with an ACL, the configured time range is applied on all the WLAN SSID with the specific ACL.
 - If a time range is disabled or if the time range profile is deleted for an ACL, all WLAN SSID with the specific ACL will be able to access the network without any time constraint.
8. Click **Save**.

For more information on time range configuration, see the *Aruba Instant User Guide*.

Configuring Authentication and Security Profiles on IAPs

This section describes the authentication and security parameters to configure on an Instant Access Point (IAP):

- [Supported Authentication Methods](#)
- [Authentication Servers for IAPs](#)
- [Denylisting IAP Clients](#)
- [Configuring Network Service ACLs](#)
- [Enabling ALG Protocols on IAPs](#)
- [Configuring External Authentication Servers for APs](#)
- [Configuring Role Derivation Rules for AP Clients](#)
- [Configuring Firewall Parameters for Wireless Network Protection](#)
- [Intra VLAN Traffic Allowlist](#)
- [Configuring an MPSK Local Profile](#)
- [Creating a Role Derivation Rules for AP Clients](#)
- [Configuring User Roles for AP Clients](#)
- [Configuring Firewall Parameters for Inbound Traffic](#)
- [Firewall and ACL Rules](#)
- [Configuring Roles and Policies on IAPs for User Access Control](#)
- [Support for Multiple PSK in WLAN SSID](#)
- [Configuring WPA3 Encryption](#)

Supported Authentication Methods

Authentication is a process of identifying a user through a valid username and password. Clients can also be authenticated based on their MAC addresses.

The authentication methods supported by the Instant Access Points (IAPs) managed through Aruba Central (on-premises) are described in the following sections.

802.1X Authentication

802.1X is a method for authenticating the identity of a user before providing network access to the user. The Aruba Central (on-premises) network supports internal RADIUS server and external RADIUS server for 802.1X authentication. For authentication purpose, the wireless client can associate to a NAS or RADIUS client such as a wireless IAP. The wireless client can pass data traffic only after successful 802.1X authentication.



The NAS acts as a gateway to guard access to a protected resource. A client connecting to the wireless network first connects to the NAS.

Configuring 802.1X Authentication for a Network Profile

To configure 802.1X authentication for a wireless network profile, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click the **WLANS** tab.
The WLANs details page is displayed.
5. In the **Wireless SSIDs** table, select a network profile for which you want to enable 802.1X authentication, and then click the edit icon.



You can directly edit the SSID name under the **Display Name** column in the **Wireless SSIDs** table. Double-click the relevant SSID that you want to rename, and type the new name. Press Enter to complete the process.

6. Under **Security**, for the **Enterprise** security level, select the preferred option from **Key Management**.
7. To terminate the EAP portion of 802.1X authentication on the IAP instead of the RADIUS server, set **Termination** to **Enabled**.
For 802.1X authorization, by default, the client conducts an EAP exchange with the RADIUS server, and the AP acts as a relay for this exchange. When **Termination** is enabled, the IAP itself acts as an authentication server, terminates the outer layers of the EAP protocol, and only relays the innermost layer to the external RADIUS server.
8. Specify the type of authentication server to use.
9. Click **Save Settings**.

MAC Authentication

MAC authentication is used for authenticating devices based on their physical MAC addresses. MAC authentication requires that the MAC address of a machine matches a manually defined list of addresses.

This authentication method is not recommended for scalable networks and the networks that require stringent security settings.

MAC authentication can be used alone or it can be combined with other forms of authentication such as WEP authentication.

Configuring MAC Authentication for a Network Profile

To configure MAC authentication for a wireless profile, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click the **WLANS** tab.
The WLANS details page is displayed.
5. In the **WLANS** tab, select a network profile for which you want to enable MAC authentication and click the edit icon.
6. In **Security**, turn on the **MAC Authentication** toggle switch to enable **Personal** or **Open** security level.
7. Specify the type of authentication server to use.
8. Click **Save Settings**.

MAC Authentication with 802.1X Authentication

The administrators can enable MAC authentication for 802.1X authentication. MAC authentication shares all the authentication server configurations with 802.1X authentication. If a wireless or wired client connects to the network, MAC authentication is performed first. If MAC authentication fails, 802.1X authentication does not trigger. If MAC authentication is successful, 802.1X authentication is attempted. If 802.1X authentication is successful, the client is assigned an 802.1X authentication role. If 802.1X authentication fails, the client is assigned a **deny-all** role or **mac-auth-only** role.

You can also configure the following authentication parameters for MAC+802.1X authentication:

- **MAC authentication only**—Allows you to create a **mac-auth-only** role to allow role-based access rules when MAC authentication is enabled for 802.1X authentication. The **mac-auth-only** role is assigned to a client when the MAC authentication is successful and 802.1X authentication fails. If 802.1X authentication is successful, the **mac-auth-only** role is overwritten by the final role. The **mac-auth-only** role is primarily used for wired clients.
- **L2 authentication fall-through**—Allows you to enable the **l2-authentication-fallthrough** mode. When this option is enabled, the 802.1X authentication is allowed even if the MAC authentication fails. If this option is disabled, 802.1X authentication is not allowed. The **l2-authentication-fallthrough** mode is disabled by default.

Configuring MAC Authentication with 802.1X Authentication

To configure MAC authentication with 802.1X authentication for wireless network profile, configure the following parameters:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click the **WLANS** tab.
The WLANS details page is displayed.
5. In the **WLANS** tab, select a network profile for which you want to enable MAC and 802.1X authentication and click the edit icon.
6. Turn on the **Perform MAC Authentication Before 802.1X** toggle switch to use 802.1X authentication only when the MAC authentication is successful.
7. Turn on the **MAC Authentication Fail Through** toggle switch to use 802.1X authentication even when the MAC authentication fails.
8. Click **Save Settings**.

Captive Portal Authentication

Captive portal authentication is used for authenticating guest users. For more information, see [Configuring Wireless Networks for Guest Users on IAPs](#).

MAC Authentication with Captive Portal Authentication

The following conditions apply to a network profile with MAC authentication and Captive Portal authentication enabled:

- If the captive portal splash page type is **Internal-Authenticated** or **External-RADIUS Server**, MAC authentication reuses the server configurations.
- If the captive portal splash page type is **Internal-Acknowledged** or **External-Authentication Text** and MAC authentication is enabled, a server configuration page is displayed.
- If the captive portal splash page type is **None**, MAC authentication is disabled.
- The MAC authentication with captive portal authentication supports the **mac-auth-only** role.

Configuring MAC Authentication with Captive Portal Authentication

To configure the MAC authentication with captive portal authentication for a network profile, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one AP. The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**. A list of access points is displayed in the **List** view.
3. Click the **Config** icon. The tabs to configure the access points are displayed.
4. Click the **WLANS** tab. The WLANS details page is displayed.
5. In the **WLANS** tab, select an existing wireless profile for which you want to enable MAC authentication with captive portal authentication, and then click the edit icon.
6. Under **Access**, specify the following parameters for a network with **Role Based** rules:
 - a. Turn on the **Enforce Machine Authentication** toggle switch, when MAC authentication is enabled for captive portal. If the MAC authentication fails, the captive portal authentication role

is assigned to the client.

- b. For wireless network profile, turn on the **Enforce MAC Auth Only Role** toggle switch, when MAC authentication is enabled for captive portal. After successful MAC authentication, the **MAC Auth Only** role is assigned to the client.

7. Click **Next**.

802.1X Authentication with Captive Portal Authentication

This authentication method allows you to configure different captive portal settings for clients on the same SSID. For example, you can configure an 802.1X SSID and create a role for captive portal access, so that some of the clients using the SSID derive the captive portal role. You can configure rules to indicate access to external or internal Captive portal, or none.

For more information on configuring captive portal roles for an SSID with 802.1X authentication, see [Configuring Wireless Networks for Guest Users on IAPs](#).

WISPr Authentication

WISPr authentication allows a smart client to authenticate on the network when they roam between wireless Internet service providers, even if the wireless hotspot uses an ISP with whom the client may not have an account.

If a hotspot is configured to use WISPr authentication in a specific ISP and a client attempts to access the Internet at that hotspot, the WISPr AAA server configured for the ISP authenticates the client directly and allows the client to access the network. If the client only has an account with a *partner* ISP, the WISPr AAA server forwards the client's credentials to the partner ISP's WISPr AAA server for authentication. When the client is authenticated on the partner ISP, it is also authenticated on your hotspot own ISP as per their service agreements. The IAP assigns the default WISPr user role to the client when your ISP sends an authentication message to the IAP.

IAPs support the following smart clients:

- iPass
- Boingo

These smart clients enable client authentication and roaming between hotspots by embedding iPass Generic Interface Specification (GIS) *redirect*, *authentication*, and *logoff* messages within HTML messages that are sent to the IAP.

Configuring WISPr Authentication

To configure WISPr authentication, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
The System page is displayed.

6. Click the **WISPr** accordion.
7. Under **WISPr**, configure the following parameters:
 - **ISO Country Code**—The ISO Country Code for the WISPr Location ID.
 - **E.164 Area Code**—The E.164 Area Code for the WISPr Location ID.
 - **Operator Name**—The operator name of the hotspot.
 - **E.164 Country Code**—The E.164 Country Code for the WISPr Location ID.
 - **SSID/Zone**—The SSID/Zone for the WISPr Location ID.
 - **Location Name**—Name of the hotspot location. If no name is defined, the name of the IAP, to which the user is associated, is used.
8. Click **Save Settings**.

The WISPr RADIUS attributes and configuration parameters are specific to the RADIUS server used by your ISP for the WISPr authentication. Contact your ISP to determine these values. You can find a list of ISO and ITU country and area codes at the ISO and ITU websites (www.iso.org and <http://www.itu.int>).



A Boingo smart client uses a NAS identifier in the format <CarrierID>_<VenueID> for location identification. To support Boingo clients, ensure that you configure the NAS identifier parameter in the RADIUS server profile for the WISPr server.

Walled Garden

On the Internet, a walled garden typically controls access to web content and services. The Walled garden access is required when an external captive portal is used. For example, a hotel environment where the unauthenticated users are allowed to navigate to a designated login page (for example, a hotel website) and all its contents.

The users who do not sign up for the Internet service can view the allowed websites (typically hotel property websites). The website names must be DNS-based and support the option to define wildcards. When a user attempts to navigate to other websites that are not in the allowlist of the walled garden profile, the user is redirected to the login page. IAP supports Walled Garden only for the HTTP requests. For example, if you add yahoo.com in Walled Garden allowlist and the client sends an HTTPS request (<https://yahoo.com>), the requested page is not displayed and the users are redirected to the captive portal login page.

In addition, a denylisted walled garden profile can also be configured to explicitly block the unauthenticated users from accessing some websites.

Configuring Walled Garden Access

To configure walled garden access, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
The Security page is displayed.

6. Click the **Walled Garden** accordion.
7. To allow access to a specific set of websites, click + under **Allowlist**, enter the domain name in the window. This allows access to a domain while the user remains unauthenticated. Specify a POSIX regular expression (regex(7)). For example:
 - yahoo.com matches various domains such as news.yahoo.com, travel.yahoo.com and finance.yahoo.com
 - www.apple.com/library/test is a subset of www.apple.com site corresponding to path /library/test/*
 - favicon.ico allows access to /favicon.ico from all domains.
8. To deny users access to a domain, click + under **Denylist**, and enter the domain name in the window. This prevents the unauthenticated users from viewing specific websites. When a URL specified in the denylist is accessed by an unauthenticated user, IAP sends an HTTP 403 response to the client with an error message.
9. Click **Save Settings**.

Authentication Servers for IAPs

Based on the security requirements, you can configure internal or external RADIUS servers. This section describes the types of authentication servers and authentication termination, that can be configured for a network profile.

External RADIUS Server

In the external RADIUS server, the IP address of the Virtual Controller (VC) is configured as the NAS IP address. Aruba Central RADIUS is implemented on the VC, and this eliminates the need to configure multiple NAS clients for every Instant Access Points (IAPs) on the RADIUS server for client authentication. Aruba Central RADIUS dynamically forwards all the authentication requests from a NAS to a remote RADIUS server. The RADIUS server responds to the authentication request with an **Access-Accept** or **Access-Reject** message, and users are allowed or denied access to the network depending on the response from the RADIUS server.

When you enable an external RADIUS server for the network, the client on the IAP sends a RADIUS packet to the local IP address. The external RADIUS server then responds to the RADIUS packet.

Aruba Central (on-premises) supports the following external authentication servers:

- RADIUS
- LDAP

To use an LDAP server for user authentication, configure the LDAP server on the VC, and configure user IDs and passwords.

To use a RADIUS server for user authentication, configure the RADIUS server on the VC.

RADIUS Server Authentication with VSA

An external RADIUS server authenticates network users and returns to the IAP the VSA that contains the name of the network role for the user. The authenticated user is placed into the management role specified by the VSA.

Internal RADIUS Server

Each IAP has an instance of free RADIUS server operating locally. When you enable the internal RADIUS server option for the network, the client on the IAP sends a RADIUS packet to the local IP address. The

internal RADIUS server listens and replies to the RADIUS packet.

The following authentication methods are supported in the Aruba Central network:

- **EAP-TLS**—The EAP-TLS method supports the termination of EAP-TLS security using the internal RADIUS server. The EAP-TLS requires both server and CA certificates installed on the IAP. The client certificate is verified on the virtual controller (the client certificate must be signed by a known CA), before the username is verified on the authentication server.
- **EAP-TTLS (MSCHAPv2)**—The EAP-TTLS method uses server-side certificates to set up authentication between clients and servers. However, the actual authentication is performed using passwords.
- **EAP-PEAP (MSCHAPv2)**—EAP-PEAP is an 802.1X authentication method that uses server-side public key certificates to authenticate clients with server. The PEAP authentication creates an encrypted SSL / TLS tunnel between the client and the authentication server. Exchange of information is encrypted and stored in the tunnel ensuring the user credentials are kept secure.
- **LEAP**—LEAP uses dynamic WEP keys for authentication between the client and authentication server.

To use the internal database of an AP for user authentication, add the names and passwords of the users to be authenticated.



Aruba does not recommend the use of LEAP authentication because it does not provide any resistance to network attacks.

RADIUS Communication over TLS (RadSec)

RADIUS over TLS, also known as RadSec, is a RADIUS protocol that uses TLS protocol for end-to-end secure communication between the RADIUS server and IAP. RadSec wraps the entire RADIUS packet payload into a TLS stream. Enabling RadSec increases the level of security for authentication that is carried out across the cloud network. When configured, this feature ensures that the RadSec protocol is used for safely transmitting the authentication and accounting data between the IAP and the RadSec server.

The following conditions applies to RadSec configuration:

- The RADIUS packets go through the tunnel when TLS tunnel is established.
- By default, the TCP port 2083 is assigned for RadSec. Separate ports are not used for authentication, accounting, and dynamic authorization changes.
- Aruba Central supports dynamic CoA (RFC 3576) over RadSec and the RADIUS server uses an existing TLS connection opened by the IAP to send the request.
- By default, the IAP uses its device certificate to establish a TLS connection with RadSec server. You can also upload your custom certificates on to IAP. For more information on uploading certificates, see [Mapping IAP Certificates](#).

Authentication Termination on IAP

Aruba Central allows EAP termination for PEAP-Generic Token Card (PEAP-GTC) and Protected Extensible Authentication Protocol-Microsoft Challenge Authentication Protocol version 2 (PEAP-MSCHAPv2). PEAP-GTC termination allows authorization against an LDAP server and external RADIUS server while PEAP-MSCHAPv2 allows authorization against an external RADIUS server.

This allows the users to run PEAP-GTC termination with their username and password to a local Microsoft Active Directory server with LDAP authentication.

- **EAP-GTC**—This EAP method permits the transfer of unencrypted usernames and passwords from client to server. The EAP-GTC is mainly used for one-time token cards such as SecureID and the use of LDAP or RADIUS as the user authentication server. You can also enable caching of user credentials on the IAP to an external authentication server for user data backup.
- **EAP-MSCHAPv2**—This EAP method is widely supported by Microsoft clients. A RADIUS server must be used as the back-end authentication server.

Dynamic Load Balancing between Authentication Servers

You can configure two authentication servers to serve as a primary and backup RADIUS server and enable load balancing between these servers. Load balancing of authentication servers ensures that the authentication load is split across multiple authentication servers and enables the IAPs to perform load balancing of authentication requests destined to authentication servers such as RADIUS or LDAP.

The load balancing in IAP is performed based on the outstanding authentication sessions. If there are no outstanding sessions and if the rate of authentication is low, only primary server will be used. The secondary is used only if there are outstanding authentication sessions on the primary server. With this, the load balance can be performed across asymmetric capacity RADIUS servers without the need to obtain inputs about the server capabilities from the administrators.

Configuring External Authentication Servers for APs

You can configure an external RADIUS server, TACACS, and LDAP server for user authentication. You can configure guest network using External Captive Portal profile for external authentication.

To configure a server, complete the following procedure:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
The Security page is displayed.
6. In the **Authentication Server** panel, click **+** to create a new server.

1. Select any of the following server types and configure the parameters for your deployment scenario.

Table 72: Authentication Server Configuration

Type of Server	Parameters
RADIUS	
Name	Name of the external RADIUS server.
IP Address	IP address or the FQDN of the external RADIUS server.
Radsec	<p>Set Radsec to Enabled to enable secure communication between the RADIUS server and IAP by creating a TLS tunnel between the IAP and the server.</p> <p>If Radsec is enabled, the following configuration options are displayed:</p> <p>Radsec Port—Communication port number for RadSec TLS connection. By default, the port number is set to 2083.</p> <ul style="list-style-type: none"> ▪ NAS Identifier ▪ NAS IP Address ▪ Service Type Framed User ▪ Query Status of RADIUS Servers (RFC 5997) ▪ Dynamic Authorization
Auth Port	Authorization port number of the external RADIUS server. The default port number is 1812.
Accounting Port	The accounting port number used for sending accounting records to the RADIUS server. The default port number is 1813.
Shared Key and Retype Shared Key	Shared key for communicating with the external RADIUS server.
Timeout	The timeout duration for one RADIUS request. The IAP retries sending the request several times (as configured in the Retry count) before the user is disconnected. For example, if the Timeout is 5 seconds, Retry counter is 3, user is disconnected after 20 seconds. The default value is 5 seconds.
Retry Count	The maximum number of authentication requests that can be sent to the server group by the IAP. You can specify a value within the range of 1–5. The default value is 3 requests.
Dynamic Authorization	To allow the APs to process RFC 3576-compliant CoA and disconnect messages from the RADIUS server, select this check box. Disconnect messages terminate the user session immediately, whereas the CoA messages modify session authorization attributes such as data filters. When you enable the Dynamic Authorization option, the AirGroup CoA Port field is displayed with the port number for sending Bonjour support CoA on a different port than on the standard CoA port. The default value is 5999.
NAS IP Address	Enter the IP address. For IAP-based cluster deployments, ensure that you enter the VC IP address as the NAS IP address.
NAS Identifier	Use this to configure strings for RADIUS attribute 32, NAS Identifier, to be sent with RADIUS requests to the RADIUS server.

Type of Server	Parameters
Dead Time	<p>Specify a dead time for authentication server in minutes. When two or more authentication servers are configured on the IAP and a server is unavailable, the dead time configuration determines the duration for which the authentication server is available if the server is marked as unavailable.</p> <p>If Dynamic RADIUS Proxy (DRP) is enabled on the APs, configure the following parameters:</p> <ul style="list-style-type: none"> ▪ DRP IP—IP address to be used as source IP for RADIUS packets. ▪ DRP MASK—Subnet mask of the DRP IP address. ▪ DRP VLAN—VLAN in which the RADIUS packets are sent.
Service Type Framed User	<p>Select any of the following check boxes to send the service type as Framed User in the access requests to the RADIUS server:</p> <ul style="list-style-type: none"> ▪ 802.1X—Changes the service type to frame for 802.1X authentication. ▪ MAC—Changes the service type to frame for MAC authentication. ▪ Captive Portal—Changes the service type to frame for Captive Portal authentication.
Query Status of RADIUS Servers (RFC 5997)	<p>Select any of the following check boxes to detect the server status of the RADIUS server:</p> <p>Authentication—Select this check-box to ensure the IAP sends a status-server request to determine the actual state of the authentication server before marking the server as unavailable.</p> <p>Accounting—Select this check-box to ensure the IAP sends a status-server request to determine the actual state of the accounting server before marking the server as unavailable.</p>
LDAP	
Name	Name of the LDAP server.
IP Address	IP address of the LDAP server.
Auth Port	Authorization port number of the LDAP server. The default port number is 389.
Admin-DN	A distinguished name for the admin user with read and search privileges across all the entries in the LDAP database (the admin user need not have write privileges, but the admin user must be able to search the database, and read attributes of other users in the database).
Admin Password and Retype Admin Password	Password for the admin user.
Base-DN	Distinguished name for the node that contains the entire user database.
Filter	The filter to apply when searching for a user in the LDAP database. The default filter string is (objectclass=*) .
Key Attribute	The attribute to use as a key while searching for the LDAP server. For Active Directory, the value is sAMAccountName .

Type of Server	Parameters
Timeout	Timeout interval within a range of 1–30 seconds for one RADIUS request. The default value is 5.
Retry Count	The maximum number of authentication requests that can be sent to the server group. You can specify a value within the range of 1–5. The default value is 3.
TACACS	
Name	Name of the server.
Shared Key and Retype Key	The secret key to authenticate communication between the TACACS client and server.
Auth Port	The TCP IP port used by the server. The default port number is 49.
Timeout	A number between 1 and 30 seconds to indicate the timeout period for TACACS+ requests. The default value is 20 seconds.
IP Address	IP address of the server.
Retry Count	The maximum number of authentication attempts to be allowed. The default value is 3.
Dead Time (in mins)	Specify a dead time for authentication server in minutes. When two or more authentication servers are configured on the AP and a server is unavailable, the dead time configuration determines the duration for which the authentication server is available if the server is marked as unavailable.
Session Authorization	Enable this option to allow the authorization of sessions.
External Captive Portal —The external captive portal servers are used for authenticating guest users in a WLAN.	
Name	Enter a name for the profile.
Type	Select any one of the following types of authentication: <ul style="list-style-type: none"> ■ Radius Authentication—Select this option to enable user authentication against a RADIUS server. ■ Authentication Text—Select this option to specify an authentication text. The specified text will be returned by the external server after a successful user authentication.
IP or Hostname	Enter the IP address or the host name of the external splash page server.
URL	Enter the URL of the external captive portal server.
Port	Enter the port number that is used for communicating with the external captive portal server.

Type of Server	Parameters
Use HTTPS	Select this to enforce clients to use HTTPS to communicate with the captive portal server. This option is available only if RADIUS Authentication is selected.
Captive Portal Failure	This field allows you to configure Internet access for the guest users when the external captive portal server is not available. Select Deny Internet to prevent guest users from using the network, or Allow Internet to access the network.
Server Offload	Select the check box to enable the server offload feature. The server offload feature ensures that the non-browser client applications are not unnecessarily redirected to the external captive portal server, thereby reducing the load on the external captive portal server.
Prevent Frame Overlay	Select this check box to prevent the overlay of frames. When enabled, the frames display only those pages that are in the same domain as the main page.
Automatic URL Allowlisting	On enabling this for the external captive portal authentication, the URLs that are allowed for the unauthenticated users to access are automatically allowlisted.
Auth Text	If the External Authentication splash page is selected, specify the authentication text that is returned by the external server after successful authentication. This option is available only if Authentication Text is selected.
Redirect URL	Specify a redirect URL if you want to redirect the users to another URL.
Dynamic Authorization Only	
Name	Name of the server.
IP Address	IP address of the server.
AirGroup CoA Port	A port number for sending Bonjour support CoA on a different port than on the standard CoA port. The default value is 5999.
Shared Key and Retype Key	A shared key for communicating with the external RADIUS server. Change of Authorization(CoA) is a subset of Dynamic Authorization include disconnecting messages.

2. Click **Save**.

To assign the authentication server to a network profile, select the newly added server when configuring security settings for a wireless or wired network profile.



You can also add an external RADIUS server when configuring a WLAN SSID profile.

Creating a Role Derivation Rules for AP Clients

Aruba Central (on-premises) allows you to configure role and VLAN derivation-rules. You can configure these rules to assign a user role or VLAN to the clients connecting to an SSID or a wired profile.

Creating a Role Derivation Rule

You can configure rules for determining the role that is assigned for each authenticated client.



When creating more than one role assignment rule, the first matching rule in the rule list is applied.

To create a role assignment rule, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click the **WLANS** tab.
The WLANS details page is displayed.
5. In the **Wireless SSIDs** table, select a network profile and then click the edit icon.
6. Click the **Access** tab.
7. Under **Access rules**, select **Role Based** to enable access based on user roles.
8. Under **Role Assignment Rules**, click **+Add Role Assignment**. In **New Role Assignment Rule**, define a match method by which the string in *Operand* is matched with the attribute value returned by the authentication server.
9. Select the attribute from the **Attribute** list that the rule it matches against. The list of supported attributes includes RADIUS attributes, dhcp-option, dot1x-authentication-type, mac-address, and mac-address-and-dhcp-options. For information on a list of RADIUS attributes, see [RADIUS Server Authentication with VSA](#).
10. Select the operator from the **Operator** list. The following types of operators are supported:
 - **contains**—The rule is applied only if the attribute value contains the string specified in *Operand*.
 - **Is the role**—The rule is applied if the attribute value is the role.
 - **equals**—The rule is applied only if the attribute value is equal to the string specified in *Operand*.
 - **not-equals**—The rule is applied only if the attribute value is not equal to the string specified in *Operand*.
 - **starts-with**—The rule is applied only if the attribute value starts with the string specified in *Operand*.
 - **ends-with**—The rule is applied only if the attribute value ends with string specified in *Operand*.
 - **matches-regular-expression**—The rule is applied only if the attribute value matches the regular expression pattern specified in *Operand*. This operator is available only if the **mac-address-and-dhcp-options** attribute is selected in the **Attribute** list. The **mac-address-and-dhcp-options** attribute and **matches-regular-expression** are applicable only for WLAN clients.
11. Enter the string to match in the **String** box.
12. Select the appropriate role from the **Role** list.
13. Click **Save**.

Configuring VLAN Derivation Rules

The users are assigned to a VLAN based on the attributes returned by the RADIUS server after users authenticate.

To configure VLAN derivation rules for an SSID profile:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click the **WLANs** tab.
The WLANs details page is displayed.
5. In the **Wireless SSIDs** table, select a network profile and then click the edit icon.
6. Under **WLANs**, select **Dynamic** under **Client VLAN Assignment**.
7. Click **+Add Rule** to create a VLAN assignment rule. The **New VLAN Assignment Rule** window is displayed. In this window, you can define a match method by which the string in *Operand* is matched with the attribute values returned by the authentication server.
8. Select an attribute from the **Attribute** list.
9. Select an operator from the **Operator** list. The following types of operators are supported:
 - **contains**—The rule is applied only if the attribute value contains the string specified in *Operand*.
 - **equals**—The rule is applied only if the attribute value is equal to the string specified in *Operand*.
 - **not-equals**—The rule is applied only if the attribute value is not equal to the string specified in *Operand*.
 - **starts-with**—The rule is applied only if the attribute value starts with the string specified in *Operand*.
 - **ends-with**—The rule is applied only if the attribute value ends with string specified in *Operand*.
 - **matches-regular-expression**—The rule is applied only if the attribute value matches the regular expression pattern specified in *Operand*. This operator is available only if the **mac-address-and-dhcp-options** attribute is selected in the **Attribute** list. The **mac-address-and-dhcp-options** attribute and **matches-regular-expression** are applicable only for the WLAN clients.
10. Enter the string to match in the **String** field.
11. Select the appropriate VLAN ID from **VLAN**. Ensure that all other required parameters are configured.
12. Click **OK**.

Configuring Users Accounts for the IAP Management Interface

You can configure RADIUS or TACACS authentication servers to authenticate and authorize the management users of an Instant Access Point (IAP). The authentication servers determine if the user has access to administrative interface. The privilege level for different types of management users is defined on the RADIUS or TACACS server. The IAPs map the management users to the corresponding privilege level and provide access to the users based on the attributes returned by the RADIUS or TACACS server.



In Aruba Central (on-premises), the IAP management user passwords are stored and displayed as hash instead of plain text. The **hash-mgmt-user** command is enabled by default on the IAPs provisioned in the template and UI groups. If a pre-configured IAP joins Aruba Central and is moved to a new group, Aruba Central uses the **hash-mgmt-user** configuration settings and discards **mgmt-user** configuration settings, if any, on the IAP. In other words, Aruba Central hashes management user passwords irrespective of the management user configuration settings running on an IAP.

To configure authentication parameters for local admin, read-only, and guest management administrator account settings, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
The System page is displayed.

- Click the **Administrator** accordion and configure the following parameters:

Table 73: Configuration Parameters for the IAP Users

Type of the User	Authentication Options	Steps to Follow
Client Control	Internal	In the Authentication drop-down list, select Internal if you want to specify a single set of user credentials. If using an internal authentication server: <ol style="list-style-type: none"> In Username and Password, enter a username and password. In Retype Password, retype the password to confirm.
	Authentication Server	In the Authentication drop-down list, select the RADIUS or TACACS authentication servers. You can also create a new server by selecting New from the Authentication server drop-down list.
	Authentication Server with fallback to Internal	In the Authentication drop-down list, select Authentication server w/ fallback to internal option if you want to use both internal and external servers. When enabled, the authentication switches to Internal if there is no response from the RADIUS server (RADIUS server timeout). To use this option, select the authentication servers and configure the user credentials for internal server based authentication. <ol style="list-style-type: none"> In Username and Password, enter a username and password. In Retype Password, retype the password to confirm.
	Load Balancing	If two servers are configured, the users can use them in the primary or backup mode, or load balancing mode. To enable load balancing, select Enabled from the Load balancing drop-down list. For more information on load balancing, see Authentication Servers for IAPs .
	TACACS Accounting	If a TACACS server is selected, enable TACACS accounting to report management commands, if required.
View Only		To configure a user account with the read-only privileges: <ol style="list-style-type: none"> In Username and Password, enter a username and password. In Retype Password, retype the password to confirm.
Guest Registration Only		To configure a guest user account with the read-only privileges: <ol style="list-style-type: none"> In Username and Password, enter a username and password. In Retype Password, retype the password to confirm.

- Click **Save Settings**.

Configuring Guest and Employee User Profiles on IAPs

The local database of an Instant Access Point (IAP) consists of a list of guest and employee users. The addition of a user involves specifying a login credentials for a user. The login credentials for these users are provided outside the Aruba Central system.

A guest user can be a visitor who is temporarily using the enterprise network to access the Internet. However, if you do not want to allow access to the internal network and the Intranet, you can segregate the guest traffic from the enterprise traffic by creating a guest WLAN and specifying the required authentication, encryption, and access rules.

An employee user is the employee who is using the enterprise network for official tasks. You can create employee WLANs, specify the required authentication, encryption and access rules and allow the employees to use the enterprise network.



The user database is also used when an IAP is configured as an internal RADIUS server. The local user database of APs can support up to 512 user entries except IAP-92 and IAP-93. IAP-92 and IAP-93 supports only 256 user entries. If there are already 512 users, IAP-92 and IAP-93 will not be able to join the cluster.

To configure users, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
The Security page is displayed.
6. Click **User For Internal Server**.
7. In the **Users** pane, click the + icon.
8. In the **Add User** window, enter the following information, and then click **OK**.
 - In the **Username** text-box, enter a username.
 - In the **Password** text-box, enter the password.
 - In the **Retype** text-box, retype the password to confirm.
 - In the **Type** drop-down list, select a type of user from the drop-down list.
9. To edit a user settings:
 - a. In the **Users** pane, select the username to edit.
 - b. Click the edit icon to modify the user settings.
 - c. Click **OK**.
10. To delete a user:
 - a. In the **Users** pane, select the username to delete.
 - b. Click the delete icon.
 - c. Click **OK**.
11. To delete all users, select **Delete All** in the **Users** pane, and then click **Yes**.



Deleting a user only removes the user record from the user database, and will not disconnect the online user associated with the username.

Firewall and ACL Rules

The Aruba Central (on-premises) firewall provides identity-based controls to enforce application-layer security, prioritization, traffic forwarding, and network performance policies for wired and wireless networks. Using the Aruba Central (on-premises) firewall, you can enforce network access policies that define access to the network, areas of the network that users may access, and the performance thresholds of various applications.

Aruba Central (on-premises) supports a role-based stateful firewall. Aruba Central (on-premises) firewall recognizes flows in a network and keeps track of the state of sessions. The Aruba Central (on-premises) firewall manages packets according to the first rule that matches packet. The firewall logs on the Instant Access Points (IAPs) are generated as syslog messages. The Aruba Central (on-premises) firewall also supports the Application Layer Gateway (ALG) functions such as SIP, Vocera, Alcatel NOE, and Cisco Skinny protocols.

ACL Rules

You can use Access Control List (ACL) rules to either permit or deny data packets passing through the IAP. You can also limit packets or bandwidth available to a set of user roles by defining access rules. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses.

You can create access rules to allow or block data packets that match the criteria defined in an access rule. You can create rules for either inbound traffic or outbound traffic. Inbound rules explicitly allow or block the inbound network traffic that matches the criteria in the rule. Outbound rules explicitly allow or block the network traffic that matches the criteria in the rule. For example, you can configure a rule to explicitly block outbound traffic to an IP address through the firewall.

The IAP clients are associated with user roles, which determine the client's network privileges and the frequency at which clients re-authenticate. Aruba Central (on-premises) supports the following types of ACLs:

- ACLs that permit or deny traffic based on the source IP address of the packet.
- ACLs that permit or deny traffic based on source or destination IP address, or source or destination port number.



You can configure up to 64 access control rules for a firewall policy.

Configuring Network Address Translation Rules

Network Address Translation (NAT) is the process of modifying network address information when packets pass through a routing device. The routing device acts as an agent between the public (the Internet) and private (local network), which allows translation of private network IP addresses to a public address space.

Aruba Central (on-premises) supports the NAT mechanism to allow a routing device to use the translation tables to map the private addresses into a single IP address and packets are sent from this address, so that they appear to originate from the routing device. Similarly, if the packets are sent to the private IP address, the destination address is translated as per the information stored in the translation tables of the routing device.

Support for Multiple PSK in WLAN SSID

Aruba Central (on-premises) allows you to configure multiple PSK (MPSK) in WLAN network profiles that include APs running a minimum of Aruba InstantOS 8.4.0.0 firmware version and later. MPSK enhances the WPA2 PSK mode by allowing device-specific or group-specific passphrases, which are generated by ClearPass Policy Manager and sent to the Instant Access Point (IAP).

WPA2 PSK-based deployments generally consist of a single passphrase configured as part of the WLAN SSID profile. This single passphrase is applicable for all clients that associate with the SSID. Starting from Aruba InstantOS 8.4.0.0, multiple PSKs in conjunction with ClearPass Policy Manager are supported for WPA and WPA2 PSK-based deployments. Every client connected to the WLAN SSID can have its own unique PSK.

A MPSK passphrase requires MAC authentication against a ClearPass Policy Manager server. The MPSK passphrase works only with wpa2-psk-aes encryption and not with any other PSK-based encryption. The Aruba-MPSK-Passphrase radius VSA is added and the ClearPass Policy Manager server populates this VSA with the encrypted passphrase for the device.

The workflow is as follows:

1. A user registers the device on a ClearPass Policy Manager guest-registration or device-registration webpage and receives a device-specific or group-specific passphrase.
2. The device associates with the SSID using wpa2-psk-aes encryption and uses MPSK passphrase.
3. The IAP performs MAC authentication of the client against the ClearPass Policy Manager server. On successful MAC authentication, the ClearPass Policy Manager returns Access-Accept with the VSA containing the encrypted passphrase.
4. The IAP generates a PSK from the passphrase and performs 4-way key exchange.
5. If the device uses the correct per-device or per-group passphrase, authentication succeeds. If the ClearPass Policy Manager server returns Access-Reject or the client uses incorrect passphrase, authentication fails.
6. The IAP stores the MPSK passphrase in its local cache for client roaming. The cache is shared between all the IAPs within a single cluster. The cache can also be shared with standalone IAPs in a different cluster provided the APs belong to the same multicast VLAN. Each IAP first searches the local cache for the MPSK information. If the local cache has the corresponding MPSK passphrase, the IAP skips the MAC authentication procedure, and provides access to the client.



When multiple PSK is enabled on the wireless SSID profile, make sure that MAC authentication is not configured for RADIUS authentication. Multiple PSK and MAC authentication are mutually exclusive and follows a special procedure which does not require enabling MAC authentication in the WLAN SSID manually. Also, ensure that the RADIUS server configured for the wireless SSID profile is not an internal server.

Points to Remember

The following configurations are mutually exclusive with MPSK for the WLAN SSID profile and does not require to be configured manually:

- MPSK and MAC authentication
- MPSK and Denylisting
- MPSK and internal RADIUS server

Configuring Multiple PSK for Wireless Networks

To configure multiple PSK for wireless networks, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **WLANs** tab.
The WLANs detail page is displayed.
5. Click **+Add SSID** to create a new SSID. To modify an existing SSID, select a wireless SSID from the **Wireless SSIDs** table and then click the edit icon.
6. Click the **Security** tab.
7. Select **Personal** from the **Security Level**. The authentication options applicable to the Enterprise network are displayed.
8. From the **Key Management** drop-down list, select the **MPSK-AES** option.
9. From the **Primary Server** drop-down list, select a server. The radius server selected from the list is the CPPM server.
10. Click **Save Settings**.

Enabling MPSK Local for Wireless Networks

To configure MPSK Local for wireless networks, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **WLANs** tab.
The WLANs detail page is displayed.
5. Click **+Add SSID** to create a new SSID. To modify an existing SSID, select a wireless SSID from the **Wireless SSIDs** table and then click the edit icon.
6. Click the **Security** tab.
7. Select **Personal** from the **Security Level**.
The authentication options applicable to the personal network are displayed.
8. From the **Key Management** drop-down list, select the **Mpsk Local** option.
9. From the **Mpsk Local** drop-down list, select an MPSK Local profile.



MPSK Local feature is supported for Aruba InstantOS 8.7.0.0 or later versions. You cannot select an MPSK Local profile from the **Mpsk Local** drop-down list if the AP version is less than 8.7.0.0.

10. Click **Save Settings**.

Configuring an MPSK Local Profile

MPSK Local allows the user to configure 24 PSKs per SSID locally on the device. These local PSKs would serve as an extension of the base MPSK functionality.

Configuring a MPSK Local Profile

To configure an MPSK Local profile, complete the following steps

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
The Security page is displayed.
6. Click the **Mpsk Local** accordion.
7. In the **MPSK Local** window, click **+** and enter a name for the MPSK Local profile.
8. To create an MPSK Local passphrase, enter the following information in the **Mpsk Local Passphrase** window:
 - a. **Name**—Enter a name.
 - b. **Passphrase**—Enter a passphrase.
 - c. **Retype Passphrase**—Retype the passphrase to confirm.
9. Click **OK**.
10. In the **Mpsk Local Passphrase** window, select the MPSK Local passphrase name created in the previous step, and then click **OK**.
11. Click **Save Settings**.

Configuring WPA3 Encryption

Aruba Central (on-premises) supports WPA3 encryption for security profiles in SSID creation for networks that include access points (APs) running Aruba InstantOS 8.4.0.0 firmware version and above. The WPA3 security provides robust protection with unique encryption per user session thereby ensuring a highly secured connection even on a public Wi-Fi hotspot.

The following are the WPA3 encryptions based on the **Enterprise**, **Personal**, or **Open** network types:

- **WPA-3 Enterprise** when the security level is **Enterprise**.
- **WPA-3 Personal** when the security level is **Personal**.
- **Enhanced Open** when the security level is **Open**.

WPA3 Enterprise

WPA3-Enterprise enforces top secret security standards for an enterprise Wi-Fi in comparison to secret security standards. Top secret security standards includes:

- Deriving at least 384-bit PMK/MSK using Suite B compatible EAP-TLS.
- Securing pairwise data between STA and authenticator using AES-GCM-256.

- Securing group addressed data between STA and authenticator using AES-GCM-256.
- Securing group addressed management frames using BIP-GMAC-256.



Aruba Instant supports WPA3-Enterprise only in non-termination 802.1X and tunnel-forward modes. WPA3-Enterprise compatible 802.1x authentication occurs between STA and CPPM.

WPA3-Enterprise advertises or negotiates the following capabilities in beacons, probes response, or 802.11 association:

- AKM Suite Selector as 00-0F-AC:12
- Pairwise Cipher Suite Selector as 00-0F-AC:9
- Group data cipher suite selector as 00-0F-AC:9
- Group management cipher suite (MFP) selector as 00-0F-AC:12

If WPA3-Enterprise is enabled, STA is successfully associated only if it uses one of the four suite selectors for AKM selection, pairwise data protection, group data protection, and group management protection. If a STA mismatches any one of the four suite selectors, the STA association fails.

To configure WPA3 for enterprise security, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **WLANs** tab.
The WLANs detail page is displayed.
5. Click **+Add SSID** to create a new SSID. To modify an existing SSID, select a wireless SSID from the **Wireless SSIDs** table, and then click the edit icon.
6. Click the **Security** tab.
7. Select **Enterprise** from the **Security Level**.
The authentication options applicable to the Enterprise network are displayed.
8. Select one of the following from the **Key Management** drop-down list:
 - **WPA-3 Enterprise(GCM 256)**—Select this option to use WPA-3 security employing GCM encryption operation mode limited to encrypting 256 bits of plain text.
 - **WPA-3 Enterprise(CCM 128)**—Select this option to use WPA-3 security employing CCM encryption operation mode limited to encrypting 128 bits of plain text.
9. Click **Save Settings**.

Configuring WPA3 for Personal Security

To configure WPA3 for personal security, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.

2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **WLANs** tab.
The WLANs detail page is displayed.
5. Click **+Add SSID** to create a new SSID. To modify an existing SSID, select a wireless SSID from the **Wireless SSIDs** table and then click the edit icon.
6. Click the **Security** tab.
7. Select **Personal** from the **Security Level**.
The authentication options applicable to the Personal network are displayed.
8. Select **WPA-3 Personal** from the **Key Management** drop-down list.
9. Click **Save Settings**.

Intra VLAN Traffic Allowlist

The Intra VLAN Traffic Allowlist is a global allowlist for all WLAN SSIDs and wired networks configured with the feature. For servers to serve the network, you must add them to the Intra VLAN Traffic Allowlist using their IP or MAC address. When you configure wired servers with their IP address or MAC address, the Instant Access Point (IAP) allows client traffic to the destination MAC addresses.

Configuring a Wired Server with the IP Address

To configure a wired server with the IP address, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
The Security page is displayed.
6. Click the **Intra VLAN Traffic Allowlist** accordion.
7. In the **Wired Server IP** window, click **+** and enter the IP address of the server.
8. Click **OK**.
9. Click **Save Settings**.

To edit a wired server, select the IP address of the wired server in the **Wired Server IP** window, and then click the edit icon.

To delete a wired server, select the IP address of the wired server in the **Wired Server IP** window, and then click the delete icon.

Configuring a Wired Server with the MAC Address

To configure a wired server with the MAC address, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
The Security page is displayed.
6. Click the **Intra VLAN Traffic Allowlist** accordion.
7. In the **Wired Server MAC** window, click **+** and enter the MAC address of the server.
8. Click **OK**.
9. Click **Save Settings**.

To edit a wired server, select the IP address of the wired server in the **Wired Server MAC** window, and then click the edit icon.

To delete a wired server, select the IP address of the wired server in the **Wired Server MAC** window, and then click the delete icon.

Mapping IAP Certificates

When an Instant Access Points (IAPs) joins a group that does not have a certificate, the IAPs existing certificate is retained. When an IAP joins a group that already has a certificate, the certificate of the IAP is overwritten by the group certificate.

To map an IAP certificate name to a specific certificate type or category, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
The Security page is displayed.
6. Expand the **Certificate Usage** accordion.
7. To map a certificate, for each usage type under **Usage Type**, select the suitable certificate from the **Certificate** drop-down list:
 - **Certificate Authority**—To verify the identity of a client.
 - **Authentication Server**—To verify the identity of the server to a client.
 - **Captive Portal**—To verify the identity of internal captive portal server.
 - **Radsec use EST Server**—Turn on the **Radsec use EST Server** toggle switch to allow EST certificates to be used in RADSEC applications.



-
- To enable **Radsec use EST Server**, you must enable **EST Activate** in **EST Profile**.
 - If **Radsec use EST Server** is enabled, **RadSec** and **RadSec Certificate Authority** will not be available in **Certificate Usage**.
-

- **RadSec**—To verify the identity of the TLS server.
 - **RadSec Certificate Authority**—To verify the authentication between the IAP and the TLS server.
 - **Clearpass**—To verify the identity of the ClearPass server.
 - **AP1X CA**—Sets the CA certificate used for 802.1X authentication.
 - **AP1X Client Cert**—Sets the certificate used for 802.1X authentication.
8. Click **Save Settings**.



To enable certificates for the **Cloud Guest Service**, contact the Aruba Central support team.

Configuring an EST Profile

EST supports automatic enrollment of certificates with the EST Server. The certificates can now be enrolled or re-enrolled automatically by configuring an EST profile on the AP. Certificate enrollment with EST allows you to use your own PKI instead of the factory or self-signed certificates available on the AP. This enables you to have maximum visibility and control over the management of the PKI used and can address any issues related to security in a scaled environment.

To configure an EST profile, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
The Security page is displayed.
6. Expand the **Certificate Usage > EST Profile** accordion.
7. Configure the following parameters:
 - **EST Activate**—Activates the EST profile.
 - **EST CA Certificate**—Sets the **EST CA Certificate** from the drop-down list.
 - **Server Name/IP Address**—Hostname of the EST server.
 - **Server Port**—Indicates the port value of the EST server. The default value is 443.
 - **Arbitrary Label**—Sets an arbitrary label for the EST URI to distinguish it from the other EST profiles running on the EST server.
 - **Arbitrary Label Enrollment**—Sets an arbitrary enrollment label for EST URL.
 - **Arbitrary Label Reenrollment**—Sets an arbitrary re-enrollment label for EST URL.
 - **Challenge Password**—Sets a challenge password used in CSR.

- **Retype Challenge Password**—Retype challenge password used in CSR.
- **Trust Anchor**—Denotes the server's trust anchor.
- **Organizational Unit Name**—Sets the organizational unit name.
- **Username**—Sets a username for the EST Client.
- **Password**—Sets a password for the EST Client.
- **Retype Password**—Retype password for the EST Client.

8. Click **Save Settings**.

Configuring Roles and Policies on IAPs for User Access Control

Instant Access Points (IAPs) support identity-based access control to enforce application-layer security, prioritization, traffic forwarding, and network performance policies for wired and wireless networks. Using the IAP firewall policies, you can enforce network access policies to define access to the network, areas of the network that the user may access, and the performance thresholds of various applications.

IAPs supports a role-based stateful firewall. In other words, Instant firewall can recognize flows in a network and keep track of the state of sessions. The firewall logs on the IAPs are generated as syslog messages. The firewall feature also supports ALG functions such as SIP, Vocera, Alcatel NOE, and Cisco Skinny protocols.

ACL Rules

You can use ACL rules to either permit or deny data packets passing through the IAP. You can also limit packets or bandwidth available to a set of user roles by defining access rules. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses.

You can create access rules to allow or block data packets that match the criteria defined in an access rule. You can create rules for either inbound traffic or outbound traffic. Inbound rules explicitly allow or block the inbound network traffic that matches the criteria in the rule. Outbound rules explicitly allow or block the network traffic that matches the criteria in the rule. For example, you can configure a rule to explicitly block outbound traffic to an IP address through the firewall.

The IAP clients are associated with user roles, which determine the client's network privileges and the frequency at which clients re-authenticate. IAP supports the following types of ACLs:

- ACLs that permit or deny traffic based on the source IP address of the packet.
- ACLs that permit or deny traffic based on source or destination IP address, or source or destination port number.



You can configure up to 64 access control rules for a firewall policy.

Configuring Network Address Translation Rules

NAT is the process of modifying network address information when packets pass through a routing device. The routing device acts as an agent between the public (the Internet) and private (local network), which allows translation of private network IP addresses to a public address space.

IAP supports the NAT mechanism to allow a routing device to use the translation tables to map the private addresses into a single IP address and packets are sent from this address, so that they appear to originate from the routing device. Similarly, if the packets are sent to the private IP address, the destination address is translated as per the information stored in the translation tables of the routing device.

For more information, see:

- [Configuring Network Service ACLs](#)
- [Configuring ACLs for Deep Packet Inspection](#)
- [Configuring User Roles for AP Clients](#)
- [Configuring Role Derivation Rules for AP Clients](#)
- [Configuring Firewall Parameters for Inbound Traffic](#)

Configuring Network Service ACLs

To configure access rules for network services, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
The Security page is displayed.
6. Click the **Roles** accordion.
7. Under **Access Rules For Selected Roles**, click + to add a new rule.
The Access Rule window is displayed.
8. Under **Rule Type**, select **Access Control**.
9. To configure access to applications or application categories, select a service category from the following list:
 - **Network**
 - **App Category**
 - **Application**
 - **Web Category**
 - **Web Reputation**
10. Based on the selected service category, configure the following parameters:

Table 74: Access Rule Configuration Parameters

Data Pane Item	Description
Rule Type	Select a rule type from the list, for example Access Control .
Service	Select a service from the list of available services. You can allow or deny access to any or all of the following services based on your requirement: <ul style="list-style-type: none"> ■ Any—Access is allowed or denied to all services. ■ CUSTOM—Available options are TCP, UDP, and Other. If you select the TCP or UDP options, enter appropriate port numbers. If you select the Other option, enter the appropriate ID.

Table 74: Access Rule Configuration Parameters

Data Pane Item	Description
	If TCP and UDP uses the same port, ensure that you configure separate access rules to permit or deny access.
Action	Select any of following attributes: <ul style="list-style-type: none"> ■ Select Allow to allow access users based on the access rule. ■ Select Deny to deny access to users based on the access rule. ■ Select Destination-NAT to allow the changes to destination IP address. ■ Select Source-NAT to allow changes to the source IP address.
Destination	Select a destination option. You can allow or deny access to any the following destinations based on your requirements. <ul style="list-style-type: none"> ■ To all destinations—Access is allowed or denied to all destinations. ■ To a particular server—Access is allowed or denied to a particular server. After selecting this option, specify the IP address of the destination server. ■ Except to a particular server—Access is allowed or denied to servers other than the specified server. After selecting this option, specify the IP address of the destination server. ■ To a network—Access is allowed or denied to a network. After selecting this option, specify the IP address and netmask for the destination network. ■ Except to a network—Access is allowed or denied to networks other than the specified network. After selecting this option, specify the IP address and netmask of the destination network. ■ To a Domain Name—Access is allowed or denied to the specified domains. After selecting this option, specify the domain name in the Domain Name text box. ■ To AP IP—Traffic to the specified IAP is allowed. After selecting this option, specify the domain name in the IP text box. ■ To AP Network—Traffic to the specified IAP network is allowed. After selecting this option, specify the domain name in the IP text box. ■ To conductor IP—Traffic to the specified conductor IAP or virtual controller is allowed. After selecting this option, specify the domain name in the IP text box.
Log	Select Log to create a log entry when this rule is triggered. The Aruba Central firewall supports firewall based logging. Firewall logs on the IAPs are generated as security logs.
Denylist	Select Denylist to denylist the client when this rule is triggered. The denylisting lasts for the duration specified as Auth failure denylist time on the Denylisting tab of the Security window.
Classify Media	Select Classify Media to prioritize video and voice traffic. When enabled, a packet inspection is performed on all non-NAT traffic and the traffic is marked as follows: <ul style="list-style-type: none"> ■ Video: Priority 5 (Critical) ■ Voice: Priority 6 (Internetwork Control)
Disable Scanning	Select Disable Scanning to disable ARM scanning when this rule is triggered. The selection of the Disable Scanning applies only if ARM scanning is enabled.
DSCP TAG	Select DSCP TAG to specify a DSCP value to prioritize traffic when this rule is triggered. Specify a value within the range of 0 to 63.

Table 74: Access Rule Configuration Parameters

Data Pane Item	Description
802.1p priority	Select 802.1p priority to specify an 802.1 priority. Specify a value between 0 and 7.
Time Range	Select this check-box to allow a specific user to access the network for a specific time range. You can select the time range profile from the drop-down list that appears when the Time Range check box is selected.

11. Click **Save Settings**.

Configuring ACLs for Deep Packet Inspection

To configure ACL rules for a user role for Deep Packet Inspection (DPI), complete the following procedure:

1. In the **Network Operations** app, set the filter to a group that contains at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of access points is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the access points are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
The **Security** page is displayed.
6. Under **Roles**, select the role for which you want to configure access rules.
7. Under **Access Rules For Selected Roles**, click + to add a new rule.
The **Access Rule** window is displayed.
8. Under **Rule Type**, select **Access Control**.
9. To configure access to applications or application categories, select a service category from the following list:
 - Network
 - App Category
 - Application
 - Web Category
 - Web Reputation
10. Based on the selected service category, configure the following parameters:

Table 75: Access Rule Configuration Parameters

Service category	Description
App Category	Select the application categories to which you want to allow or deny access.
Application	Select the applications to which you want to allow or deny access.
Application Throttling	<p>Application throttling allows you to set a bandwidth limit for an application and application categories. For example, you can limit the bandwidth rate for video streaming applications such as YouTube or Netflix, or assign a low bandwidth to high risk sites. To specify a bandwidth limit:</p> <ul style="list-style-type: none"> ■ Select the Application Throttling check box. ■ Specify the Downstream and Upstream rates in Kbps per user.
Action	<p>Select one of the following actions:</p> <ul style="list-style-type: none"> ■ Destination-NAT—Translation of the destination IP address of a packet entering the network. ■ Source-NAT—Used by internal users to access the internet. ■ Allow—Select Allow to allow access users based on the access rule. ■ Deny—Select Deny to deny access to users based on the access rule.
Destination	<p>Select a destination option for the access rules for network services, applications, and application categories. You can allow or deny access to any the following destinations based on your requirements.</p> <ul style="list-style-type: none"> ■ To all destinations— Access is allowed or denied to all destinations. ■ To a particular server—Access is allowed or denied to a particular server. After selecting this option, specify the IP address of the destination server. ■ Except to a particular server—Access is allowed or denied to servers other than the specified server. After selecting this option, specify the IP address of the destination server. ■ To a network—Access is allowed or denied to a network. After selecting this option, specify the IP address and netmask for the destination network. ■ Except to a network—Access is allowed or denied to networks other than the specified network. After selecting this option, specify the IP address and netmask of the destination network. ■ To a Domain Name—Access is allowed or denied to the specified domains. After selecting this option, specify the domain name in the Domain Name text box. ■ To AP IP—Traffic to the specified IAP is allowed. After selecting this option, specify the domain name in the IP text box. ■ To AP Network—Traffic to the specified IAP network is allowed. After selecting this option, specify the domain name in the IP text box. ■ To conductor IP—Traffic to the specified conductor IAP or virtual controller is allowed. After selecting this option, specify the domain name in the IP text box.
Log	Select this check box if you want a log entry to be created when this rule is triggered. Aruba Central supports firewall based logging. Firewall logs on the IAPs are generated as security logs.

Table 75: Access Rule Configuration Parameters

Service category	Description
Denylist	Select the Denylist check-box to denylist the client when this rule is triggered. The denylisting lasts for the duration specified as Auth failure denylist time on the Denylisting tab of the Security window. .
Classify Media	Select the Classify Media check box to classify and tag media on https traffic as voice and video packets.
Disable Scanning	Select Disable Scanning check box to disable ARM scanning when this rule is triggered. The selection of the Disable Scanning applies only if ARM scanning is enabled.
DSCP Tag	Select this check box to add a DSCP tag to the rule. DSCP is an L3 mechanism for classifying and managing network traffic and providing QoS on the network. To assign a higher priority, specify a higher value.
802.1p priority	Select this check box to enable 802.1p priority. 802.1p priority is an L2 protocol for traffic prioritization to manage QoS on the network. There are eight levels of priority, 0-7. To assign a higher priority, specify a higher value.
Time Range	Select this check box to enable user to access network for a specific time period. You can select the time range profile from the drop-down list that appears when the Time Range check box is selected..

11. Click **Save**.

Configuring ACLs on APs for Website Content Classification

You can configure web policy enforcement on an access point (AP) to block certain categories of websites based on your organization specifications by defining ACL rules.

To configure ACLs for website content classification, follow the below procedure:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
6. Under **Roles**, select the role to modify.
7. Under **Access Rules For Selected Roles**, click + to add a new rule.
The Access Rule window is displayed.
8. Under **Rule Type**, select **Access Control**.
9. To set an access policy based on web categories:
 - a. Under **Service**, select **Web Category**.
 - b. Select the categories to which you want to deny or allow access. You can also search for a web category and select the required option.

- c. Under **Action**, select **Allow** or **Deny**.
 - d. Click **Save**.
10. To filter access based on the security ratings of the website:
 - a. Select **Web Reputation** under **Service**.
 - b. Move the slider to select a specific web reputation value to deny access to websites with a reputation value lower than or equal to the configured value or to permit access to websites with a reputation value higher than or equal to the configured value. The following options are available:
 - **Trustworthy WRI > 81**—These are well known sites with strong security practices and may not expose the user to security risks. There is a very low probability that the user will be exposed to malicious links or payloads.
 - **Low Risk WRI 61-80**—These are benign sites and may not expose the user to security risks. There is a low probability that the user will be exposed to malicious links or payloads.
 - **Moderate WRI 41-60**—These are generally benign sites, but may pose a security risk. There is some probability that the user will be exposed to malicious links or payloads.
 - **Suspicious WRI 21-40**—These are suspicious sites. There is a higher than average probability that the user will be exposed to malicious links or payloads.
 - **High Risk WRI < 20**—These are high risk sites. There is a high probability that the user will be exposed to malicious links or payloads.
 - c. Under **Action**, select **Allow** or **Deny** as required.
11. To set a bandwidth limit based on web category or web reputation score, select the **Application Throttling** check box and specify the downstream and upstream rates in Kbps. For example, you can set a higher bandwidth for trusted sites and a low bandwidth rate for high risk sites.
12. If required, select the following check boxes:
 - **Denylist**—Select this check box to denylist the client when this rule is triggered. The denylisting lasts for the duration specified as **Auth Failure Denylist Time** on the **Denylisting** pane of the **Security** window. For more information, see [Denylisting IAP Clients](#).
 - **Disable Scanning**—Select **Disable scanning** check box to disable ARM scanning when this rule is triggered. The selection of the **Disable scanning** applies only if ARM scanning is enabled, For more information, see [Configuring Radio Parameters](#).
 - **DSCP Tag**—Select this check box to add a DSCP tag to the rule. DSCP is an L3 mechanism for classifying and managing network traffic and providing QoS on the network. To assign a higher priority, specify a higher value.
 - **802.1p priority**—Select this check box to enable 802.1p priority. 802.1p priority is an L2 protocol for traffic prioritization to manage QoS on the network. There are eight levels of priority, 0-7. To assign a higher priority, specify a higher value.
13. Click **Save** to save the rules.
14. Click **Save Settings** in the **Roles** pane to save the changes to the role for which you defined ACL rules.

Configuring User Roles for AP Clients

Every client in the Aruba Central (on-premises) network is associated with a user role, which determines the client's network privileges, the frequency of re-authentication, and the applicable bandwidth contracts. The user role configuration on an Instant Access Point (IAP) involves the following procedures:

- [Creating a User Role](#)
- [Configuring User Roles for AP Clients](#)

Creating a User Role

To create a user role, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
The Security page is displayed.
6. Click the **Roles** accordion.
7. In the **Roles** pane, click **+**.
8. In the **Add Role** window, enter a name for the new role in **Roles**, and then click **OK**.



You can also create a user role when configuring wireless profile. For more information, see [Configuring Wireless Network Profiles on IAPs](#).

Assigning Bandwidth Contracts to User Roles

The administrators can manage bandwidth utilization by assigning maximum bandwidth rates, or bandwidth contracts to user roles. The administrator can assign a bandwidth contract configured in Kbps to upstream (client to the IAP) or downstream (IAP to clients) traffic for a user role. The bandwidth contract will not be applicable to the user traffic on the bridged out (same subnet) destinations. For example, if clients are connected to an SSID, you can restrict the upstream bandwidth rate allowed for each user to 512 Kbps.

By default, all users that belong to the same role share a configured bandwidth rate for upstream or downstream traffic. The assigned bandwidth will be served and shared among all the users. You can also assign bandwidth per user to provide every user a specific bandwidth within a range of 1 to 65535 Kbps. If there is no bandwidth contract specified for a traffic direction, unlimited bandwidth is allowed.

To assign bandwidth contracts to a user role, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
The Security page is displayed.
6. Click the **Roles** accordion.
7. [Create a user role](#) or select an existing role.

8. In the **Access Rules For Selected Roles** pane, click **+**.
9. In the **Access Rule** window, select **Bandwidth Contract** under **Rule Type**.
10. Specify the downstream and upstream rates in Kbps. If the assignment is specific for each user, select **Per User**.
11. Click **Save**. Associate the user role to a WLAN SSID or wired profile.

You can also create a user role and assign bandwidth contracts while configuring an SSID.

Configuring Role Derivation Rules for AP Clients

Aruba Central (on-premises) allows you to configure role and VLAN derivation-rules. You can configure these rules to assign a user role or VLAN to the clients connecting to an SSID or a wired profile.

Creating a Role Derivation Rule

You can configure rules for determining the role that is assigned for each authenticated client.



When creating more than one role assignment rule, the first matching rule in the rule list is applied.

To create a role assignment rule, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click the **WLANs** tab.
The WLANs details page is displayed.
5. In the **Wireless SSIDs** table, select a network profile and then click the edit icon.
6. Click the **Access** tab.
7. Under **Access rules**, select **Role Based** to enable access based on user roles.
8. Under **Role Assignment Rules**, click **+Add Role Assignment**. In **New Role Assignment Rule**, define a match method by which the string in *Operand* is matched with the attribute value returned by the authentication server.
9. Select the attribute from the **Attribute** list that the rule it matches against. The list of supported attributes includes RADIUS attributes, dhcp-option, dot1x-authentication-type, mac-address, and mac-address-and-dhcp-options.
10. Select the operator from the **Operator** list. The following types of operators are supported:
 - **contains**—The rule is applied only if the attribute value contains the string specified in *Operand*.
 - **Is the role**—The rule is applied if the attribute value is the role.
 - **equals**—The rule is applied only if the attribute value is equal to the string specified in *Operand*.
 - **not-equals**—The rule is applied only if the attribute value is not equal to the string specified in *Operand*.
 - **starts-with**—The rule is applied only if the attribute value starts with the string specified in *Operand*.
 - **ends-with**—The rule is applied only if the attribute value ends with string specified in *Operand*.

- **matches-regular-expression**—The rule is applied only if the attribute value matches the regular expression pattern specified in *Operand*. This operator is available only if the **mac-address-and-dhcp-options** attribute is selected in the **Attribute** list. The **mac-address-and-dhcp-options** attribute and **matches-regular-expression** are applicable only for WLAN clients.
11. Enter the string to match in the **String** box.
 12. Select the appropriate role from the **Role** list.
 13. Click **Save**.

Configuring VLAN Assignment Rule

To configure VLAN assignment rules for an SSID profile:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click the **WLANs** tab.
The WLANs details page is displayed.
5. In the **Wireless SSIDs** table, select a network profile and then click the edit icon.
6. Click the **Access** tab.
7. Select the access rule from **Access rules**.
8. In the **Access Rules For Selected Roles**, click **+ Add Rule** to add a new rule. The **Access Rule** page is displayed.



The **VLAN Assignment** option is also listed in the **Access Rule** page when you create or edit a rule for wired port profiles in the **Ports > Create a New Network > Access** tab.

9. From the **Rule Type** drop-down list, select **VLAN Assignment** option.
10. Enter the VLAN ID in the **VLAN ID** field under **Service** section. Alternatively, you can select the VLAN ID or the VLAN name from the drop-down list provided next to the VLAN ID field.
11. Click **Save**.

Configuring VLAN Derivation Rules

The users are assigned to a VLAN based on the attributes returned by the RADIUS server after users authenticate.

To configure VLAN derivation rules for an SSID profile:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.

4. Click the **WLANs** tab.
The WLANs details page is displayed.
5. In the **Wireless SSIDs** table, select a network profile and then click the edit icon.
6. Under **VLANs**, select **Dynamic** under **Client VLAN Assignment**.
7. Click **+ Add Rule** to create a VLAN assignment rule. The **New VLAN Assignment Rule** window is displayed. In this window, you can define a match method by which the string in *Operand* is matched with the attribute values returned by the authentication server.
8. Select an attribute from the **Attribute** list.
9. Select an operator from the **Operator** list. The following types of operators are supported:
 - **contains**—The rule is applied only if the attribute value contains the string specified in *Operand*.
 - **equals**—The rule is applied only if the attribute value is equal to the string specified in *Operand*.
 - **not-equals**—The rule is applied only if the attribute value is not equal to the string specified in *Operand*.
 - **starts-with**—The rule is applied only if the attribute value starts with the string specified in *Operand*.
 - **ends-with**—The rule is applied only if the attribute value ends with string specified in *Operand*.
 - **matches-regular-expression**—The rule is applied only if the attribute value matches the regular expression pattern specified in *Operand*. This operator is available only if the **mac-address-and-dhcp-options** attribute is selected in the **Attribute** list. The **mac-address-and-dhcp-options** attribute and **matches-regular-expression** are applicable only for the WLAN clients.
10. Enter the string to match in the **String** field.
11. Select the appropriate VLAN ID from **VLAN**. Ensure that all other required parameters are configured.
12. Click **OK**.

Configuring Firewall Parameters for Wireless Network Protection

To configure firewall settings, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
The Security page is displayed.
6. Click the **Wireless IDS/IPS** accordion.
7. Under **Firewall Settings**, turn on the toggle switch to enable **SIP, VOCERA, ALCATEL NOE, Auto Topology Rules, Restrict Corporate Access**, and **CISCO Skinny** protocols.
8. Under **Protection**, in the **Protection Against Wired Attacks** section, enable the following options:

- **Drop Bad ARP**—Drops the fake ARP packets.
- **Fix Malformed DHCP**—Fixes the malformed DHCP packets.
- **ARP Poison Check**—Triggers an alert on ARP poisoning caused by the rogue APs.

Configuring Management Subnets

You can configure subnets to ensure that the IAP management is carried out only from these subnets. When the management subnets are configured, Telnet, SSH, and UI access is restricted to these subnets only.

To configure management subnets, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
The Security page is displayed.
6. Click the **Wireless IDS/IPS** accordion.
7. Click **Firewall Settings**.
8. Under **Management Subnets** pane, to add a new management subnet, complete the following steps:
 - a. Enter the subnet address in **Subnet**.
 - b. Enter the subnet mask in **Mask**.
 - c. Click **Add**.
9. Click **Save Settings**.

Configuring Custom Redirection URLs for IAP Clients

You can create a list of URLs to redirect users to when they access the blocked websites. You can define an access rule to use these redirect URLs and assign the rule to a user role in the WLAN network.

Creating a List of Error Page URLs

To create a list of error page URLs, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
The Security page is displayed.

6. Under **Custom Blocked Page URL**, click **+** and enter the URL to block.
7. Repeat the procedure to add more URLs. You can add up to 8 URLs to the list of blocked web pages.
8. Click **OK**.

Configuring ACL Rules to Redirect Users to a Specific URL

To configure ACL rules to redirect users to a specific URL, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
The Security page is displayed.
6. Under **Roles**, select the role for which you want to configure access rules.
7. Click **+** in the **Access Rules** section.
8. In the **New Rule Window**, select the rule type as **Blocked Page URL**.
9. Select the URLs from the existing list of custom redirect URLs. To add a new URL, click **+**.
10. Click **Save**.

Configuring Firewall Parameters for Inbound Traffic

Instant Access Points (IAPs) support an enhanced inbound firewall for the traffic that flows into the network through the uplink ports of an IAP.

To configure the firewall rules, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
The Security page is displayed.
6. Click the **Wireless IDS/IPS** accordion.
7. Click **Firewall Settings**.
8. In the **Access Rule** section, click the **+** icon.
The **Inbound Firewall** page is displayed.
9. In the **Inbound Firewall** page, enter the following information:

Table 76: Inbound Firewall Rule Configuration Parameters

Parameter	Description
Service	<p>Select a service from the list of available services. You can allow or deny access to any or all of the services based on your requirement:</p> <ul style="list-style-type: none"> ■ Any—Access is allowed or denied to all services. ■ Custom—Customize the access based on available options such as TCP, UDP, and other options. If you select the TCP or UDP options, enter appropriate port numbers. If the Other option is selected, ensure that an appropriate ID is entered.
Action	<p>Select any of following actions:</p> <ul style="list-style-type: none"> ■ Select Allow to allow user access based on the access rule. ■ Select Deny to deny user access based on the access rule. ■ Select Destination-NAT to allow making changes to the destination IP address and the port. Select Source-NAT to allow making changes to the source IP address. The destination NAT and source NAT actions apply only to the network services rules.
Source	<p>Select any of the following options:</p> <ul style="list-style-type: none"> ■ From all sources—Traffic from all sources is either allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. ■ From a particular host—Traffic from a particular host is either allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the IP address of the host. ■ From a network—Traffic from a particular network is either allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the IP address and netmask of the source network.
Destination	<p>Select a destination option for the access rules for network services, applications, and application categories. You can allow or deny access to any the following destinations based on your requirements.</p> <ul style="list-style-type: none"> ■ To all destinations—Traffic for all destinations is allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. ■ To a particular server—Traffic to a specific server is allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the IP address of the destination server. ■ Except to a particular server—Access is allowed or denied to servers other than the specified server. After selecting this option, specify the IP address of the destination server. ■ To a network—Traffic to the specified network is allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the IP address and netmask for the destination network. ■ Except to a network—Access is allowed or denied to networks other than the specified network. After selecting this option, specify

Parameter	Description
	<p>the IP address and netmask of the destination network.</p> <ul style="list-style-type: none"> ■ To a Domain name—Traffic to the specified domain is allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the domain name in the Domain Name text box. ■ To AP IP—Traffic to the specified IAP is allowed. After selecting this option, specify the domain name in the IP text box. ■ To AP Network—Traffic to the specified IAP network is allowed. After selecting this option, specify the domain name in the IP text box. ■ To conductor IP—Traffic to the specified conductor IAP or virtual controller is allowed. After selecting this option, specify the domain name in the IP text box.
Log	Select the Log check box if you want a log entry to be created when this rule is triggered. Instant supports firewall-based logging function. Firewall logs on the Instant APs are generated as security logs.
Denylist	Select the Denylist check box to denylist the client when this rule is triggered. The denylisting lasts for the duration specified in the Auth failure denylist time on the Denylisting tab of the Security window.
Classify Media	Select the Classify Media check box to classify and tag media on HTTPS traffic as voice and video packets.
Disable scanning	Select Disable scanning check box to disable ARM scanning when this rule is triggered. The selection of Disable scanning applies only if ARM scanning is enabled.
DSCP TAG	Select the DSCP TAG check box to specify a DSCP value to prioritize traffic when this rule is triggered. Specify a value within the range of 0–63. To assign a higher priority, specify a higher value.
802.1p priority	Select the 802.1p priority check box to specify an 802.1p priority. Specify a value between 0 and 7. To assign a higher priority, specify a higher value.

10. Click **Ok**.

11. Click **Save Settings**.



For all subnets, a deny rule is created by default as the last rule. If at least one rule is configured, the deny all rule is applied to the upstream traffic by default. The inbound firewall is not applied to traffic coming through the GRE tunnel.

Configuring Restricted Access to Corporate Network

You can configure restricted corporate access to block unauthorized users from accessing the corporate network. When restricted corporate access is enabled, corporate access is blocked from the uplink port of conductor IAP, including clients connected to a member IAP.

To configure restricted corporate access, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
The Security page is displayed.
6. Click the **Wireless IDS/IPS** accordion.
7. Click **Firewall Settings**.
8. To restrict corporate access, turn on the **Restrict Corporate Access** toggle switch.
9. Click **Save Settings**.

Enabling ALG Protocols on IAPs

To configure ALG protocols on Instant Access Points (IAPs), complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
The Security page is displayed.
6. Click the **Wireless IDS/IPS** accordion.
7. Under **Firewall Settings**, set the toggle button against the corresponding protocol to enable **SIP**, **VOCERA**, **ALCATEL NOE**, **Auto Topology Rules**, **Restrict Corporate Access**, and **CISCO Skinny** protocols.
8. Click **Save Settings**.



When the protocols for the ALG are disabled, the changes do not take effect until the existing user sessions have expired. Reboot the IAP and the client, or wait a few minutes for changes to take effect.

Denylisting IAP Clients

The client denylisting denies connection to the denylisted clients. When a client is denylisted, it is not allowed to associate with an Instant Access Point (IAP) in the network. If a client is connected to the network when it is denylisted, a deauthentication message is sent to force client disconnection.

Denylisting Clients Manually

Manual denylisting adds the MAC address of a client to the denylist. These clients are added into a permanent denylist. These clients are not allowed to connect to the network unless they are removed from

the denylist.

To add a client to the denylist manually, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
The Security page is displayed.
6. Click the **Denylisting** accordion.
7. Under **Manual Denylisting**, click **+** and enter the MAC address of the client to be denylisted.
8. Click **OK**.
9. Click **Save Settings**.

To delete a client from the manual denylist, select the MAC Address of the client under the **Manual Denylisting**, and then click the delete icon.



For the denylisting to take effect, you must enable the denylisting option when you create or edit the WLAN SSID profile. Go to **WLANs > Security > Advanced Settings** and enable the **Denylisting** option. For more information, see [Configuring Wireless Network Profiles on IAPs](#).

Denylisting Clients Dynamically

The clients can be denylisted dynamically when they exceed the authentication failure threshold or when a denylisting rule is triggered as part of the authentication process.

When a client takes time to authenticate and exceeds the configured failure threshold, it is automatically denylisted by an IAP.

In session firewall based denylisting, an ACL rule automates denylisting. When the ACL rule is triggered, it sends out denylist information and the client is denylisted.

To configure the denylisting duration, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
The Security page is displayed.
6. Click the **Denylisting** accordion.

7. Under **Dynamic Denylisting**, enter the following information:
 - a. For **Auth Failure Denylist Time**, enter the duration after which the clients that exceed the authentication failure threshold must be denylisted.
 - b. For **Policy Enforcement Failure Rule Denylist Time**, enter the duration after which the clients can be denylisted due to an ACL rule trigger.
8. Click **Save Settings**.



-
- You can configure a maximum number of authentication failures by the clients, after which a client must be denylisted. For more information on configuring maximum authentication failure attempts, see [Configuring Wireless Network Profiles on IAPs](#).
 - To enable session-firewall-based denylisting, select the **Denylist** check box in the **Access Rule** page during the WLAN SSID profile creation. For more information, see [Configuring Network Service ACLs](#).
-

Configuring IAPs for VPN Services

This section describes the following VPN configuration procedures:

- [IAP VPN Overview](#)
- [Configuring IAPs for VPN Tunnel Creation](#)
- [Configuring Routing Profiles for IAP VPN](#)

Configuring IAPs for VPN Tunnel Creation

Instant Access Point (IAP) supports the configuration of tunneling protocols such as GRE, IPsec, and L2TPv3. This section describes the procedure for configuring VPN host settings on an IAP to enable communication with a controller in a remote location:

- [Configuring IPsec VPN Tunnel](#)
- [Configuring Automatic GRE VPN Tunnel](#)
- [Configuring a GRE VPN Tunnel](#)
- [Configuring an L2TPv3 VPN Tunnel](#)

IAP VPN Overview

As Instant Access Point (IAP) use a virtual controller architecture, the IAP network does not require a physical controller to provide the configured WLAN services. However, a physical controller is required for terminating VPN tunnels from the IAP networks at branch locations or data centers, where the Aruba controller acts as a VPN Concentrator.

When the VPN is configured, the IAP acting as the virtual controller creates a VPN tunnel to Aruba Mobility Controller in your corporate office. The controller acts as a VPN endpoint and does not supply the IAP with any configuration.

The VPN features are recommended for:

- Enterprises with many branches that do not have a dedicated VPN connection to the corporate office.
- Branch offices that require multiple APs.
- Individuals working from home, connecting to the VPN.

Supported VPN Protocols

IAPs support the following VPN protocols for remote access:

Table 77: *VPN Protocols*

VPN Protocol	Description
Aruba IPsec	<p>IPsec is a protocol suite that secures IP communications by authenticating and encrypting each IP packet of a communication session.</p> <p>You can configure an IPsec tunnel to ensure that the data flow between the networks is encrypted. However, you can configure a split-tunnel to encrypt only the corporate traffic.</p> <p>When IPsec is configured, ensure that you add the IAP MAC addresses to the allowlist database stored on the controller or an external server. IPsec supports Local, L2, and L3 modes of IAP-VPN operations.</p> <p>NOTE: The IAPs support IPsec only with Aruba Controllers.</p>
Layer-2 (L2) GRE	<p>GRE is a tunnel protocol for encapsulating multicast, broadcast, and L2 packets between a GRE-capable device and an endpoint. IAPs support the configuration of L2 GRE (Ethernet over GRE) tunnel with an Aruba Controller to encapsulate the packets sent and received by the IAP. You can use the GRE configuration for L2 deployments when there is no encryption requirement between the Instant AP and controller for client traffic.</p> <p>IAPs support two types of GRE configuration:</p> <ul style="list-style-type: none">■ Manual GRE—The manual GRE configuration sends unencrypted client traffic with an additional GRE header and does not support failover. When manual GRE is configured on the IAP, ensure that the GRE tunnel settings are enabled on the controller.■ Aruba GRE—With Aruba GRE, no configuration on the controller is required except for adding the IAP MAC addresses to the allowlist database stored on the controller or an external server. Aruba GRE reduces manual configuration when Per-AP Tunnel configuration is required and supports failover between two GRE endpoints. <p>IAPs support manual and Aruba GRE configuration only for L2 mode of operations. Aruba GRE configuration is supported only with Aruba Controllers.</p>
L2TP	<p>The L2TP version 3 feature allows IAP to act as L2TP Access Concentrator (LAC) and tunnel all wireless clients L2 traffic from AP to LNS. In a centralized L2 model, the VLAN on the corporate side are extended to remote branch sites. Wireless clients associated with IAP gets the IP address from the DHCP server running on LNS. For this, AP has to transparently allow DHCP transactions through the L2TPv3 tunnel.</p>

Configuring IPsec VPN Tunnel

An IPsec tunnel is configured to ensure that the data flow between the networks is encrypted. When configured, the IPsec tunnel to the controller secures corporate data. You can configure an IPsec tunnel from virtual controller using Aruba Central (on-premises).

To configure an IPsec tunnel from virtual controller, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.

4. Click **Show Advanced**.
5. Click the **VPN** tab.
The VPN page is displayed.
6. Click the **Controller** accordion.
7. In the **Protocol** drop-down list, select **Aruba IPsec**.
8. In the **Primary host** field, enter the IP address or FQDN for the main VPN/IPsec endpoint.
9. In the **Backup host** field, enter the IP address or FQDN for the backup VPN/IPsec endpoint. This entry is optional. When you enter the primary host IP address and backup host IP address, other fields are displayed.
10. Specify the following parameters.
 - a. Select the **Preemption** check-box to allow the VPN tunnel to switch back to the primary host when it becomes available again. This step is optional. If **Preemption** is enabled, specify a value in seconds for **Hold time**. When preemption is enabled and the primary host comes up, the VPN tunnel switches to the primary host after the specified hold-time. The default value for **Hold time** is 600 seconds.
 - b. Select the **Fast Failover** check-box to allow the IAP to create a backup VPN tunnel to the controller along with the primary tunnel, and maintain both the primary and backup tunnels separately. When fast failover is enabled and if the primary tunnel fails, the IAP can switch the data stream to the backup tunnel. This reduces the total failover time to less than one minute.
 - c. Specify a value in seconds for **Secs Between Test Packets**. Based on the configured frequency, the IAP can verify if an active VPN connection is available. The default value is 5 seconds, which means that the IAP sends one packet to the controller every 5 seconds.
 - d. Enter a value for **Max Allowed Test Packet Loss** to define a number for lost packets, after which the IAP can determine that the VPN connection is unavailable. The default value is 2.
 - e. Select the **Reconnect User On Failover** check-box to disconnect all wired and wireless users when the system switches during VPN tunnel transition from primary to backup and backup to primary.
 - f. Specify a value in seconds for **Reconnect Time On Failover** to configure an interval for which wired and wireless users are disconnected during a VPN tunnel switch. By default, the reconnection duration is set to 60 seconds. The **Reconnect Time on Failover** field is displayed only when **Reconnect User On Failover** is enabled.
 - g. From the **Branch Name** drop-down list, select the branch name.

When the IPsec tunnel configuration is completed, the packets that are sent from and received by an IAP are encrypted.

11. Click **Save Settings**.



You will be unable to upload the self-signed certificate from Aruba Central. You must upload the self-signed certificate to Aruba Activate followed by the AP reboot procedure. When the AP contacts Aruba Activate, the Aruba Activate informs the AP about the self-signed AP certificate that is required to be downloaded. The AP then installs a new certificate before connecting to Aruba Central. For more information, see *Aruba Activate User Guide*.

Configuring Automatic GRE VPN Tunnel

In Aruba Central (on-premises), you can configure an Instant Access Point (IAP) to automatically set up a GRE tunnel from the IAP to the controller.

To configure an IAP to automatically set up a GRE tunnel, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **VPN** tab.
The VPN page is displayed.
6. Click the **Controller** accordion.
7. In the **Protocol** drop-down list, select **Aruba GRE**.
8. In the **Primary host** field, enter the IP address or FQDN for the main VPN/IPsec endpoint.
9. In the **Backup host** field, enter the IP address or FQDN for the backup VPN/IPsec endpoint. This entry is optional. When you enter the primary host IP address and backup host IP address, other fields are displayed.
10. Specify the following parameters:
 - a. Select the **Preemption** check-box to allow the VPN tunnel to switch back to the primary host when it becomes available again. This step is optional. If **Preemption** is enabled, specify a value in seconds for **Hold time**. When preemption is enabled and the primary host comes up, the VPN tunnel switches to the primary host after the specified hold time. The default value for **Hold time** is 600 seconds.
 - b. Select the **Fast Failover** check-box to allow the IAP to create a backup VPN tunnel to the controller along with the primary tunnel, and maintain both the primary and backup tunnels separately. If the primary tunnel fails, the IAP can switch the data stream to the backup tunnel. This reduces the total failover time to less than one minute.
 - c. Select the **Reconnect User On Failover** to disconnect all wired and wireless users when the system switches during VPN tunnel transition from primary to backup and backup to primary,
 - d. Specify a value in seconds for **Reconnect Time On Failover** to configure an interval for which wired and wireless users are disconnected during a VPN tunnel switch. By default, the reconnection duration is set to 60 seconds.
 - e. Specify a value in seconds for **Seconds Between Test Packets**. Based on the configured frequency, the IAP can verify if an active VPN connection is available. The default value is 5 seconds, which means that the IAP sends one packet to the controller every 5 seconds.
 - f. Enter a value for **Max Allowed Test Packet Loss** to define a number for lost packets, after which the IAP can determine that the VPN connection is unavailable. The default value is 2.
 - g. Select the **Per-AP-Tunnel** check-box to create a GRE tunnel from each IAP to the VPN/GRE Endpoint rather than the tunnels created just from the conductor IAP. When enabled, the traffic to the corporate network is sent through a Layer-2 GRE tunnel from the IAP itself and need not be forwarded through the conductor IAP.
 - h. From the **Branch Name** drop-down list, select the branch name.
11. Click **Save Settings**.

Configuring a GRE VPN Tunnel

You can also manually configure a GRE tunnel by configuring the GRE tunnel parameters on the Instant Access Point (IAP) and controller. This procedure describes the steps involved in the manual configuration of a GRE tunnel from virtual controller by using Aruba Central (on-premises).

During the manual GRE setup, you can either use the virtual controller IP or the IAP IP to create the GRE tunnel at the controller side depending upon the following IAP settings:

- If a virtual controller IP is configured and if Per-AP tunnel is disabled, the virtual controller IP is used to create the GRE tunnel.
- If a virtual controller IP is not configured or if Per-AP tunnel is enabled, the IAP IP is used to create the GRE tunnel.

To configure the GRE tunnel manually, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **VPN** tab.
The VPN page is displayed.
6. Click the **Controller** accordion.
7. In the **Protocol** drop-down list, select **Manual GRE**.
8. Specify the following parameters:
 - a. **Host**—Enter the IPv4 or IPv6 address or FQDN for the main VPN/GRE tunnel.
 - b. **Backup Host**—(Optional) Enter the IPv4 or IPv6 address or FQDN for the backup VPN/GRE tunnel. You can edit this field only after you enter the IP address or FQDN in the **Host** field.
 - c. **Reconnect User On Failover**—When you enter the host IP address and backup host IP address, this field appears. Select this check-box to disconnect all wired and wireless users when the system switches during VPN tunnel transition from primary to backup and backup to primary. To disconnect all wired and wireless users when the system switches during VPN tunnel transition from primary to backup and backup to primary, select the **Reconnect User On Failover**.
 - d. **Reconnect Time On Failover**—If you select the **Reconnect User On Failover** check-box, this field appears. To configure an interval for which wired and wireless users must be disconnected during a VPN tunnel switch, specify a value within a range of 30-90 seconds. By default, the reconnection duration is set to 60 seconds.
 - e. **GRE Type**—Enter a value for the parameter.
 - f. **GRE Mtu**—Specify a size for the **GRE MTU** within the range of 1024-1500. After GRE encapsulation, if packet length exceeds the configured MTU, IP fragmentation occurs. The default MTU size is 1300.
 - g. **Per-AP-Tunnel**—The administrator can enable this option to create a GRE tunnel from each IAP to the VPN/GRE endpoint rather than the tunnels created just from the conductor IAP. When enabled, the traffic to the corporate network is sent through a Layer-2 GRE tunnel from the IAP

itself and need not be forwarded through the conductor IAP.



By default, the **Per-AP tunnel** option is disabled.

- h. **Branch Name**—Select the branch name from the **Branch Name** drop-down list.
9. When the GRE tunnel configuration is completed on both the IAP and Controller, the packets sent from and received by an IAP are encapsulated, but not encrypted.

Configuring an L2TPv3 VPN Tunnel

The Layer 2 Tunneling Protocol version 3 (L2TPv3) feature allows Instant Access Point (IAP) to act as L2TP Access Concentrator (LAC) and tunnel all wireless clients L2 traffic from AP to LNS. In a centralized L2 model, the VLAN on the corporate side are extended to remote branch sites. Wireless clients associated with IAP gets the IP address from the DHCP server running on LNS. For this, AP has to transparently allow DHCP transactions through the L2TPv3 tunnel.

To configure an L2TPv3 tunnel by using Aruba Central (on-premises), complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **VPN** tab.
The VPN page is displayed.
6. Click the **Controller** accordion.
7. In the **Protocol** drop-down list, select **L2TPv3**.
8. To configure a tunnel profile, complete the following steps:
 - a. Turn on the **Enable Tunnel Profile** toggle switch.
 - b. Enter the profile name in the **Profile Name** text-box.
 - c. Enter the primary server IP address in the **Primary Peer Address** text-box.
 - d. Enter the remote end backup tunnel IP address in the **Backup Peer Address** text-box. This is an optional field and is required only when backup server is configured.
 - e. Enter the peer UDP port numbers in the **Peer UDP Port** text-box. The default value is 1701.
 - f. Enter the local UDP port numbers in the **Local UDP Port** text-box. The default value is 1701.
 - g. Enter the interval in the **Hello Interval** text-box at which the hello packets are sent through the tunnel. The default value is 60 seconds.
 - h. Select the message digest as MD5 or SHA from the **Message Digest Type** drop-down list for message authentication.
 - i. Enter a shared key in the **Shared Key** text-box for the message digest. This key should match with the tunnel end point shared key.
 - j. Ensure that **Checksum** check-box is enabled.
 - k. Specify a tunnel MTU value in the MTU check-box. The default value is 1460.
9. To configure a session profile, complete the following steps:
 - a. Turn on the **Enable Session Profile** toggle switch.
 - b. Enter the session profile name.

- c. Enter the tunnel profile name where the session will be associated.
 - d. Configure the tunnel IP address with the corresponding network mask and VLAN ID. This is required to reach an AP from a corporate network. For example, SNMP polling.
 - e. Select the cookie length and enter a cookie value corresponding to the length. By default, the cookie length is not set.
 - f. From the **Branch Name** drop-down list, select the branch name.
10. Click **Save Settings**.

Configuring Routing Profiles for IAP VPN

Aruba Central (on-premises) can terminate a single VPN connection on Aruba Mobility Controller. The routing profile defines the corporate subnets which need to be tunneled through IPsec.

You can configure routing profiles to specify a policy based on routing into the VPN tunnel.

1. In the **Network Operations** app, set the filter to a group that contains at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of access points is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the access points are displayed.
4. Click **Show Advanced**, and click the **VPN** tab.
The VPN details page is displayed.
5. Click the **Routing** accordion.
6. Click + in the **Routing** pane.
The **New Route** page with the route parameters is displayed.
7. Update the following parameters:
 - **Destination**—Specify the destination network that is reachable through the VPN tunnel. This defines the IP or subnet that must reach through the IPsec tunnel. Traffic to the IP or subnet defined here will be forwarded through the IPsec tunnel.
 - **Netmask**—Specify the subnet mask to the destination defined for **Destination**.
 - **Gateway**—Specify the gateway to which traffic must be routed. In this field, enter one of the following based on the requirement:
 - The controller IP address on which the VPN connection will be terminated. If you have a primary and backup host, configure two routes with the same destination and netmask, but ensure that the gateway is the primary controller IP for one route and the backup controller IP for the second route.
 - The "tunnel" string if you are using the IAP in **Local** mode during local DHCP configuration.
 - **Metric**—Specify the best optimal path for routing traffic. A value of 1 indicates the best path, 15 indicates the worst path, and 16 indicates that the destination is unreachable on the route.
8. Click **OK**.
9. Click **Save Settings**.

Configuring DHCP Pools and Client IP Assignment Modes on IAPs

This section provides the following information:

- [Configuring DHCP Scopes on IAPs](#)
- [Configuring DHCP Server for Assigning IP Addresses to IAP Clients](#)

Configuring DHCP Scopes on IAPs

The Virtual Controller (VC) supports the following types of DHCP address assignments:

- [Configuring DHCP Scopes on IAPs](#)
- [Configuring DHCP Scopes on IAPs](#)
- [Configuring DHCP Scopes on IAPs](#)

Configuring Distributed DHCP Scopes

Aruba Central (on-premises) allows you to configure the DHCP address assignment for the branches connected to the corporate network through VPN. You can configure the range of DHCP IP addresses used in the branches and the number of client addresses allowed per branch. You can also specify the IP addresses that must be excluded from those assigned to clients, so that they are assigned statically.

Aruba Central (on-premises) supports the following distributed DHCP scopes:

- **Distributed, L2**—In this mode, the VC acts as the DHCP server, but the default gateway is in the data center. Based on the number of clients specified for each branch, the range of IP addresses is divided. Based on the IP address range and client count configuration, the DHCP server in the VC controls a scope that is a subset of the complete IP Address range for the subnet distributed across all the branches. This DHCP Assignment mode is used with the L2 forwarding mode.
- **Distributed, L3**—In this mode, the VC acts as the DHCP server and the default gateway. Based on the number of clients specified for each branch, the range of IP addresses is divided. Based on the IP address range and client count configuration, the DHCP server in the VC is configured with a unique subnet and a corresponding scope.

To configure distributed DHCP scopes such as Distributed, L2 or Distributed, L3, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
The System page is displayed.
6. Click the **DHCP** accordion.
7. To configure distributed DHCP scope, click + under **Distributed DHCP Scopes**.
The **New Distributed DHCP Scopes** pane is displayed.
8. Based on the type of distributed DHCP scope, configure the following parameters:

Table 78: Distributed DHCP Scope Configuration Parameters

Data pane item	Description
Name	Enter a name for the DHCP scope.
Type	Select any of the following options: <ul style="list-style-type: none"> ■ Distributed, L2—On selecting Distributed, L2, the VC acts as the DHCP Server but the default gateway is in the data center. Traffic is bridged into VPN tunnel. ■ Distributed, L3—On selecting Distributed, L3, the VC acts as both DHCP Server and default gateway. Traffic is routed into the VPN tunnel.
VLAN	Specify a VLAN ID. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile.
Netmask	If Distributed, L2 is selected for type of DHCP scope, specify the subnet mask. The subnet mask and the network determine the size of subnet.
Default Router	If Distributed, L2 is selected for type of DHCP scope, specify the IP address of the default router.
DNS Server	If required, specify the IP address of a DNS server.
Domain Name	If required, specify the domain name.
Lease Time	Specify a lease time for the client in minutes.
IP Address Range	Specify a range of IP addresses to use. To add another range, click the + icon. You can specify up to four different ranges of IP addresses. <ul style="list-style-type: none"> ■ For Distributed, L2 mode, ensure that all IP ranges are in the same subnet as the default router. On specifying the IP address ranges, a subnet validation is performed to ensure that the specified ranges of IP address are in the same subnet as the default router and subnet mask. The configured IP range is divided into blocks based on the configured client count. ■ For Distributed, L3 mode, you can configure any dis-contiguous IP ranges. The configured IP range is divided into multiple IP subnets that are sufficient to accommodate the configured client count. You can allocate multiple branch IDs (BID) per subnet. The Instant Access Point (IAP) generates a subnet name from the DHCP IP configuration, which the controller can use as a subnet identifier. If static subnets are configured in each branch, all of them are assigned the with BID 0, which is mapped directly to the configured static subnet.
DHCP Reservation	Displays the total number of DHCP reservations. Click the number to view the list of DHCP reservations. <p>You can configure DHCP reservation only on virtual controllers. From the filter bar, select a virtual controller and click the + icon to configure DHCP reservation. Specify the following details:</p> <ul style="list-style-type: none"> ■ MAC—Specify the MAC address of the device for which the IP address has to be reserved. ■ IP—Specify the IP address that has to be reserved for the MAC address. The IP address should be in the IP address range. <p>NOTE: Aruba Central allows you to configure a maximum of 32 DHCP reservations.</p>

Table 78: *Distributed DHCP Scope Configuration Parameters*

Data pane item	Description
	To delete a DHCP reservation, click the delete icon.
Option	Specify the type and a value for the DHCP option. You can configure the organization-specific DHCP options supported by the DHCP server. For example, 176, 242, 161, and so on. To add multiple DHCP options, click the + icon. You can add up to eight DHCP options.

9. Click **Next**. The **Branch Size** tab is displayed. Specify the number of clients to use per branch. The client count configured for a branch determines the use of IP addresses from the IP address range defined for a DHCP scope. For example, if 20 IP addresses are available in an IP address range configured for a DHCP scope and a client count of 9 is configured, only a few IP addresses (in this example, 9) from this range will be used and allocated to a branch. The IAP does not allow the administrators to assign the remaining IP addresses to another branch, although a lower value is configured for the client count.
10. Click **Next**. The **Static IP** tab is displayed. Specify the number of first and last IP addresses to reserve in the subnet.
11. Click **Finish**.

Configuring a Centralized DHCP Scope

The centralized DHCP scope supports L2 and L3 clients.

When a centralized DHCP scope is configured:

- The virtual controller does not assign an IP address to the client and the DHCP traffic is directly forwarded to the DHCP Server.
- For L2 clients, the virtual controller bridges the DHCP traffic to the controller over the VPN/GRE tunnel. The IP address is obtained from the DHCP server behind the controller serving the VLAN/GRE of the client. This DHCP assignment mode also allows you to add the DHCP option 82 to the DHCP traffic forwarded to the controller.
- For L3 clients, the virtual controller acts as a DHCP relay agent that forwards the DHCP traffic to the DHCP server located behind the controller in the corporate network and reachable through the IPsec tunnel. The centralized L3 VLAN IP is used as the source IP. The IP address is obtained from the DHCP server.

To configure a centralized DHCP scope, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP. The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**. A list of APs is displayed in the **List** view.
3. Click the **Config** icon. The tabs to configure the APs are displayed.
4. Click **Show Advanced**.

5. Click the **System** tab.
The System page is displayed.
6. Click the **DHCP** accordion.
7. To configure centralized DHCP scopes, click **+** under **Centralized DHCP Scopes**.
The New Centralized DHCP Scope data pane is displayed.
8. Based on type of centralized DHCP scope, configure the following parameters:

Table 79: DHCP mode configuration parameters

Data pane item	Description
Name	Enter a name for the DHCP scope.
Type	Select one of the following options: <ul style="list-style-type: none"> ■ Centralized, Layer-2 ■ Centralized, Layer-3
VLAN	Specify a VLAN ID. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile.
Split Tunnel	<p>Enable the split tunnel function if you want allow a VPN user to access a public network and a local LAN or WAN network at the same time through the same physical network connection. For example, a user can use a remote access VPN software client connecting to a corporate network using a home wireless network. When the split tunnel function is enabled, the user can connect to file servers, database servers, mail servers, and other servers on the corporate network through the VPN connection.</p> <p>When the user connects to resources on the Internet (websites, FTP sites, and so on), the connection request goes directly to the gateway provided by the home network. The split DNS functionality intercepts DNS requests from clients for non-corporate domains (as configured in Enterprise Domains list) and forwards to the IAP's own DNS server.</p> <p>When split tunnel is disabled, all the traffic including the corporate and the Internet traffic is tunneled irrespective of the routing profile specifications. If the GRE tunnel is down and when the corporate network is not reachable, the client traffic is dropped.</p>
DHCP Relay	Select the DHCP Relay check box to allow the IAPs to intercept the broadcast packets and relay DHCP requests.
Helper Address	Enter the IP address of the DHCP server.
VLAN IP	Field is applicable only if you select Centralized, Layer-3 . Specify the VLAN IP address of the DHCP relay server.
VLAN Mask	Field is applicable only if you select Centralized, Layer-3 . Specify the VLAN subnet mask of the DHCP relay server.
Option 82	Select one of the following options: <ul style="list-style-type: none"> ■ None—If you have configured the DHCP Option 82 XML file, the ALU option scope is disabled in the drop-down list. To enable ALU, set the drop-down list to None and delete the DHCP Option 82 XML file. To enable the XML option, select None from the drop-down list and select the XML file from the DHCP Option 82

Table 79: DHCP mode configuration parameters

Data pane item	Description
	<p>XML drop-down list.</p> <ul style="list-style-type: none"> ■ ALU—ALU option is disabled if an XML file is selected from the DHCP Option 82 XML drop-down list in the System > General pane. Select ALU to enable DHCP Option 82 to allow clients to send DHCP packets with the Option 82 string. The Option 82 string is available only in the Alcatel (ALU) format. The ALU format for the Option 82 string consists of the following: <ul style="list-style-type: none"> ■ Remote Circuit ID; X AP-MAC; SSID; SSID-Type ■ Remote Agent; X IDUE-MAC ■ XML—XML option is enabled only if an XML file is selected from the DHCP Option 82 XML drop-down list in the System > General pane. Alternatively, to enable the XML option, select None from the drop-down list and select the XML file from the DHCP Option 82 XML drop-down list. <p>For information related to XML files, see Configuring System Parameters for an AP</p>

9. Click **Save Settings**.

The following table describes the behavior of the DHCP Relay Agent and Option 82 in the IAP.

Table 80: DHCP Relay and Option 82

DHCP Relay	Option 82	Behavior
Enabled	Enabled	DHCP packet relayed with the ALU-specific Option 82 string
Enabled	Disabled	DHCP packet relayed without the ALU-specific Option 82 string
Disabled	Enabled	DHCP packet not relayed, but broadcast with the ALU-specific Option 82 string
Disabled	Disabled	DHCP packet not relayed, but broadcast without the ALU-specific Option 82 string

Configuring Local DHCP Scopes

You can configure the following types of local DHCP scopes on an IAP:

- **Local**—In this mode, the VC acts as both the DHCP Server and default gateway. The configured subnet and the corresponding DHCP scope are independent of subnets configured in other IAP clusters. The VC assigns an IP address from a local subnet and forwards traffic to both **corporate** and **non-corporate** destinations. The network address is translated appropriately and the packet is forwarded through the IPsec tunnel or through the uplink. This DHCP assignment mode is used for the NAT forwarding mode.
- **Local, L2**—In this mode, the VC acts as a DHCP server and the gateway is located outside the IAP.
- **Local, L3**—In this mode, the VC acts as a DHCP server and default gateway, and assigns an IP address from the local subnet. The IAP routes the packets sent by clients on its uplink. This DHCP assignment mode is used with the L3 forwarding mode.

To configure a new local DHCP scope, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
The System page is displayed.
6. Click the **DHCP** accordion.
7. To configure local DHCP scopes, click **+** under **Local DHCP Scopes**.
The New DHCP Scopes data pane is displayed.
8. Based on type of local DHCP scope, configure the following parameters:

Table 81: Local DHCP Configuration Parameters

Data pane item	Description
Name	Enter a name for the DHCP scope.
Type	Select any of the following options: <ul style="list-style-type: none"> ■ Local—On selecting Local, the DHCP server for local branch network is used for keeping the scope of the subnet local to the IAP. In the NAT mode, the traffic is forwarded through the uplink. ■ Local, L2—On selecting Local, L2, the VC acts as a DHCP server and a default gateway in the local network is used. ■ Local, L3—On selecting Local, L3, the VC acts as a DHCP server and gateway.
VLAN	Enter the VLAN ID. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile.
Network	Specify the network to use.
Netmask	Specify the subnet mask. The subnet mask and the network determine the size of subnet.
Excluded Address	Specify a range of IP addresses to exclude. You can add up to two exclusion ranges. Based on the size of the subnet and the value configured for Excluded address , the IP addresses either before or after the defined range are excluded.
DHCP Reservation	Displays the total number of DHCP reservations. Click the number to view the list of DHCP reservations. You can configure DHCP reservation only on virtual controllers. From the filter bar, select a virtual controller and click the + icon to configure DHCP reservation. Specify the following details: <ul style="list-style-type: none"> ■ MAC—Specify the MAC address of the device for which the IP address has to be reserved. ■ IP—Specify the IP address that has to be reserved for the MAC address. The IP address should be in the IP address range.

Table 81: Local DHCP Configuration Parameters

Data pane item	Description
	NOTE: Aruba Central allows you to configure a maximum of 32 DHCP reservations. To delete a DHCP reservation, click the delete icon.
Default Router	Enter the IP address of the default router.
DNS Server	Enter the IP address of a DNS server.
Domain Name	Enter the domain name.
Lease Time	Enter a lease time for the client in minutes.
DHCP Relay	Select the DHCP Relay check box to allow the IAPs to intercept the broadcast packets and relay DHCP requests.
Helper Address	Enter the IP address of the DHCP server.
Option	Specify the type and a value for the DHCP option. You can configure the organization-specific DHCP options supported by the DHCP server. To add multiple DHCP options, click the + icon.

9. Click **Save Settings**.

Configuring DHCP Server for Assigning IP Addresses to IAP Clients

The DHCP server is a built-in server, used for networks in which clients are assigned IP address by the Virtual Controller (VC). You can customize the DHCP pool subnet and address range to provide simultaneous access to more number of clients. The largest address pool supported is 2048. The default size of the IP address pool is 512.

-
- When the DHCP server is configured and if the **Client IP assignment** parameter for an SSID profile is set to **Virtual Controller Assigned**, the virtual controller assigns the IP addresses to the WLAN or wired clients. By default, the Instant Access Point (IAP) automatically determines a suitable DHCP pool for **Virtual Controller Assigned** networks.
 - The IAP typically selects the 172.31.98.0/23 subnet. If the IP address of the IAP is within the 172.31.98.0/23 subnet, the IAP selects the 10.254.98.0/23 subnet. However, this mechanism does not avoid all possible conflicts with the wired network. If your wired network uses either 172.31.98.0/23 or 10.254.98.0/23, and you experience problems with the **Virtual Controller Assigned** networks after upgrading to Aruba Central, manually configure the DHCP pool by following the steps described in this section.
-



To configure a domain name, DNS server, and DHCP server for client IP assignment, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP. The dashboard context for the group is displayed.

2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
The System page is displayed.
6. Click the **DHCP** accordion.
7. Click **DHCP For WLANs** and enter the following information:
 - a. Enter the domain name of the client in **Domain Name**.
 - b. Enter the IP addresses of the DNS servers in **DNS Server**. To add another DNS server, click the **+** icon.
 - c. Enter the duration of the DHCP lease in **Lease Time**. Select **Minutes**, **Hours**, or **Days** for the lease time from the list next to **Lease Time**. The default lease time is 0.
 - d. Enter the network name in the **Network** box.
 - e. Enter the mask name in the **Mask** box.
 - f. Select the **DHCP Relay** check box to allow the IAPs to intercept the broadcast packets and relay DHCP requests.
 - g. Enter the IP address of the DHCP server in the **Helper Address**.
8. Click **Save Settings**.



To provide simultaneous access to more than 512 clients, use the **Network** and **Mask** fields to specify a larger range. While the network (prefix) is the common part of the address range, the mask (suffix) specifies how long the variable part of the address range is.

Configuring Services

This section describes how to configure AirGroup, location services, Lawful Intercept, OpenDNS, and Firewall services.

- [Configuring AirGroup Services on page 321](#)
- [Configuring an IAP for RTLS Support](#)
- [Configuring an IAP for ALE Support](#)
- [Managing BLE Beacons](#)
- [Configuring OpenDNS Credentials on IAPs](#)
- [Configuring CALEA Server Support on IAPs](#)
- [Configuring IAPs for Palo Alto Networks Firewall Integration](#)
- [Configuring XML API Interface](#)
- [Enabling Application Visibility Service on APs](#)

Configuring AirGroup Services

AirGroup is a zero configuration networking protocol that enables service discovery, address assignment, and name resolution for desktop computers, mobile devices, and network services. It is designed for flat, single-subnet IP networks such as wireless networking at home.

Bonjour can be installed on computers running Microsoft Windows and is supported by the new network-capable printers. Bonjour uses multicast DNS (mDNS) to locate devices and the services offered by these

devices. The AirGroup solution supports both wired and wireless devices. Wired devices that support Bonjour services are part of AirGroup when connected to a VLAN that is terminated on the Virtual Controller.

In addition to the mDNS protocol, Instant Access Points (IAPs) also support UPnP, and DLNA enabled devices. DLNA is a network standard derived from UPnP, which enables devices to discover the services available in a network.

DLNA also provides the ability to share data between the Windows or Android-based multimedia devices. All the features and policies applicable to mDNS are extended to DLNA to ensure full interoperability between compliant devices.

AirGroup Features

AirGroup provides the following features:

- Send unicast responses to mDNS queries and reduces mDNS traffic footprint.
- Ensure cross-VLAN visibility and availability of AirGroup devices and services.
- Allow or block AirGroup services for all users.
- Allow or block AirGroup services based on user roles.
- Allow or block AirGroup services based on VLANs.

For more information on AirGroup solution, see *Aruba Instant User Guide*.

AirGroup Services

Bonjour supports zero-configuration services. The services are pre-configured and are available as part of the factory default configuration. The administrator can also enable or disable any or all services.

The following services are available for IAP clients:

- AirPlay — Apple AirPlay allows wireless streaming of music, video, and slide shows from your iOS device to Apple TV and other devices that support the AirPlay feature.
- AirPrint — Apple AirPrint allows you to print from an iPad, iPhone, or iPod Touch directly to any AirPrint compatible printer.
- iTunes— The iTunes service is used by iTunes Wi-Fi sync and iTunes home-sharing applications across all Apple devices.
- RemoteMgmt— Use this service for remote login, remote management, and FTP utilities on Apple devices.
- Sharing— Applications such as disk sharing and file sharing, use the service ID that are part of this service on one or more Apple devices.
- Chat— The iChat® (Instant Messenger) application on Apple devices uses this service.
- ChromeCast—The ChromeCast service allows you to use a ChromeCast device to play audio or video content on a high-definition television by streaming content through Wi-Fi from the Internet or local network.
- DLNA Media—Applications such as Windows Media Player use this service to browse and play content on a remote device.
- DLNA Print—This service is used by printers that support DLNA.

To enable AirGroup services:

1. In the **Network Operations** app, set the filter to a group that contains at least one AP. The dashboard context for the group is displayed.

2. Under **Manage**, click **Devices > Access Points**.
3. Click the **Config** icon. The tabs to configure access points is displayed.
4. Click **Show Advanced**, and click **Services** tab. The Services page is displayed.
5. Click the **AirGroup** accordion.
6. Select the **AirGroup** check-box.

The **mDNS (Bonjour)** and **SSDP (DLNA/UPNP)** check-boxes are selected by default.

Select at least **mDNS (Bonjour)** or **SSDP (DLNA/UPNP)** to proceed further.



Optionally, select the **Guest Bonjour Multicast** check-box to allow guest users to use the Bonjour services that are enabled in a guest VLAN. When **Guest Bonjour Multicast** is enabled, the Bonjour devices are visible only in the guest VLAN and AirGroup does not discover or enforce policies in guest VLAN.

7. Under the **AirGroup Settings** sub-accordion, select the check-box against one or more AirGroup services listed in [AirGroup Services](#).
 - Optionally, when enabling an AirGroup service, define disallowed roles. The disallowed roles are not allowed to use the specific AirGroup service. To disallow roles:
 1. Click **Edit** against **Disallowed Roles**.
 2. Move the roles from the **Available** pool to the **Selected** pool.
 3. Click **Ok**.
 - Optionally, when enabling an AirGroup service, define disallowed VLANs. The disallowed VLANs are not allowed to use the specific AirGroup service. To disallow VLANs:
 1. Click **Edit** against **Disallowed VLANs**.
 2. Type the VLANs in **Enter comma-separated list of VLAN IDs**. Separate multiple VLANs with a comma.
 3. Click **Ok**.
 - Optionally, configure and enable a new AirGroup service. If defined, disallowed roles or VLANs are not allowed to use the new AirGroup service. To configure and enable a new AirGroup service:
 1. Click **Add New Service**.
 2. Type the service name in **Service Name**. Use alphanumeric characters.
 3. Type a service ID in **Service ID**. Use **+** to add additional service IDs.
 - Sample service ID: **urn:schemas-upnp-org:service:RenderingControl:1** or **_sleep-proxy._udp**.
 1. Click **Ok**.
 2. Select the check-box against the new AirGroup service.
 - Optionally, under **ClearPass Settings** sub-accordion, configure the parameters listed in [Table 83](#).

Table 82: AirGroup Services

Mode	Description
AirGroup Across Mobility Domains	AirGroup service availability in inter cluster domains.
AirPrint	Wireless printing between AirPrint capable devices and AirPrint compatible printers.
Enable AirPlay	Wireless streaming of music, video, or slide shows from AirPlay capable devices and AirPlay compatible devices.
iTunes	iTunes service for home-sharing applications.
Remote Management	Remote login, remote management, or FTP utilities on compatible devices.
Sharing	Applications like disk sharing or file sharing on compatible devices.
Chat	Instant messenger application between compatible devices.
Googlecast	Wireless streaming of audio or video content from the Internet or local network on a HDTV through a Chromecast device.

Mode	Description
DIAL	Wireless streaming between DIAL compatible devices like Roku, Chromecast, or FireTV.
AmazonTV	Wireless playing of content from the Internet or local network on a HDTV through a FireTV device.
DLNA Print	Wireless printing between DLNA capable devices and DLNA compatible printers.
DLNA Media	Wireless browsing or playing audio or video content by applications like Windows Media Player on remote devices.
Allow All	All AirGroup services.

Table 83: *ClearPass Settings*

Mode	Description
ClearPass Policy Manager Server 1	Specify the ClearPass Policy Manager server to use. Select one from the drop-down or define a new ClearPass Policy Manager server.
Enforce ClearPass Registration	Specify is ClearPass registration should be enforced.

8. Click **Save Settings**.

Configuring an IAP for RTLS Support

Aruba Central supports the real time tracking of devices. With the help of the RTLS, the devices can be monitored in real time or through history.

To configure RTLS, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
 2. Under **Manage**, click **Devices > Access Points**.
 3. Click the **Config** icon. The tabs to configure access points is displayed.
 4. Click **Show Advanced**, and click **Services**. The Services page is displayed.
 5. Click **Real Time Locating System > Aruba**.
 6. Select **Aruba RTLS** to send the RFID tag information to the Aruba RTLS server.
 7. Click **3rd Party** and select **Aeroscout** to send reports on the stations to a third-party server.
 8. In the **IP/FQDN** and **Port** field, specify the IP address and port number of the RTLS server, to which location reports must be sent.
 9. In the **Passphrase** field, enter the passphrase required for connecting to the RTLS server.
 10. Retype the passphrase in the **Retype Passprahrse** field.
 11. Specify the update interval within the range of 6–60 seconds in the **Update every** field. The default interval is 30 seconds.
 12. If **3rd Party** is selected, specify the IP address and port number of the 3rd party server.
 13. Select **Include Unassociated Stations** to send reports on the stations that are not associated to any Instant AP.
1. Click **Save Settings**.

Configuring an IAP for ALE Support

ALE is designed to gather client information from the network, process it and share it through a standard API. The client information gathered by ALE can be used for analyzing a client's Internet behavior for business such as shopping preferences.

ALE includes a location engine that calculates the associated and unassociated device location every 30 seconds by default. For every device on the network, ALE provides the following information through the Northbound API:

- Client user name
- IP address
- MAC address
- Device type
- Application firewall data, showing the destinations and applications used by associated devices.
- Current location
- Historical location
- ALE requires the access point (AP) placement data to be able to calculate location for the devices in a network.

ALE with Aruba Central

Aruba Central supports Analytics and Location Engine (ALE). The ALE server acts as a primary interface to all third-party applications and the IAP sends client information and all status information to the ALE server.

To integrate IAP with ALE, the ALE server address must be configured on an IAP. If the ALE sever is configured with a host name, the Virtual Controller performs a mutual certificated-based authentication with ALE server, before sending any information.

Enabling ALE support on an IAP

To configure an IAP for ALE support:

1. In the **Network Operations** app, set the filter to a group that contains at least one AP. The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the **Config** icon. The tabs to configure access points is displayed.
4. Click **Show Advanced**, and click **Services** tab. The Services page is displayed.
5. Click the **Real Time Locating System** accordion.
6. Click **Aruba**, and then select **Analytics & Location**.
7. Specify the ALE server name or IP address.
8. Specify the reporting interval within the range of 6–60 seconds. The IAP sends messages to the ALE server at the specified interval. The default interval is 30 seconds.
9. Click **Save Settings**.

Managing BLE Beacons

Instant Access Points (IAPs) support Aruba BLE devices, such as BT-100 and BT-105, which are used for location tracking and proximity detection. The BLE devices can be connected to an IAP and are managed by a cloud-based Beacon Management Console. The BLE Beacon Management feature allows you to configure parameters for managing the BLE beacons and establishing secure communication with the Beacon Management Console.

Support for BLE Asset Tracking

IAP assets can be tracked using BLE tags, IAP beacons scan the network. When a tag is detected, the IAP sends a beacon with information about the tag including the MAC address and RSSI of the tag to the Virtual Controller.

To manage beacons and configure BLE operation mode, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one AP. The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the **Config** icon. The tabs to configure access points is displayed.
4. Click **Show Advanced**, and click **Services** tab. The Services page is displayed.
5. Click the **Real Time Locating System** accordion.
6. Click **Aruba**.
7. Select **Manage BLE Beacons** to manage the BLE devices using BMC.
 - a. Enter the authorization token in **Authorization token**. The authorization token is a text string of 1–255 characters used by the BLE devices in the HTTPS header when communicating with the BMC. This token is unique for each deployment.
 - b. Enter the server URL in **Endpoint URL**. The BLE data is sent to the server URL for monitoring.
8. Select any of the following options from **BLE Operation Mode** drop-down list:

Table 84: BLE Operation Modes

Mode	Description
beaconing	The built-in BLE chip in the IAP functions as an iBeacon combined with the beacon management functionality.
disabled	The built-in BLE chip of the IAP is turned off. The BLE operation mode is set to Disabled by default.
dynamic-console	The built-in BLE chip of the IAP functions in the beaconing mode and dynamically enables access to IAP console over BLE when the link to LMS is lost.
persistent-console	The built-in BLE chip of the IAP provides access to the IAP console over BLE and also operates in the Beaconing mode.

9. To configure BLE web socket management server, enter the URL of BLE web socket management server in **BLE Asset Tag Mgmt Server(wss)**.
10. Select **BLE Asset Tag Mgmt Server(https)** to configure BLE HTTPS management server.
 - a. Enter the URL of BLE HTTPS management server in **Server URL**.
 - b. Enter the authorization token in **Authorization token**.
 - c. Enter the location ID in **Location ID**.
11. Click **Save Settings**.

Configuring OpenDNS Credentials on IAPs

Instant Access Points (IAPs) use the OpenDNS credentials to provide enterprise-level content filtering.

To configure OpenDNS credentials:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the **Config** icon. The tabs to configure access points is displayed.
4. Click **Show Advanced**, and click **Services**. The Services page is displayed.
5. Click the **OpenDNS** accordion.
6. Enter the **Username** and **Password**.
7. Click **Save Settings**.

Configuring CALEA Server Support on IAPs

LI allows the Law Enforcement Agencies to perform an authorized electronic surveillance. Depending on the country of operation, the ISPs are required to support LI in their respective networks.

In the United States, Service Providers are required to ensure LI compliance based on CALEA specifications.

Aruba Central supports CALEA integration with an Instant Access Point (IAP) in a hierarchical and flat topology, mesh IAP network, the wired and wireless networks.



Enable this feature only if lawful interception is authorized by a law enforcement agency.

For more information on the communication and traffic flow from an IAP to CALEA server, see *Aruba Instant User Guide*.

To enable an IAP to communicate with the CALEA server, complete the following steps:

- [Creating a CALEA Profile](#)
- [Creating ACLs for CALEA Server Support](#)

Creating a CALEA Profile

To create a CALEA profile, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one AP. The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the **Config** icon. The tabs to configure access points is displayed.
4. Click **Show Advanced**, and click **Services** tab. The Services page is displayed.
5. Click the **CALEA** accordion.
6. Specify the following parameters:
 - **IP address**— Specify the IP address of the CALEA server.
 - **Encapsulation type**— Specify the encapsulation type. The current release of Aruba Central supports GRE only.
 - **GRE type**— Specify the GRE type.
 - **MTU**— Specify a size for the MTU within the range of 68—1500. After GRE encapsulation, if packet length exceeds the configured MTU, IP fragmentation occurs. The default MTU size is 1500. fragmentation occurs. The default MTU size is 1500.
7. Click **Save Settings**.

Creating ACLs for CALEA Server Support

To create an access rule for CALEA, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. If you select a group, perform the following steps:
 - a. Under **Manage**, click **Devices > Access Points**.
 - b. Click the **Config** icon. The tabs to configure the group is displayed.
3. If you select a device, under **Manage**, click **Devices**.
4. Click **Show Advanced**, and click **Security** tab. The Security page is displayed.
5. Click the **Roles** accordion.
6. Under **Access Rules for Selected Roles**, click + icon. The **New Rule** window is displayed.
7. Set the **Rule Type** to **CALEA**.
8. Click **Save**.
9. Create a role assignment rule if required.
10. Click **Save Settings**.

Configuring IAPs for Palo Alto Networks Firewall Integration

Instant Access Points (IAPs) maintains the network (such as mapping IP address) and user information for its clients in the network. To integrate the IAP network with a third-party network, you can enable an IAP to provide this information to the third-party servers.

To integrate an IAP with a third-party network, you must add a global profile. This profile can be configured on an IAP with information such as IP address, port, user name, password, firewall enabled or disabled status.

Configuring an IAP for Network Integration

To configure an IAP for network integration:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the **Config** icon. The tabs to configure access points is displayed.
4. Click **Show Advanced**, and click **Services**. The Services page is displayed.
5. Click the **Network Integration** accordion.
6. Select **Enable** to enable PAN firewall.
7. Specify the **Username** and **Password**. Ensure that you provide user credentials of the PAN firewall administrator.
8. Re-enter the password in **Retype**.
9. Enter the PAN firewall **IP Address**.
10. Enter the port number within the range of 1—65535. The default port is 443.
11. Enter the client domain in **Client Domain**.
12. Click **Save Settings**.

Enabling Application Visibility Service on APs

To view application usage metrics for WLAN clients, enable the Application Visibility service on access points (APs).

To enable the Application Visibility feature, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select an AP group in the filter:
 - a. Set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
 - To select an AP in the filter:
 - a. Set the filter to **Global** or a group containing at least one AP.
 - b. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
 - c. Click an AP listed under **Device Name**.
The dashboard context for the AP is displayed.
 - d. Under **Manage**, click **Devices > Access Point**.
2. Click the **Config** icon.
The tabs to configure the APs are displayed.
3. Click **Show Advanced**.
4. Click the **Services** tab.
The Services page is displayed.

5. Expand the **AppRF** accordion.
6. Select any of the following options for **Deep Packet Inspection**:
 - **All**—Performs deep packet inspection on client traffic to application, application categories, website categories, and websites with a specific reputation score.
 - **App**—Performs deep packet inspection on client traffic to applications and application categories.
 - **WebCC**—Performs deep packet inspection on client traffic to specific website categories and websites with specific reputation ratings.
 - **None**—Disables deep packet inspection.
7. Click **Save Settings**

Enabling AirSlice on APs

Aruba AirSlice, based on IEEE 802.11ax standard, is similar to 5G network slicing architecture which allows network operators to build virtual networks tailored for specific application requirements. AirSlice allows network operators to monitor applications used by clients. AirSlice supports multiple services such as gaming, IoT, voice, video, and so on. AirSlice is available for all clients; however, 802.11ax clients have enhanced benefits due to efficient uplink and downlink traffic scheduling mechanism.

The AirSlice feature is available for only Advanced access points (APs) licenses. For devices that have Advanced licenses, the AirSlice feature provides custom-applications prioritization with visibility, configuration, and supports unlimited applications. For customers with legacy licenses, the Aruba AirSlice feature is allow listed till the expiry of the legacy licenses.



AirSlice is supported only on 550 Series and 530 Series APs running Aruba InstantOS 8.7.0.0 and later version. You must enable **Deep Packet Inspection** before configuring AirSlice.

AirSlice support is available only for the following applications:

- Zoom
- Slack
- Skype
- WebEx
- GoToMeeting Online Meeting
- Microsoft Office 365
- Dropbox
- Amazon Web Services/Cloudfront CDN
- GitHub
- Microsoft Teams
- ALG Wi-fi Calling

To enable AirSlice, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.

5. Click the **Services** tab.
The Services page is displayed.
6. Expand the **AppRF** accordion.
7. Select **App** from the **Deep Packet Inspection** drop-down list.
8. Enable the **Application Monitoring** toggle switch.
9. Enable the **AirSlice Policy** toggle switch.
10. Click **Save Settings**.

Configuring XML API Interface

The XML API interface allows Instant Access Points (IAPs) to communicate with an external server. The communication between IAP and an external server through XML API Interface includes the following steps:

- An API command is issued in the XML format from the server to the virtual controller.
- The virtual controller processes the XML request and identifies where the client is and sends the command to the correct member IAP.
- Once the operation is completed, the virtual controller sends the XML response to the XML server.
- The administrators can use the response and take appropriate action to suit their requirements. The response from the virtual controller is returned using the predefined formats.

To configure XML API for servers, complete the following steps:

1. In the **Network Operations** app, set the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the **Config** icon. The tabs to configure access points is displayed
4. Click **Show Advanced**, and click **Services**. The Services page is displayed.
5. Go to **Network Integration > XML API Server Configuration**.
6. Click **+** to add a new XML API server.
7. Enter a name for the XML API server in the **Name** text box.
8. Enter the IP address of the XML API server in the **IP Address** text box.
9. Enter the subnet mask of the XML API server in the **Mask** text box.
10. Enter a passcode in the **Passphrase** text box, to enable authorized access to the XML API Server.
11. Re-enter the passcode in the **Retype Passphrase** box.
12. To add multiple entries, repeat the procedure.
13. Click **Add**.
14. Click **Save Settings**.
15. To edit or delete the server entries, use the **Edit** and **Delete** buttons, respectively.

For information on adding an XML API request, see *Aruba Instant User Guide*.

Client Match

Client Match is an Aruba Central service which helps to improve the experience of wireless clients. Client match 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 access point (AP) radio that can provide better service and thereby improves user experience.

Steer Types

Client match periodically checks the health of current association of the clients and determines if a sticky steer or band steer should be considered.

Sticky Steer

Sticky clients tend to stay associated to an AP despite deteriorating signal levels. Client match continuously monitors the RSSI of sticky clients while they are associated to an AP, and if needed, move them to a radio that would offer better experience. This prevents clients from remaining associated to an AP with less than ideal RSSI, which can cause poor connectivity and reduce performance for other clients associated with that AP.

Band Steer

Dual-band clients can associate with a 2.4 GHz radio or 5 GHz radio. In band steer, client match moves dual-band clients from the 2.4 GHz radio to the 5 GHz radio of the same AP.

Steering Methods

After determining the steer type, client match determines the best neighbor radio to steer the client to and orchestrates the client steer by sending action messages to the APs to carry out the steer. The way client match steers the clients depends on whether the clients are 802.11v-capable.

Steering for 802.11v-capable Client

To steer 802.11v-capable clients, client match triggers the AP to send out an 802.11v BSS transition management request to the client and waits for a response.

Steering for Non-802.11v-capable Client

To steer non-802.11v-capable clients, client match triggers all neighboring AP radios (except the intended destination) to block the client from associating for 5 seconds. 2 seconds after that, the AP to which the client is currently associated sends an 802.11 deauthentication management frame to the client. When the client tries to re-associate, only the intended AP radio allows the client to associate with it.

Monitoring Client Match in Aruba Central

To view client match events in Aruba Central:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Analyze**, click **Alerts & Events > Events**.
3. Click **Click here for advanced filtering**.
4. Select **Client Match Steer**.
5. Click **Filter**.
6. Hover over the required event.

Configuring Uplink Interfaces on IAPs

This section provides the following information:

- [Uplink Interfaces](#)
- [Uplink Preferences and Switching](#)

Uplink Interfaces

Aruba Central (on-premises) supports 3G and 4G USB modems, and the Wi-Fi uplink to provide access to the corporate network.



By default, the AP-318, AP-374, AP-375, and AP-377 access points (APs) have Eth1 as the uplink port and Eth0 as the downlink port. Aruba recommends you not to upgrade the mentioned access points to 8.5.0.0 and 8.5.0.1 firmware versions as the upgrade process changes the uplink from Eth1 to Eth0 port thereby making the devices non-reachable.

The following types of uplinks are supported on Aruba Central:

- [3G/4G Uplink](#)
- [Ethernet Uplink](#)
- [Wi-Fi Uplink](#)

3G/4G Uplink

Aruba Central (on-premises) supports the use of 3G/4G USB modems to provide the Internet back haul to Aruba Central (on-premises). The 3G/4G USB modems can be used to extend client connectivity to places where an Ethernet uplink cannot be configured. This enables the IAPs to automatically choose the available network in a specific region.

Types of Modems

Aruba Central (on-premises) supports the following three types of 3G modems:

- **True Auto Detect**—Modems of this type can be used only in one country and for a specific ISP. The parameters are configured automatically and hence no configuration is necessary.
- **Auto-detect + ISP/country**—Modems of this type require the user to specify the Country and ISP. The same modem is used for different ISPs with different parameters configured for each of them.
- **No Auto Detect**—Modems of this type are used only if they share the same Device-ID, Country, and ISP details. You need to configure different parameters for each of them. These modems work with Aruba Central when the appropriate parameters are configured.

Table 85: 4G Supported Modem

Modem Type	Supported 4G Modem
True Auto Detect	<ul style="list-style-type: none">■ Pantech UML290■ Ether-lte



When UML290 runs in auto detect mode, the modem can switch from 4G network to 3G network or vice-versa based on the signal strength. To configure the UML290 for the 3G network only, manually set the USB type to **pantech-3g**. To configure the UML290 for the 4G network only, manually set the 4G USB type to **pantech-lte**.

Configuring Cellular Uplink Profiles

To configure 3G or 4G uplinks using Aruba Central, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Interfaces** tab.
The Interfaces page is displayed.
6. Click the **Uplink** accordion.
7. Under **3G/4G**, perform any of the following steps:
 - To configure a 3G or 4G uplink automatically, select the **Country** and **ISP**. The parameters are automatically populated.
 - To configure a 3G or 4G uplink manually, perform the following steps:
 - a. Select the country from the **Country** drop-down list.
 - b. Select the service protocol from the **ISP** drop-down list.
 - c. Enter the type of the 3G/4G modem driver type:
 - For 3G—Enter the type of 3G modem in the **USB Type** text box.
 - For 4G—Enter the type of 4G modem in the **4G USB Type** text box.
 - a. Enter the device ID of modem in the **USB DEV** text box.
 - b. Enter the TTY port of the modem in the **USB TTY** text box.
 - c. Enter the parameter to initialize the modem in the **USB INIT** text box.
 - d. Enter the parameter to dial the cell tower in the **USB Dial** text box.
 - e. Enter the parameter used to switch a modem from the storage mode to modem mode in the **USB Mode Switch** text box.
 - f. Select the USB authentication type from the **USB Auth Type** drop-down list.
 - g. Enter the username used to dial the ISP in the **USB User** text box.
 - h. Enter the password used to dial the ISP in the **USB Password** text box.
8. Click **Save Settings**.
9. Reboot the IAP for changes to affect.

Ethernet Uplink

The Ethernet 0 port on an IAP is enabled as an uplink port by default. The Ethernet uplink supports the following:

- **PPPoE**
- **DHCP**
- **Static IP**

You can use **PPPoE** for your uplink connectivity in a single AP deployment.



Uplink redundancy with the **PPPoE** link is not supported.

When the Ethernet link is up, it is used as a PPPoE or DHCP uplink. After the PPPoE settings are configured, PPPoE has the highest priority for the uplink connections. The IAP can establish a PPPoE session with a PPPoE server at the ISP and get authenticated using PAP or the CHAP. Depending upon the request from the PPPoE server, either the PAP or the CHAP credentials are used for authentication. After configuring PPPoE, reboot the IAP for the configuration to take effect. The PPPoE connection is dialed after the AP comes up. The PPPoE configuration is checked during IAP boot and if the configuration is correct, Ethernet is used for the uplink connection.



When PPPoE is used, do not configure Dynamic RADIUS Proxy and IP address of the VC. An SSID created with default VLAN is not supported with PPPoE uplink

You can also configure an alternate Ethernet uplink to enable uplink failover when an Ethernet port fails.

Configuring PPPoE Uplink Profile

To configure PPPoE settings, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Interfaces** tab.
The Interfaces page is displayed.
6. Click the **Uplink** accordion.
7. Under **PPPoE**, configure the following parameters:
 - a. Enter the PPPoE service name provided by your service provider in the **Service Name**.
 - b. In the **CHAP Secret** and **Retype CHAP Secret** fields, enter the secret key used for CHAP authentication. You can use a maximum of 34 characters for the CHAP secret key.
 - c. To set a local interface for the PPPoE uplink connections, select a value from **Local Interface**.
The selected DHCP scope is used as a local interface on the PPPoE interface and the Local, L3 DHCP gateway IP address as its local IP address. When configured, the local interface acts as an unnumbered PPPoE interface and allocated the entire Local, L3 DHCP subnet to the clients.
 - d. Enter the user name for the PPPoE connection in the **User** field.
 - e. In the **Password** and **Retype Password** fields, enter a password for the PPPoE connection and confirm it.



The options in **Local Interface** are displayed only if a Local, L3 DHCP scope is configured on the IAP.

8. Click **Save Settings**.
9. Reboot the IAP.

Wi-Fi Uplink

The Wi-Fi uplink is supported for all IAP models, except 802.11ac APs. Only the conductor IAP uses the Wi-Fi uplink. The Wi-Fi allows uplink to open, PSK-CCMP, and PSK-TKIP SSIDs.

Important Points

- For single radio IAPs, the radio serves wireless clients and Wi-Fi uplink.
- For dual radio IAPs, both radios can be used to serve clients but only one of them can be used for Wi-Fi uplink.



When Wi-Fi uplink is in use, the client IP is assigned by the internal DHCP server.

Configuring a Wi-Fi Uplink Profile

The following configuration conditions apply to the Wi-Fi uplink:

- To bind or unbind the Wi-Fi uplink on the 5 GHz band, reboot the IAP.
- If Wi-Fi uplink is used on the 5 GHz band, mesh is disabled. The two links are mutually exclusive.

To provision an IAP with Wi-Fi Uplink, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Interfaces** tab.
The Interfaces page is displayed.
6. Click the **Uplink** accordion.
7. Under **Wi-Fi**, enter the name of the wireless network that is used for Wi-Fi uplink in the **Name(SSID)** box.
8. From **Band**, select the band in which the VC currently operates. The following options are available:
 - **2.4 GHz (default)**
 - **5 GHz**
9. From **Key Management** drop-down list, select the type of key for uplink encryption and authentication.
 - When **WPA Personal** or **WPA-2 Personal** key management type is selected, the passphrase options are available for configuration.
 - a. Select a passphrase format from the **Passphrase Format** drop-down list.
The following passphrase options are available:
 - **8 - 63 alphanumeric characters**
 - **64 hexadecimal characters**



Ensure that the hexadecimal password string is exactly 64 digits in length.

- b. Enter a PSK passphrase in **Passphrase** text box.
 - When **WPA Enterprise** or **WPA-2 Enterprise** key management type is selected, the 802.1x authentication options are available for configuration.
 - a. From the WiFi1X drop-down list, select 802.1x authentication protocol to be used:
 - Specify the certificate type to be used by selecting **Cert TPM** or **Cert User**.
 - If **PEAP** authentication type is selected, enter the user credentials in the **Username** and **Password** text box.
 - b. Toggle the **Validate Server** button to enable or disable server certificate verification by the AP.
10. Click **Save Settings** and reboot the IAP.



If the uplink wireless router uses mixed encryption, **WPA-2 Personal** or **WPA-2 Enterprise** is recommended for Wi-Fi uplink.

Uplink Preferences and Switching

This section describes the following topics:

- [Enforcing Uplinks](#)
- [Setting an Uplink Priority](#)
- [Enabling Uplink Pre-emption](#)

Enforcing Uplinks

The following conditions apply to the uplink enforcement:

- When an uplink is enforced, the Instant Access Points (IAP) uses the specified uplink regardless of uplink pre-emption configuration and the current uplink status.
- When an uplink is enforced and multiple Ethernet ports are configured and uplink is enabled on the wired profiles, the IAP tries to find an alternate Ethernet link based on the priority configured.
- When no uplink is enforced and pre-emption is not enabled, and if the current uplink fails, the IAP tries to find an available uplink based on the priority configured.
- When no uplink is enforced and pre-emption is enabled, and if the current uplink fails, the IAP tries to find an available uplink based on the priority configured. If current uplink is active, the IAP periodically tries to use a higher priority uplink and switches to the higher priority uplink even if the current uplink is active.

To enforce a specific uplink on an IAP, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.

4. Click **Show Advanced**.
5. Click the **Interfaces** tab.
The Interfaces page is displayed.
6. Expand the **Uplink** accordion.
7. Under **Management > Enforce Uplink**, select the type of uplink from the drop-down list. If Ethernet uplink is selected, the **Port** field is displayed.
8. Specify the Ethernet interface port number.
9. Click **Save Settings**.

The selected uplink is enforced on the IAP.

Setting an Uplink Priority

To set an uplink priority, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Interfaces** tab.
The Interfaces page is displayed.
6. Click the **Uplink** accordion.
7. Under **Management > Uplink Priority List**, select the uplink to increase or decrease the priority.
By default, the **Eth0** uplink is set as a high priority uplink.
8. Click **Save Settings**.

The selected uplink is prioritized over other uplinks.

Enabling Uplink Pre-emption

The following configuration conditions apply to uplink pre-emption:

- Pre-emption can be enabled only when no uplink is enforced.
- When pre-emption is disabled and the current uplink fails, the IAP tries to find an available uplink based on the uplink priority configuration.
- When pre-emption is enabled and if the current uplink is active, the IAP periodically tries to use a higher priority uplink, and switches to a higher priority uplink even if the current uplink is active.

To enable uplink pre-emption, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.

3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Interfaces** tab.
The Interfaces page is displayed.
6. Click the **Uplink** accordion.
7. Under **Management**, ensure that the **Enforce Uplink** is set to **None**.
8. Select the **Pre-emption** check-box.
9. Specify value for **Pre-emption Interval**.
10. Click **Save Settings**.

Switching Uplinks based on the Internet Availability

You can configure Aruba Central to switch uplinks based on the Internet availability.

When the uplink switchover based on Internet availability is enabled, the IAP continuously sends ICMP packets to some well-known Internet servers. If the request is timed out due to a bad uplink connection or uplink interface failure, and the Internet is not reachable from the current uplink, the IAP switches to a different connection.

To configure uplink switching, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Interfaces** tab.
The Interfaces page is displayed.
6. Click the **Uplink** accordion.
7. Under **Management**, specify a value for **Failover Internet IP**.
8. Select the **Internet Failover** check-box.
9. Specify values for **Failover Internet Packet Send Frequency**, **Failover Internet Packet Lost Count**, and **Internet Check Count**.
10. Click **Save Settings**.

-
- By default, the conductor AP sends the ICMP packets to 8.8.8.8 IP address only if the out-of-service operation based on Internet availability (internet-down state) is configured on the SSID. You can use **Failover Internet IP** as an alternative to the default option to configure an IP address to which the AP must send AP packets, and verify if the Internet is reachable when the uplink is down.
 - When **Internet Failover** is enabled, the IAP ignores the VPN status, although uplink switching based on VPN status is enabled.
-



Configuring Preferred Uplink on AP-318 and 370 Series APs

The AP-318 and 370 Series APs have an ethernet port for Eth0 and a fibreport for Eth1. Either of these ports can be configured as the uplink port as required. By default, Eth1 port is configured as the uplink for these AP platforms. All functionality of the Eth0 port is supported by Eth1 port with exception to the following:

- Eth0 bridging feature is not supported when the Eth1 port is configured as preferred uplink.
- If LACP is enabled, the Eth1 port cannot be configured as the preferred uplink.



By default, the AP-318, AP-374, AP-375, and AP-377IAPs have Eth1 as the uplink port and Eth0 as the downlink port. Aruba recommends you not to upgrade the mentioned access points to 8.5.0.0 and 8.5.0.1 firmware versions as the upgrade process changes the uplink from Eth1 to Eth0 port thereby making the devices non-reachable

Configuring Enterprise Domains

In a typical Instant Access Point (IAP) deployment without tunneling, all DNS requests from a client are forwarded to the client's DNS server by default. However, if an IAP is configured for tunneling, the IAP-VPN enables split DNS by default, and the DNS behavior for both the clients on the IAP network is determined by the enterprise domain settings.

The enterprise domain setting on the IAP specifies the domains for which DNS resolution must be forwarded to the default DNS server of the client. For example, if the enterprise domain is configured for **arubanetworks.com**, the DNS resolution for host names in the **arubanetworks.com** domain is forwarded to the default DNS server of the client. The DNS resolution for host names in all other domains is forwarded to the local DNS server of the IAP.



In a full-tunnel mode, all DNS traffic is forwarded over IPsec tunnel to DNS server of the client regardless of the enterprise domain configuration. If an asterisk is configured in the enterprise domain list instead of a domain name, then all DNS requests are forwarded to the default DNS server of the client. Split DNS functionality is supported for IAP-VPN scenarios only.

To configure an enterprise domain, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
The System page is displayed.
6. Click the **Enterprise Domains** accordion.
7. Click + in the **Enterprise Domains** pane, and enter a name in the **New Domain Name** window.
8. Click **OK**.
9. Click **Save Settings**.

To delete an enterprise domain, select the domain in the **Enterprise Domains** pane, and then click the delete icon.

Configuring SNMP Parameters

This section describes the following topics:

- [Configuring SNMP Parameters](#)
- [Configuring SNMP Parameters](#)
- [Configuring SNMP Parameters](#)

SNMP Configuration Parameters

Aruba Central (on-premises) supports SNMPv1, SNMPv2c, and SNMPv3 for reporting purposes only. An Instant Access Point (IAP) cannot use SNMP to set values in an Aruba system.

You can configure the following parameters for an IAP:

Table 86: *SNMP Parameters*

Data Pane Item	Description
Community Strings for SNMPV1 and SNMPV2	An SNMP Community string is a text string that acts as a password, and is used to authenticate messages sent between the virtual controller and the SNMP agent.
If you are using SNMPv3 to obtain values from the IAP, you can configure the following parameters:	
Name	A string representing the name of the user.
Authentication Protocol	An indication of whether messages sent on behalf of this user can be authenticated, and if so, the type of authentication protocol used. This can take one of the two values: <ul style="list-style-type: none">■ MD5—HMAC-MD5-96 Digest Authentication Protocol■ SHA—HMAC-SHA-96 Digest Authentication Protocol
Authentication protocol password	If messages sent on behalf of this user can be authenticated, the (private) authentication key for use with the authentication protocol. This is a string password for MD5 or SHA depending on the choice above.
Privacy protocol	An indication of whether messages sent on behalf of this user can be protected from disclosure, and if so, the type of privacy protocol which is used. This takes the value DES (CBC-DES Symmetric Encryption).
Privacy protocol password	If messages sent on behalf of this user can be encrypted/decrypted with DES, the (private) privacy key for use with the privacy protocol.

Configuring Community String for SNMP

This section describes the procedure for configuring SNMPv1, SNMPv2, and SNMPv3 community strings in Aruba Central.

Creating Community strings for SNMPv1 and SNMPv2 using Aruba Central

To create community strings for SNMPv1 and SNMPv2, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.

2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
The System page is displayed.
6. Click the **SNMP** accordion.
7. Under **SNMP**, click **+** to add a new community string.
8. In the **New SNMP** window, enter a name for the community string.
9. Click **OK**.
10. To delete a community string, select the string in the **SNMP** pane, and then click the delete icon.

Creating community strings for SNMPv3 using Aruba Central

To create community strings for SNMPv3, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
The System page is displayed.
6. Click the **SNMP** accordion.
7. Under **User for SNMPV3**, click **+** to add a new community string for **SNMPv3**.
8. In the **New SNMPv3 User** window, enter the following information:
 - a. In the **Auth protocol** drop-down list, select the type of authentication protocol.
 - b. In the **Password** text-box, enter the authentication password and retype the password in the **Retype Password** text-box.
 - c. In the **Privacy protocol** drop-down list, select the type of privacy protocol.
 - d. In the **Password** text-box, enter the privacy protocol password and retype the password in the **Retype Password** text box.
 - e. Click **OK**.
9. To edit the details for a particular user, select the user, and then click the edit icon.
10. To delete a particular user, select the user, and then click the delete icon.

Configuring SNMP Trap Receivers

Aruba Central (on-premises) supports the configuration of external trap receivers. Only the Instant AP acting as the VC generates traps. The OID of the traps is 1.3.6.1.4.1.14823.2.3.3.1.200.2.X.

To configure SNMP traps, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
The System page is displayed.
6. Click the **SNMP** accordion.
7. Under **SNMP Traps Receivers**, click **+** to add a new community string for **SNMP Traps Receivers**.
8. In the **New SNMP Trap Receiver** window, enter the following information:
 - a. In the **IP Address** text-box, enter the IP address of the new SNMP Trap Receiver.
 - b. In the **Version** drop-down list, select the SNMP version, such as **v1**, **v2c**, **v3**. The version specifies the format of traps generated by the access point.
 - c. In the **Community/Username** text-box, specify the community string for SNMPv1 and SNMPv2c traps and a username for SNMPv3 traps.
 - d. In the **Port** text-box, enter the port to which the traps are sent. The default value is 162.
 - e. In the **Inform** drop-down list, select **Yes** or **No**. When enabled, traps are sent as SNMP INFORM messages. It is applicable to SNMPv3 only. The default value is **Yes**.
 - f. Click **OK**.

Configuring Syslog and TFTP Servers for Logging Events

This section describes the following topics:

- [Configuring Syslog Server on IAPs](#)
- [Configuring TFTP Dump Server IAPs](#)

Configuring Syslog Server on IAPs

To specify a syslog server for sending syslog messages to the external servers, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
The System page is displayed.
6. Click the **Logging** accordion.
7. In the **Servers** section, enter the IP address of the syslog server in the **Syslog Server** text-box.
8. Click **Syslog Facility Levels**, and enter the required logging level from the drop-down in each of the fields.

Syslog facility is an information field associated with a syslog message. It is an application or operating system component that generates a log message. The IAP supports the following syslog facilities:

- **Syslog Level**—Detailed log about syslog levels.
- **AP-Debug**—Detailed log about the AP device.
- **Network**—Log about change of network, for example, when a new IAP is added to a network.
- **Security**—Log about network security, for example, when a client connects using wrong password.
- **System**—Log about configuration and system status.
- **User**—Important logs about client.
- **User-Debug**—Detailed log about client.
- **Wireless**—Log about radio.

[Table 87](#) describes the logging levels in order of severity, from the most severe to the least.

Table 87: *Logging Levels*

Logging level	Description
Emergency	Panic conditions that occur when the system becomes unusable.
Alert	Any condition requiring immediate attention and correction.
Critical	Any critical condition such as a hard drive error.
Error	Error conditions.
Warning	Warning messages.
Notice	Significant events of a non-critical nature. The default value for all syslog facilities.
Information	Messages of general interest to system users.
Debug	Messages containing information useful for debugging.

9. Click **Save Settings**.

Configuring TFTP Dump Server IAPs

To configure a TFTP server for storing core dump files, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
The System page is displayed.

6. Click the **Logging** accordion.
7. In the **Servers** section, enter the IP address of the TFTP server in the **TFTP Dump Server** text-box.
8. Click **Save Settings**.

Mobility and Client Management

This section provides the following information on Layer-3 Mobility for Instant Access Points (IAPs) clients:

- [Mobility and Client Management](#)
- [Mobility and Client Management](#)

Layer-3 Mobility

IAPs form a single Aruba Central (on-premises) network when they are in the same Layer-2 (L2) domain. As the number of clients increase, multiple subnets are required to avoid broadcast overhead. In such a scenario, a client must be allowed to roam away from the Aruba Central (on-premises) network to which it first connected (home network) to another network supporting the same WLAN access parameters (foreign network) and continue its existing sessions.

Layer-3 (L3) mobility allows a client to roam without losing its IP address and sessions. If WLAN access parameters are the same across these networks, clients connected to IAPs in a given Aruba Central (on-premises) network can roam to IAPs in a foreign Aruba Central (on-premises) network and continue their existing sessions using their IP addresses. You can configure a list of Virtual Controller IP addresses across which L3 mobility is supported.

Home Agent Load Balancing

Home Agent Load Balancing is required in large networks where multiple tunnels might terminate on a single border or lobby AP and overload it. When load balancing is enabled, the VC assigns the home AP for roamed clients by using a round robin policy. With this policy, the load for the APs acting as Home Agents for roamed clients is uniformly distributed across the IAP cluster.

Configuring L3 Mobility Domain

To configure a mobility domain, you have to specify the list of all Aruba Central (on-premises) networks that form the mobility domain. To allow clients to roam seamlessly among all the APs, specify the VC IP for each foreign subnet. You may include the local Aruba Central (on-premises) or VC IP address, so that the same configuration can be used across all Aruba Central (on-premises) networks in the mobility domain.

Aruba recommends that you configure all client subnets in the mobility domain. When client subnets are configured:

- If a client is from a local subnet, it is identified as a local client. When a local client starts using the IP address, the L3 roaming is terminated.
- If the client is from a foreign subnet, it is identified as a foreign client. When a foreign client starts using the IP address, the L3 roaming is set up.
- To configure a Layer-3 Mobility domain, complete the following steps:
 1. In the **Network Operations** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
 2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.

3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
The System page is displayed.
6. Click the **Layer-3 Mobility** accordion.
7. Turn on the **Home Agent Load Balancing** toggle switch. By default, home agent load balancing is disabled.
8. Under **IP Address**, click **+**, and enter an IP address name in the **New IP Address** window, and then click **OK**.
Repeat Step 7 to add the IP addresses of all VCs that form the L3 mobility domain.
9. Under **Subnets**, click **+**, and specify the following:
 - a. Enter the client subnet in the **IP Address** box.
 - b. Enter the mask in the **Subnet Mask** box.
 - c. Enter the VLAN ID in the home network in the **VLAN ID** box.
 - d. Enter the home VC IP address for this subnet in the **Virtual Controller IP** box.
10. Click **OK**.

Renaming an AP

You can change the name of an access point (AP) provisioned in Aruba Central. The AP can be online or offline. When you rename an AP or a VC, the AP or VC does not reboot, and the client traffic is not affected. The new name must be a character string of upto 32 ASCII or non-ASCII characters, including spaces.

To rename an AP, complete the following steps:

1. In the **Network Operations** app, select one of the following options:

To select a group in the filter:

 - a. Set the filter to one of the options under **Groups**. Ensure that the filter selected contains at least one active access point.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Access Points**.
A list of access points is displayed in the **List** view.

To select an access point in the filter:

 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices > Access Points**.
A list of access points is displayed in the **List** view.
 - c. Click an access point listed under **Device Name**.
The dashboard context for the access point is displayed.
 - d. Under **Manage**, click **Device > Access Point**.
2. Click the **Config** icon.
The tabs to configure access points are displayed.
3. Click the **Access Points** tab.
The **Access Points** table is displayed.
4. To edit an AP, select an AP in the **Access Points** table, and then click the edit icon.

5. Under **Basic Info**, modify the AP or VC name in the **Name** field.
6. Click **Save Settings**.

The AP name is updated on the AP immediately. It may take up to 1 minute for the new AP name to get reflected in Aruba Central (on-premises).



Renaming an AP depends on various privileges and access permissions that are assigned to each user to make configuration changes.

Monitoring APs

The access point (AP) dashboard enables you to manage, configure, monitor and troubleshoot APs provisioned and managed through Aruba Central (on-premises).

For a list of all the available menu items in the AP dashboard, see [The Access Point Dashboard](#).

The AP Health Bar provides a snapshot of the overall health of the APs configured in Aruba Central (on-premises). For more information, see [Health Bar Dashboard for Access Point](#).

The AP Foundation license is applicable for Access Point Monitoring.

Monitoring APs in Summary View

The access point (AP) Summary page provides all the metrics about the health, status, and clients information associated with the AP provisioned and managed in Aruba Central (on-premises).

Viewing the AP Summary Page

To navigate to the AP Summary page, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.

The dashboard context for the selected filter is displayed.

2. Under **Manage**, click **Devices > Access Points**.

A list of APs is displayed in the **List** view.

3. Click the **Summary** icon.

The AP Summary page is displayed.

The AP Summary page displays the following information:

- **Access Points**—Displays the overall usage metrics for the APs provisioned in your Aruba Central (on-premises) account. Consists of the following tabs:
 - **Usage**—Displays the incoming and outgoing data traffic detected on the APs.
 - **Clients**—Displays the number of clients connected to an AP over a specific time period.
 - **Bandwidth Usage Per Network**—Displays the incoming and outgoing traffic for all APs per SSID over a specific duration.
 - **Client Count Per Network**—Displays the number of clients connected to an AP per SSID over a specific time period.

- **Radios**—Displays the channel distribution and power distribution metrics for the AP radios. For more information on radios in the summary view, see [Monitoring Radios in Summary View](#).

You can change the time range for the AP Summary page by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

Monitoring Radios in Summary View

The **Radios** tab in the access point (AP) Summary page displays the channel distribution, power distribution, channel changes, and power changes metrics for the radios provisioned and managed in Aruba Central (on-premises). When you click the **Radios** tab, the **2.4 GHz** and **5 GHz** tabs are displayed.

Viewing the Radios Summary Page

To navigate to the Radios Summary page, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels**, or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP. The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Access Points**. A list of APs is displayed in the **List** view.
3. Click the **Summary** icon. The AP Summary page is displayed.
4. Click the **Radios** tab.

When you click the **Radios** tab, it displays the following information:

- **Radios**—Click the **Radios** tab to display the graphs related to channel distribution and power distribution.
- **2.4 GHz**—Click the **2.4 GHz** tab to display the graphs related to channel distribution and power distribution for 2.4 GHz radios.
- **5 GHz**—Click the **5 GHz** tab to display the graphs related to channel distribution and power distribution for 5 GHz and 5 GHz (Secondary) radios.

The tri-radio feature is available only for AP-555. In the **5 GHz** tab, the **Radio 5 GHz (Secondary)** data is available only if the tri-radio mode is enabled. For more information, see [About Tri-Radio Mode](#).

You can change the time range for the AP Summary page by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.



When you click the **Radios**, **2.4 GHz**, and **5 GHz** tab, the **Radios** tab provides the following information:

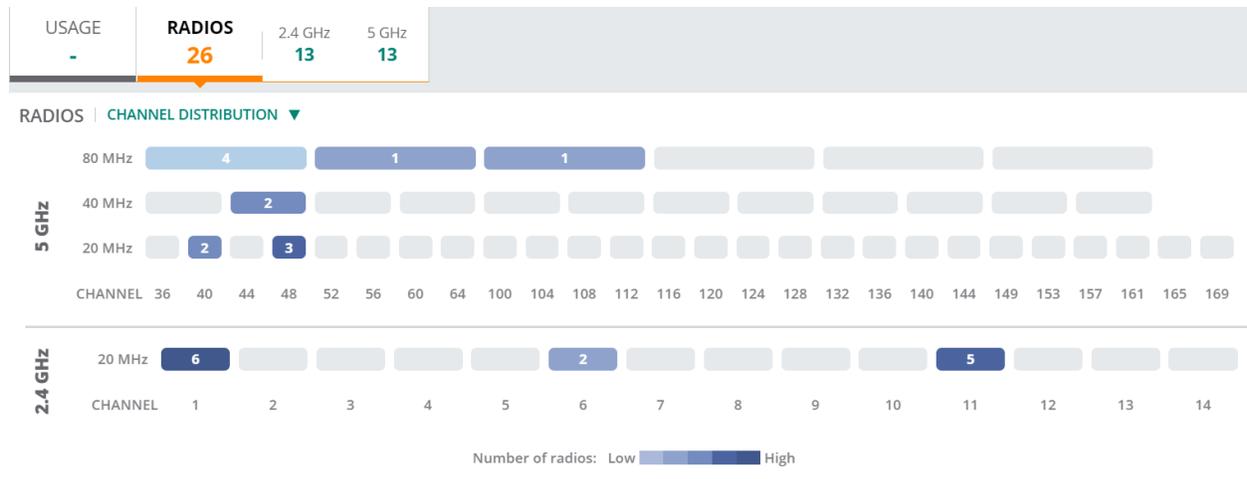
Radios

The **Radios** section displays the channel distribution and power distribution graphs for the radios.

Channel Distribution

From the drop-down list, select **Channel Distribution** to display information on the frequency, at which each of the channels of the radio operate.

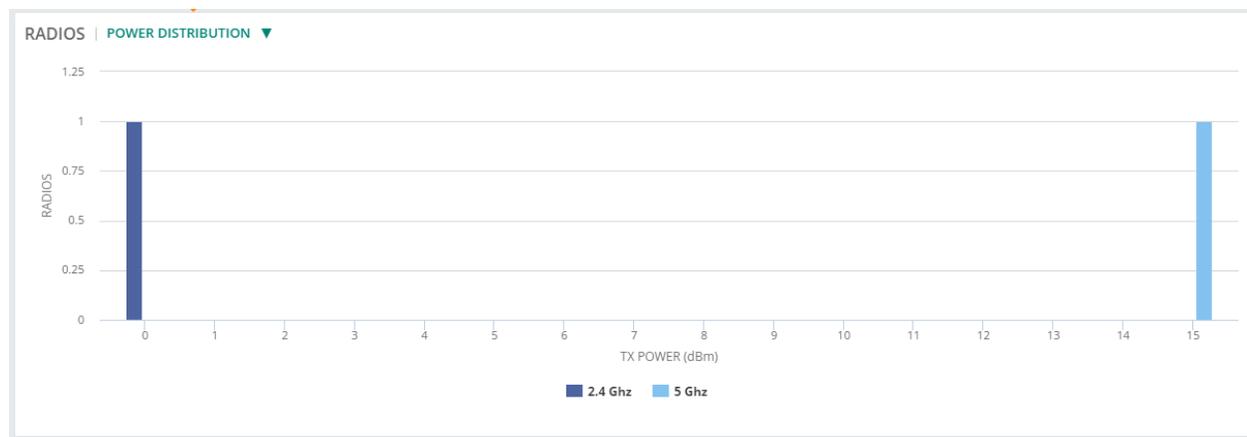
Figure 20 Channel Distribution



Power Distribution

From the drop-down list, select **Power Distribution** to display the power distributed across each of the radios.

Figure 21 Power Distribution

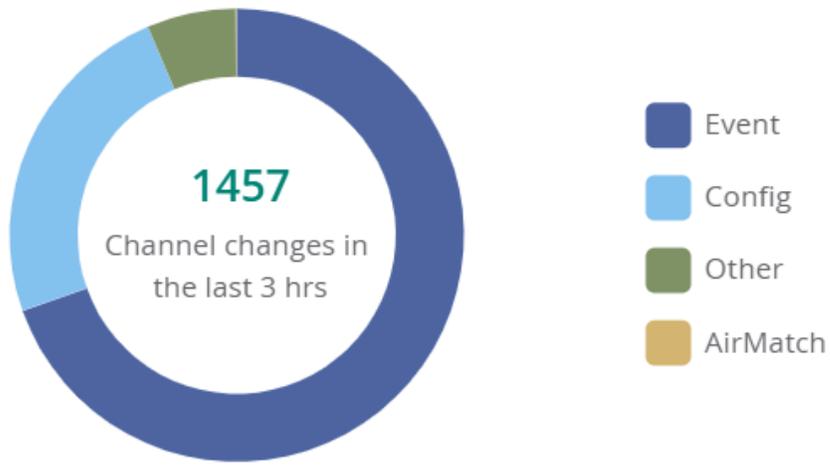


Channel Changes

The **Channel Changes** graph displays the number of channel changes that has occurred in the radios.

Figure 22 Channel Changes

CHANNEL CHANGES

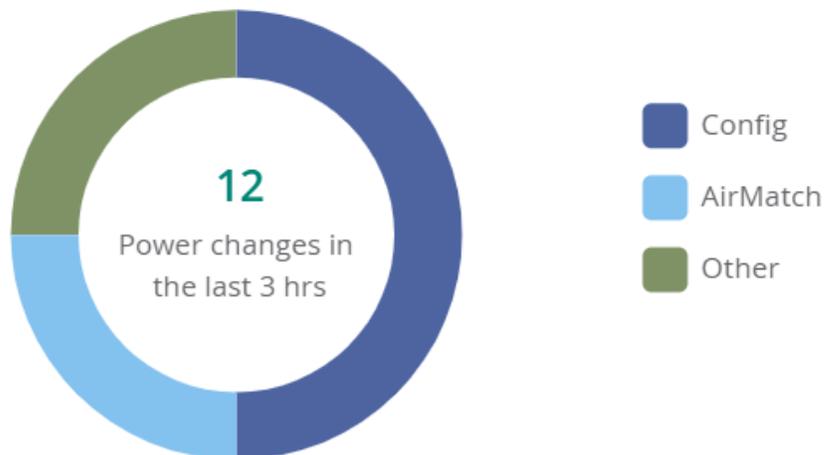


Power Changes

The **Power Changes** graph indicates the power change by each of the radios, from ARM to AirMatch EIRP.

Figure 23 Power Changes

POWER CHANGES



Monitoring APs in List View

The access point (AP) List page provides information associated with the APs and radios provisioned and managed in Aruba Central (on-premises).

The AP List page is available for Foundation and Advanced licenses for APs.

The AP List page displays the following sections:

- [Access Points Table](#)
- [Monitoring APs in List View](#)
- [Monitoring APs in List View](#)
- [Monitoring APs in List View](#)

Viewing the AP List Page

To navigate to the AP List page, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under Groups, Labels, or Sites. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP. The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.

The AP List page displays the following information:

- **Access Points**—Displays the total number of APs. When you click the **Access Points** tab, it provides information about all APs in the **Access Points** table.
- **Online**—Displays the total number of online APs. When you click the **Online** tab, it provides information about the online APs in the **Access Points** table.
- **Offline**—Displays the total number of offline APs. When you click the **Offline** tab, it provides information about the offline APs in the **Access Points** table.
- **Radios**—Displays the total number of radios. When you click the **Radios** tab, it provides information about all radios in the **Radios** table.
 - **2.4 GHz**—Displays the total number of 2.4 GHz radios. When you click the **2.4 GHz** tab, it provides information about 2.4 GHz radios in the **Radios** table.
 - **5 GHz**—Displays the total number of active 5 GHz and 5 GHz (Secondary) radios. When you click the **5 GHz** tab, it provides information about 5 GHz and 5 GHz (Secondary) radios in the **Radios** table.



The tri-radio feature is available only for AP-555. In the **5 GHz** tab, the **Radio 5 GHz (Secondary)** data is available only if the tri-radio mode is enabled. For more information, see [About Tri-Radio Mode](#).

Access Points Table

The **Access Points** table displays the following information:

- **Device Name**—Name of the AP.
- **Status**—Displays the operational status of the AP. The status is as follows:
 - **Online**—Indicates that the AP is online.
 - **Offline**—Indicates that the AP is offline.

- **Online**—Indicates that the AP is operating under thermal management. For more information, see [Thermal Shutdown Support in IAP](#).
- **IP Address**—IP address of the AP.
- **Model**—The model number of the AP.
- **Serial**—The serial number of the device.
- **Firmware Version**—The firmware version running on the AP.
- **Clients**—Clients connected to the AP.
- **Alerts**—Opens alerts related to APs.
- **MAC Address**—MAC address of the AP.
- **Controller**—The name of the controller.
- **Secondary Controller**—The name of the secondary controller.
- **Config Status**—The configuration changes associated with the AP. The **Config Status** column is not supported in the exported CSV file.
- **Group**—Group to which the AP belongs.
- **Labels**—Labels associated with the AP. If multiple labels are associated with the AP, hover over the label link to view all the labels.
- **Site**—The site to which the device belongs.
- **Uptime**—Time since when the device is operational. The **Uptime** column is not applicable for offline devices and remains blank for all the devices in the **Offline** page.
- **Last Seen**—The last active time and date of the device. The **Last Seen** column is not applicable for online devices and remains blank for all the devices in the **Online** page.
- **Public IP**—IP address logged by servers when the device is connected through internet connection.
- **Persona**—Displays the type of role of the AP. For example, CAP and IAP.
- **LLDP Neighbor**—Displays the name of the LLDP neighbor. Click the LLDP Neighbor name to view the switch details page, if the switch is managed by Aruba Central (on-premises).
- **LLDP Port**—Displays the port number of LLDP neighbor.
- **AI Insights**—The number of insights generated for the AP in the last three hours. The **AI Insights** column is not supported in the exported CSV file.
- **Note**—Displays the information captured in the **Note** parameter, in the AP Details section. The search filter allows you to search for exact and partial text search with prefix. The text search with suffix is not supported.
- **Zone**—Zone to which the AP belongs. Zone details are displayed in the column only for APs with firmware version ArubaOS 8.7.0.0 or later.



- From Aruba Central (on-premises) 2.5.4 release, **LLDP Neighbor** and **LLDP Port** details are also available for Campus APs and not only Instant APs.
- A search filter is provided only for the **Device Name, IP Address, Model, Serial, MAC Address, Controller, Secondary Controller, Group, Labels, Site, LLDP Neighbor, Note**, and **done** columns. The  and  icons allow you to sort the **Device Name, IP Address, Serial, MAC Address, Controller**, and **Zone** columns in an ascending and descending order.
- By default, the AP List table displays the **Device Name, Status, IP Address, Model, Serial**, and **Firmware Version**. You can customize the view of AP List table with additional columns such as the **Clients, Alerts, MAC Address, Controller, Secondary Controller, Config Status, Group, Labels, Site, Uptime, Last Seen, Public IP, Persona, LLDP Neighbor, LLDP Port, AI Insights, Note**, and **Zone**. These additional columns can be selected by clicking the icon provided at the right corner of the table that displays the AP list. Click the **Reset to default** button provided in the drop-down list to reset the AP List with default columns only. To autofit the columns, click the icon and select **Autofit columns**.

To download the **.csv** file of the AP list table, click the  icon. If the table contains unicode value, you must use a UTF-8 enabled software to view the contents. To view the file in Microsoft Excel 2007 spreadsheet software, perform the following steps to view table with unicode values:

1. Open the Microsoft Excel 2007 software.
2. Click on the Data menu bar option.
3. Click on the **From Text** icon.
4. Browse to the location of the file that you want to import.
5. Select the file name and click **Import**.
6. The **Text Import** wizard is displayed.
7. Select the file type. For **.csv** format, select the **Delimited** option.
8. Select the **65001: Unicode (UTF-8)** option from the drop-down list that is displayed next to the **File** origin.
9. Click **Next**. The **Text Import Wizard-Step 1 of 3** page is displayed.
10. Place a check mark next to the delimiter such as the comma or full stop that was used in the file you wish to import into Microsoft Excel 2007.
11. The **Data Preview** window displays the data based on the selected delimiter.
12. Click **Next**. The **Text Import Wizard-Step 3 of 3** page is displayed. Select the appropriate data format for each column that you want to import.



Importing one or more columns is optional.

13. Click **Finish** to import the data into Microsoft Excel 2007.

Deleting an Offline AP

To delete an offline AP, see .

Rebooting an AP

To reboot an AP, see [Rebooting an AP in the List View](#)

Radios Table

The **Radios** table displays the following information:

- **Access Point**—Name of the AP.



The online radios are displayed with a  green dot and offline radios are displayed with a  red dot.

- **Radio MAC Address**—The MAC address of the radios connected to the AP.
- **Band**—The type of radio band. For example, **2.4 GHz**, **5 GHz**, and **5 GHz (Secondary)**.



The tri-radio feature is available only for AP-555. In the **Band** column, the **Radio 5 GHz (Secondary)** data is available only if the tri-radio mode is enabled. For more information, see [About Tri-Radio Mode](#).

- **Bandwidth**—The bandwidth of data transferred through the radios.
- **Channel**—Channels assigned for the radios.
- **Utilization (%)**—The percentage of time (normalized to 255) that the channels of the radios are sensed to be busy. The AP uses either the physical or the virtual carrier sense mechanism to sense a busy channel. This percentage not only depends on the data bits transferred but also with the transmission overhead that makes use of the channel.
- **Channel Changes**—Displays the number of channel changes that has occurred in an AP. When you click the number, the **Channel Changes** pop-up window is displayed, that provides the following information:
 - **Event Time**—Displays the time period when the channel change occurred, in the format of days-hours-minutes.
 - **Reason**—Displays the reason for the channel change.
 - **From Channel**—Displays the channel number from which the channel change occurred.
 - **To Channel**—Displays the channel number to which the channel change occurred.
 - **Band**—The type of radio band. For example, **2.4 GHz**, **5 GHz**, and **5 GHz (Secondary)**.
 - **Access Point**—Name of the AP.
- **Power (dBm)**—The transmit power of the radios measured in decibels.
- **Power Changes**—Displays the number of power changes that has occurred in an AP. When you click the number, the **Power Changes** pop-up window is displayed, that provides the following information:
 - **Event Time**—Displays the time period when the power change occurred, in the format of days-hours-minutes.
 - **Reason**—Displays the reason for the power change.
 - **From Power (dBm)**—Displays the transmit power from which the power change occurred.
 - **To Power (dBm)**—Displays the transmit power to which the power change occurred.
 - **Band**—The type of radio band. For example, **2.4 GHz**, **5 GHz**, and **5 GHz (Secondary)**.
 - **Access Point**—Name of the AP.
- **Noise Floor (dBm)**—The noise at the radio receivers of the radios. Along with the thermal noise, Noise Floor may be affected by certain types of interference sources, though not all interference types result in increased noise floor. Noise Floor value may vary depending on the noise introduced by components

used in the computer or client device.



A search filter is provided only for the **Access Point** column.

Deleting an Offline AP

To delete an offline access point (AP), complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.

The dashboard context for the selected filter is displayed.

2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. In the **Access Points** table, hover over the offline AP that you want to delete.
4. Click the  delete icon.



To delete multiple offline APs, select the offline APs that you want to delete and click the  delete icon.

5. Click **Delete** in the confirmation dialog box.

Rebooting an AP in the List View

You can reboot an Instant Access Point, Campus Access Point, or Remote Access Point using the Aruba Central (on-premises) UI.

For information about how to reboot an AP in the **Details** page, see [Rebooting an AP in the List View](#) and [Rebooting an AP in the Details Page](#).

To reboot an access point (AP), complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under groups, labels, or sites. For all devices, set the filter to **Global**.

The dashboard context for the selected filter is displayed.



You can reboot only the APs that are in the online status (active).

2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. In the **Access Points** table, hover over the AP that you want to reboot.
4. Click the  reboot icon.



To reboot multiple online APs, select the APs that are in online status and click the  reboot icon.

5. Click **Reboot** in the confirmation dialog box.

Thermal Shutdown Support in IAP

ArubaAP-555 and AP-535 Instant Access Point (IAP) devices are equipped with an internal thermal sensor. The sensor initiates a shutdown when the operating temperature crosses the temperature threshold recommended for an Instant AP. When an IAP operates under thermal management, all the radios are in **Disabled** mode in the AP Health Bar.

- In swarm mode, the thermal shutdown support is as follows:
 - In swarm mode, when the member IAP operates beyond the recommended temperature threshold, the Virtual AP profile is disabled. Once the member IAP attains the optimum temperature again, it reboots with the **Recovery from Thermal Management Mode** message, and then reconnects with the virtual controller. This process of reboot and reconnection is executed for five times. If the connection between the member IAP and the virtual controller does not restore after five times, the member IAP remains in the shutdown state until it is manually turned on.
 - In swarm mode, when the conductor IAP operates beyond the recommended temperature threshold, it reboots with the **Reboot due to Thermal Management** message. Once the conductor IAP attains the optimum temperature again, it turns into a member IAP, reboots with the **Recovery from Thermal Management Mode** message, and then reconnects with the virtual controller. This process of reboot and reconnection is executed for five times. If the connection between the member IAP and the virtual controller does not restore after five times, the member IAP remains in the shutdown state until it is manually turned on.
 - In swarm mode, when the conductor IAP operates beyond the recommended temperature threshold and the number of IAPs is one in the swarm scale, the Virtual AP profile is disabled. Once the conductor IAP attains the optimum temperature again, it reboots with the **Recovery from Thermal Management Mode** message. This process of reboot is executed for five times. If the conductor IAP does not reboot after five times, the conductor IAP remains in the shutdown state until it is manually turned on.
- In standalone mode, when the IAP operates beyond the recommended temperature threshold, the Virtual AP profile is disabled. Once the IAP attains the optimum temperature again, it reboots with the **Recovery from Thermal Management Mode** message. This process of reboot is executed for five times. If the IAP does not reboot after five times, it remains in the shutdown state until it is manually turned on.

Thermal Shutdown Events

To view the thermal shutdown events, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
 - The dashboard context for the selected filter is displayed. To select a device in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices**, and then click **Access Points**.
 - c. Click an AP listed under **Device Name**.The dashboard context for the AP is displayed.
2. Under **Analyze**, click **Alerts & Events**.
 - The **Alerts & Events** page is displayed in the **List** view.

3. Click the **Events** tab.

A list of events is displayed in the **Events** table.

When the thermal shutdown feature is either enabled or disabled in an IAP, the **Events** table displays the following details:

- The **Event Type** column includes the **AP Thermal Shutdown** type which can be used to filter thermal shutdown events.
- The **Description** column includes the status of the thermal shutdown feature in the IAP. For example, **Thermal management enabled** or **Thermal management disabled**.



In Aruba Central (on-premises), the thermal shutdown feature is supported on IAPs running Aruba Instant 8.6.0.0 or later versions.

About Tri-Radio Mode

Aruba Central (on-premises) offers tri-radio mode support in ArubaAP-555, a flagship 802.11ax access point (AP). In tri-radio mode or split 5 GHz mode, the 8x8 5 GHz radio is split into two independent 4x4 5 GHz radios. In the split 5 GHz Mode, **Radio 5 GHz Secondary** operates on channels from 36 to 64 and **Radio 5 GHz** operates on channels from 100 to 165.

To enable tri-radio, go to **Access Points > Radio** in the AP configuration dashboard, and select the **Split Radio** check-box.

The split 5 GHz radio can operate in the following modes:

- Access
- Monitor
- Spectrum

Enabling Tri-Radio Mode

To enable the tri-radio mode, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a group in the filter:
 - a. Set the filter to one of the options under **Groups**. Ensure that the filter selected contains at least one active access point.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Access Points**.
A list of access points is displayed in the **List** view.
 - To select an access point in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices > Access Points**.
A list of access points is displayed in the **List** view.
 - c. Click an access point listed under **Device Name**.
The dashboard context for the access point is displayed.
 - d. Under **Manage**, click **Devices > Access Point**.

2. Click the **Config** icon.
The tabs to configure access points are displayed.
3. Click the **Access Points** tab.
The **Access Points** page is displayed.
4. To edit an AP, select an AP in the **Access Points** table, and then click the edit icon.
5. Click **Radio**.
6. Select the **Split Radio** check-box.
7. Click **Save Settings**.

Tri-Radio Events

To view the tri-radio events, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed. To select a device in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices**, and then click **Access Points**.
 - c. A list of APs is displayed in the **List** view.
 - d. Click an AP listed under **Device Name**. The dashboard context for the AP is displayed.
2. Under **Analyze**, click **Alerts & Events**. The **Alerts & Events** page is displayed in the **List** view.
3. Click the **Events** tab.
A list of events is displayed in the **Events** table.

When the tri-radio mode is either enabled or disabled in an AP, the **Events** table displays the following details:

- The **Event Type** column includes the **AP Tri-Radio** type which can be used to filter tri-radio events.
- The **Description** column includes the status of the tri-radio mode in AP.



In Aruba Central (on-premises), the tri-radio feature is available only on AP-555 running Aruba Instant 8.6.0.0 or later versions.

By default, the AP-555 operates in dual radio mode.

Access Point > Overview > Summary

In the access point (AP) dashboard, the **Summary** tab displays the device details, network information, radio details including the topology of clients connected to each radio, and the health status of the AP in the network. The **Summary** tab displays the following sections:

- [Device](#)
- [Network](#)
- [Radios](#)
- [Data Path](#)
- [Health Status](#)

- [WLANS](#)
- [Actions](#)
- [Go Live](#)

Viewing the Overview > Summary Tab

To navigate to the **Summary** tab in the AP dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under Groups, Labels, or Sites. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP. The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**.
The **Summary** tab is displayed.
To exit the AP dashboard, click the back arrow on the filter.
You can change the time range for the **Summary** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

Device

The **Device** section displays all or some of the following details:

- **AP Model**—The AP hardware model.
- **Country Code**—Country code in which the AP operates.
- **MAC**—MAC address of the AP.
- **Serial Number**—Serial number of the AP.
- **Uptime**—Time since when the AP is operational.
- **Last Reboot Reason**—The reason for the latest rebooting of AP.
- **Firmware Version**—The firmware version running on the AP. If the device is running an older firmware version, this field prompts the user to upgrade to the latest firmware version along with the link to the **Maintenance > Firmware** page.
- **Configuration Status**—Displays the configuration status and the timestamp of the last device configuration changes.
- **Band Selection**—Displays the operating band of the AP. The supported bands are **Dual Band**, **Dual 5 GHz**, or **Tri-Radio**.
- **Power Draw**—The power utilized by the device in watts (W) or kilowatts (kW).
- **Power Negotiation**—The power in watts (W) negotiated on the ethernet port of the device in a wired network.
- **Recommended Power**—The recommended power in watts (W) negotiated on the ethernet port of the device in a wired network.
- **Controller**—The name of the controller.
- **Secondary Controller**—The name of the secondary controller.
- **Group**—The group to which the AP belongs. Click the group name to go to the **Overview > Summary** page for that group.



When an AP belongs to an unprovisioned group, the hyperlink to the unprovisioned group is disabled

- **Labels**—The labels associated with the AP. You can also add a new label to the AP by clicking the edit icon. To view all the labels associated with a device, hover your mouse over the **Labels** column.
- **LEDs on Access Point**—Enables the blinking of LEDs on the AP to identify the location. Click **Blink LED** to enable the blinking of LEDs on the AP. The default blinking time is set to 5 minutes and it stops automatically after 5 minutes. To stop the blinking, click **Stop Blinking**.
- **Site**—The site to which the AP belongs. Click the site name to go to the **Overview > Site Health** page for that site.
- **Location**—The currently configured physical location of an AP. Location detail is displayed only for APs with firmware version ArubaOS 8.9.0.0 or later.
- **Contact**—The currently configured contact of an AP. For example, E-mail ID, or contact number. Contact detail is displayed only for APs with firmware version ArubaOS 8.9.0.0 or later.
- **Note**—When you click the  edit icon, a text-box is displayed. It allows you to add information that can be used as reference. For example, AP location, and upgrade information.

Network

The **Network** section displays information of the network and interfaces to which the AP is connected. Along with the network profile name, the following fields are displayed in the **Network** section:

- **ETH0**—Displays the status of the ETH0 network.
- **Speed (Mbps)/Duplex**—The speed of the network measured in Mbps. This field also indicates whether the network has a full-duplex or half-duplex communication.
- **VLAN**—The number of VLAN connections associated with the network.
 - **LLDP Details**—Click the **LLDP Details** link to view the ETH0 LLDP details. The pop-up window displays the **Neighbor Name**, **Neighbor MAC**, **Neighbor Port**, and **Neighbor VLAN** details.
- **ETH1**—Displays the status of the ETH1 network.
- **Speed (Mbps)/Duplex**—The speed of the network measured in Mbps. This field also indicates whether the network has a full-duplex or half-duplex communication.
- **VLAN**—The number of VLAN connections associated with the network.
 - **LLDP Details**—Click the **LLDP Details** link to view the ETH1 LLDP details. The pop-up window displays the **Neighbor Name**, **Neighbor MAC**, **Neighbor Port**, and **Neighbor VLAN** details.
- **Current Uplink**—The current uplink connection on the AP.
- **Uplink connected to**—The switch name to which the AP is connected. Click this link to view the switch details page, if the switch is managed by Aruba Central (on-premises).
 - **Port**—The port number of the switch to which the AP is connected.
- **IP Address**—IP address of the AP.
- **Public IP Address**—IP address logged by servers when the AP device is connected through internet connection.
- **DNS Name Servers**—The server that has a directory of domain names and their associated IP addresses.
- **Default Gateway**—A 32 bit value that is used to uniquely identify the device on a public network.
- **NTP Server**—Displays information about the NTP Server.



From Aruba Central (on-premises) 2.5.4 release, **LLDP Details** feature is supported for Campus APs as well.

Radios

The **Radios** section displays the following information related to **Radio 2.4 GHz**, **Radio 5 GHz**, and **Radio 5 GHz Secondary**:

- **Mode**—The type of mode for the radios. For example, Client Access, Monitor, and Spectrum.
- **Status**—Displays the operational status of the radios connected to the AP. The status is as follows:
 - ● **Up**—Indicates that the radio is online.
 - ○ **Down**—Indicates that the radio is offline.
 - ○ **Down - Thermal shutdown**—Indicates that the radio is offline as the AP is operating under thermal management. For more information, see [Thermal Shutdown Support in IAP](#).
- **Radio MAC Address**—The MAC address of the radios connected to the AP.
- **Channel**—The channels assigned to the radios.
- **Power**—The transmit power of the radios.
- **Type**—The type of wireless LAN used for the radios.
- **Clients**—The number of clients connected to the AP.
- **Wireless Networks**—The number of SSIDs configured in the network.
- **Antenna**—The type of antennae. For example, internal and external.
- **Spatial Stream**—Displays the number of spatial streams. By default, the spatial stream value for **Radio 5 GHz** is 8x8. When tri-radio mode is enabled, the spatial stream values for **Radio 5 GHz** and **Radio 5 GHz (Secondary)** is 4x4.



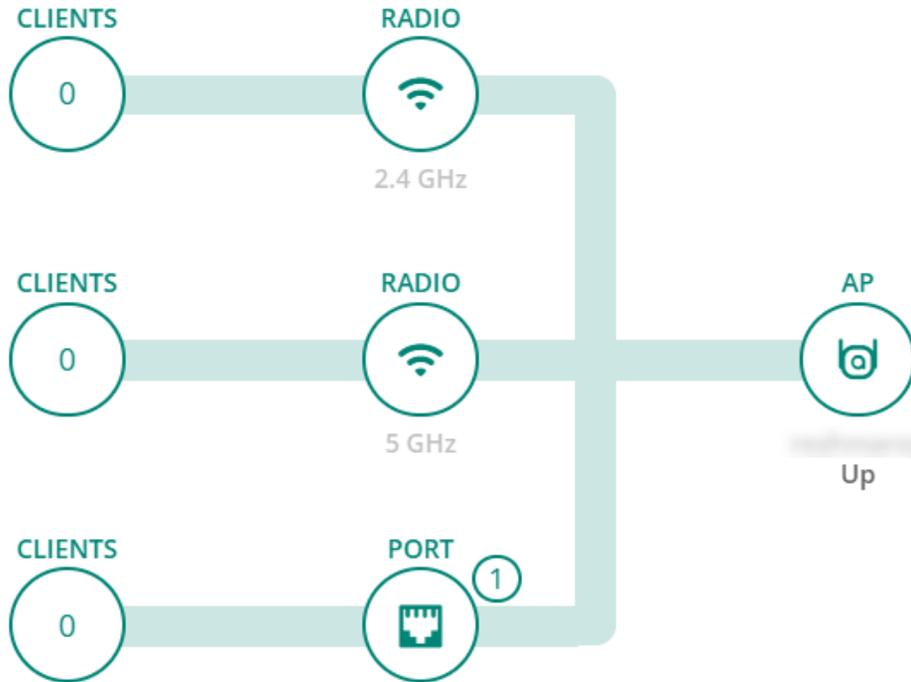
-
- When the Instant AP radios are set to spectrum scan mode, the **Channel** and **Power** values are empty.
 - The tri-radio feature is available only for AP-555. In the **Radios** section, the **Radio 5 GHz (Secondary)** data is available only if the tri-radio mode is enabled. For more information, see [About Tri-Radio Mode](#).
-

Data Path

The **Data Path** section displays the topology of the clients connected to each of the radios of the AP, which in turn is connected to switches or gateways through VLAN. When you hover over the upstream device in the data path topology, a pop-up displays the **Name**, **Serial Number**, and **Port** details of the upstream devices.

PORT shows the number of ports available in the AP that also includes USB ports. **CLIENTS** connected to the **PORT** in the data path shows the number of wired clients connected to the port.

Figure 24 Data Path



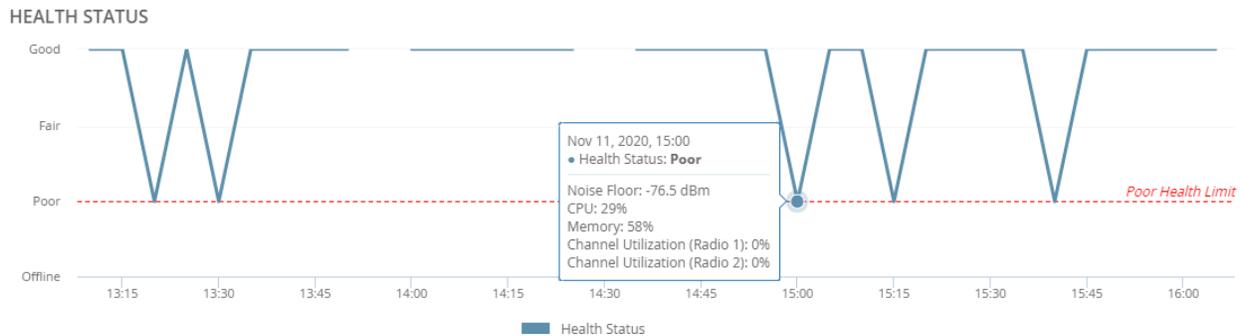
The tri-radio feature is available only for AP-555. In the **Data Path** section, the **5 GHz (Secondary)** data is available only if the tri-radio mode is enabled. For more information, see [About Tri-Radio Mode](#).

Health Status

The **Health Status** trend graph indicates the health status of the device in the network for the time selected in the time range filter. When you hover over the graph, you can view information such as date and time, Health Status, Noise Floor, CPU, Memory, Channel Utilization (Radio 1), Channel Utilization (Radio 2), and Channel Utilization (Radio 3).

In the **Health Status** graph, the **Poor Health Limit** text indicates the poor health limit of the device in the network.

Figure 25 Health Status



The tri-radio feature is available only for AP-555. In the **Health Status** section, the **Channel Utilization (Radio 3)** data is available only if the tri-radio mode is enabled. For more information, see [About Tri-Radio Mode](#).

WLANS

The **WLANS** table provides a list of all the SSIDs configured for the AP.

Figure 26 *WLANS*

WLANS (14) 				
Name	Type	VLANs	Security	
AP_555_gyu01Psk-Link05	Employee	1	WPA2 Personal	
BSSID (2)				
2.4 GHz		5 GHz (Secondary)		
BSSID	80:8d:b7:80:ce:1f	BSSID	80:8d:b7:80:ce:2f	
Radio Type	802.11ax	Radio Type	802.11ax	
Clients	0	Clients	0	
AP_555_gyu01Psk-Link06	Employee	1	WPA2 Personal	
AP_555_gyu01Psk-Link07	Employee	1	WPA2 Personal	

The **WLANS** table provides the following information:

- **Name**—Displays the name of the SSID.



In the **WLANS** table, the **Type**, **VLANs**, and **Security** values are empty.

Click  to expand an SSID in the **WLANS** table. When you expand an SSID in the **WLANS** table, you can view the following information for **2.4 GHz**, **5 GHz**, and **5 GHz (Secondary)** radios:

- **BSSID**—Displays the MAC address of the radio.
- **Radio Type**—Displays the type of radio.
- **Clients**—Displays the number of connected clients.

Click  to download the **.csv** file of the **WLANS** table.



- The tri-radio feature is available only for AP-555. In the **WLANS** table, the **5 GHz (Secondary)** data is available only if the tri-radio mode is enabled. For more information, see [About Tri-Radio Mode](#).
- In the **.csv** file of the **WLANS** table, the **5 GHz (Secondary)** columns are available only if the tri-radio mode is enabled.

Actions

The **Actions** drop-down list contains the following options:

- **Reboot AP**—Reboots the AP point. For more information, see [Rebooting an AP in the List View](#) and [Rebooting an AP in the Details Page](#).
- **Reboot Swarm**—Reboots the AP cluster. For more information, see [Rebooting an IAP Cluster](#).
- **Tech Support**—Enables the administrator to generate a tech support dump required for troubleshooting the AP. For more information, see [Tech Support for an IAP](#).

Go Live

Aruba Central (on-premises) supports live monitoring of IAPs that support Aruba Instant 8.4.0.0 firmware version and above. Aruba Central (on-premises) allows you to monitor live data of an AP updated at every 5

seconds. For more information, see [Enabling Live IAP Monitoring](#).

Access Point > Overview > AI Insights

In the access point (AP) dashboard, the **AI Insights** tab displays information on AP performance issues such as excessive channel changes, excessive reboots, airtime utilization, and memory utilization.

Viewing Access Points > AI Insights

To navigate to the **AI Insights** tab in the AP dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Access Points**. A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**.
The dashboard context for the AP is displayed.
4. In the AP dashboard context, click the **AI Insights** tab.
The **Insights** page is displayed.
5. To exit the AP dashboard, click the back arrow on the filter.

You can change the time range for the **AI Insights** tab by clicking the time range filter and selecting one of the available options: **3 hours, 1 day, 1 week, 1 month, and 3 months**.



AI Insights are displayed for the time range selected. Select the time range from the **Time Range Filter** (🔄) to filter reports.

AI Insights Categories

AI Insights are categorized in high, medium, and low priorities depending on the number of occurrences.

-  Red—High priority
-  Orange—Medium priority
-  Yellow—Low priority

AI Insights listed in the dashboard are sorted from high priority to low priority. The **AI Insights** dashboard displays a report of network events that could possibly affect the quality of the overall network performance. Each insight report provides specific details on the occurrences of these events for ease in debugging. For more information, see [The AI Insights Dashboard](#)

The **AP Insights** page displays the following insights:

- [Clients with High Wi-Fi Security Key-Exchange Failures](#)
- [Clients with High 802.1X Authentication Failures](#)
- [Clients with DHCP Server Connection Problems](#)
- [Clients with High Number of MAC Authentication Failures](#)
- [Clients with High Number of Wi-Fi Association Failures](#)
- [Clients with Captive Portal Authentication Problems](#)

Access Point > Overview > Floor Plan

In the access point (AP) dashboard, the **Floor Plan** tab provides information regarding the current location of the Instant Access Point (IAP).

Viewing the Overview > Floor Plan Tab

To navigate to the **Floor Plan** tab in the AP dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.

The dashboard context for the selected filter is displayed.

2. Under **Manage**, click **Devices > Access Points**.

A list of APs is displayed in the **List** view.

3. Click an AP listed under **Device Name**.

The dashboard context for the AP is displayed.

4. In the AP dashboard context, click the **Floor Plan** tab. The **Floor Plan** tab is displayed.

To exit the AP dashboard, click the back arrow on the filter.

You can change the time range for the **Floor Plan** tab by clicking the time range filter and selecting one of the available options: **3 hours, 1 day, 1 week, 1 month, and 3 months**.

The **Floor Plan** tab displays a sitemap and the floor plan showing the current location of the IAP. The sitemap is derived from the Visual RF application, if Visual RF service is enabled for the Aruba Central (on-premises) account. You can also edit the location of the IAP device by clicking the edit icon provided next to the address in the **Floor Plan** tab.

Actions

The **Actions** drop-down list contains the following options:

- **Reboot AP**—Reboots the AP. For more information, see [Rebooting an AP in the Details Page](#) and [Rebooting an AP in the List View](#).
- **Reboot Swarm**—Reboots the AP cluster. For more information, see [Rebooting an IAP Cluster](#).
- **Tech Support**—Enables the administrator to generate a tech support dump required for troubleshooting the AP. For more information, see [Tech Support for an IAP](#).

Go Live

Aruba Central (on-premises) supports live monitoring of IAPs that support Aruba Instant 8.4.0.0 firmware version and above. Aruba Central (on-premises) allows you to monitor live data of an AP updated at every 5 seconds. For more information, see [Enabling Live IAP Monitoring](#).

Access Point > Overview > Performance

In the access point (AP) dashboard, the **Performance** tab displays the size of data transmitted through the AP.

Viewing the Overview > Performance Tab

To navigate to the **Performance** tab in the AP dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under groups, labels, or sites. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP. The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Access Points**. A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**. The dashboard context for the AP is displayed.
4. In the AP dashboard context, click the **Performance** tab. The **Performance** tab is displayed.

To exit the AP dashboard, click the back arrow on the filter.

You can change the time range for the **Performance** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

The **Performance** tab provides the following details:

■ **Throughput**

The **Throughput** graph indicates the size of data sent to and received by the device in bits per second for the wired or wireless networks. For example, Eth 0 or Eth 1 wired network profiles and specific SSIDs of wireless networks. You can also view data for all the wireless SSIDs by selecting **All SSIDs** from the drop-down list. You can view the overall data usage measured in bytes in the **Overall Usage** field.

■ **Clients**

The **Clients** graph indicates the number of clients connected to the device for the wired, wireless, or radio network profiles for a selected time range in the time range filter. For example, wired for wired network profile, specific SSID or All SSIDs for wireless network profile, and 2.4 GHz, 5 GHz, or 2.4 GHz&5 GHz for radio network profile. You can select a specific network profile from the drop-down list provided in the **Clients** section to view the date, time and number of clients connected.



When you hover over the **Throughput** and **Clients** graphs, it displays specific data for the selected timestamp.

Actions

The **Actions** drop-down list contains the following options:

- **Reboot AP**—Reboots the AP. For more information, see [Rebooting an AP in the Details Page on page 375](#) and [Rebooting an AP in the List View on page 356](#).
- **Reboot Swarm**—Reboots the AP cluster. For more information, see [Rebooting an IAP Cluster](#).
- **Tech Support**—Enables the administrator to generate a tech support dump required for troubleshooting the AP. For more information, see [Tech Support for an IAP](#).

Go Live

Aruba Central (on-premises) supports live monitoring of IAPs that support Aruba Instant 8.4.0.0 firmware version and above. Aruba Central (on-premises) allows you to monitor live data of an AP updated at every 5 seconds. For more information, see [Enabling Live IAP Monitoring](#).

Access Point > Overview > RF

In the access point (AP) dashboard, the **RF** tab provides details corresponding to 2.4 GHz, 5 GHz, and 5 GHz Secondary radios of the AP.

Viewing the Overview > RF Tab

To navigate to the **RF** tab in the AP dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under groups, labels, or sites. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP. The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Access Points**. A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**. The dashboard context for the AP is displayed.
4. In the AP dashboard context, click the **RF** tab. The **RF** tab is displayed.

To exit the AP dashboard, click the back arrow on the filter.

You can change the time range for the **RF** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

You can hover over the graph to view more information. You can select or clear an option in each graph to filter the data displayed on the graph. For example, if you uncheck the box corresponding to **Receiving** and **Non-Wifi interference** in the **Channel Utilization** graph, only **Transmitting** data is displayed on the graph.

The **RF** tab provides the following details corresponding to **2.4 GHz** and **5 GHz** radio channels of the AP:

Channel Utilization

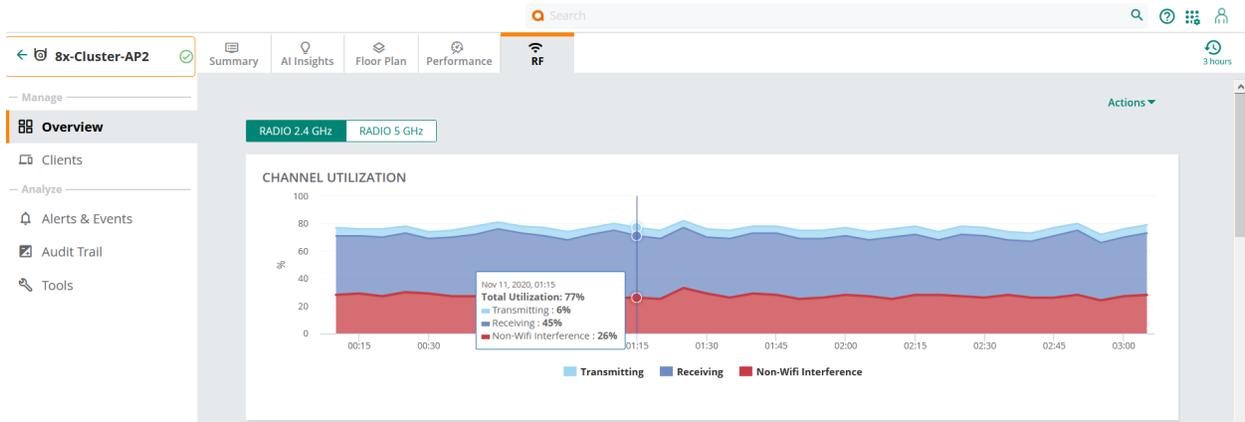
The **Channel Utilization** graph indicates the percentage of channel utilization for the selected time range from the time range filter. The channel utilization information is categorized as follows:

- **Transmitting**: The percentage of channel currently being transmitted.
- **Receiving**: The percentage of channel currently being received.
- **Non-Wifi Interference**: The percentage of channel currently being used by non-Wi-Fi interferers.



Total Utilization is the sum of **Transmitting**, **Receiving**, and **Non-Wifi interference**, which indicates the total percentage of channel utilization for the selected time range.

The following figure displays the channel utilization graph for 2.4 GHz radio channel:



Noise Floor

The **Noise Floor** graph indicates the noise floor detected in the network to which the device belongs.

Frames - 802.11

The **Frames - 802.11** line graph indicates the trend of frames transmitted through the network. The frames can be one of the following types: **Drops**, **Errors**, and **Retries**. The graph indicates the status of data frames that were dropped, encountered errors, retried to be transferred, in a wireless network. You can see the graph in percentage or frames/sec.



Only Campus APs and Remote APs support the **Issues & Transmitted Frames** and **Issue %** filter options.

Select one of the following option from the drop-down:

- **Issues & Transmitted Frames**—Select to view the trend value for transmitted frames along with retries, errors, and drops in frames per second
- **Issue %**—Select to view the trend value for retries, errors, and drops in percentage.

Figure 27 *Frames - 802.11 Graph*



Radio Errors

The **Radio Errors** graph indicates the **Total Packets**, **Physical Errors**, and **MAC Errors** in packets per second.



Only Campus APs and Remote APs support the **Physical Errors**, and **MAC Errors** options.

Figure 28 Radio Errors Graph



Channel Quality

The **Channel Quality** graph indicates the quality of channel in percentage.



When you hover over the **Channel Utilization**, **Noise Floor**, **Frames - 802.11**, and **Channel Quality** graphs, it displays specific data for the selected timestamp.

The tri-radio feature is available only for AP-555. In the **RF** tab, the **Radio 5 GHz (Secondary)** tab is available only if the tri-radio mode is enabled. For more information, see [About Tri-Radio Mode](#).

Actions

The **Actions** drop-down list contains the following options:

- **Reboot AP**—Reboots the AP. For more information, see [Rebooting an AP in the Details Page](#).
- **Reboot Swarm**—Reboots the AP cluster. For more information, see [Rebooting an IAP Cluster](#).
- **Tech Support**—Enables the administrator to generate a tech support dump required for troubleshooting the AP. For more information, see [Tech Support for an IAP](#).

Go Live

Aruba Central (on-premises) supports live monitoring of IAPs that support Aruba Instant 8.4.0.0 firmware version and above. Aruba Central (on-premises) allows you to monitor live data of an AP updated at every 5 seconds. For more information, see [Enabling Live IAP Monitoring](#).

Access Point > Overview > Spectrum

In the access point (AP) dashboard, the **Spectrum** tab provides details for all Wifi and non-Wifi devices associated to each radio.

When the radios of Instant Access Point (IAP) are set to spectrum scan mode, the IAP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference from neighboring IAPs or interfering devices such as microwaves and cordless phones. To enable the spectrum scan feature on a specific radio of an AP, see [Access Points Configuration Parameters](#).



The spectrum scan feature is available only on IAP devices running Aruba Instant 8.5.0.1 firmware version and later.

When the spectrum scan feature is enabled, the Instant AP does not provide services to clients. The **Spectrum** tab displays the following sections:

- [Channel Utilization and Quality](#)
- [Interfering Devices](#)
- [Actions](#)
- [Go Live](#)

Viewing the Overview > Spectrum Tab

To navigate to the **Spectrum** tab in the AP dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**.
The dashboard context for the AP is displayed.
4. In the AP dashboard context, click the **Spectrum** tab. The **Spectrum** tab is displayed.

To exit the AP dashboard, click the back arrow on the filter.

You can change the time range for the **Spectrum** tab by clicking the time range filter and selecting one of the available options: **3 hours, 1 day, 1 week, 1 month, and 3 months**.

Channel Utilization and Quality

Click the **Chart** icon to view the **Channel Utilization and Quality** details corresponding to **2.4 GHz** and **5 GHz** radios of the AP. Click the **2.4 GHz** and **5 GHz** tabs on the **Channel Utilization and Quality** label to view the **Channel Utilization** and **Quality** graphs for the radios.

- **Channel Utilization**—The **Channel Utilization** graph indicates the percentage of channel utilization for the **Available, Interference, and Wi-Fi Utilization** categories associated to **2.4 GHz** and **5 GHz** radios. You can view the following channel metrics when you hover over the **Channel Utilization** bar graph:

Table 88: *Channel Utilization Metrics*

Metrics	Description
Channel	The channel number of the radio.
Available	The percentage of the channel currently available for use.
Interference	The percentage of the channel currently being used by interfering devices.

Metrics	Description
Microwave	The percentage of the channel currently being used by microwaves. Common residential microwave ovens with a single magnetron are classified as a Microwave. These types of microwave ovens may be used in cafeterias, break rooms, dormitories, and similar environments. Some industrial, healthcare, or manufacturing environments may also have other equipment that functions like a microwave and may also be classified as a Microwave device.
Bluetooth	The percentage of the channel currently being used by bluetooth devices. Any device that uses the Bluetooth protocol to communicate in the 2.4 GHz band is classified as a Bluetooth device. Bluetooth uses a frequency hopping protocol.
Cordless Phone	The percentage of the channel currently being used by cordless phones.
Wi-Fi Utilization	The percentage of the channel currently being used by Wi-Fi devices.

- **Quality**—The **Quality** graph display the channel quality corresponding to each of the WiFi and non-WiFi devices connected to the radios. When you hover over the **Quality** bar graph, the following channel metrics are displayed:

Table 89: *Channel Quality Metrics*

Metrics	Description
Channel	The channel number of the radio.
Quality	Current relative quality of the channel.
Known APs	Number of valid Instant APs identified on the radio channel.
Unknown APs	Number of invalid or rogue Instant APs identified on the radio channel.
Max AP Signal	Signal strength of the Instant AP that has the maximum signal strength on a channel in dBm.
Max Interference	Signal strength of the non-Wi-Fi device that has the highest signal strength in dBm.
Max AP SSID	The network SSID with maximum APs.
Max AP BSSID	The network SSID with maximum APs.
SNIR	The measure of SNIR detected in the network in dB.
Noise Floor	The noise at the radio receivers of the radios.

Interfering Devices

Table 90: *Interfering Devices Table*

Metrics	Description
Type	Device type. This parameter can be any of the following: <ul style="list-style-type: none">■ Audio FF (fixed frequency)■ Bluetooth■ Cordless base FH (frequency hopper)■ Cordless phone FF (fixed frequency)■ Cordless network FH (frequency hopper)■ Generic FF (fixed frequency)■ Generic FH (frequency hopper)■ Generic interferer■ Microwave■ Microwave inverter■ Video■ Xbox
ID	ID number assigned to the device by the spectrum monitor. Spectrum monitors assign a unique spectrum ID per device type.
Central Frequency	Center frequency of the signal sent from the device.
Bandwidth	Channel bandwidth used by the device in KHz.
Affected Channels	Radio channels affected by the wireless device.
Signal Strength	Strength of the signal sent from the device measured in dBm.
Duty Cycle	The device duty cycle. This value represents the percent of time the device broadcasts a signal.
First Seen	Time at which the device was first detected.
Last Seen	Time at which the device status was updated.

Click the **List** icon to view **Interfering Devices** details detected by the spectrum scanner. The page displays a table with following details of interfering devices:



The data displayed in the **Spectrum** tab is refreshed every 15 seconds. Aruba Central (on-premises) displays the last recorded data for 30 minutes, if the device turns offline.

Actions

The **Actions** drop-down list contains the following options:

- **Reboot AP**—Reboots the AP. For more information, see [Rebooting an AP in the Details Page on page 375](#) and [Rebooting an AP in the List View on page 356](#).
- **Reboot Swarm**—Reboots the AP cluster. For more information, see [Rebooting an IAP Cluster](#).

- **Tech Support**—Enables the administrator to generate a tech support dump required for troubleshooting the AP. For more information, see [Tech Support for an IAP](#).

Go Live

Aruba Central (on-premises) supports live monitoring of IAPs that support Aruba Instant 8.4.0.0 firmware version and above. Aruba Central (on-premises) allows you to monitor live data of an AP updated at every 5 seconds. For more information, see [Enabling Live IAP Monitoring](#).

Access Point > Security > VPN

The **VPN** tab provides information on VPN connections associated with the virtual controller along with information on the tunnels and the data usage through each of the tunnels.

Viewing the Security > VPN Tab

To navigate to the **VPN** tab, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**.
The dashboard context for the AP is displayed.
4. Under **Manage**, click **Security > VPN**.
The **VPN** tab is displayed.

You can change the time range for the **VPN** tab by clicking the time range filter and selecting one of the available options: **3 hours, 1 day, 1 week, 1 month, and 3 months**.

The **VPN** tab provides the following information:

- **VPNC Tunnels Summary**—The section displays information on tunnels with the following details:
 - **Total**—Total tunnels established.
 - **Up**—Number of tunnels currently active.
 - **Down**—Number of tunnels currently inactive.
 - **Peers**—Number of peer tunnels currently active.
The **Tunnel** table displays information on tunnels with the following columns:
 - **Tunnel**—The type of the tunnels used in the VPN. For example, primary, secondary, or backup.
 - **Status**—The status of the tunnel.
 - **Source**—The source address of the tunnel.
 - **Destination**—The destination address of the tunnel.
- **Throughput Usage Per VPN**—The **Throughput Usage Per VPN** graph indicates the successful data usage per VPN in Mbps for the primary or backup tunnel selected from the drop-down list. The **Throughput Usage Per VPN** displays a linear graph of sent and received data in the virtual private network.

- The **Gateway** tab provides information on the gateways to which the AP is connected. The tab displays the following details:
- **Tunnels Summary**—The section displays information on tunnels with the following details:

Rebooting an AP in the Details Page

You can reboot an Instant Access Point, Campus Access Point, or Remote Access Point using the Aruba Central (on-premises) UI.

For information about how to reboot an AP in the **List** view, see [Rebooting an AP in the List View](#).

To reboot, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under groups, labels, or sites. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP. The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**.
The dashboard context for the AP is displayed.
4. In the **Actions** drop-down list, click **Reboot AP**.
A **Reboot** dialog box is displayed.
5. Click **Reboot** to reboot the AP.



The AP dashboard takes approximately a minute to update the interface status, after the AP is rebooted and reconnected to Aruba Central (on-premises).

Rebooting an IAP Cluster

You can reboot an Instant Access Point (IAP) cluster using the Aruba Central (on-premises) UI.

To reboot an IAP cluster, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**.
The dashboard context for the AP is displayed.
4. In the **Actions** drop-down list, click **Reboot Swarm**.
A **Reboot** dialog box is displayed.
5. Click **Yes** to reboot the AP cluster.



The AP dashboard takes less than a minute to update the interface status, after the VC is rebooted and reconnected to Aruba Central (on-premises).

Tech Support for an IAP

In Aruba Central (on-premises) UI, the administrators can generate a tech support dump required for troubleshooting the Instant Access Point (IAP).

To generate a tech support dump for an IAP, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**.
The dashboard context for the AP is displayed.
4. In the **Actions** drop-down list, click **Tech Support**.
The **Commands** page is displayed. In the **Commands** page, the **Device Type** and **Available Devices** fields are automatically selected. The `AP Tech Support Dump` command is automatically selected in the **Selected Commands** pane.
5. Click **Run**. The output is displayed in the **Device Output** section.

For more information, see [Advanced Device Troubleshooting](#).

Enabling Live IAP Monitoring

Aruba Central (on-premises) supports live monitoring of Instant APs that support Aruba Instant 8.4.0.0 firmware version and above. Aruba Central (on-premises) allows you to monitor live data of an AP updated at every 5 seconds.

Enabling and Disabling Go Live

To enable and disable the live monitoring of an AP, complete the following steps:

- In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active access point. The dashboard context for the selected filter is displayed.
- Under **Manage**, click **Devices > Access Points**. A list of access points is displayed in the **List** view.
- Click an access point listed under **Device Name**. The dashboard context for the access point is displayed.
- Click the **Go Live** button to start live monitoring of the AP.
- Click the **Stop Live** button to exit live monitoring of the AP.

The **Go Live** feature is not applicable for offline Instant APs. The **Go Live** button remains grayed-out for all the APs that are not associated with Instant AP devices running Aruba Instant 8.4.0.0 firmware version and above

Aruba Central (on-premises) allows you to monitor live data for 15 minutes. After this time period, Aruba Central (on-premises) redirects to the AP dashboard in a non-live mode to display the monitoring details for the time selected in the **Time Range Filter**. For more information on AP dashboard in a non-live mode, see [Access Point > Overview > Summary](#).



AP Details in Go Live Mode

When you click the **Go Live** button, the page displays live graphs based on noise floor, frames, and channel quality of the neighboring RF devices for 15 minutes, until you select **Stop Live** button.

The page displays **Noise Floor**, **Frames**, and **Channel Quality** live graphs for **Radio 2.4 GHz**, **Radio 5 GHz**, and **Radio 5 GHz Secondary** radios.

Important Information

- The Go Live feature is not applicable for offline APs.
- Aruba Central allows you to monitor live data for 15 minutes. After this time period, Aruba Central redirects to the AP dashboard in a non-live mode to display the monitoring details for the time selected in the **Time Range Filter**. For more information on AP dashboard in a non-live mode, see [Access Point > Overview > Summary](#).
- In **Go Live** mode, AP dashboard updates and displays data at every 5 seconds.
- The tri-radio feature is available only for AP-555. In the **Go Live** page, the **Radio 5 GHz (Secondary)** tab is available only if the tri-radio mode is enabled. For more information, see [About Tri-Radio Mode](#).
- The time range selected in the **Time Range Filter** is not applicable when the **Go Live** button is enabled.
- You can monitor live data for multiple APs simultaneously on different tabs.

Replacing an Access Point

Aruba Central (on-premises) now supports Campus AP, Remote AP, and Instant Access Point replacement workflow. You can now replace the APs from the AP dashboard in the Aruba Central (on-premises) WebUI. Navigate to **Manage > Overview > Summary** page to replace the AP.

Before you Replace a Campus AP or Remote AP

Following are the important points to consider before you replace a Campus AP or Remote AP:

- The device that has to be replaced must be offline.
- The model number of the old AP and the new AP can be different. The AP that replaces another AP need not be of the same model.
- The old AP must be a licensed device, and ensure to have an additional license available because the new AP will procure a license during replacement.
- The new AP must be part of the device inventory.
- After the AP is replaced, the new AP gets licensed and inherits the Group, Label, and Site parameters along with floor plan from the old device.
- The new AP does not inherit any configuration from the old AP.
- After the AP is replaced, the old AP is removed from:
 - Device inventory
 - Monitoring view, if associated
 - Visual RF if the AP is associated with the Visual RF floor plan
 - Site, Label, and Group, if associated
- The new AP replaces the old AP in the VisualRF floor plan if the old AP was associated with the VisualRF floor plan.
- The old AP is deleted from the monitoring view only after the validation process is complete. This validation process takes about 15 minutes.

Before you Replace an Instant AP

Following are the important points to consider before you replace an Instant Access Point:

- The device that has to be replaced must be offline.
- The model number of the old AP and the new AP must be the same. For example, an AP-505 must be replaced with an AP-505 only.
- The new AP must be part of the device inventory.
- Subscription must be assigned for the new AP.
- If the AP that is going to be replaced is a member, the new AP automatically inherits the configuration from the leader of the group.
- If the AP that is going to be replaced is a leader, the new AP does not automatically become the leader. Although the replacement procedure ensures that the new AP inherits the configuration settings, a new leader is elected after the new AP joins the cluster.
- After the AP is replaced, the new AP inherits the Group, Label, Site parameters, firmware version, and device name from the old device.
- The old AP is deleted from the monitoring view only after the validation process is complete. This validation process takes 15 minutes.
- After the device is replaced, the old AP is not removed from the device inventory. The AP can be reused in the future.

Replacing an AP from the Summary Page

To replace an AP from the summary page, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click **Offline** to view a list of offline APs in the **Access Points** table.
4. In the **Device Name** column, click the AP that you want to replace.
The **Overview > Summary** page is displayed in the AP dashboard.
5. In the **Actions** drop-down list, click **Replace Device**.
6. In the **Replace Device** pop-up window, click **Replace**.
7. In the **Replace Access Point** page, perform the following steps:
 - a. Select a replacement AP and click **Next**.
 - b. Verify the attributes and click **Next**.

Table 91: *Parameters for Campus AP and Remote AP*

Parameters	Description
Device name	The device name of the new AP.
Serial number	The serial number for each AP is a unique value. The serial number reflects the value of the new AP.
Subscription assigned	The new AP is assigned the same subscription as the old one. For example, if the old AP had a Foundation license, the new AP is assigned the same Foundation license.

Table 91: Parameters for Campus AP and Remote AP

Parameters	Description
Model number	The model number of the new AP.
Group name	The group name that is inherited from the old AP.
Site assigned	The site that is inherited from the old AP.
Label(s) assigned	The label(s) that is inherited from the old AP.

Table 92: Parameters for an Instant Access Point

Parameters	Description
Device name	The name that is inherited from the old AP.
Serial number	The serial number for each AP is a unique value. The serial number reflects the value of the new AP.
Subscription assigned	The same subscription is assigned to the new AP. For example, if the old AP had a Foundation license, the new AP is assigned the same Foundation license.
Model number	The model number is inherited from the old AP.
Group name	The group name that is inherited from the old AP.
Site assigned	The site that is inherited from the old AP.
Firmware version	Firmware version is displayed as Unknown for the new AP. However, after the new AP is connected and the configuration is synchronized, the firmware is upgraded to the same version as the old device.



In the **Confirmation** page, the following warning is displayed:

This is an irreversible operation. Do you want to proceed with the device replacement?

- c. In the **Confirmation** page, review the old and new device details and click **Replace**.
 - d. In the **Request Accepted** pop-up window, click **Done** to continue the workflow.
8. In the **Access Point Details** page, a progress bar displays the device replacement status. Hover over the progress bar to view more details.
 9. Optionally, hover over the progress bar and click **Terminate** if you wish you to discontinue replacing the device.



If the device replacement process fails, click **Terminate** to end the procedure and retry.

10. Connect the new AP.

The status in the progress bar changes to **Device replacement in progress**. Hover over the progress bar to view more details.



If the firmware upgrade fails for an Instant Access Point, Aruba Central automatically retries one more time. If the firmware upgrade fails for the second time, the **Firmware Updated** status changes to **Failed**. You can manually upgrade the firmware. For more information, see [Upgrading Device Firmware](#).

11. Navigate to the AP **Summary** page of the new device.
 - a. In the **Network Operations** app, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
 - b. Under **Manage**, click **Devices > Access Points**.
A list of AP is displayed in the **List** view.
 - c. Click **Online** to view a list of online APs in the **Access Points** table.
 - d. In the **Device Name** column, click the new AP.
The **Overview > Summary** page is displayed in the AP dashboard.
 - e. In the **Device** section, you can view the following details:
 - AP Model
 - Country Code
 - MAC Address
 - Serial Number
 - Last Seen
 - Last Reboot Reason
 - Firmware version
 - Configuration Status
 - Band Selection
 - Power Negotiation
 - Group
 - Labels
 - Site

12. The **Audit Trail** page displays all the logs generated during the device replacement process. To view the logs, set the filter to **Global**. Under **Analyze**, click **Audit Trail**.

The **Audit Trail** table is displayed.

Replacing APs in Bulk

Aruba Central (on-premises) now allows you to perform bulk replacement of Campus APs and Remote APs in the WebUI. You can replace the APs in bulk by using one of the following pages available under **Network Operations** app:

- **Manage > Overview > Device Replacement** under **Sites** filter. For more information, see [Bulk Replacement from the Device Replacement Page](#).
- **Manage Sites** under **Maintain > Organization > Network Structure > Sites**. For more information, see [Bulk Replacement from the Manage Sites Page](#).

Important Points

Following are the important points to consider when replacing APs in bulk:

- You can replace only the APs that are offline.
- The model number of the old APs and the new APs can be different.
- Bulk replacement of APs is applicable to Campus APs and Remote APs only.
- You cannot rename APs by using **Device Replacement** or **Manage Sites** page. To rename APs, see [Renaming an AP](#).
- The old APs must be licensed devices. Also, ensure to have additional licenses available because the new APs will procure licenses during replacement.
- The new APs must be part of the device inventory, and must be licensed in Aruba Central (on-premises).
- After the APs are replaced, the new APs inherit the Group, Label, Site, and Visual RF parameters along with licenses from the old APs.
- After the APs are replaced, the old APs are removed from:
 - Device inventory
 - Monitoring view, if associated
 - Visual RF, if the APs are associated with the Visual RF floor plan
 - Site, Label, and Group, if associated
- The new APs replace the old or faulty APs that were associated with the VisualRF floor plan.
- Bulk replacement of APs is an irreversible process. After the APs are replaced in bulk, you cannot revert to the old APs.

Bulk Replacement from the Device Replacement Page

To replace APs in bulk by using the **Device Replacement** page, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the relevant options under **Sites**. The dashboard context for the selected site is displayed.
2. Under **Manage**, click **Overview > Device Replacement**. The **Bulk Device Replacement** page is displayed.
3. Select the number of offline APs under **Devices** table that you want to replace, and click the  icon. The **Replace Devices** page is displayed.



You can select a maximum of 30 offline devices from the **Devices** table for bulk replacement.

4. In the **Devices** table, select the serial number of the new AP from the **New Device** drop-down list.



In the **Confirmation** page, the following warning is displayed—
This is an irreversible operation. Do you want to proceed with the device replacement?

5. Click **Replace**. The **Replacement Status** pop-up window is displayed.



The **Replacement Status** pop-up window displays the **The replacement request has been accepted** message for each of the newly replaced APs.

6. Click **Done**.

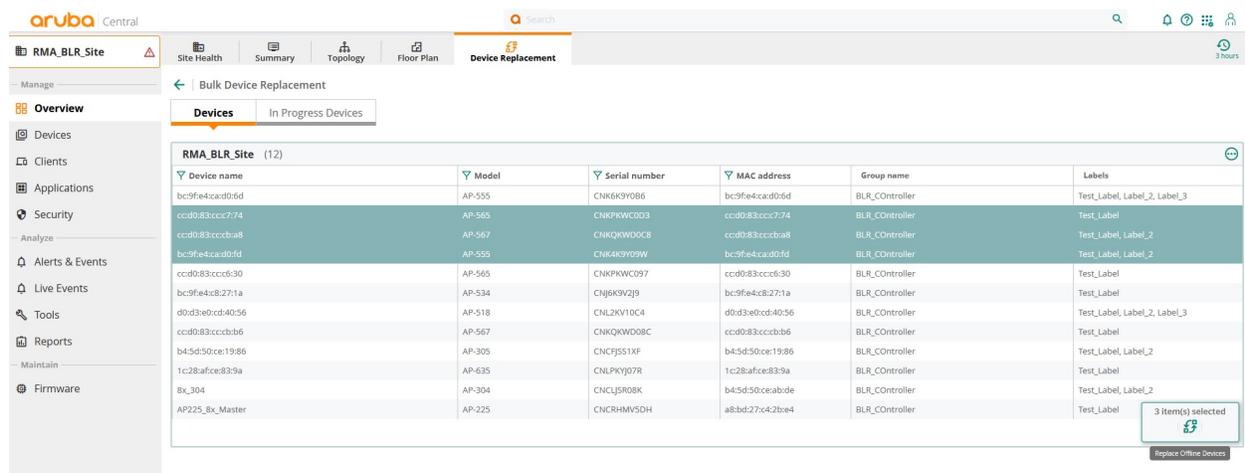
The **In Progress Devices** table under **Bulk Device Replacement** displays the parameters of the new devices as described in [Table 93](#).

Table 93: *In Progress Devices Parameters*

Parameters	Description
Faulty device serial	The faulty serial number of the previous AP.
New device serial	The serial number for each AP is a unique value. The serial number reflects the value of the new AP.
License assignment	The status of the license assigned to the new AP.
Group assignment	The status of the group name inherited from the old AP.
Site assignment	The status of the site that is inherited from the old AP.
Labels assignment	The status of the labels that are inherited from the old AP.
Status	The bulk device replacement status.

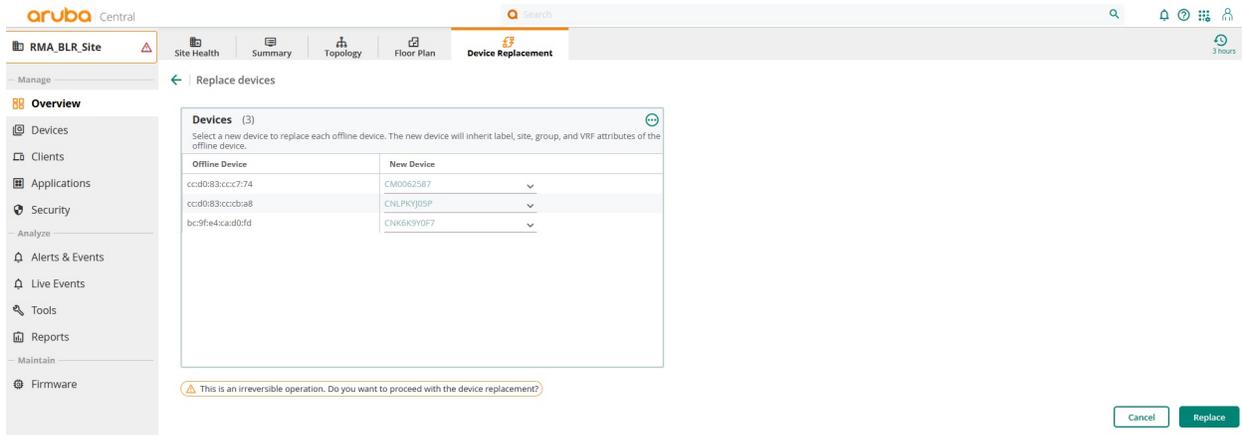
The following figure displays three offline APs that are selected for replacement in the **Bulk Device Replacement** page.

Figure 29 *Bulk Device Replacement*



The following figure displays the **Replace Devices** page where serial number of the new APs are selected for replacement from the **New Device** drop-down list.

Figure 30 *Replace Devices*



Bulk Replacement from the Manage Sites Page

To replace APs in bulk by using the **Manage Sites** page, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Sites** tile.
The **Manage Sites** page is displayed.
4. From the list of sites, select the site whose APs you want to replace.
5. Click the  icon.
The **Replace Offline Devices** pop-up window is displayed.
6. Click **Replace**.
The **Bulk Device Replacement** page under **Manage > Overview > Device Replacement** is displayed.
7. Select the number of offline APs under **Devices** table that you want to replace, and click the  icon.
The **Replace Devices** page is displayed.



You can select a maximum of 30 offline devices from the **Devices** table for bulk replacement.

8. In the **Devices** table, select the serial number of the new AP from the **New Device** drop-down list.



In the **Confirmation** page, the following warning is displayed—
This is an irreversible operation. Do you want to proceed with the device replacement?

9. Click **Replace**.
The **Replacement Status** pop-up window is displayed.

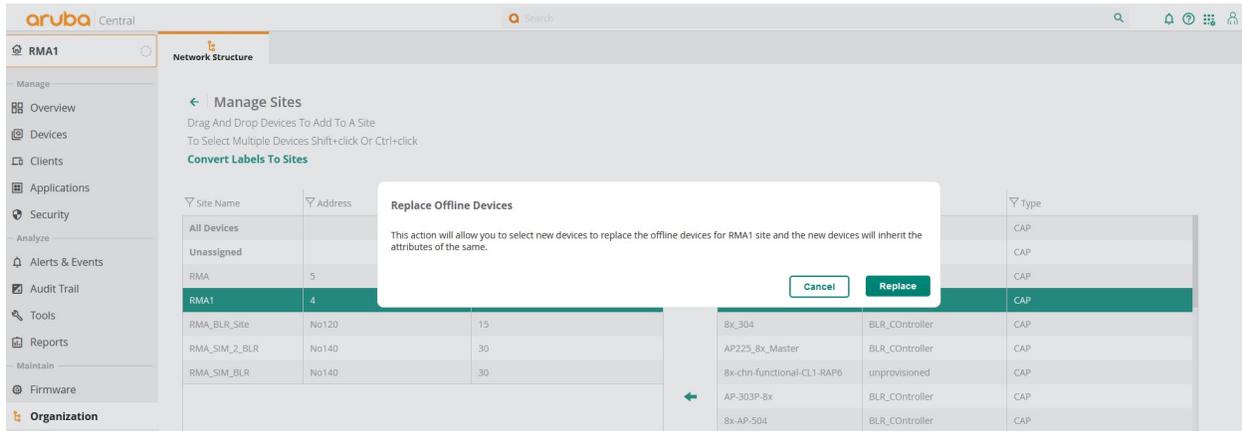


The **Replacement Status** pop-up window displays the **The replacement request has been accepted** message for each of the newly replaced APs.

10. Click **Done**.

The following figure displays the **Replace Offline Devices** pop-up window under **Manage Sites** page.

Figure 31 *Manage Sites*



Access Point > Clients > Clients

In the access point (AP) dashboard, the **Clients** tab displays details of all the clients connected to a specific AP.

Viewing the Access Point > Clients > Clients Tab

To navigate to the **Clients** tab in the AP dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.

The dashboard context for the selected filter is displayed.

2. Under **Manage**, click **Devices > Access Points**.

A list of APs is displayed in the **List** view.

3. Click an AP listed under **Device Name**.

The dashboard context for the AP is displayed.

4. Under **Manage**, click **Clients**.

The **Clients** page is displayed in the **List** view.

To exit the Clients dashboard, click the back arrow on the filter.

You can change the time range for the **Clients** tab by clicking the time range filter and selecting one of the available options: **3 hours, 1 day, 1 week, 1 month, and 3 months**.



For more information, see [All Clients](#).

Access Point > Alerts & Events > Alerts & Events

In the access point (AP) dashboard, the **Alerts & Events** tab displays details of the alerts and events generated for the AP.

Viewing the Access Point > Alerts & Events > Alerts & Events Tab

To navigate to the **Alerts & Events** tab in the AP dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**.
The dashboard context for the AP is displayed.
4. Under **Analyze**, click **Alerts & Events**.
The **Alerts & Events** page is displayed in the **List** view.
To exit the Alerts & Events dashboard, click the back arrow on the filter.



For more information, see [Alerts & Events](#). You can also configure and enable certain categories of AP alerts.
For more information, see [Access Point Alerts](#).

AP Live Events

Aruba Central (on-premises) allows you to troubleshoot issues related to access points (APs). The AP Live events feature is similar to client live troubleshooting, but in this case, we can enable live events at the AP level. Currently users can subscribe to Radio, VPN, and Spectrum events.



The AP must be running Aruba InstantOS 8.5.0.0 or later versions to support this feature. AP Live Events is not supported in single node deployments.

Troubleshooting an AP

Aruba Central allows you to troubleshoot issues related to an AP in real time for detailed analysis.

To troubleshoot an AP at the device level, perform the following steps:

1. In the **Network Operations** app, select an AP from the **Device** list.
The dashboard context for the selected AP is displayed.
2. Under **Analyze**, click **Live Events**. The **Live Events** page is displayed.

The live monitoring session starts automatically. The status of the troubleshooting is displayed every minute. The troubleshooting session runs for a duration of 15 minutes. You can stop live troubleshooting at any point by clicking **Stop Troubleshooting** to go back to the historical view.

After the live troubleshooting session ends, the details of the events are displayed in the live events table.

Live Events Details

The following details are captured and displayed in the **Live Events** table:

- **Occurred On**—Displays the timestamp of the event. Use the filter option to filter the events by date and time.
- **Category**—Displays the category of the event. Use the filter option to filter the events by category.
- **Description**—Displays a description of the event. Use the filter option to filter the events based on description.

You can download the list of live events to a CSV file for offline analysis. To download live events, click the

Download CSV  icon on the **Live Events** table.

AOS-CX is a modern and fully programmable operating system built using a database-centric design, which ensures higher availability and dynamic software process changes for reduced downtime. In addition to robust hardware reliability, the AOS-CX operating system includes additional software elements not available with traditional systems, including:

- Automated visibility to help IT organizations scale
- Simplified programmability
- Faster resolution with network insights
- High availability
- Ease of roll-back to previous configurations

The AOS-CX operating system is a modular, database-centric operating system. Every aspect of the switch configuration and state information is modeled in the AOS-CX switch configuration and state database, including configuration information, status of all features, and network analytics. The AOS-CX operating system also includes a time series database, which acts as a built-in network record. The time series database makes the data seamlessly available to Aruba Network Analytics Engine agents that use rules that evaluate network conditions over time.

Aruba Central (on-premises) offers a cloud-based management platform for managing AOS-CX infrastructure. It simplifies switch management with flexible configuration options, monitoring dashboards, and troubleshooting tools.

- [Getting Started with AOS-CX Deployments](#)
- [Provisioning Factory Default AOS-CX Switches](#)
- [Provisioning Pre-Configured AOS-CX Switches](#)
- [Using Configuration Templates for AOS-CX Switch Management](#)
- [Configuring AOS-CX Switches in UI Groups](#)
- [Configuration Workflow for AOS-CX Switches in UI Groups](#)
- [Caveats for Using AOS-CX Switches in Aruba Central \(on-premises\)](#)
- [Managing an AOS-CX VSF Stack](#)

Getting Started with AOS-CX Deployments

Before you get started with your onboarding and provisioning operations, browse through the list of [Supported AOS-CX Switch Platforms](#) in Aruba Central (on-premises).

Provisioning Workflow

The following sections list the steps required for provisioning AOS-CX switches in Aruba Central (on-premises).

Provisioning a Factory Default AOS-CX Switch

Like most Aruba devices, AOS-Switches support ZTP. Switches with factory default configuration have very basic configuration for all ports in VLAN-1. You must manually add either the serial number, MAC address, or part number of the new factory default switch in Aruba Central (on-premises). When the switch identifies Aruba Central (on-premises) as its management entity, it connects to Aruba Central (on-premises).

To manage AOS-CX switches from Aruba Central (on-premises), you must onboard the switches to the device inventory and assign a valid subscription.

For step-by-step instructions, see [Provisioning Factory Default AOS-CX Switches](#).

Provisioning a Pre-configured or Locally-Managed AOS-CX Switch

Pre-configured switches have customized configuration; for example, an additional VLAN or static IP address configured on the default.

Aruba Central (on-premises) management service is enabled by default on AOS-CX switches. When the switch is powered on, it identifies Aruba Central (on-premises) as its management entity and connects to Aruba Central (on-premises).

To manage AOS-CX switches from Aruba Central (on-premises), you must onboard the switches to the device inventory and assign a valid subscription.

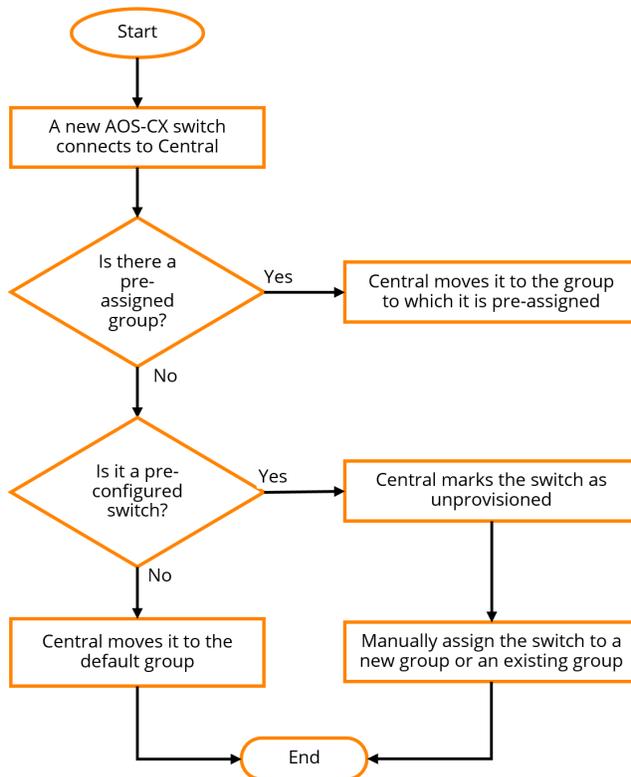
For step-by-step instructions, see [Provisioning Pre-Configured AOS-CX Switches](#).

Group Assignment

Aruba Central (on-premises) supports provisioning AOS-CX switches in template groups. Template groups allow you to configure devices using CLI-based configuration templates.

The following figure illustrates the group assignment workflow in Aruba Central (on-premises):

Figure 32 Group Assignment-AOS-CX Switches



AOS-CX Switch Configuration

Aruba Central (on-premises) supports managing AOS-CX switches configuration using configuration templates and UI group configuration.

When an AOS-CX switch is connected to Aruba Central (on-premises) and managed using the **Network Operations** app, Aruba Central (on-premises) becomes the single source of configuration for the switch. In the Aruba Central (on-premises) Managed mode, the switch cannot be configured using any of the other switch configuration interfaces, such as the switch CLI, REST APIs, NBAPIs, and SNMP. You can use any configuration options available in Aruba Central (on-premises) to configure the AOS-CX switches in the Managed mode. You can use the MultiEdit mode on the UI to run commands on the switch through Aruba Central (on-premises). For information, see [Using MultiEdit View for AOS-CX](#).

The Aruba Central (on-premises) Managed mode is applicable to AOS-CX switches running the firmware version 10.07 or later, and to those switches that have been added to an Aruba Central (on-premises) group. This mode is not applicable to switches in the unprovisioned state.

Configuration Using Templates

Aruba Central (on-premises) supports managing AOS-CX switches configuration using configuration templates. Ensure that you assign the AOS-CX switches to a template group.



When initially onboarding an AOS-CX switch to Aruba Central (on-premises), you must manually create the template for the switch in a group, along with the password in plaintext format. You can use the output of the `show running-config` command to create the template. You can also add variables to use the same template for onboarding multiple AOS-CX switches.

For more information on managing AOS-CX switches in Aruba Central (on-premises) using templates, see [Using Configuration Templates for AOS-CX Switch Management](#).

Configuration Using UI Groups

Aruba Central (on-premises) supports managing AOS-CX switches configuration using UI groups. You can configure AOS-CX switches that are added to a UI group, using the UI options and MultiEdit mode. You can pre-configure groups in the absence of switches.

For more information on managing AOS-CX switches in Aruba Central (on-premises) using UI group configuration, see [Configuring AOS-CX Switches in UI Groups](#).

AOS-CX Stack Configuration

Aruba Central (on-premises) supports managing AOS-CX switch stacks configuration using UI group configuration and templates.

For more information on managing AOS-CX switch stacks in Aruba Central (on-premises) using UI group configuration, see [Configuring AOS-CX VSF Stacks Using UI Groups](#).

For more information on managing AOS-CX switch stacks in Aruba Central (on-premises) using templates, see [Using Configuration Templates for AOS-CX Switch Management](#).

AOS-CX Switch Monitoring

To view the operation status of switches and health of wired access network:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**.
For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active switch.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
3. a. Click an AOS-CX switch under **Device Name**.
The dashboard context for the switch is displayed.

For more information, see [Monitoring Switches and Switch Stacks](#).



To view AOS-CX switches in the monitoring pages, you must create a template configuration for the switch with the password in plaintext. See [Using Configuration Templates for AOS-CX Switch Management](#).

Viewing VSX Details

Aruba Central (on-premises) displays information about VSX configuration of AOS-CX switches. For more information, see [Switch > VSX](#).

Viewing Topology Map

In Aruba Central (on-premises), the **Topology** tab in the site dashboard provides a graphical representation of the site including the network layout, details of the devices deployed and health of the WAN uplinks and tunnels. Aruba Central (on-premises) supports AOS-CX switches to be displayed in the **Topology** tab. For more information, see [Monitoring Sites in the Topology Tab](#).



To view AOS-CX switches in the topology map, you must create a template configuration for the switch with the password in plaintext. See [Using Configuration Templates for AOS-CX Switch Management](#).

Troubleshooting and Diagnostics

If you are unable to view all details of the AOS-CX switch, then maybe the template configuration was not applied correctly, the password was missing in the template configuration, or the password was not in plaintext. See the audit trail to check the status of the switch. The audit trail should show the device onboarded message for the switch serial number followed by the configuration push and login successful messages. For more information on troubleshooting AOS-CX switch onboarding issues, see [Troubleshooting AOS-CX Switch Onboarding Issues](#).

Configuration Status

The **Configuration Audit** page under **Network Operations > Device(s) > Switches** in the Aruba Central (on-premises) UI displays errors in configuration sync, template configuration, and a list of configuration overrides. For more information, see [Viewing Audit Trail](#).

The **Configuration Status** page under **Network Operations > Device(s) > Switches** in the Aruba Central (on-premises) UI displays errors in configuration sync, templates, and a list of configuration overrides. For more information, see [Using Configuration Status on AOS-CX](#).

Troubleshooting Tools

To troubleshoot AOS-CX switches remotely, use the tools available under **Network Operations > Analyze > Tools**. For more information, see [Using Troubleshooting Tools](#).

Actions Drop-down

You can also reboot, connect to the remote console of the switch, or generate a tech support dump for troubleshooting the device, by using the tools available under the **Actions** drop-down. The **Actions** drop-down is available in the switch monitoring pages.

The **Actions** tab displays the various options available for remote administration of the switch. The following options are available:

- **Reboot**—Reboots the switch. See [Rebooting Switches](#).
- **Tech Support**—Allows the administrators to generate a tech support dump for troubleshooting the device. See [Troubleshooting Aruba Switches](#).
- **Console**—Opens the remote console for a CLI session through SSH. Ensure that you allow SSH over port 443. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See [Opening Remote Console for Switch](#).



For AOS-CX 8320 and 8325 switch series, you must enable SSH server on the default VRF. Add the `ssh server vrf default` code to the template.

If the Copy and Paste function from the keyboard shortcut keys (CTRL+C and CTRL+V) do not work in your web browser, use the Copy and Paste functions available under the menu options in the web browser.

Caveats for Using AOS-CX Switches in Aruba Central (on-premises)

The following sections provide details on the caveats to be noted when onboarding, configuring, monitoring, and troubleshooting AOS-CX switches using Aruba Central (on-premises).



Monitor-only mode is not supported for the AOS-CX switches in the UI or template groups. You can add the AOS-CX switches to the UI or template groups to configure, monitor, and troubleshoot the AOS-CX switches.

Plaintext Password Override after Migrating from Version 2.5.3 to 2.5.4

After upgrading Aruba Central (on-premises) to version 2.5.4, for security reasons, any plaintext passwords, previously configured directly or using variables in the AOS-CX switch template, are hidden and displayed as asterisk (*) symbols. The plaintext passwords, previously configured in the template, directly or using variables, will work as expected; however, these plaintext passwords, displayed as asterisk (*) symbols, will not work if you copy them to a new template. You must re-enter the plaintext passwords in the new template for the template to work correctly.

Onboarding

The following limitations should be taken into consideration when onboarding AOS-CX switches in Aruba Central (on-premises):

- ZTP does not work on inline data ports for AOS-CX 8320 and 8325 switch series. The following is an example configuration for onboarding AOS-CX 8320 and 8325 switch series to Aruba Central (on-premises):

```
interface 1/1/1
    no shutdown
    no routing
interface vlan 1
    ip address <IP-ADDRESS/MASK>
ip route 0.0.0.0/0 <IP-GATEWAY>
ip dns server-address <DNS-SERVER>
https-server vrf default
ztp force-provision
```

- After the `erase startup-config` command is executed on the AOS-CX switches, the switches do not onboard to Aruba Central (on-premises). It is recommended to execute the `erase all zeroize` command, instead of the `erase startup-config` command.
- When an AOS-CX switch is first onboarded to Aruba Central (on-premises), Aruba Central (on-premises) must perform the following actions, before it can perform events such as rebooting the switch and

upgrading the firmware:

- Login to the switch using the password provided in the template configuration
- Apply the template to the switch
- Only DHCP-based ZTP is supported on Aruba Central (on-premises) for AOS-CX. Activate-based ZTP is not supported.
- FQDN or hostname for Aruba Central (on-premises) server is not supported. You must provide only the IP address.
- The Aruba Central (on-premises) URI that is received as part of DHCP option is not persistent across reboots. You must include the Aruba Central (on-premises) URI configuration when applying the template configuration to avoid connectivity issues after initial onboarding using the DHCP option.

Applying Template

The following limitations should be taken into consideration when applying the template to AOS-CX switches in Aruba Central (on-premises):

- You must configure the admin password in the template configuration only in plaintext. The format of the password configuration command must be `user admin group administrators password plaintext <string>`.
- If the template for AOS-CX switches contains % in the configuration, Aruba Central (on-premises) will not save the configuration.
Although the % character is allowed in AOS-CX switches, for example in banners, the same is not allowed in Aruba Central (on-premises). In Aruba Central (on-premises), the % character is reserved for variables.
- The maximum number of lines supported in the configuration template is 84000. Beyond this limit, Aruba Central (on-premises) will not apply the template to the AOS-CX switch.
- Onboarding an AOS-CX switch with 10.05 firmware to Aruba Central, using the **Import Configuration as Template** option on the **Add Template** window, fails to import the configuration and displays an error message. In this case, you must manually create the template for the switch using the output of the `show running-config` command. You can successfully import the configuration as a template for an AOS-CX switch with 10.05 firmware, only when the switch is part of a template group and the config-sync status is in-sync.

To import the configuration as template when onboarding an AOS-CX switch, without the error message, you must upgrade the switch to 10.06 firmware.

Configuring AOS-CX VSF Stack

The following are the VSF stacking limitations of AOS-CX switches in Aruba Central (on-premises):



These limitations apply only when the switches are running AOS-CX 10.06 or earlier firmware versions.

Aruba Central (on-premises) supports only a few functions related to Aruba CX switch stack, such as onboarding a stack to Aruba Central (on-premises) and replacing member switches having the same model and part number, through template configuration. All other stacking related functions, such as creating a stack, deleting, or adding a new member to the stack, must be performed offline, that is, outside Aruba Central (on-premises). These stacking related functions must be performed before or after onboarding the stack to Aruba Central (on-premises) depending on the function.

For example, you must create a stack offline before onboarding the stack to Aruba Central (on-premises). For more information, see [Managing an AOS-CX VSF Stack](#).

AOS-CX VSF Stack Related Functions Not Supported on Aruba Central (on-premises)

The following stack related functions are not supported on Aruba Central (on-premises):

- Creating a new stack
- Adding a new member to an existing stack
- Deleting a member from the stack
- Replacing a member with different part number
- Modifying standby member ID
- Adding, deleting, and modifying VSF links

Using AOS-CX VSX

The following limitations apply when configuring VSX or viewing VSX data for AOS-CX switches in Aruba Central (on-premises):

- Enabling VSX synchronization using template configuration in Aruba Central (on-premises) is not recommended. By enabling VSX synchronization, the peer switch might get into an unknown configuration state.
- Last synced data is not displayed on the **VSX** page, in Aruba Central (on-premises), if VSX synchronization is not enabled.

Managing Firmware Upgrade

- To upgrade an AOS-CX switch in Aruba Central (on-premises), a WAN connection with a minimum speed of 2 Mbps is required. The upgrade activity will time out after a period of 60 minutes.
- Uploading AOS-CX switch images to Aruba Central (on-premises) server for firmware upgrade fails.

Troubleshooting

The following are the limitations while troubleshooting AOS-CX switches in Aruba Central (on-premises):

- For AOS-CX 8320 and 8325 switch series, to use the remote console feature, you must enable SSH server on the VRF that the switch uses to connect to Aruba Central (on-premises). You must add one of the following commands in the template:
 - If the switch is connecting to Aruba Central (on-premises) using the inline default VRF, add `ssh server vrf default` to the template.
 - If the switch is connecting to Aruba Central (on-premises) using the OOBM management VRF, add `ssh server vrf mgmt` to the template.
- The **Chassis Locate** option, in the **Analyze > Tools > Device Check** tab, is not displayed for AOS-CX 8320 and 8325 switch series.
- When an AOS-CX switch is in the Aruba Central (on-premises) Managed mode, and at any instant both device-generated automatic changes are detected and there are any pending changes in Aruba Central (on-premises), then Aruba Central (on-premises) discards the pending changes and absorbs the device changes. Device-generated changes can be any of the following physical modifications:
 - Adding or removing a VSF stack member
 - Adding or removing a line card in the chassis
 - Enabling VSX-sync when VSX enabled devices are managed by Aruba Central.

To view details of the changes that were discarded by Aruba Central (on-premises), check the Audit Trail details.

Monitoring

In the monitoring pages in Aruba Central (on-premises), the IP address for the connected wired clients on AOS-CX switches might not be displayed if the Client IP tracker is not enabled on the switch.

To enable Client IP tracker, perform one of following steps:

- Using Template—Add the `client track ip` command to the template at the device and VLAN level.
- Using MultiEdit mode—Add the `client track ip` command in the MultiEdit mode at the device and VLAN level.

For more information, see [Switch > Clients > Clients](#).

For more information on `client track ip` command, see the IP Client Tracker chapter in the *AOS-CX IP Routing Guide*.

Provisioning Factory Default AOS-CX Switches

Switches that run default configuration either after shipped from a factory or a factory reset are referred to as factory default switches. This topic describes the steps for provisioning factory default switches in Aruba Central (on-premises).

- [Step 1: Onboard the AOS-CX Switch to Aruba Central \(on-premises\)](#)
- [Step 2: Assign the AOS-CX Switch to a Group](#)
- [Step 3: Connect the AOS-CX Switch to Aruba Central \(on-premises\)](#)
- [Step 4: Provision the AOS-CX Switch to a Group](#)
- [Step 5: Verify the Configuration Status](#)

Step 1: Onboard the AOS-CX Switch to Aruba Central (on-premises)

Log in to Aruba Central (on-premises) and [onboard the switch](#).

Step 2: Assign the AOS-CX Switch to a Group

Before assigning a group, determine if the switch must be provisioned in a UI or template group. By default, Aruba Central (on-premises) assigns the factory default switches to default group. You can create a new group and assign switch to the new group.

For more information on creating a group, see [Creating a Group](#).

To assign a device to a group from the **Account Home** page:

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**. The Device Inventory page is displayed
2. Select the device that you want to assign to a group.
3. Click **Assign Group**. The **Assign a Group to the Selected Devices** window is displayed.
4. Select the group to which you want to assign.
5. Click **Assign Device(s)**.

To assign a device to a group from the **Network Operations** app:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.

3. Click the **Groups** tile.
The Groups page is displayed.
4. From the list of devices, select the switches to assign.
5. Click the  **Move devices** icon.
The Move Devices page is displayed.
6. Select the **Destination Group** from the drop-down list.
7. Click **Move**.
The selected devices are moved to the destination group. These devices will adopt the destination group configuration.

Step 3: Connect the AOS-CX Switch to Aruba Central (on-premises)

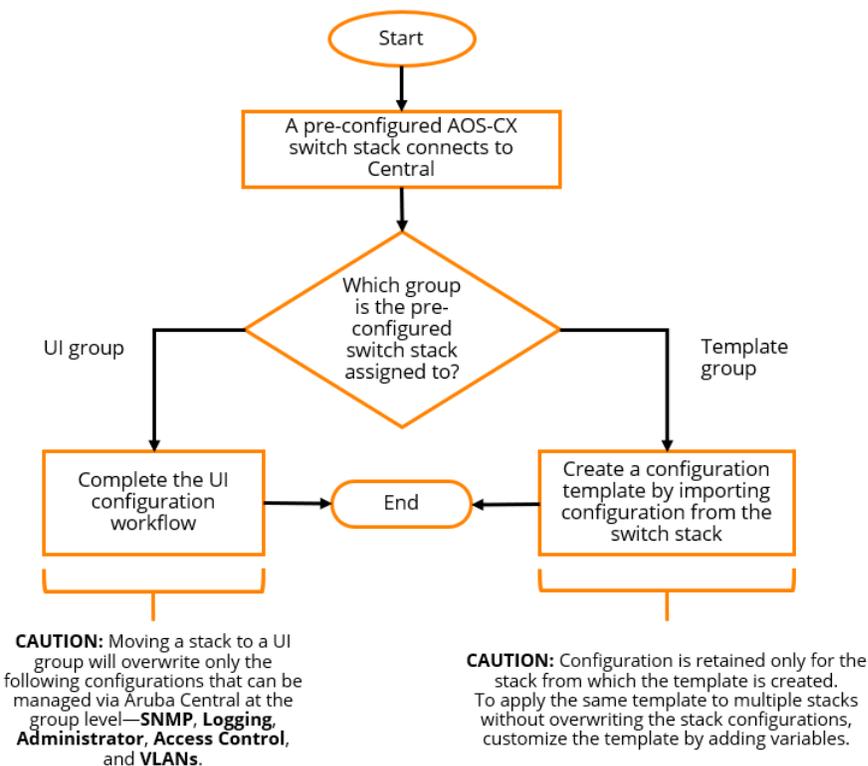
Switches with factory default configuration have very basic configuration for all ports in VLAN-1 that is required for obtaining an IP address and automatic provisioning (ZTP). For ZTP, switches must have a valid IP address, DNS, and NTP configuration. You must manually add either the serial number, MAC address, or part number of the factory default switch in Aruba Central (on-premises)

Step 4: Provision the AOS-CX Switch to a Group

When the switch connects to Central, if it is already added to the device inventory and is assigned a subscription in Aruba Central (on-premises), Aruba Central (on-premises) assigns it to a pre-assigned group. If there is no pre-assigned group, Aruba Central (on-premises) moves the device to the **default** group. Based on your configuration requirements, you create a template group and assign the switch.

The following figure illustrates the provisioning step required for each group type.

Figure 33 AOS-CX Switch Provisioning Steps Per Group Type



If the switch is assigned to a new UI group, you can modify the configuration of switches using the UI menu options under the **Network Operations** app > **Manage** > **Devices** > **Switches**. For more information, see [Configuring AOS-CX Switches in UI Groups](#).

Provisioning AOS-CX Switches in Template Groups

After assigning the switch to a template group, create a new configuration template. To create a configuration template:

1. In the **Network Operations** app, set the filter to a template group.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Switches**.
3. Click the **Config** icon.
The tabs to configure switches using templates is displayed.
4. Click the **Templates** tab. The Templates page is displayed.
5. Click **+** to add a new template. The **Add Template** window is displayed.
6. In the **Basic Info** tab, enter a name for the template in the **Template Name** field.
7. In the **Device Type** drop-down, select **Aruba CX**.
8. Select the switch model and software version. You can specify any of the following combinations:
 - **ALL** for both **Model** and **Version**—To apply the template to all switch models and all supported switch software versions.
 - **ALL** for **Model** and a software version for **Version**—To apply the template to all switch models running the selected software version.
 - **ALL** for **Version** and a switch model for **Model**—To apply the template to a switch model and all software versions supported by the selected switch model.
 - A switch model and a software version—To apply the template to a specific switch model and the software version. The template created for a switch model and a software version takes precedence over the template that is created for all platforms and versions.
9. Select the manufacturing part number of the switch in the **Part Number** drop-down.



-
- The **Part Number** drop-down is displayed only if you select a switch model in the **Model** drop-down.
 - If you select a specific switch model and part number, you can apply the template to a standalone switch and not to a stack.
 - If you select **All** in the **Model** drop-down, or if you select a switch model and **All** in the **Part Number** drop-down, you can apply a template to both a standalone switch and stack.
-

10. Click **Next**. The **Template** tab is displayed.
11. Build a new template by adding the output of the `show running-config` from the switch CLI in the **Template** text box. Ensure that the template text adheres to the guidelines listed in [Important Points to Note](#).



-
- You must manually create the template for the AOS-CX switch in a group, along with the password in plaintext format. You can use the output of the `show running-config` command to create the template. You can also add variables to use the same template for onboarding multiple AOS-CX switches. For more information on variables, see [Managing Variable Files](#).
 - All switch templates must include a password command to set a password for the device. The template cannot be saved without adding a password command. If the configuration that is pushed from Aruba Central (on-premises) to the device does not contain a password command, the configuration push is aborted for the device and a log is added to the audit trail. For example, if you add the password command in a condition block and the condition evaluates to false, the configuration that is pushed will not contain the password command. For more information, see [Managing Password in Configuration Templates](#).
 - For AOS-CX switches, you must configure the password only in plaintext. Also, the format of password must be `user admin group administrators password plaintext <string>`.
-

12. Click **Save**. After you apply the configuration template, switches reboot and reconnect to Aruba Central (on-premises) with the new configuration.

Step 5: Verify the Configuration Status

To verify the configuration status:

1. In the **Network Operations** app, set the filter to a template group.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Switches**.
3. Click the **Config** icon.
The tabs to configure switches using templates is displayed.
 - To verify the configuration status for the template group, click **Configuration Audit**. The **Configuration Audit** dashboard displays the number of devices with template and configuration synchronization errors.
 - To view configuration errors for a specific device, select a switch from the filter bar. The **Configuration Audit** dashboard displays the number of template and configuration synchronization errors for the device.
4. To view template errors, click **View Template Errors**.
5. To view configuration synchronization errors, click **View Details** under **Configuration Status**.
6. To compare running configuration and pending changes, click **View** under **Config Comparison Tool**.

Provisioning Pre-Configured AOS-CX Switches

Unlike factory default switches, locally managed switches and the switches with custom configuration require one touch provisioning. On AOS-CX switches, Aruba Central (on-premises) is enabled, by default, as their management platform, and therefore the switches connect to Aruba Central (on-premises) automatically.

To onboard a locally-managed or a pre-configured AOS-CX switch to Aruba Central (on-premises), follow one of the following options:

- Connect the AOS-CX switch directly to Aruba Central (on-premises). Aruba recommends that you use this option if you want to preserve the current configuration running on the switch. For more information on this procedure, see the workflows described in this topic.



To manually connect the switch to Aruba Central (on-premises), you must configure the Aruba Central (on-premises) URL on the switch. Execute the following commands in the switch CLI:

```
config terminal
aruba-central <Aruba Central (on-premises) URL> vrf mgmt
exit
```

Aruba does not recommend to manually provision the URL in a cloud deployment.

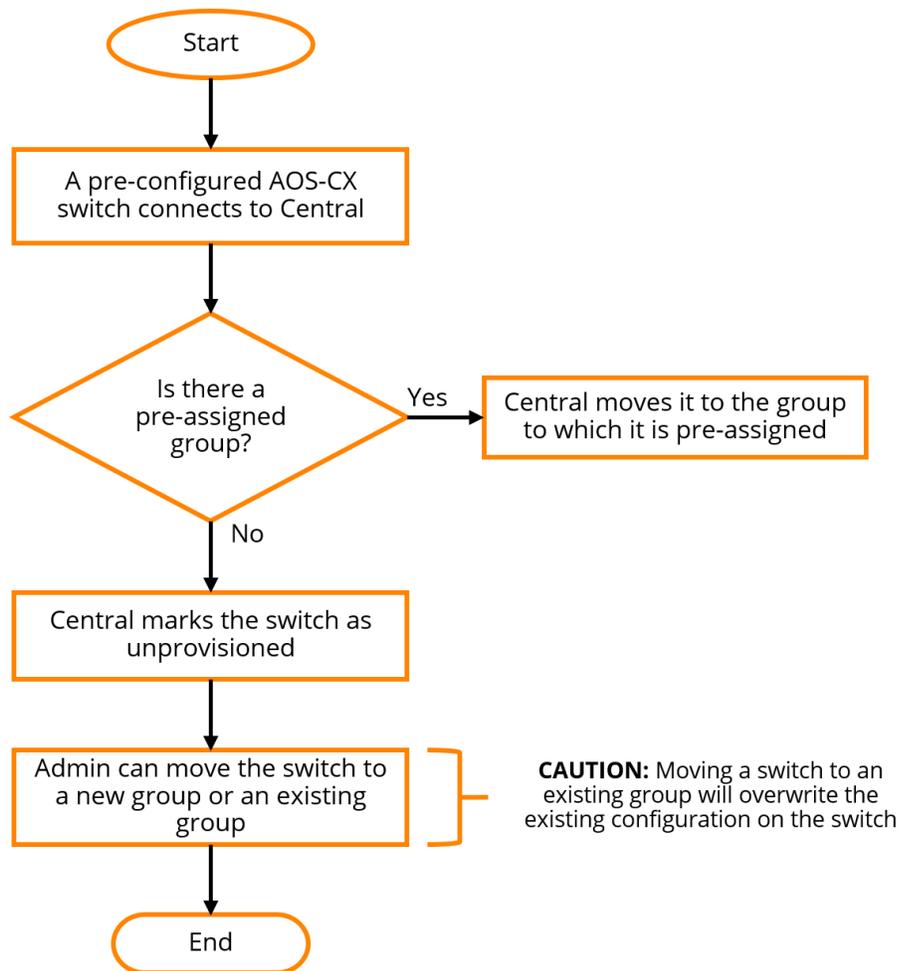
- Reset the switch configuration and use ZTP to provision the switch. You must first create a backup of the configuration, then reset the switch using the `erase all zeroize` command in the CLI. This initiates ZTP on the switch, enabling the switch to obtain the IP address from the option 43 sent by the DHCP server and then connect to Aruba Central (on-premises).

Aruba Central (on-premises) supports provisioning AOS-CX switches using one of the following methods:

- Pre-provisioning—In this workflow, a switch is added to the device inventory and assigned a group in Aruba Central (on-premises) before it connects to Aruba Central (on-premises).
- See [Workflow 1—Pre-Provisioning an AOS-CX Switch](#).
- Onboarding connected switches—In this workflow, Aruba Central (on-premises) onboards the switch that attempts to connect and then assigns a group.
- See [Workflow 2—Provisioning an AOS-CX Switch On-Demand](#).

The following figure illustrates provisioning procedure for a pre-configured switch.

Figure 34 Provisioning Workflow for Pre-Configured AOS-CX Switches



Workflow 1—Pre-Provisioning an AOS-CX Switch

The pre-provisioning workflow includes the following steps:

- [Step 1: Onboard the AOS-CX Switch to Aruba Central \(on-premises\)](#)
- [Step 2: Assign the AOS-CX Switch to a Group](#)
- [Step 3: Provision the AOS-CX Switch to a Group](#)
- [Step 4: Verify the Configuration Status](#)

Step 1: Onboard the AOS-CX Switch to Aruba Central (on-premises)

To onboard AOS-CX switches to the device inventory in Aruba Central (on-premises), complete the following steps:

- [Add switches to Aruba Central](#)
- [Assign Subscriptions](#)

Step 2: Assign the AOS-CX Switch to a Group

AOS-CX switches can be provisioned in a template group only. If you want to preserve the existing configuration on the switch, Aruba recommends that you create a new group for the switch.

For more information on creating a group, see [Creating a Group](#).

To assign a device to a group from the **Account Home** page:

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.
The Device Inventory page is displayed
2. Select the device that you want to assign to a group.
3. Click **Assign Group**. The **Assign a Group to the Selected Devices** window is displayed.
4. Select the group to which you want to assign.
5. Click **Assign Device(s)**.

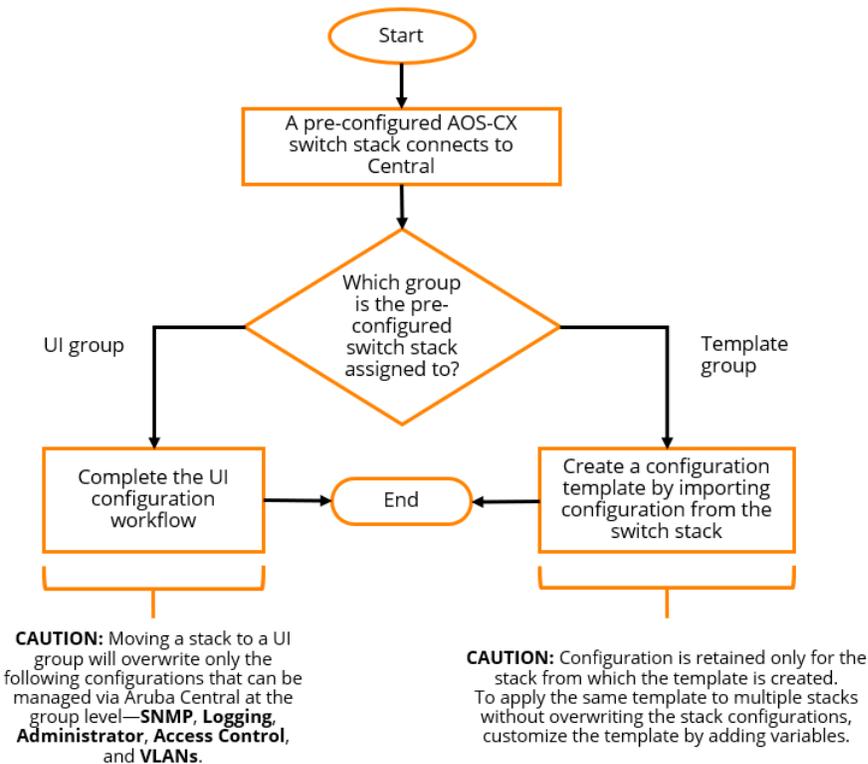
To assign a device to a group from the **Network Operations** app:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Groups** tile.
The Groups page is displayed.
4. From the list of devices, select the switches to assign.
5. Click the  **Move devices** icon.
The Move Devices page is displayed.
6. Select the **Destination Group** from the drop-down list.
7. Click **Move**.
The selected devices are moved to the destination group. These devices will adopt the destination group configuration.

Step 3: Provision the AOS-CX Switch to a Group

When the switch connects to Aruba Central (on-premises), Aruba Central (on-premises) automatically assigns it to the pre-assigned group. The following figure illustrates the provisioning steps for each group type.

Figure 35 Switch Provisioning Steps Per Group Type



If the switch is assigned to a new UI group, you can modify the configuration of switches in a group using the UI menu options under the **Network Operations** app > **Manage** > **Device(s)** > **Switches**. For more information, see [Configuring AOS-CX Switches in UI Groups](#).

If you have assigned the switch to a template group, you can import the existing configuration to a new configuration template and apply this template to other devices in the group. To create a configuration template using the existing configuration on the switch:

1. In the **Network Operations** app, set the filter to a template group.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Switches**.
3. Click the **Config** icon.
The tabs to configure switches using templates is displayed.
4. Click the **Templates** tab. The Templates page is displayed.
5. Click + to add a new template. The **Add Template** window is displayed.
6. In the **Basic Info** tab, enter a name for the template in the **Template Name** field.
7. In the **Device Type** drop-down, select **Aruba CX**.
8. Select the switch model and software version. You can specify any of the following combinations:
 - **ALL** for both **Model** and **Version**—To apply the template to all switch models and all supported switch software versions.
 - **ALL** for **Model** and a software version for **Version**—To apply the template to all switch models running the selected software version.
 - **ALL** for **Version** and a switch model for **Model**—To apply the template to a switch model and all software versions supported by the selected switch model.

- A switch model and a software version—To apply the template to a specific switch model and the software version. The template created for a switch model and a software version takes precedence over the template that is created for all platforms and versions.

9. Select the manufacturing part number of the switch in the **Part Number** drop-down.



- The **Part Number** drop-down is displayed only if you select a switch model in the **Model** drop-down.
- If you select a specific switch model and part number, you can apply the template to a standalone switch and not to a stack.
- If you select **All** in the **Model** drop-down, or if you select a switch model and **All** in the **Part Number** drop-down, you can apply a template to both a standalone switch and stack.

10. Click **Next**. The **Template** tab is displayed.

11. Build a new template by adding the output of the `show running-config` from the switch CLI in the **Template** text box. Ensure that the template text adheres to the guidelines listed in [Important Points to Note](#).



- You must manually create the template for the AOS-CX switch in a group, along with the password in plaintext format. You can use the output of the `show running-config` command to create the template. You can also add variables to use the same template for onboarding multiple AOS-CX switches. For more information on variables, see [Managing Variable Files](#).
- All switch templates must include a password command to set a password for the device. The template cannot be saved without adding a password command. If the configuration that is pushed from Aruba Central (on-premises) to the device does not contain a password command, the configuration push is aborted for the device and a log is added to the audit trail. For example, if you add the password command in a condition block and the condition evaluates to false, the configuration that is pushed will not contain the password command. For more information, see [Managing Password in Configuration Templates](#).
- For AOS-CX switches, you must configure the password only in plaintext. Also, the format of password must be `user admin group administrators password plaintext <string>`.
- For AOS-CX switches, the password configured in the template must match the password configured on the switch. Aruba Central (on-premises) cannot override the password that is configured on the switch.

12. Click **Save**. After you apply the configuration template, switches reboot and reconnect to Aruba Central (on-premises) with the new configuration.

Step 4: Verify the Configuration Status

To verify the configuration status:

1. In the **Network Operations** app, set the filter to a template group.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Switches**.
3. Click the **Config** icon.
The tabs to configure switches using templates is displayed.
 - To verify the configuration status for the template group, click **Configuration Audit**. The **Configuration Audit** dashboard displays the number of devices with template and configuration

synchronization errors.

- To view configuration errors for a specific device, select a switch from the filter bar. The **Configuration Audit** dashboard displays the number of template and configuration synchronization errors for the device.
4. To view template errors, click **View Template Errors**.
 5. To view configuration synchronization errors, click **View Details** under **Configuration Status**.
 6. To compare running configuration and pending changes, click **View** under **Config Comparison Tool**.

Workflow 2—Provisioning an AOS-CX Switch On-Demand

To dynamically provision switches on-demand, complete the following steps:

- [Step 1: Add the AOS-CX Switch to Aruba Central \(on-premises\)](#)
- [Step 2 Assign a Subscription to the AOS-CX Switch](#)
- [Step 3: Provision the AOS-CX Switch to a Group](#)
- [Step 4: Verify the Configuration Status](#)

Step 1: Add the AOS-CX Switch to Aruba Central (on-premises)

Add the switch to the Aruba Central (on-premises) device inventory. For more information, see [Onboarding Devices](#).

Step 2 Assign a Subscription to the AOS-CX Switch

To allow Aruba Central (on-premises) to manage the switch, ensure that a valid subscription is assigned to the switch.

Step 3: Provision the AOS-CX Switch to a Group

If the switch has a valid subscription assigned, Aruba Central (on-premises) marks the switch as **unprovisioned**. To preserve the switch configuration, move it to a new template group.

To move the device to a UI group:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Groups** tile.
The Groups page is displayed.
4. Select the device.
5. Click **Import configuration**. Aruba Central (on-premises) imports the switch configuration to the new group.

You can also modify the configuration of switches in a group using the UI menu options under the **Network Operations** app > **Manage** > **Devices** > **Switches**. For more information, see [Configuring AOS-CX Switches in UI Groups](#).

To move the device to a template group:

1. [Create a template group](#).
2. In the **Network Operations** app, set the filter to **Global**.

3. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
4. Click the **Groups** tile.
The Groups page is displayed.
5. Select the AOS-CX switch from a group.
6. Click the  **Move devices** icon.
The Move Devices page is displayed.
7. Select the **Destination Group** from the drop-down list.
8. Click **Move**.
The selected devices are moved to the destination group. These devices will adopt the destination group configuration.
9. To build a new configuration template:
 - a. In the **Network Operations** app, set the filter to a template group.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **Config** icon.
The tabs to configure switches using templates is displayed.
 - d. Click the **Templates** tab. The Templates page is displayed.
 - e. Click **+** to add a new template. The **Add Template** window is displayed.
 - f. In the **Basic Info** tab, enter a name for the template in the **Template Name** field.
 - g. In the **Device Type** drop-down, select **Aruba CX**.
 - h. Select the switch model and the software version to which you want to apply the new template. You can specify any of the following combinations:
 - **ALL** for both **Model** and **Version**—To apply the template to all switch models and all supported switch software versions.
 - **ALL** for **Model** and a software version for **Version**—To apply the template to all switch models running the selected software version.
 - **ALL** for **Version** and a switch model for **Model**—To apply the template to a switch model and all software versions supported by the selected switch model.
 - A switch model and a software version—To apply the template to a specific switch model and the software version. The template created for a switch model and a software version takes precedence over the template that is created for all platforms and versions.
 - i. Select the manufacturing part number of the switch in the **Part Number** drop-down.

- The **Part Number** drop-down is displayed only if you select a switch model in the **Model** drop-down.
 - If you select a specific switch model and part number, you can apply the template to a standalone switch and not to a stack.
 - If you select **All** in the **Model** drop-down, or if you select a switch model and **All** in the **Part Number** drop-down, you can apply a template to both a standalone switch and stack.

 - j. Click **Next**. The **Template** tab is displayed.
 - k. Build a new template by adding the output of the `show running-config` from the switch CLI in the **Template** text box. Ensure that the template text adheres to the guidelines listed in the

Important Points to Note.



- You must manually create the template for the AOS-CX switch in a group, along with the password in plaintext format. You can use the output of the `show running-config` command to create the template. You can also add variables to use the same template for onboarding multiple AOS-CX switches. For more information on variables, see [Managing Variable Files](#).
 - All switch templates must include a password command to set a password for the device. The template cannot be saved without adding a password command. If the configuration that is pushed from Aruba Central (on-premises) to the device does not contain a password command, the configuration push is aborted for the device and a log is added to the audit trail. For example, if you add the password command in a condition block and the condition evaluates to false, the configuration that is pushed will not contain the password command. For more information, see [Managing Password in Configuration Templates](#).
 - For AOS-CX switches, you must configure the password only in plaintext. Also, the format of password must be `user admin group administrators password plaintext <string>`.
 - For AOS-CX switches, the password configured in the template must match the password configured on the switch. Aruba Central (on-premises) cannot override the password that is configured on the switch.
-

- I. Click **Save**. After you apply the configuration template, switches reboot and reconnect to Aruba Central (on-premises) with the new configuration.

Step 4: Verify the Configuration Status

To verify the configuration status:

1. In the **Network Operations** app, set the filter to a template group.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Switches**.
3. Click the **Config** icon.
The tabs to configure switches using templates is displayed.
 - To verify the configuration status for the template group, click **Configuration Audit**. The **Configuration Audit** dashboard displays the number of devices with template and configuration synchronization errors.
 - To view configuration errors for a specific device, select a switch from the filter bar. The **Configuration Audit** dashboard displays the number of template and configuration synchronization errors for the device.
4. To view template errors, click **View Template Errors**.
5. To view configuration synchronization errors, click **View Details** under **Configuration Status**.
6. To compare running configuration and pending changes, click **View** under **Config Comparison Tool**.

Using Configuration Templates for AOS-CX Switch Management

Templates in Aruba Central (on-premises) refer to a set of configuration commands that can be used by the administrators for provisioning devices in a group. Configuration templates enable administrators to apply a set of configuration parameters simultaneously to multiple switches in a group and thus automate switch deployments.



- To minimize configuration errors and troubleshoot device-specific configuration issues, Aruba recommends that the device administrators familiarize themselves with the CLI configuration commands available on AOS-CX switches.
- The `vsf member 1` line must be present in the configuration template for stackable AOS-CX switches running 10.07 or later versions. This is required to apply configuration to the switches. In case, if a template is applied to the switch that does not contain the `vsf member 1` line, then the switch will be zeroized.

Creating a Group for Template-Based Configuration

For template-based provisioning, switches must be assigned to a group with template-based configuration method enabled.

For more information, see [Creating a Group](#) and [Assigning Devices to Groups](#).



The **Import Configuration As Template** feature is supported only on AOS-CX switches running firmware version 10.06 or later.

Creating a Configuration Template

To create a configuration template for switches:

1. In the **Network Operations** app, set the filter to a template group.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Switches**.
3. Click the **Config** icon.
The tabs to configure switches using templates is displayed.
4. Click the **Templates** tab. The Templates page is displayed.
5. Click **+** to add a new template. The **Add Template** window is displayed.
6. In the **Basic Info** tab, enter a name for the template in the **Template Name** field.
7. In the **Device Type** drop-down, select **Aruba CX**.
8. Select the switch model and software version. You can specify any of the following combinations:
 - **ALL** for both **Model** and **Version**—To apply the template to all switch models and all supported switch software versions.
 - **ALL** for **Model** and a software version for **Version**—To apply the template to all switch models running the selected software version.

- **ALL** for **Version** and a switch model for **Model**—To apply the template to a switch model and all software versions supported by the selected switch model.
 - A switch model and a software version—To apply the template to a specific switch model and the software version. The template created for a switch model and a software version takes precedence over the template that is created for all platforms and versions.
9. Select the manufacturing part number of the switch in the **Part Number** drop-down.



-
- The **Part Number** drop-down is displayed only if you select a switch model in the **Model** drop-down.
 - If you select a specific switch model and part number, you can apply the template to a standalone switch and not to a stack.
 - If you select **All** in the **Model** drop-down, or if you select a switch model and **All** in the **Part Number** drop-down, you can apply a template to both a standalone switch and stack.
-

10. Click **Next**. The Template tab is displayed.
11. Build a new template by adding the output of the `show running-config` from the switch CLI in the **Template** text box. Ensure that the template text adheres to the guidelines listed in the [Important Points to Note](#).



-
- You must manually create the template for the AOS-CX switch in a group, along with the password in plaintext format. You can use the output of the `show running-config` command to create the template. You can also add variables to use the same template for onboarding multiple AOS-CX switches. For more information on variables, see [Managing Variable Files](#).
 - All switch templates must include a password command to set a password for the device. The template cannot be saved without adding a password command. If the configuration that is pushed from Aruba Central (on-premises) to the device does not contain a password command, the configuration push is aborted for the device and a log is added to the audit trail. For example, if you add the password command in a condition block and the condition evaluates to `false`, the configuration that is pushed will not contain the password command. For more information, see [Managing Password in Configuration Templates](#).
 - For AOS-CX switches, you must configure the password only in plaintext. Also, the format of password must be `user admin group administrators password plaintext <string>`.
-

12. Click **Save**. After you apply the configuration template, switches reboot and reconnect to Aruba Central (on-premises) with the new configuration.

Important Points to Note

Note the following points when adding configuration text to a template:

- The CLI syntax in the switch template must be accurate. Aruba recommends that you validate the configuration syntax on the switch before adding it to the template text.
- Ensure that the command text indentation matches the indentation in the running configuration.
- The commands in the template are case-sensitive and cannot contain the **%** character. In the template-based configuration, the **%** character is reserved and is used to denote variables.

- The following example illustrates the case discrepancies that the users must avoid in the template text:

```
ssh server vrf default
ssh server vrf mGmt
vsf member 1
    type j1660ab
vlan 1
spanning-tree
interface Mgmt
    no shutdown
    ip dhcp
interface 1/1/1
    no shutdown
    no routing
    vlan access 1
interface 1/1/2
    no shutdown
    no routing
    vlan access 1
interface 1/1/3
    no shutdown
    no routing
    vlan access 1
interface 1/1/4
    no shutdown
    no routing
    vlan access 1
interface 1/1/5
    no shutdown
    no routing
    vlan access 1
interface 1/1/6
    no shutdown
    no routing
    vlan access 1
interface 1/1/7
    no shutdown
    no routing
    vlan access 1
interface 1/1/8
    no shutdown
    no routing
    vlan access 1
interface 1/1/9
    no shutdown
    no routing
    vlan access 1

interface vlan 1
    ip dhcp
!
!
!
!
!
https-server vrf default
https-server vrf MGMT
```

Configuring AOS-CX Switches in UI Groups

You can configure AOS-CX switches that are added to a UI group, using the UI options and MultiEdit mode. You can pre-configure groups in the absence of switches. You can configure 4100i, 6100, 6200, 6300, 8320, 8325, 8360 Switch Series using UI options, MultiEdit mode, and templates. You can configure 6405, 6410, and 8400 Switch Series using only templates.

To configure AOS-CX switches using templates, see [Using Configuration Templates for AOS-CX Switch Management](#).



The UI options and MultiEdit mode are available only when the AOS-CX switches are added to a UI group. The UI options and MultiEdit mode are not available when the AOS-CX switches are added to a template group.

To configure or view the properties of AOS-CX switches that are added to UI groups, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a UI group in the filter:
 - a. Set the filter to a UI group.

The dashboard context for the UI group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-CX** or **Config** icon to view the AOS-CX switch configuration dashboard.
 - To select a switch:
 - a. Set the filter to **Global** or a UI group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.

A list of switches is displayed in the **List** view.
 - c. Click an AOS-CX switch under **Device Name**.

The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.

The AOS-CX UI configuration page is displayed.

The following table describes the different configuration pages and their functions.

Table 94: *Configuring AOS-CX Switches Provisioned in UI Groups*

Feature	Description
Properties	Edit system property settings such as contact, location, time zone, and administrator password. You can also select the VRF to be used and add the DNS and NTP servers. See Configuring System Properties on AOS-CX .
HTTP Proxy	Configure to enhance security for device management. An IP address can be made a proxy for all HTTP connections. See Configuring HTTP Proxy on AOS-CX .
SNMP	Add, edit, or delete the following: <ul style="list-style-type: none">■ SNMP v2c communities■ SNMP v3 users■ Trap notifications for SNMP v2c and v3

Feature	Description
	See Configuring SNMP on AOS-CX .
Logging	Add, edit, or delete logging servers to view event logs from the AOS-CX switches. Configure FQDN or IP address, log severity level, and the VRF to be used for each of the logging servers. Also configure the global level debug log severity. See Configuring Logging Servers for AOS-CX .
Administrator	Add, edit, or delete server groups to be used for authentication, authorization, and accounting. You must also configure the protocol required to enable connection to these server groups. See Configuring AAA for AOS-CX .
Source Interface	Add, modify, or delete source interface configuration for Central and User-based tunneling interfaces for AOS-CX switches. See Configuring Source Interface for AOS-CX .
Stacking	Create stack, add stack members, modify VSF link, change the secondary conductor, delete stack and delete stack members. See Configuring AOS-CX VSF Stacks Using UI Groups .
Static Routing	Add, edit, or delete static routes manually and configure destination IP addresses and next hop values, VRF, and the administrative distance. You can add different static routes for different VRFs on the switch. See Configuring Static Routing on AOS-CX .
Ports & Link Aggregations	View and edit port settings such as description, VLAN mode, speed duplex, routing, and the operational status of the port. Add, edit, or delete LAGs by combining different ports and configuring the speed duplex, VLAN mode, aggregation mode, and the operational status of the LAG. See Configuring Ports and LAGs on AOS-CX .
Authentication Servers	Add, edit, or view the RADIUS and TACACS servers for authentication. Add settings such as FQDN or IP address of the servers, authentication port number, response timeout, retry count, and the VRF to be used when communicating with the servers. See Configuring Authentication Servers on AOS-CX .
Authentication	View or edit details about 802.1X and MAC authentication methods. Configure the precedence order and other parameters such as reauthentication timeout, cached reauthentication timeout, and quiet period. See Configuring Authentication on AOS-CX .
Access Control	View or add access policies and rules to permit or deny passage of traffic. See Configuring Access Control on AOS-CX .
User-Based Tunneling	Enable to use GRE to tunnel ingress traffic on a switch interface to a gateway. For further processing, provide a centralized security policy using per-user authentication and access control to ensure consistent access and permissions. See Configuring User-Based Tunneling for AOS-CX .
Client Roles	Configure to allow administrators to assign network access to clients. The network admin can create configuration profiles (roles) and associate them to clients. See Configuring Client Roles for AOS-CX .
VLANs	Add, edit, delete, or view VLANs, and associated parameters such as type of IP assignment, operational status, IP address of the DHCP relay. See Configuring VLANs on AOS-CX .

Feature	Description
Loop Prevention	Enable or disable loop protection and spanning tree protocol, and associated parameters such as the mode and priority. Enable or disable various MSTP mode-related settings such as BPDU filter, BPDU protection, admin edge, and root guard. See Configuring Loop Prevention on AOS-CX .

- To enable MultiEdit mode, move the **MultiEdit** toggle switch to the on position.

The **Device-Level Configuration** page is displayed with the list of devices displayed in the **Devices** table.



At the device level, the **Devices** table lists only the switch that you have selected. Also, a pop-up is displayed on the bottom-right corner of the page with the options **View Config**, **Edit Config**, and **Express Config**.

Search for a switch by entering a search query in the **Contextual Search Engine** field.

For more information about search queries, see [Using Device Search on AOS-CX](#).

The following table describes the options available in the MultiEdit mode of configuring AOS-CX switches.

Table 95: *Configuring AOS-CX Switches Provisioned in UI Groups using the MultiEdit Mode*

Feature	Description
MultiEdit	View and edit configuration on the AOS-CX switches using the CLI syntax. You can also apply predefined set of configuration settings such as NAE to the switches. See Using MultiEdit View for AOS-CX .
View Config	View configuration of AOS-CX switches and find differences in the configuration across switches. See Viewing Configuration Using MultiEdit on AOS-CX .
Edit Config	Edit configuration for one or more AOS-CX switches in the MultiEdit mode. Edit the entire configuration in a familiar looking CLI with syntax checking, colorization, and command completion. See Editing Configuration Using MultiEdit on AOS-CX .
Express Config	Apply predefined set of configuration settings such as NAE scripts and device profile to a single or multiple switches. See Express Configuration Using MultiEdit on AOS-CX .
Device Search	Search for AOS-CX switches in the Devices table, in the MultiEdit mode, using search queries such as device attributes, wildcard characters, Boolean operators, and by grouping characters. See Using Device Search on AOS-CX .

- To view configuration status, pending changes, and local overrides on the switches, click **Configuration Status**.

This page allows you to commit the pending changes in a configuration. At the device level, this page allows you to change the auto-commit state of the switch.

For more information, see [Using Configuration Status on AOS-CX](#).

Multiple Browser Tab Support

You can open multiple browser tab sessions of the same Aruba Central (on-premises) instance with different switch group or device pages opened simultaneously. For example, you can open the group configuration of a switch in one browser tab and the device-level configuration of a switch in another browser tab. Aruba Central (on-premises) stores the data from the different browser tabs separately.

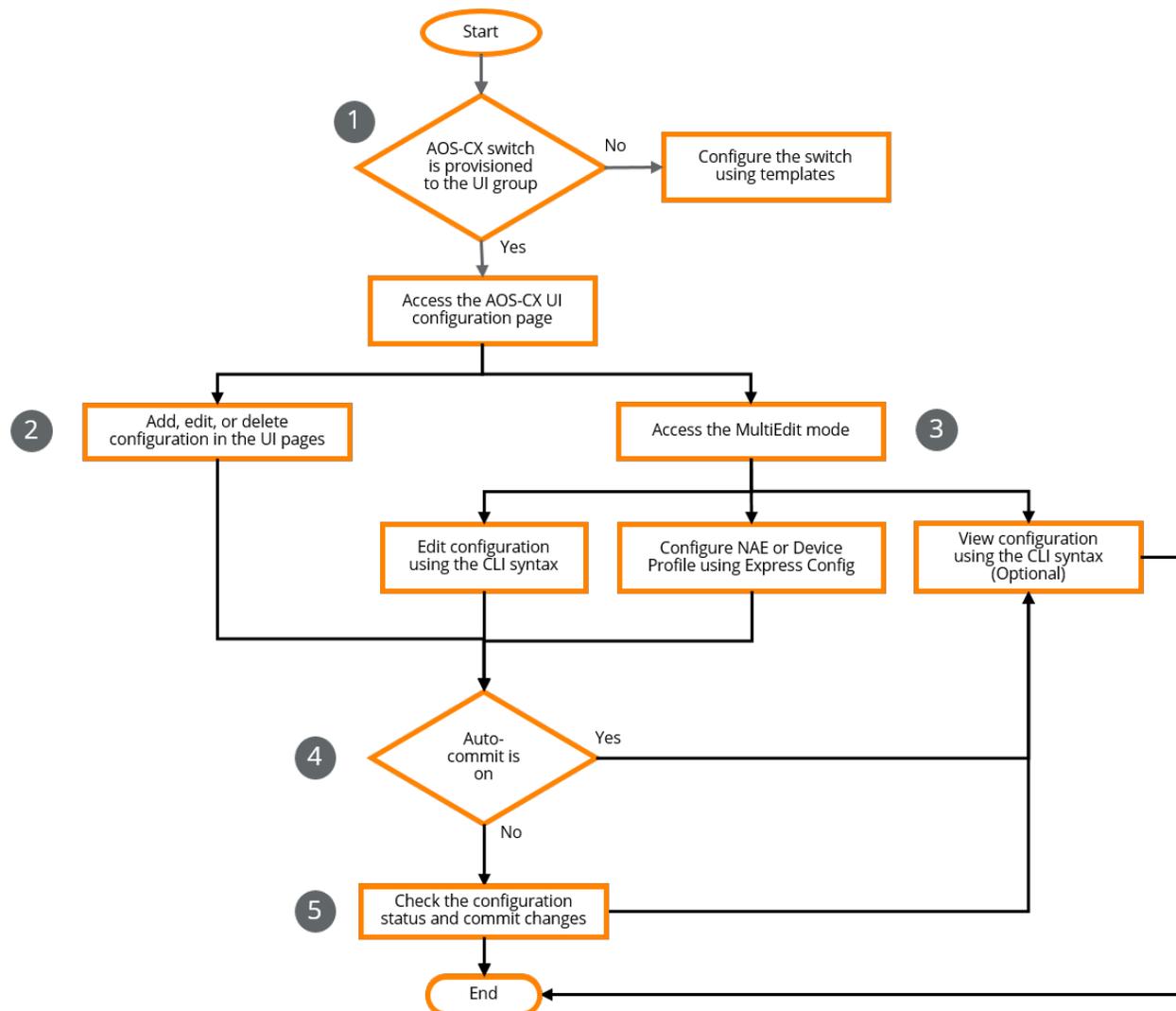
However, if you edit the configuration of one AOS-CX switch in the MultiEdit mode in two different browser tab sessions, and try to save the configuration one after the other, the following events occur:

1. The configuration that you save first in the editor in any of the two browser tabs is saved on the switch.
2. When you try to save the configuration in the editor in the other browser tab, Aruba Central (on-premises) displays a warning that the configuration has been changed outside the current editor.
3. If you ignore the warning and continue to save the configuration, Aruba Central (on-premises) overwrites the changes saved earlier with the current changes.

Configuration Workflow for AOS-CX Switches in UI Groups

The following workflow explains the process to configure AOS-CX switches using UI options.

Figure 36 UI Configuration Workflow for AOS-CX Switches



Workflow Steps

1. Provision an AOS-CX switch to a UI group in Aruba Central (on-premises). See [Getting Started with AOS-CX Deployments](#).

When you add AOS-CX switches to a UI group, you can configure them using the following options:

- Various UI options
- MultiEdit mode

2. Configure the switch using the different configuration options available on the UI. You can add, edit, or delete configurations using the UI options.

See [Configuring AOS-CX Switches in UI Groups](#).

3. Configure the switch in the MultiEdit mode—The MultiEdit mode offers a CLI syntax-based configuration functionality for AOS-CX switches. You can view or edit the running configuration on the switch or apply express configuration.

See [Using MultiEdit View for AOS-CX](#).

- **Edit Config**—Edit switch configuration using the CLI syntax. You can edit the configuration of switches. After you edit the configuration, you can view the difference between the running configuration and the edited configuration in the same window. See [Editing Configuration Using MultiEdit on AOS-CX](#).
- **Express Config**—Apply a predefined set of configuration settings to switches using this option for device profile and NAE configurations. See [Express Configuration Using MultiEdit on AOS-CX](#).
- **View Config**—View the running configuration on the switch using this option. The changes made on the UI options, Edit Config, or the Express Config pages will appear on this page only if the Auto-Commit state is on or if the changes are committed manually. See [Viewing Configuration Using MultiEdit on AOS-CX](#).

4. Depending on the Auto-Commit state of the switch, you can either view the configuration changes immediately or commit the changes first and then view the configuration changes.

- If the Auto-Commit state is on, Aruba Central (on-premises) applies the configuration changes immediately to the switch. You can view the configuration on the View Config page in the MultiEdit mode.
- If the Auto-Commit state is off, you must manually commit changes to the switch and then view the configuration.

See [Using Configuration Status on AOS-CX](#).

5. When the Auto-Commit state is off, check whether there are any pending changes to be applied to the switch, in the Configuration Status page. Commit any pending configuration changes to the switch and view the updated configuration.

Managing Configuration Overrides

Aruba Central (on-premises) supports two levels of configuration hierarchy:

- **Group-level**—When you add a switch to a group, or move a switch from one group to, another, the switch inherits the configuration of the group. Any configuration changes made at the group-level are applied to the devices in the group. You can also pre-configure groups before adding switches.



Only configurations that are supported at the group-level are applied to the devices. The configurations that are supported only at the device-level are preserved.

- Device-level—Any modifications made at the device-level override the configurations inherited from the group. Local overrides are those modifications that you make on a particular device in a group. Once a local override exists on a device, then any configuration changes performed at the group level will not be applied or inherited to that device.



Configuration overrides are applicable to only those parameters, which are present at both group and device levels.

Managing Passwords for Groups and Devices using UI groups

In Aruba Central (on-premises), you can set a password for UI groups when creating a new group. This group password is used to onboard the AOS-CX switches to the group. The group password must match with the device password to onboard the device successfully to the group. For more information, see [Groups](#).

You can use the **Properties** page to change the administrator password for groups and devices. If you set different password at the device-level, then the device can no longer be managed at the group-level. For more information, [Configuring System Properties on AOS-CX](#).

If you upgrade Aruba Central (on-premises) from earlier versions to the latest version, the administrator password is considered blank. Aruba Central (on-premises) prompts the user to specify an administrator password for the devices in the group. You cannot make any configuration update until a new password is set.

Configuring System Properties on AOS-CX

From the Properties page, you can view or configure system property settings such as contact, location, timezone, administrator username, and administrator password for AOS-CX switches. In addition, you can select management VRF or default VRF, and configure DNS and NTP servers for the selected VRF.

To edit system properties, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-CX** or **Config** icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click an AOS-CX switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The AOS-CX UI configuration page is displayed.
2. Click **System > Properties**.
The Edit Properties page is displayed.

3. Edit the following properties:

Table 96: Switches Properties

Name	Description	Value
Name	Name of the switch. This field is available only at the device level.	You can enter up to a maximum of 32 characters including letters, numbers, and special characters, except question mark (?) and double quotes (").
Contact	Contact details for the switch.	Name, Email address, or phone number. You can enter up to a maximum of 128 characters including letters, numbers, and special characters, except question mark (?) and double quotes (").
Location	Location of the switch.	You can enter up to a maximum of 128 characters including letters, numbers, and special characters, except question mark (?) and double quotes (") For example: Portland, Oregon.
Timezone	The time zone corresponding to the location of the switch.	Time zone selected from the drop-down.
VRF	The VRF to be used for communicating with DNS and NTP servers. NOTE: If you change the VRF setting, then the existing DNS and NTP server settings will be removed.	Default or Management OOBM NOTE: Management VRF is not supported on the AOS-CX 4100i and 6100 switch series.
DNS servers	The IP address of DNS servers for the selected VRF. Click + to add another DNS server. You can add up to three servers.	IPv4 address or IPv6 address
NTP servers	The IP address of NTP servers for the selected VRF. Click + to add another NTP server. You can add up to three servers.	IPv4 address or IPv6 address
Administrator password	The password for the administrator username. NOTE: To manage devices in the group, the password must be same at group and device-levels.	You can enter up to a maximum of 32 characters including letters, numbers, and special characters except question mark (?) and double quotes (").

4. Click **Save**.

Configuring HTTP Proxy on AOS-CX

HTTP proxy enhances security for device management. An IP address can be made a proxy for all HTTP connections. If your network requires a proxy server for Internet access, ensure that you configure the HTTP proxy on AOS-CX switch to download the image from the cloud server. After setting up the HTTP

proxy settings, the AOS-CX switch connects to Aruba Central (on-premises) or OpenDNS server through a secure HTTP connection.

To configure HTTP proxy on the AOS-CX switch, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a group in the filter:
 - a. Set the filter to a group.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-CX** or **Config** icon to view the AOS-CX switch configuration dashboard.
2. Click **System > HTTP Proxy**. The **Edit HTTP Proxy** page is displayed.
The **Ports** table displays the following information:

Table 97: HTTP Proxy parameters

Parameter	Description	Value
FQDN or IP address	FQDN or IPv4 address of the HTTP proxy location.	IPv4 address in the x.x.x.x format or FQDN of the proxy location.
Port	Port number of the switch.	Default value used for port is 80.
VRF	VRF on which the system is configured.	Default and Management.

3. To save the changes, click **SAVE**.

Configuring SNMP on AOS-CX

Simple Network Management Protocol (SNMP) is a TCP/IP standard protocol for managing devices on IP networks. It is used mostly in network management systems to monitor network-attached devices for events that require administrative attention.

From the SNMP page, you can perform the following actions:

- Enable or disable SNMP on the switch
- Select the VRF on which you want to configure SNMP
- Configure SNMP versions v2c or v3
- Configure communities and traps

For more information, see the following topics:

- [Configuring SNMPv2c on AOS-CX](#)
- [Configuring SNMPv3 on AOS-CX](#)

Configuring SNMPv2c on AOS-CX

You can configure SNMPv2c community settings and trap destinations through the UI.

To configure SNMPv2c on switch, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-CX** or Config icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click an AOS-CX switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The AOS-CX UI configuration page is displayed.
2. Click **System > SNMP**.
The SNMP page is displayed.
3. Enable SNMP on the switch by moving the **SNMP** toggle to the on position.
4. Select the VRF on which you want to configure SNMP by selecting one or both of the following check boxes under **Enable SNMP on the selected VRF**:
 - **Default VRF**
 - **Management VRF**



Management VRF is not supported on the AOS-CX 4100i and 6100 switch series.

5. Select **v2c** from the **SNMP** drop-down.
The **Read Community** and **Trap Destination** tables are displayed.

Adding an SNMP Community

You can add SNMP communities to restrict access to the switch from the SNMP management stations. The default community name is Public.

To add an SNMP community, complete the following steps:

1. In the **Read Community** table, click the + add icon. A new row is added in the table.
2. Type the name of the community in the new row. You can enter up to a maximum of 32 characters including letters, numbers, and special characters.
3. Click **Save**.

Editing an SNMP community

To edit an SNMP community, point to the row for the SNMP community, and click the edit icon.



You can edit an SNMP community name only before saving it to Aruba Central (on-premises). If the SNMP community is saved, then it cannot be edited.

Deleting an SNMP Community

To delete an SNMP community, point to the row for the SNMP community, and click the delete icon.



If you delete an SNMP community, trap destinations that belong to the community will also get deleted.

Adding a Trap Destination

You can add trap destinations to send notifications to SNMP management stations.



When adding a trap destination, you cannot edit the **SNMP** toggle switch and the **Enable SNMP on the selected VRF** options.

To add a trap destination, complete the following steps:

1. In the **Trap Destination** table, click the + add icon. A new row is added in the table.
2. Configure the following parameters:
 - **IP Address**—Enter a valid IPv4 or IPv6 address of the SNMP host.
 - **VRF**—Select the available VRF on the switch from the drop-down.
 - **Community**—Select the name of the community from the drop-down.
3. Click **Save**.

Editing a Trap Destination

To edit a trap destination, point to the row for the trap destination, and click the edit icon.



You can edit only the community name.

Deleting a Trap Destination

To delete a trap destination, point to the row for the trap destination, and click the delete icon.

Configuring SNMPv3 on AOS-CX

SNMPv3 provides a secured access to SNMP management stations using authentication and privacy protocols. You can add SNMPv3 user and configure notification settings using UI groups.

To configure SNMPv3 on switch, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-CX** icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.

- c. Click a switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The tabs to configure the switch is displayed.
2. Click **System > SNMP**.
The SNMP page is displayed.
 3. Enable SNMP service on the switch by moving the **SNMP** toggle to the on position.
 4. Select the VRF on which you want to configure SNMP by selecting one or both of the following check boxes under **Enable SNMP on the selected VRF**:
 - **Default VRF**
 - **Management VRF**



Management VRF is not supported on the AOS-CX 4100i and 6100 switch series.

5. Select **v3** from the **SNMP** drop-down.
The **User** and **Trap Destination** tables are displayed.

Adding an SNMPv3 User

You can add SNMPv3 users to provide secured access to SNMP management stations.

To add an SNMPv3 user, complete the following steps:

1. In the **Users** table, click the + add icon. A new row is added in the table.
2. Configure the following parameters:
 - **Name**—Enter the name of the SNMPv3 user.
 - **Authentication Mode**—Select either **md5** (Message Digest) or **sha** (Secure Hash Algorithm) as the authentication mode to provide secured access to the user. After selecting the authentication mode, enter the authentication password. The password must be 8 to 32 characters long, and can contain alphabets, numbers, and special characters.
 - **Privacy Mode**—Select **aes** (Advanced Encryption Standard) or **des** (Data Encryption Standard) as the privacy mode to provide secured access to the user. After selecting the privacy mode, enter the privacy password. The password must be 8 to 32 characters long, and can contain alphabets, numbers, and special characters.
3. Click **Save**.

Editing an SNMPv3 User

To edit an SNMPv3 user, point to the row for the user, and click the edit icon.



You can edit an SNMPv3 user only before saving it to Aruba Central (on-premises). If the user is saved to Aruba Central (on-premises), then it cannot be edited.

Deleting an SNMPv3 User

To delete an SNMPv3 user, point to the row for the user, and click the delete icon.



If you delete the user, then the trap destination where the user is added will also get deleted.

Adding a Trap Destination

You can add trap destinations to send notifications to SNMP management stations.



When adding a trap destination, you cannot edit the **SNMP** toggle switch and the **Enable SNMP on the selected VRF** options.

To add a trap destination, complete the following steps:

1. In the **Trap Destination** table, click the + add icon. A new row is added in the table.
2. Configure the following parameters:
 - **IP Address**—Enter a valid IPv4 or IPv6 address of the SNMP host.
 - **VRF**—Select the available VRF on the switch from the drop-down.
 - **Name**—Select the user to whom the notifications should be sent.
3. Click **Save**.

Editing a Trap Destination

To edit a trap destination, point to the row for the trap destination, and click the edit icon.



You can only edit the user name.

Deleting a Trap Destination

To delete a trap destination, point to the row for the trap destination, and click the delete icon.

Configuring Logging Servers for AOS-CX

Logging allows you to add syslog servers where the event log messages related to the AOS-CX switches are saved. For each of the syslog server you add, you can configure the severity of the event logs to be saved on these servers. You can also configure the severity level for the debug logs by configuring the severity at the global level. However, you must add a minimum of one syslog server to configure the global severity level.

To configure logging servers, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a group in the filter:
 - a. Set the filter to a group.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-CX** or **Config** icon to view the AOS-CX switch configuration dashboard.
 - To select a switch:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click an AOS-CX switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The AOS-CX UI configuration page is displayed.

2. Click **System > Logging**.
The Logging page is displayed.
3. Select the debug syslog severity level at the global level from the **Level** drop-down.
This severity level is applied to the debug logs that are saved on the syslog servers. You must add a minimum of one event syslog server before configuring the global severity level.
4. In the **Logging Servers** table, click the + add icon to add a logging server and configure the following parameters in the Add Logging Server page:

Table 98: *Logging Server Parameters*

Parameters	Description	Value
FQDN or IP address	FQDN hostname or IP address of the logging server.	IPv4 address in the <code>x.x.x.x</code> format or hostname of the server.
Level	Severity level of the events that the logging server must log.	Following severity levels are supported: <ul style="list-style-type: none"> ■ Emergency ■ Critical ■ Alert ■ Error ■ Warning ■ Notice ■ Information ■ Debug
VRF	VRF on which the logging server is configured.	Default or Management . NOTE: Management VRF is not supported on the AOS-CX 4100i and 6100 switch series.

5. Click **Apply** and then click **Save**.
6. To edit parameters of a logging server, select the row in the **Logging Servers** table and click the edit icon.
The Edit Logging Server page is displayed. You can edit only the event log severity level and the VRF.
7. Click **Apply** and then click **Save**.
8. To delete the syslog server, select the row in the **Logging Servers** table and click the delete icon.
9. Click **OK** in the confirmation pop-up and then click **Save**.

Configuring AAA for AOS-CX

Authentication, Authorization, and Accounting (AAA) is a security framework to authenticate users, authorize the type of access based on user credentials, and record authentication events and information about the network access and network resource consumption.

From the Administrator page, you can configure the following AAA properties:

- Authentication using TACACS, RADIUS, and local server groups.
- Authorization using TACACS and local server groups.
- Accounting using TACACS, RADIUS, and local server groups.

To configure AAA properties for AOS-CX switches, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-CX** or **Config** icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click an AOS-CX switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The AOS-CX UI configuration page is displayed.
2. Click **System > Administrator**.
The Administrator page is displayed with Authentication, Authorization, and Accounting tables.
3. You can configure Authentication, Authorization and Accounting from the respective tables.
 - To configure Authentication, click + in the **Authentication** table and configure the following parameters.

Table 99: *Authentication Parameters*

Name	Description	Value
Protocol	The type of protocol to enable connection to the server groups for authentication. You can add one or more protocols by clicking + in the Authentication table.	Console, Default, HTTPS Server, and SSH.
Server Groups	The list of server groups to be used for authentication. You can select one server group at a time. To add the next server group, click + either in the protocol row or any of the server group rows. The server groups are accessed in the top-down order. You can rearrange the order by dragging the server group to a different position using the  drag-and-drop icon.	TACACS, RADIUS, and Local.

- To configure Authorization, click + in the **Authorization** table and configure the following

parameters.

Table 100: *Authorization parameters*

Name	Description	Value
Protocol	The type of protocol to enable connection to the server groups for authorization. You can add one or more protocols by clicking + in the Authorization table.	Console, Default, and SSH.
Server Groups	The list of server groups to be used for authorization. You can select one server group at a time. To add the next server group, click + either in the protocol row or any of the server group rows. The server groups are accessed in the top-down order. You can rearrange the order by dragging the server group to a different position using the  drag-and-drop icon.	TACACS, Local, and None.

- To configure Accounting, click + in the **Accounting** table and configure the following parameters.

Table 101: *Accounting Parameters*

Name	Description	Value
Protocol	The type of protocol to enable connection to the server groups for accounting. You can add one or more protocols by clicking + in the Accounting table.	Console, Default, HTTPS Server, and SSH.
Server Groups	The list of server groups to be used for accounting. You can select one server group at a time. To add the next server group, click + either in the protocol row or any of the server group rows. The server groups are accessed in the top-down order. You can rearrange the order by dragging the server group to a different position using the  drag-and-drop icon.	TACACS, RADIUS, and Local.

4. Click **Save**.

Deleting AAA properties

To delete Authentication, Authorization, or Accounting, point to the row for the AAA property in the respective tables, and click the delete icon.

Configuring Source Interface for AOS-CX

Source interface allows you to configure a single source interface for a service so that all traffic routed through the switch is sent with the same IP address. The IP address is configured on the ports, LAGs, or VLANs at the device level.

You can add, modify, or delete source interface configuration in Aruba Central (on-premises). At the group level, Aruba Central (on-premises) allows you to configure only the port or LAG information for the interface. However, at the device level, you can also configure VLANs and IP address for the interface. Aruba Central (on-premises) supports only Central and User-based tunneling source interfaces in the UI. However, in the MultiEdit mode, you can configure source interfaces for other protocols such as, DNS, NTP, and PTP. The source interfaces that you add in the MultiEdit mode (other than Central and User-based tunneling) will not appear in the Source Interface page at the device level.

When you downgrade a switch from AOS-CX 10.07.0020 (with Central as source interface) to an earlier firmware version where source interface is not supported, Aruba Central does not allow the configuration to sync and displays a configuration conflict.



In such instances, you must delete the conflicting source interface configuration for Aruba Central to sync the configuration.

Table 102: Supported AOS-CX Switch Series

Switch Platform	Supported Source Interfaces		
	10.05, 10.06	10.07	10.08
AOS-CX 4100i Switch Series	-N/A-	-N/A-	<ul style="list-style-type: none"> ■ Central and User-based tunneling ■ IP address, VLAN configuration only
AOS-CX 6100 Switch Series	-N/A-	<ul style="list-style-type: none"> ■ Central only ■ IP address, VLAN configuration only 	-N/A-
AOS-CX 6200 Switch Series	<ul style="list-style-type: none"> ■ User-based tunneling only ■ IP address, VLAN configuration only 	<ul style="list-style-type: none"> ■ Central and User-based tunneling ■ IP address, VLAN configuration only 	-N/A-
AOS-CX 6300 Switch Series	User-based tunneling only	Central and User-based tunneling	-N/A-
AOS-CX 8320 Switch Series	-N/A-	Central only	-N/A-
AOS-CX 8325 Switch Series	-N/A-	Central only	-N/A-
AOS-CX 8360 Switch Series	-N/A-	Central only	-N/A-



To add a source interface, you must configure the following at the device level:

- Enable routing for ports and LAGs.
- Configure an IP address for the ports, LAGs, and VLANs.

Adding a Source Interface

To add a source interface, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-CX or Config** icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click an AOS-CX switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The AOS-CX UI configuration page is displayed.
2. Click **System > Source Interface**.
The Source Interface page is displayed with a list of source interfaces that are configured.
3. In the **Source Interface** table, click the + add icon to add a source interface and configure the following parameters in the **Create Source Interface** page.



When both Central and User-based tunneling source interfaces are added for a switch, the + add icon is disabled.

Table 103: *Configuring and Viewing Source Interface Parameters*

Name	Description	Value
Interface	The interface or the service name. You can configure only two interfaces at any given time.	Central or User-based tunneling
Port/LAG	Type of interface you want to configure. The name of this field is applicable only at the group level. At the device level, the field name is Port/LAG/VLAN/Address .	<ul style="list-style-type: none"> ■ At the group level—Port or LAG ■ At the device level—Port, LAG, VLAN, or Address

Name	Description	Value
Port name	Port number for the source interface. Applicable when you select Port in the Port/LAG drop-down at the group level or Port/LAG/VLAN/Address drop-down at the device level.	Select a port from the drop-down. NOTE: <ul style="list-style-type: none"> At the group level—Only the ports that have routing enabled at the group level are available in this drop-down. At the device level—Only the ports that have routing enabled and IP address configured on the ports at the device level are listed in this drop-down.
LAG name	LAG name for the source interface. Applicable when you select Port in the Port/LAG drop-down at the group level or Port/LAG/VLAN/Address drop-down at the device level.	Select a LAG from the drop-down. NOTE: <ul style="list-style-type: none"> At the group level—Only the LAGs that have routing enabled at the group level are available in this drop-down. At the device level—Only the LAGs that have routing enabled and IP address configured on the LAGs at the device level are listed in this drop-down.
VLAN ID	VLAN ID for the source interface. NOTE: <ul style="list-style-type: none"> Available only at the device level. Applicable when you select VLAN in the Port/LAG/VLAN/Address drop-down at the device level. 	Select a VLAN from the drop-down. NOTE: <ul style="list-style-type: none"> Only the VLANs that have an IP address configured at the device level are listed in this drop-down. The IP address must be a static IP address. DHCP server is not supported.
Address	IP address for the source interface. NOTE: <ul style="list-style-type: none"> Available only at the device level. Applicable when you select Address in the Port/LAG/VLAN/Address drop-down at the device level. 	IPv4 address
VRF	Type of VRF for the source interface. NOTE: You can configure the User-based tunneling interface only on the Default VRF.	Default or Management NOTE: Management VRF is not supported on the AOS-CX 4100i and 6100 switch series.

4. Click **Save**.

The source interface information is displayed in the **Source Interface** table.

Editing a source interface

To edit a source interface, point to the row for the source interface, and click the  edit icon. You can select only one source interface at a time for editing.

- When editing the Central interface, you cannot edit the interface type.
- When editing the User-based tunneling interface, you cannot edit the interface type and the VRF.

Deleting a source interface

To delete a source interface, point to the row for the source interface, and click the  delete icon. Deleting source interface at device level and modifying configuration at group level will not add the source interface again on the device. You can select only one source interface at a time for deleting.



Deleting the user-based tunneling source interface disables all configurations that depend on this source interface, for example, **Dynamic Segmentation**, **Client Roles**.

Configuring Static Routing on AOS-CX

Static routes provide a means for restricting and troubleshooting routed traffic flows. In small networks, static routes provide the simplest and most reliable configuration for routing. Static routes are manually configured in the routing table.

For each static route, you can configure the destination and next hop IP addresses to route the packets, VRF, and the administrative distance. You can add static routes only for the management and default VRFs.

The following are the maximum number of static routes (IPv4 and IPv6) that are supported on AOS-CX switches.

- AOS-CX 4100i, 6100 switch series—512
- AOS-CX 6200 switch series—2048
- AOS-CX 6300, 8360 switch series—65536
- AOS-CX 8320 switch series—163796
- AOS-CX 8325 switch series—29696



AOS-CX 6400 and 8400 switch series are not supported in Aruba Central (on-premises) UI configuration.

To add static routes on AOS-CX switches, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a group in the filter:
 - a. Set the filter to a group.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-CX** icon to view the AOS-CX switch configuration dashboard.
 - To select a switch:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.

- c. Click an AOS-CX switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The AOS-CX UI configuration page is displayed.
2. Click **Routing > Static Routing**.
The Static Routing page is displayed.
 3. In the **Static Routing** table, click the + add icon to add a static route and configure the following parameters in the Create Static Route page.



When the maximum number of routes are added for a switch, the + add icon is disabled.

Table 104: *Static Route Parameters*

Parameters	Description	Value
Destination	A valid network or device IP address with subnet mask.	IPv4 or IPv6 address. <ul style="list-style-type: none"> ■ IPv4 address in the <code>x.x.x.x/M</code> format, where <code>x</code> is an integer from 0 to 255, and <code>/M</code> is the subnet mask. ■ IPv6 address in the <code>xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/M</code> format, where <code>x</code> is a hexadecimal number from 0 to F, and <code>/M</code> is the subnet mask.
Next Hop	Address of the next node in the route.	<ul style="list-style-type: none"> ■ IPv4 or IPv6 address without the subnet mask. ■ Port number or LAG name that has routing enabled.
VRF	VRF on which the static route is configured.	<p>Default or Management. When you select Management, you can configure only the Next Hop field.</p> <p>NOTE:</p> <ul style="list-style-type: none"> ■ When you configure a static route with the Management VRF, the configured Next Hop address is updated as the default gateway of the OOBM interface when the address mode of the OOBM interface is configured as static IP. ■ Management VRF is not supported on the AOS-CX 4100i and 6100 switch series.
Distance	The administrative distance helps routers determine the best route when there are multiple routes to the destination. A lower value is recommended.	The default administrative distance for static IP routes is 1, but can be configured to any value in the range 1 to 255.



If the administrative distance is set to a lower value for static routes, switches use the static IP routes as the best route for routing traffic. For example, if the administrative distance for a static route is set to 20 and for an OSPF-based route is set to its default value, 110, then the switch choose the static route as the best route for routing traffic.

4. Click **Save**.

Configuring Ports and LAGs on AOS-CX

Link aggregation group (LAG) bundles multiple physical Ethernet links into one logical link. Link aggregation has the following benefits:

- Increased bandwidth beyond the limits of single link. In an aggregate link, traffic is distributed across the member ports.
- Improved link reliability. The member ports dynamically back up one another. When a member port fails, its traffic is automatically switched to other member ports.

From the Ports and Link Aggregation page, you can view all the ports, configure LAGs, and modify port settings for AOS-CX switches using UI groups.

Following are the maximum number of LAGs that are supported on AOS-CX switches:

- AOS-CX 4100i, 6100 switch series—8
- AOS-CX 6200 switch series—32
- AOS-CX 6300 switch series—256
- AOS-CX 8320, 8360 switch series—54
- AOS-CX 8325 switch series—128



AOS-CX 6400 and 8400 switch series are not supported in Aruba Central (on-premises) UI configuration.

Adding a LAG

To add a LAG, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-CX** or **Config** icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click an AOS-CX switch under **Device Name**.
The dashboard context for the switch is displayed.

d. Under **Manage**, click **Device**.

The AOS-CX UI configuration page is displayed.

2. Click **Interfaces > Ports & Link Aggregations**.

The Ports & Link Aggregations page is displayed with the list of ports configured on the switch.



In the device view, all access ports are shown by default. Click the filter in the **Name** column to select **All Uplink Ports** or **All Access Ports**. You can also search for a port using the port name.

3. In the **Ports & Link Aggregations** table, click the + add icon to add a Lag. The Add Lag window is displayed.



When the maximum number of LAGs are added for a switch, the + add icon is disabled.

4. Configure the following parameters:

Table 105: Link Aggregation Parameters

Name	Description	Value
Name	Name of the LAG.	Name starting with the string lag . Example: lag1, Lag23, LAG123.
Description	Description of the LAG.	A maximum of 64 characters including letters, numbers, and special characters, except question mark (?) and double quotes (").
Port Members	The switch port members for the LAG.	Select from the drop-down list.
Speed Duplex	The speed and duplex configuration for the client traffic. NOTE: Speed Duplex is shown or hidden depending on the value in Port Members field	Select from the drop-down list.
Routing	Indicates whether routing is enabled. If routing is enabled at the device level, then specify the IP address with subnet mask for the destination network. Format: (x.x.x.x/x). NOTE: If Routing is enabled at the device level, then port authentication configuration is reset on all the selected ports.	Toggle the switch to on or off position.
VLAN Mode	The operational mode of VLAN. This field is available only when Routing is disabled. In the access mode, port carries traffic only for the VLAN to which it is assigned. In the trunk mode, a port can carry traffic for multiple VLANs.	trunk or access For access mode, an Access VLAN can be specified.

Name	Description	Value
		<p>For trunk mode, the Native VLAN and Allowed VLANs can be configured. You can enter multiple Allowed VLANs by specifying the range of VLANs or VLANs separated by comma. For example, 1-7 or 55, 56, 57.</p> <p>NOTE: To specify the VLANs here, you must have already added the VLANs in the VLAN configuration page. See Configuring VLANs on AOS-CX.</p>
Admin Up	The operational status of the LAG. If the check box is selected, then the LAG can receive and transmit data as long as a cable is connected and no physical or operational problems exists.	Select the check box to enable.
Aggregation Mode	<p>The operational mode of link aggregation control protocol (LACP). LACP operates in these two modes:</p> <ul style="list-style-type: none"> ■ LACP active—When the LACP is operating in active mode on either end of a link, both ports can send Protocol Data Units (PDUs). The active LACP initiates an LACP connection by sending LACPDUs. ■ LACP passive—When the LACP is operating in passive mode on a local member port and its peer port, both ports cannot send PDUs. The passive LACP will wait for the remote end to initiate the link. 	None, LACP active, or LACP passive.

5. Click **Add**. The configured parameters are displayed in the **Ports & Link Aggregations** table.

Editing a LAG

To edit a LAG, point to the row for the LAG, and click the edit icon.



You can edit only one LAG at a time.

Deleting a LAG

To delete a LAG, point to row for the LAG, and click the delete icon.

Editing Ports settings

You can edit port settings by selecting one or more ports. If ports selected have different values configured, then changes made will be deployed on all the selected ports.



If a port is added to a LAG, then the port will not be displayed in the **Ports and Link Aggregation** table.

To edit ports, complete the following steps:

1. In the **Ports & Link Aggregations** table, select one or more ports you want to edit and click the edit icon.

The Edit Ports window is displayed.



- To edit a single port, click the edit icon on the corresponding row.
- To edit multiple ports, select the rows you want to edit and click the edit icon in the **<number of ports> item(s) selected** window at the right bottom of the page.
- In the device view, all ports are shown by default. Click the filter in the **Name** column to select **All Uplink Ports** or **All Access Ports**. You can also search for a port using the port name.

2. Edit the following parameters:

Table 106: Ports Parameters

Name	Description	Value
Description	Description of the ports. When multiple ports are selected, then you can provide the same description for all the selected ports by selecting a set same value for all ports check box. You can also provide different descriptions by clicking on the individual port fields.	A maximum of 64 characters including alphabets and numbers. Special characters are not allowed.
Speed Duplex	The speed and duplex configuration for the client traffic.	Select from the drop-down list. By default, Speed Duplex is set to Auto .
Routing	Indicates whether routing is enabled. If routing is enabled at the device level, then specify the IP address with subnet mask for the destination network. Format: (x.x.x.x/x), whereas IP address is not required at the group level. NOTE: If Routing is enabled at the device level, then port authentication configuration is reset on all the selected ports.	Toggle the switch to on or off position.
VLAN Mode	The operational mode of VLAN. This field is available only when Routing is disabled. By default, a port is in access mode and carries traffic only for the VLAN to which it is assigned. In trunk mode, a port can carry traffic for multiple VLANs. NOTE: This option is not visible for VSF ports.	trunk or access For access mode, an Access VLAN can be specified. For trunk mode, the Native VLAN and Allowed VLANs can be configured. You can enter multiple Allowed VLANs by specifying the range of VLANs or VLANs separated by comma. For example, 1-7 or 55, 56, 57.
Admin Up	The operational status of the port. If the check box is selected, then the port can send and receive data as long as a cable is connected and no physical or operational problems exist.	Select the check box to enable.

3. Click **Save**.

Editing OOBM Port

You can edit the Out of Band Management (OOBM) port at the device level. To edit the OOBM port, complete the following steps:

1. Select the **OOBM** port and click the edit icon.
The Edit Port OOBM page is displayed.
2. Edit the following parameters:
 - **IP assignment**—Method of IP assignment as **Static** or **DHCP**. Enter the IP address for IP assignment if the selected method is **Static**.
 - **Admin UP**—Operational status of the port. If the check box is selected, then the port can send and receive data as long as a cable is connected and no physical or operational problems exists.
3. Click **Save**.

Configuring Authentication Servers on AOS-CX

From the Server groups page, you can configure RADIUS or TACACS authentication servers to authenticate and authorize the users of an AOS-CX switch. The authentication servers determine if the user has access to the administrative interface.

To configure authentication servers on a switch, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-CX** icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click an AOS-CX switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The AOS-CX UI configuration page is displayed.
2. Click **Security > Authentication Servers**. The Authentication Servers page is displayed with number of RADIUS and TACACS servers that are configured on the switch.

Configuring a RADIUS Server on AOS-CX

To configure a RADIUS server, complete the following steps:

1. In the **Authentication Servers** table, point to the **RADIUS** server row and click the edit icon. The RADIUS servers page is displayed with the list of RADIUS servers configured on the switch.
2. To add a RADIUS server, click the + add icon.
The Add RADIUS window is displayed.

- Configure the following parameters:

Table 108: RADIUS Parameters

Name	Description	Value
FQDN or IP address	The IP address or fully qualified domain name of the RADIUS server.	
Shared secret	The encryption key to be used during authentication sessions with the specified RADIUS server.	You can enter up to a maximum of 32 characters including letters, numbers, and special characters, except question mark (?) and double quotes (").
Authentication Port	The authentication port number for the specified server.	Range: 1-65535 Default: 1812
Timeout (secs)	The number of seconds to wait for a response from the RADIUS server before trying the next RADIUS server.	Range: 1-60 Default: 5
VRF	The VRF to be used for communicating with the RADIUS server.	Default and Management NOTE: Management VRF is not supported on the AOS-CX 4100i and 6100 switch series.
Retry Count	The number of retry attempts for contacting the specified RADIUS server.	Range: 0-5 Default: 1

- Click **Apply**. The added server is displayed in the RADIUS servers page. The server that was added first is accessed first, and if necessary, the second server is accessed second, and so on. You can rearrange the order by dragging the server to a different position using the  drag-and-drop icon.
- Click **Save**.

Configuring TACACS Server on AOS-CX

To configure a TACACS server, complete the following steps:

- In the **Authentication Servers** table, point to the **TACACS** server row and click the edit icon. The TACACS servers page is displayed with the list of TACACS servers configured on the switch.
- To add a TACACS server, click the + add icon. The Add TACACS window is displayed.

- Configure the following parameters:

Table 109: TACACS Parameters

Name	Description	Value
FQDN or IP address	The IP address or fully qualified domain name of the TACACS server.	
Shared secret	The encryption key to be used during authentication sessions with the specified TACACS server.	You can enter up to a maximum of 32 characters including letters, numbers, and special characters, except question mark (?) and double quotes (").
Authentication Port	The authentication port number for the specified TACACS server.	Range: 1-65535 Default: 49
Timeout (secs)	The number of seconds to wait for a response from the TACACS server before trying the next TACACS server.	Range: 1-60 Default: 5
VRF	The VRF to be used for communicating with the TACACS server.	Default and Management NOTE: Management VRF is not supported on the AOS-CX 4100i and 6100 switch series.

- Click **Apply**. The added server is displayed in the TACACS servers page.
The server that was added first is accessed first, and if necessary, the second server is accessed second, and so on. You can rearrange the order by dragging the server to a different position using the  drag-and-drop icon.
- Click **Save**.

Configuring Authentication on AOS-CX

Aruba Central (on-premises) supports the following authentication methods for AOS-CX switches:

- **802.1X Authentication**—Used for authenticating the identity of a user before providing network access. 802.1x
 - Supplicant: Device that tries to access the LAN.
 - Authenticator: A network device, such as an Ethernet switch that authenticates the supplicant.
 - Authentication Server: Typically a host running software supporting the RADIUS and EAP protocols that provides an authentication service to the authenticator.
- **MAC Authentication**—Used for authenticating devices based on their physical MAC addresses. For MAC authentication, the MAC address of a machine must match an approved list of MAC addresses defined on the RADIUS server.



You must configure at least one RADIUS server to use 802.1X or MAC authentication.

To configure authentication at port level, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-CX** icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click an AOS-CX switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The AOS-CX UI configuration page is displayed.
2. Click **Security > Authentication**.
The Authentication page is displayed.
3. Under the **MAC authentication**, select one of the following modes to communicate with RADIUS servers.
 - **PAP** (Password Authentication Protocol)
 - **CHAP** (Challenge-Handshake Authentication Protocol)



At the global level, **802.1X Authentication** uses the **EAP** (Extensible Authentication Protocol) mode to communicate with the RADIUS server.

4. In the **Ports** table, select one or more ports for which you want to configure authentication, and click the edit icon.
The Edit Ports page is displayed.
5. Configure the following parameters:

Table 110: *Configuring Authentication*

Name	Description	Value
Authentication	The method of authentication.	Select any one of the following authentication methods: <ul style="list-style-type: none"> ■ None—Disables authentication. By default, the authentication is disabled. ■ 802.1X—Enables 802.1X method for authentication. ■ MAC—Enables MAC method for authentication ■ 802.1X, then MAC—Enables both 802.1X

Name	Description	Value
		<p>and MAC authentication methods and sets the precedence to 802.1X authentication.</p> <ul style="list-style-type: none"> ■ MAC, then 802.1X—Enables both 802.1X and MAC authentication methods and sets the precedence to MAC authentication. ■ Concurrent—Enables both 802.1X and MAC authentication methods to start simultaneously for faster onboarding process. You can select 802.1X or MAC authentication from the Priority drop-down menu. Default priority for concurrent is 802.1X followed by MAC authentication.
Client Limit	The maximum number of clients to be allowed on the port.	<p>Enter up to a maximum of 256 clients. Default: 1</p> <p>Following are the maximum clients supported on switches:</p> <ul style="list-style-type: none"> ■ AOS-CX 4100i, 6100, 6200, switch series—32 ■ AOS-CX 6300 switch series—256 <p>At the group level, the maximum clients supported is 256.</p> <p>NOTE:</p> <ul style="list-style-type: none"> ■ Port access authentication is not supported on AOS-CX 8320, 8325, and 8360 switch series. ■ AOS-CX 6400 and 8400 switch series are not supported in Aruba Central (on-premises) UI configuration.
Reauthentication Timeout	The time (in seconds) that the switch enforces on a client to re-authenticate. The client remains authenticated while the re-authentication occurs. By default, this field is disabled and the default value is displayed. To edit the default value, select the check box and specify the value.	Default: 3600 seconds

Name	Description	Value
Cached Reauthentication Timeout	The time (in seconds) when cached re-authentication is allowed on the port. By default, this field is disabled and the default value is displayed. To edit the default value, select the check box and specify the value.	Default: 30 seconds
Quiet Period	The time (in seconds) during which the port does not try to acquire a supplicant. The period begins after the last attempt authorized by the max-requests parameter fails.	Default: 60 seconds

6. Click **Apply**. The authentication parameters are displayed in the **Ports** table.
7. Click **Save**.

Configuring Access Control on AOS-CX

Access control allows you to permit or deny traffic based on network addresses, protocols, service ports, and other packet attributes. An Access policy defines a set of rules based on network traffic addressing and uses these rules to permit or deny the passage of traffic through the switch. The permit action allows the traffic to continue through the switch and the deny action causes the traffic to be discarded (dropped).

From the Access Control page, you can add access policies and set different rules for the access policies using UI groups.

Adding an Access Policy

You can add access policies by defining traffic rules. A policy can be applied to an individual front plane port, a Link Aggregation Group (LAG) interface, or a VLAN.

The following are the maximum number of policies that are supported on AOS-CX switches.

- AOS-CX 4100i, 6100 switch series—512
- AOS-CX 6200, 6300 switch series—4000
- AOS-CX 8320 switch series—16000
- AOS-CX 8325, 8360 switch series—4000



AOS-CX 6400 and 8400 switch series are not supported in Aruba Central (on-premises) UI configuration.

To add an access policy, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-CX** or **Config** icon to view the switch configuration dashboard.

- To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click an AOS-CX switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The AOS-CX UI configuration page is displayed.
- 2. Click **Security > Access Control**.
The Access Control page is displayed with the name of the policy.
- 3. In the **Access Control** table, click the + add icon to add a policy.
The Add policy page is displayed.



When the maximum number of policies are added for a switch, the + add icon is disabled.

4. Configure the following parameters.

Table 111: Access Policy Parameters

Name	Description	Value
Name	The name of the access policy.	A maximum of 64 characters including letters, numbers, and special characters, except question mark (?) and double quotes (").
Direction	The traffic direction for Ports and LAGs. The available directions are: <ul style="list-style-type: none"> ■ Inbound—Controls the incoming traffic on the selected ports or LAGs. ■ Outbound—Controls the outgoing traffic on the selected ports or LAGs. 	Inbound or Outbound
Ports & LAGs	The ports and LAGs on which the policy is applied.	Select a value from the drop-down.
Direction	The traffic direction for VLANs. The available directions are: <ul style="list-style-type: none"> ■ Inbound—Controls the incoming traffic on the layer 2 interface VLANs. ■ Outbound—Controls the outgoing traffic on the layer 2 interface VLANs. ■ Routed Inbound—Controls the incoming traffic on the layer 3 interface VLANs. ■ Routed Outbound—Controls the outgoing traffic on the layer 3 interface VLANs. 	Inbound, Outbound, Routed Inbound, or Routed Outbound.

Name	Description	Value
VLANs	The VLANs on which the policy is applied. The list of layer 2 and layer 3 interface VLANs are displayed based on the Direction selection.	Select one or more VLANs from the drop-down list.

5. Click **Apply**. The Access Control table is displayed with the number of ports & LAGs, and VLANs configured on inbound and outbound traffic.

Editing an Access Policy

To edit a policy, point to the row for the policy, and click the edit icon.

Deleting an Access Policy

To delete a policy, point to the row for the policy, and click the delete icon.

Adding a Rule for Policy

You can add access rules for a policy to either allow or deny the traffic passing through the switch.

The following are the maximum number of rules that are supported on AOS-CX switches.

- AOS-CX 4100i, 6100 switch series—4096
- AOS-CX 6200, 6300 switch series—8000
- AOS-CX 8320 switch series—32000
- AOS-CX 8325, 8360 switch series—4000



AOS-CX 6400 and 8400 switch series are not supported in Aruba Central (on-premises) UI configuration.

To add a access rule, complete the following steps:

1. In the **Access Control** table, select the policy for which you want to add a rule by clicking on the policy.
The Policy Rules page is displayed.
2. In the **<Policy name> Rules** table, click the + add icon to add a rule.
The Add rule for policy "<policy name">page is displayed.



-
- After adding the first rule, the + add icon in the **<Policy name> Rules** table is disabled. To add more rules to the same policy, click the + add icon present in the row corresponding to the rule after which you want to add the next rule.
 - When the maximum number of rules are added for a switch series, the + add icon is disabled.
-

- Configure the following parameters.

Table 112: Access Rules Parameters

Name	Description	Value
Action	The action for the traffic passing through the switch.	Permit or Deny
Description	Description for the rule.	A maximum of 256 characters including letters, numbers, and special characters, except question mark (?) and double quotes (").
Source type	The type of source for which you want to apply a policy.	Any, Network, or Host. If you select Network, enter the IP address and Mask. If you select Host, enter the IP address.
Destination type	The type of destination for which you want to apply a policy.	Any, Network, or Host. If you select Network, enter the IP address and Mask. If you select Host, enter the IP address.
Protocol	The type of data transfer protocol. If you select SCTP, TCP, or UDP the Source port and Destination port fields are displayed.	Protocol types: Any, AH, ESP, GRE, ICMP, IGMP, IP, OSPF, PIM, SCTP, TCP, and UDP.
Source Port	The port numbers of source. You can specify a single port in the Source Port field or range of ports in the Source Port and Source Port Max fields. For example, if you want to specify the source port range as 1 to 7, then specify 1 in the Source Port field and 7 in the Source Port Max field.	An integer
Source Port Max	The end port number in the range of source ports. This field is applicable only if you want to configure a range of source ports.	An integer
Destination Port	The port numbers of destination. You can specify a single port in the Destination Port or range of ports in the Destination Port and Destination Port Max fields. For example, if you want to specify port range as 1 to 7, then specify 1 in the Destination Port field and 7 in the Destination Port Max field.	An integer
Destination Port Max	The end port number in the range of destination ports. This field is applicable only if you want to configure a range of destination ports.	An integer

- To create another rule, select **Stay and create another** check box and add a new rule.

5. Click **Apply**. The new rules are displayed in the Policy Rules table.
By default, the rules are sequenced in the order in which they are added. You can rearrange the sequence by dragging the rule to the position you want using the  drag-and-drop icon.
6. Click **Save**.

Editing a Rule

To edit a rule, point to the row for the rule, and click the edit icon.

Deleting a Rule

To delete a rule, point to the row for the rule, and click the delete icon.

Configuring User-Based Tunneling for AOS-CX

User-based tunneling (UBT) uses GRE to tunnel ingress traffic on a switch interface to a gateway for further processing. User-based tunneling enables a switch to provide a centralized security policy, using per-user authentication and access control to ensure consistent access and permissions.

User-based tunneling is supported on the following switches:

- AOS-CX 6300 F and M switch series
- AOS-CX 6400 switch series

For provisioning User-based tunnel, the following configurations are necessary:

- All devices need to be Day 0 provisioned
- Underlay network is connected and reachability established
- All devices in the underlay and topology is clearly identified

To configure user-based tunnel, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-CX** or **Config** icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click an AOS-CX switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The AOS-CX UI configuration page is displayed.
2. Click **Security > Dynamic Segmentation** to view the switch configuration dashboard.

3. Toggle the **User based tunneling** switch to on position.
The toggle switch is disabled by default. Enabling this toggle, shows a warning message on how to configure the User-based tunnel.
4. Enter **Primary controller IP address** and **Backup controller IP address**. Make sure that primary and backup IP address are different.
5. Enter the VLAN ID under **Client VLAN** only when you select the **Reserved** option.
6. In the **Source interface** drop-down, select **Add new source interface**.

The **Edit Source Interface** window is displayed. Configure the following parameters.



If a user-based tunnel source interface is already added in the **Source Interface** page, it will appear in the drop-down. For more information about source interface, see [Configuring Source Interface for AOS-CX](#).

Table 113: *New Source Interface Parameters*

Name	Description	Value
Interface	The interface or the service name. By default, only User-based tunneling is selected in the Dynamic Segmentation page.	User-based tunneling
Port/LAG	Type of interface you want to configure. The name of this field is applicable only at the group level. At the device level, the field name is Port/LAG/VLAN/Address .	<ul style="list-style-type: none"> ■ At the group level—Port or LAG ■ At the device level—Port, LAG, VLAN, or Address
Port name	Port number for the source interface. Applicable when you select Port in the Port/LAG drop-down at the group level or Port/LAG/VLAN/Address drop-down at the device level.	Select a port from the drop-down. NOTE: <ul style="list-style-type: none"> ■ At the group level—Only the ports that have routing enabled at the group level are available in this drop-down. ■ At the device level—Only the ports that have routing enabled and IP address configured on the ports at the device level are listed in this drop-down.
LAG name	LAG name for the source interface. Applicable when you select Port in the Port/LAG drop-down at the group level or Port/LAG/VLAN/Address drop-down at the device level.	Select a LAG from the drop-down. NOTE: <ul style="list-style-type: none"> ■ At the group level—Only the LAGs that have routing enabled at the group level are available in this drop-down. ■ At the device level—Only the LAGs that have routing enabled and IP address configured on the LAGs at the device level are listed in this drop-down.

Name	Description	Value
VLAN ID	VLAN ID for the source interface. NOTE: <ul style="list-style-type: none"> Available only at the device level. Applicable when you select VLAN in the Port/LAG/VLAN/Address drop-down at the device level. 	Select a VLAN from the drop-down. NOTE: <ul style="list-style-type: none"> Only the VLANs that have an IP address configured at the device level are listed in this drop-down. The IP address must be a static IP address. DHCP server is not supported.
Address	IP address for the source interface. NOTE: <ul style="list-style-type: none"> Available only at the device level. Applicable when you select Address in the Port/LAG/VLAN/Address drop-down at the device level. 	IPv4 address
VRF	The VRF to be used for communicating with DNS and NTP servers.	Default

7. Click **Save**,

Configuring Client Roles for AOS-CX

You can assign network access to clients using client roles. The network admin can create configuration profiles (roles) and associate them to clients. Client roles allow you to create and manage roles and attributes for the network.

To create a client role, complete the following steps:

- In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - Set the filter to a group.
The dashboard context for the group is displayed.
 - Under **Manage**, click **Devices > Switches**.
 - Click the **AOS-CX** icon to view the switch configuration dashboard.
- Click **Client Roles**.
- Under **Client Roles** table, click the + add icon to create a new role.
Configure the following parameters.

Table 114: *Client Roles Parameters*

Name	Description	Value
Name	Name of the role.	This is a mandatory parameter.

Name	Description	Value
		This parameter supports letters, numbers, and special characters.
VLAN mode	VLAN mode of the role.	Access or Trunk Default value is Access .
VLAN	VLAN ID of the role.	Default value is 1.
Authentication mode	Select either MD5 (Message Digest) or SHA (Secure Hash Algorithm) as the authentication mode to provide secured access to the user.	Client-Mode or Device-Mode Default value is Client-Mode .
Trust mode	Trust mode for the role.	None , DSCP , or COS Default value is None .
Reauthentication period	The time (in seconds) after which the switch enforces on a client to reauthenticate. The client remains authenticated while the reauthentication occurs.	Default value is 30 seconds.
PoE priority	PoE priority configured on the port.	Critical , High , or Low . Default value is Low .
STP admin edge port	Enable or disable STP admin edge port for the role.	By default STP admin edge port is enabled.
User-based tunnel	<p>Enable or disable user-based tunneling for the role.</p> <p>NOTE:</p> <ul style="list-style-type: none"> ■ To enable user-based tunnel for a client role, user-based tunneling must be enabled in Dynamic Segmentation. ■ If User-based tunnel is enabled for a role and if User-based tunnel feature is disabled in the Dynamic Segmentation page, then User-based tunnel for the role is disabled automatically. 	<p>Move the toggle switch to the on position to enable.</p> <p>By default, it is disabled.</p>
Gateway cluster	<p>Name of the gateway cluster zone.</p> <p>NOTE: By default, the cluster zone name is default. You cannot change the gateway cluster name.</p>	
Gateway Role	Name of the gateway role for the client role.	This parameter supports letters, numbers, and special characters.

4. Click **Save**.



You cannot edit client roles.

Deleting Client Roles

To delete a client role, point to the row for the role, and click the  delete icon.

Configuring VLANs on AOS-CX

VLANs are primarily used to provide network segmentation at layer 2. VLANs enable the grouping of users by logical function instead of physical location. VLANs make managing bandwidth usage within networks possible by:

- Allowing grouping of high-bandwidth users on low-traffic segments
- Organizing users from different LAN segments according to their need for common resources and individual protocols
- Improving traffic control at the edge of networks by separating traffic of different protocol types
- Enhancing network security by creating subnets to control in-band access to specific network resources

From VLANs page, you can add VLANs and manage VLAN settings such as name, description, admin status, and IP assignment for AOS-CX switches.

For AOS-CX 6200 and 6300 switch series, VLAN 1 (DEFAULT_VLAN_1) is associated with all interfaces on the switch. The DHCP assignment of IP address is available only on the default VLAN.



You can add only one VLAN at a time.

Adding a VLAN

To add a VLAN, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-CX** or **Config** icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click an AOS-CX switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The AOS-CX UI configuration page is displayed.
2. Click **Bridging > VLANs**.
The VLANs page is displayed with a list of VLANs.
3. In the **VLANs** table, click the + add icon to add a VLAN and configure the following parameters.



When the maximum number of VLANs are added for a switch, the + add icon is disabled.

Table 115: Configuring and Viewing VLAN Parameters

Name	Description	Value
ID	The VLAN ID number.	<p>Following are the different ranges for the VLANs supported on switches:</p> <ul style="list-style-type: none"> ■ AOS-CX 4100i, 6100 switch series—2 to 512 ■ AOS-CX 6200 switch series—2 to 2048 ■ AOS-CX 6300 and 8360 switch series—2 to 4094 ■ AOS-CX 8320 and 8325 switch series—2 to 4040 <p>At the group level, the maximum VLANs supported is 4094</p> <p>NOTE: AOS-CX 6400 and 8400 switch series are not supported in Aruba Central (on-premises) UI configuration.</p>
Name	The name of the VLAN.	Only letters (a-z) and numbers (0-9) are allowed.
Description	The description of the VLAN.	Letters, numbers, and special characters are allowed except question mark (?) and double quotes (").
Admin UP	The operational status of the VLAN. The VLAN can forward packets only when the check box is selected.	Select the check box to enable.
Voice	The VLAN support for voice.	Select the check box to enable.
IP Assignment	<p>The method of IP assignment. The options to enter the IP address is displayed only when you select Static. This field is available only at the device level.</p> <p>NOTE: The DHCP option is available only for the default VLAN on AOS-CX 6100, 6200, and 6300 switch series.</p>	Static, DHCP, or None Default: None
IP Address	<p>The IP address with subnet mask for IP assignment.</p> <p>This field is enabled only when you select Static from the IP address assignment drop-down and available only at the device level.</p>	IPv4 address or IPv6 address with subnet mask Format: (x.x.x.x/x).
DHCP Relay	The IP address of the DHCP relay server. This field is enabled only when you select DHCP or Static from the IP address assignment drop-down and available only at the device level.	IPv4 address

Name	Description	Value
	<p>NOTE:</p> <ul style="list-style-type: none"> ■ AOS-CX 6100 and 6200 switch series—DHCP relay is not supported ■ AOS-CX 6300 switch series—DHCP relay is available only on the default VLAN 	

4. Click **Add**.

The VLAN information is displayed in the VLANs table.

Editing a VLAN

To edit a VLAN, point to the row for the VLAN, and click the edit icon. You can select only one VLAN at a time for editing.



You cannot edit the name of the default VLAN and admin status.

Deleting a VLAN

To delete a VLAN, point to the row for the VLAN, and click the delete icon. Deleting VLAN at device level and modifying configuration at group level will not add the VLAN again on the device. You can select only one VLAN at a time for deleting.



You cannot delete the default VLAN.

Configuring Loop Prevention on AOS-CX

Loop prevention provides protection against infinite loops by transmitting loop protocol packets out of the switch ports. You can enable loop prevention by configuring one of the following methods:

- Loop protection at the interface level (ports, LAGs).
 - Loop protection at the interface level:
 - can find loops by sending loop protection packets on each port or LAG on which loop protection is enabled.
 - is useful when spanning tree protocols cannot prevent loops at the edge of the network.
 - can be used to find loops in untagged layer 2 links and on tagged VLANs.
 - can be configured either when the spanning tree protocol is configured on the interfaces or not.
- Spanning tree protocol at both global and interface level.
 - Spanning tree protocols such as MSTP and RPVST help prevent loops in networks by blocking redundant links.

Loop protection and spanning tree are always disabled by default on AOS-CX switches. To configure loop protection and spanning tree for switches provisioned in the UI groups, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a group in the filter:
 - a. Set the filter to a group.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-CX** or **Config** icon to view the AOS-CX switch configuration dashboard.
 - To select a switch:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click an AOS-CX switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The AOS-CX UI configuration page is displayed.
2. Click **Bridging > Loop Prevention**. The Loop Prevention page is displayed.
The **Ports** table displays the following information:

Table 116: *Information in the Ports Table*

Column	Description
Number	Port number or the name of the LAG.
Description	Description of the port or LAG interface that you configure on the Ports & Link Aggregations page.
LAG Members	List of port numbers that are grouped to form the LAG.
Loop Protection	Displays whether loop protection is enabled or disabled for that interface.

3. To enable spanning tree, move the **Spanning Tree** toggle switch to the on position.
Configure the following parameters:
 - **Mode**—Select **MSTP** from the drop-down list.
You can configure various MSTP parameters for the ports in the switches.



You cannot select **RPVST** from the **Mode** drop-down. To configure RPVST mode for spanning tree, you must use Edit Config in the **MultiEdit** mode and configure using the CLI commands.

However, after configuring the mode as **RPVST**, if you want to change the mode to MSTP, you can select **MSTP** in the **Mode** drop-down.

- **Priority**—Priority of the UI group.
At the group level, the priority is listed in multiples of 4096. A range from 0 to 61440 is supported. The default value is 32768.
4. To configure MSTP parameters for ports, select the row(s) in the **Ports** table and click the edit icon.
The Loop Prevention page is displayed with the following parameters.

Table 117: MSTP Parameters for Ports and LAGs

Parameters	Description
Loop Protection	Move the toggle switch to enable or disable loop protection on the interfaces.
Spanning Tree	
Priority	A number used to identify the root bridge in an STP instance. The priority is listed in multiples of 16 in the drop-down. The priority ranges from 0 to 240. The default priority is 128. The switch with the lowest value has the highest priority and is considered the root bridge. A higher numerical value means a lower priority; thus, the highest priority is 0.
BPDU Protection	Security feature used to protect the active STP topology by preventing manipulated BPDU packets from entering the STP domain. Select the check box to enable BPDU protection on the interface.
BPDU Filter	Enables control of STP participation for each port. The feature can be used to exclude specific ports from becoming part of STP operations. A port or LAG with the BPDU filter enabled ignores incoming BPDU packets and stays locked in the STP forwarding state. Select the check box to enable BPDU filter on the interface.
Admin-Edge	Configures the interface in the forwarding state. Select the check box to enable Admin edge on the interface. NOTE: If Admin edge is not configured on the switch, the default port type is admin-network.
Root Guard	Configures the interface to prevent from being configured as a root port when it receives superior STP BPDUs. Select the check box to enable root guard on the interface.

5. To save the changes, click **Apply**.

Using MultiEdit View for AOS-CX

This section describes the configuration and viewing procedures for the AOS-CX switches in the MultiEdit mode.



MultiEdit mode configuration is applicable only at the device level and allows configuring a single or multiple switches using the CLI syntax.

To configure or view details of the switches provisioned in UI groups, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a group in the filter:
 - a. Set the filter to a group.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-CX** or **Config** icon to view the AOS-CX switch configuration dashboard.

- To select a switch:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click an AOS-CX switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The AOS-CX UI configuration page is displayed.
- 2. To enable MultiEdit mode, move the **MultiEdit** toggle switch to the on position.
The **Device-Level Configuration** page is displayed with the list of devices displayed in the **Devices** table.



At the device level, the **Devices** table lists only the switch that you have selected. Also, a pop-up is displayed on the bottom-right corner of the page with the options **View Config**, **Edit Config**, and **Express Config**.

3. Search for a switch by entering a search query in the **Contextual Search Engine** field.
For more information about search queries, see [Using Device Search on AOS-CX](#).
The following table describes the columns in the **Devices** table.

Table 118: Columns in the Devices Table in the MultiEdit Mode

Column	Function
Name	Name of the AOS-CX switch.
Firmware Version	Firmware version installed on the switch.
Config Modified	Timestamp when the configuration on the switch was last modified.
Status	Status of the switch, whether Online or Offline .
Config Status	Status of the configuration sync between Aruba Central (on-premises) and the switch. <ul style="list-style-type: none"> ■ Sync—Configuration is in sync between Aruba Central (on-premises) and the switch. ■ Not in sync (Connection error)—Configuration is not in sync due to a connection error. ■ Not in sync (Modified outside Central)—Configuration is not in sync because configuration was modified outside Aruba Central (on-premises). ■ Not in sync (Pushing config)—Configuration is not in sync because Aruba Central (on-premises) is still pushing configuration to the switch.
NAE Status	Consolidated status of the NAE agents running on the switch. Following are the supported values: <ul style="list-style-type: none"> ■ Critical—The agent has encountered a critical error during execution. ■ Major—The agent has encountered a major error during execution. ■ Minor—The agent has encountered a minor error during execution. ■ Normal—The agent is actively monitoring network conditions and handling events.

Column	Function
	<ul style="list-style-type: none"> ■ Disabled—The agent is disabled. ■ Unknown—The agent status is unknown.
MAC Address	MAC address of the switch.
IP Address	IP address of the switch.
Serial	Serial number of the switch.
Model	Model number of the switch.

The MultiEdit mode provides an option to view or edit switch configuration or apply predefined configurations to the switches.

- [Viewing Configuration Using MultiEdit on AOS-CX](#)
- [Editing Configuration Using MultiEdit on AOS-CX](#)
- [Express Configuration Using MultiEdit on AOS-CX](#)

Using Device Search on AOS-CX

In the MultiEdit mode, the Contextual Search Engine allows you to filter a set of AOS-CX switches using search queries. The search queries can contain one or more search terms in the format, label:value. For example: model:6300F, where model is the label and 6300F is the value. When a search query contains a list of terms, by default, all terms are required to match. For example, the search query "model:8400 current-firmware:10.04.0001" will return only 8400 switches running 10.04.0001 firmware. The filtered switch details are displayed in the Devices table.

The search queries can contain the following information:

- Device attributes—Attributes that denote the device details such as the model and current-firmware.
- Wildcard characters—Asterisk (*) and question mark (?) are allowed in search queries.
- Boolean operators—For complex queries, you can use the boolean operators AND, OR, NOT, + (the plus sign), and - (the minus sign).
- Grouping characters—Multiple search terms with logical operators can be grouped using parenthesis ().

You must use quotes (" ") for any strings with spaces and for the default, running-config, and startup-config search. A default search is specified by entering quoted text instead of a label:value search term. The default search runs the search against the running configurations of the devices. For example, entering "ntp server1 72.16.0.100" searches for that string in the running configuration of all managed devices in the MultiEdit mode. Multiple search terms can be used in a query and can be combined using logical operators.

Searching for Devices

To access Contextual Search Engine and perform search, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one switch. The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Switches**.
3. Click the **Config** icon to view the switch configuration dashboard.

4. Slide the **MultiEdit** toggle switch to the on position to enable MultiEdit mode. The **Devices** table displays the list of devices in the selected group.
5. Hover over the values in the table cells to view the labels that can be used in the search query. For example, if you hover over a cell in the Status column, a pop-up is displayed with the label that can be used in the search term and an example.
6. In the **Contextual Search Engine** field, enter a search query, and click **Search & Filter** to filter a set of switches. The Devices table lists the devices that match the search query.

Device Attributes

The following table lists the field names that can be used in the search query as device attributes.

Table 119: *List of Field Names*

Field Name	Definition	Example
active-image	Active image location	active-image:primary
chassis	Name of the chassis if available	chassis:1
config-auto-commit	Configuration auto commit state	config-auto-commit:On config-auto-commit:Off
config-failure-reasons	Reason for configuration failure when the configuration-state is "Not in sync"	config-failure-reasons:"Connection error" config-failure-reasons:"Configuration conflicts" config-failure-reasons:"Internal error" config-failure-reasons:"Modified outside Central" config-failure-reasons:"Initial group config pending" config-failure-reasons:"Pushing config" config-failure-reasons:"Connection error with pending changes" config-failure-reasons:"Auto commit off"
configuration-state	Configuration sync state	configuration-state:Sync
current-firmware	Current firmware version	current-firmware:10.02.0001
default-image	Default image location	default-image:secondary
fabric-card	Name of the fabric cards, if available	fabric-card:1V1
firmware-version	Firmware version on the device	firmware-version:FL.10.1
hw-serial	Serial number of attached hardware	hw-serial:TW0989W
ip-address	Management IP address	ip-address:172.16.0.100
label	Label assigned to the device	label:Floor1
last-sync-time	Last time when configuration in central and device are in sync	last-sync-time:2020-08-27 last-sync-time:2020-08-27T19 last-sync-time:2020-08-27T19:01:20Z last-sync-time:[2020-08-27T19:01:20Z TO *] last-sync-time:[2020-08-27 TO 2020-08-28] last-sync-time:[2020-08-27T20 TO 2020-08-27T23]

Field Name	Definition	Example
		last-sync-time:[2020-08-27T19:00:00 TO 2020-08-27T23:00:00] last-sync-time:[2020-08-27T11:30:00Z TO 2020-08-27T23:00:00Z]
line-card	Name of the line cards, if available	line-card:1V1
local-override	Device local override is enabled or not	local-override:Yes local-override:No
mac-address	Base MAC address	mac-address:e7c7dc-32f000
management-module	Name of the management module, if available	management-module:1V1
manufacturer	Manufacturer name	manufacturer:Aruba
model	Model number	model:6300F
nae-status	NAE status of the switch	nae-status:normal
name	The devices user-defined name	name:cx_6300F_ERIA000001
part-number	Product names of the device and attached hardware	part-number:JL635A
power-supply	Name of the power-supply, if available	power-supply:1V1
primary-version	Primary image version	primary-version:GL.10.11
product-name	Product names of the device and attached hardware	product-name:"8325 Mgmt Mod"
product-number	Product number of the device	product-number:8325
running-config	Contents of the running configuration (this is the default search field)	running-config:"ospf"
running-config-modified	Date and time of latest running configuration change	running-config-modified:2020-08-27 running-config-modified:2020-08-27T19 running-config-modified:2020-08-27T19:01:20Z running-config-modified:[2020-08-27T19:01:20Z TO *] running-config-modified:[2020-08-27 TO 2020-08-28] running-config-modified:[2020-08-27T20 TO 2020-08-27T23] running-config-modified:[2020-08-27T19:00:00 TO 2020-08-27T23:00:00] running-config-modified:[2020-08-27T11:30:00Z TO 2020-08-27T23:00:00Z]
running-deployed-by	User who deployed running configuration	running-deployed-by:system

Field Name	Definition	Example
secondary-version	Secondary image version	secondary-version:GL.10.11
serial	Serial number	serial:SGIA000001
site	Site assigned to the device	site:"Santa Clara"
startup-config	Contents of the start-up configuration	startup-config:"ntp server 192.168.0.7"
startup-config-modified	Date and time of latest start-up configuration change	startup-config-modified:2020-08-27 startup-config-modified:2020-08-27T19 startup-config-modified:2020-08-27T19:01:20Z startup-config-modified:[2020-08-27T19:01:20Z TO *] startup-config-modified:[2020-08-27 TO 2020-08-28] startup-config-modified:[2020-08-27T20 TO 2020-08-27T23] startup-config-modified:[2020-08-27T19:00:00 TO 2020-08-27T23:00:00] startup-config-modified:[2020-08-27T11:30:00Z TO 2020-08-27T23:00:00Z]
startup-deployed-by	User who deployed start-up configuration	startup-deployed-by:system
status	Device status	status:Online status:Offline
system-contact	SNMP system contact	system-contact:JohnSmith
system-location	SNMP system location	system-location:Zurich

Wildcard Characters

Wildcard characters are used in search queries to match one or more other characters. The valid wildcard characters are asterisk (*) and question mark (?).

Use asterisk (*) to match multiple characters in a search query. For example, the search query Serial:SG* will return all the devices starting with SG, such as SG0010223, SG0110224, SG1110225, and so on.

Use question mark (?) to match a single character in a search query. For example, the search query Serial:SG001022? will return all the devices starting with SG001022 series replacing the last digit, such as SG0010221, SG0010222, SG0010223, and so on.



Search queries with wildcard characters must be used without quotes. For example: Serial:SG*.

Reserved Characters

Reserved characters are used for performing operations in search queries. For example, the plus (+) and minus (-) symbols are used as Boolean operators. Parenthesis () is used to group search queries. Reserved characters include + - && | ! () { } [] ^ " ~ * ? : \.

If reserved characters appear in searches, then they must be preceded by an escape character such as a backslash (\). If the search terms are enclosed in quotes, then you need not add a backslash (\) before the reserved characters. For example, system-location:"santaclara(offices)". If the search terms are not enclosed in quotes, then you must add a backslash (\) before the reserved characters. For example, system-location:santaclara\(\offices).

Operators

The following table lists the operators that can be used in search queries.

Table 120: *List of Operators*

Operator	Example	Result
AND	model:8400 AND current-firmware:10.04.000	Returns all 8400 model switches running the 10.04.000 firmware version.
OR	model:8400 OR current-firmware:10.04.000	Returns all 8400 model switches, all the switches running 10.04.000 firmware version, or both.
NOT	model:8400 NOT current-firmware:10.04.000	Returns all 8400 model switches, but not switches running 10.04.000 firmware version.
+ (Includes)	model:8400 + running-config:"access-list ip hvac_segmentation"	Returns all 8400 model switches that contain the ACL named "hvac_segmentation" in their running configuration.
- (Excludes)	model:8400 - running-config:"access-list ip hvac_segmentation"	Returns 8400 model switches that do not have the ACL named "hvac_segmentation" in their running configuration.
() (Grouping)	(model:8400 OR model:6300) AND NOT current-firmware:10.04.0001	Returns all 8400 and 6300 model switches that are not running firmware version 10.04.000.

Sample Queries

The following table lists some sample queries that can be used as search queries.

Table 121: *List of Sample Queries*

Query	Result
"ospf"	Switches that contain the string "ospf" in their running configuration file.
model:8400 current-firmware:10.04.0001	Model 8400 switches running firmware version 10.04.0001.
model:8400 -current-firmware:10.04.0001	All 8400 switches that are not running version 10.04.0001.
(model:8400 OR model:6300) AND NOT current-firmware:10.04.0001	All 8400 and 6300 switches that are not running version 10.04.0001.
model:6300 -running-config:"access-list ip hvac_segmentation"	Model 6300 switches that do not have the ACL named "hvac_segmentation" in their running configuration.
hostname-AUS-05-.*	Devices with a hostname matching the regular expression. For example, in a deployment where host names are encoded as (<site>-<building>-<floor>-<number>).
site:Aruba*	Devices with the Ssite name starting with Aruba.

Viewing Configuration Using MultiEdit on AOS-CX

View configuration of switches and find differences in the configuration across switches in the MultiEdit mode.

To view switch configuration in the MultiEdit mode, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a group in the filter:
 - a. Set the filter to a group.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-CX** or **Config** icon to view the AOS-CX switch configuration dashboard.
 - To select a switch:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click an AOS-CX switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The AOS-CX UI configuration page is displayed.
2. To enable MultiEdit mode, move the **MultiEdit** toggle switch to the on position.
The **Device-Level Configuration** page is displayed with the list of devices displayed in the **Devices** table.



At the device level, the **Devices** table lists only the switch that you have selected. Also, a pop-up is displayed on the bottom-right corner of the page with the options **View Config**, **Edit Config**, and **Express Config**. Go to step [6](#).

3. Search for a switch by entering a search query in the **Contextual Search Engine** field.
For more information about search queries, see [Using Device Search on AOS-CX](#).
4. In the **Devices** table, select one or more switches by clicking the corresponding rows.
A pop-up is displayed on the bottom-right corner of the page with the options **View Config**, **Edit Config**, and **Express Config**.
5. To view the configuration of switches, click **View Config**.
 - If you select a single switch, the View Configuration page is displayed. The running switch configuration is displayed in the **Configuration** window.
 - If you select multiple switches, the View Multi-Device Configuration page is displayed with the following panes:
 - **Devices**—Lists the selected switch names.
Select the switches for which you want to view the configuration by selecting the corresponding check box.
 - **Configuration**—Displays the aggregate running configuration of all selected switches.

The following features are supported in the view page:

- Configuration that is same across all switches is displayed as normal text.
- Differences in configuration is displayed as one of the following:
 - Highlighted parameters (in green)—When parameter value differs across switches. Hover over the parameter to view the list of switches that have this parameter.
 - Entire line differences—Entire line differences are displayed by highlighting the lines along with a description mentioning the switch name that has this line in the configuration. When more than one switch contains this line, a summary of the number of switches is displayed. For example, 2/7 is displayed if two out of seven switches that are selected contain this line in the configuration. To view the list of switches, hover over this summary.

To view the values of these parameters, right click on the parameter. The **View Parameters** pane is displayed. If the parameter is already configured on a switch, the value is displayed. Else, **N/A** is displayed.

Editing Configuration Using MultiEdit on AOS-CX

Edit configuration for one or more switches in the MultiEdit mode. Edit the entire configuration in a familiar looking CLI with syntax checking, colorization, and command completion.

To edit and review switch configuration in the MultiEdit mode, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a group in the filter:
 - a. Set the filter to a group.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-CX** or **Config** icon to view the AOS-CX switch configuration dashboard.
 - To select a switch:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click an AOS-CX switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The AOS-CX UI configuration page is displayed.
2. To enable MultiEdit mode, move the **MultiEdit** toggle switch to the on position.
The **Device-Level Configuration** page is displayed with the list of devices displayed in the **Devices** table.



At the device level, the **Devices** table lists only the switch that you have selected. Also, a pop-up is displayed on the bottom-right corner of the page with the options **View Config**, **Edit Config**, and **Express Config**. Go to step [6](#).

3. Search for a switch by entering a search query in the **Contextual Search Engine** field.
For more information about search queries, see [Using Device Search on AOS-CX](#).

4. In the **Devices** table, select one or multiple switches by clicking the corresponding rows.
A pop-up is displayed on the bottom-right corner of the page with the options **View Config**, **Edit Config**, and **Express Config**.

5. To edit the configuration of switches, click **Edit Config**.
 - If you select a single switch, the Edit Configuration page is displayed.
 - If you select multiple switches, the Edit Multi-Device Configuration page is displayed with the following panes:
 - **Devices**—Lists the selected switch names.
Select the switches for which you want to edit the configuration by clicking the row corresponding to the switches.
 - **Configuration**—Displays the aggregate running configuration of all switches.

In both the pages, the following views are available:

- **Editor View**—Displays the aggregate running configuration on the switches in the **Configuration** pane. Edit the configuration in this view.

When editing multiple switches, the **Devices** pane is also displayed. Select the check box for the switches you want to edit. The following features are supported in the **Editor View**:

- Configuration that is same across all switches is displayed as normal text.
- Differences in configuration is displayed as one of the following:
 - Highlighted parameters (in green)—When parameter value differs across switches. Hover over the parameter to view the list of switches that have this parameter.
 - Entire line differences—Entire line differences are displayed by highlighting the lines along with a description mentioning the switch name that has this line in the configuration. When more than one switch contains this line, a summary of the number of switches is displayed. For example, 2/7 is displayed if two out of seven switches that are selected contain this line in the configuration. To view the list of switches, hover over this summary.

To modify the values of these parameters, right-click the parameter. The **Modify Parameters** pane is displayed.

- a. If the parameter is already configured on a switch, you can modify the value. Otherwise, **N/A** is displayed for the value and it cannot be modified.
- b. If you want to apply the same value to all selected switches, select the **Set same value for all devices** check box.
- c. To save the changes, click **Save Changes** in the **Modify Parameters** pane.



Clicking **Save** at the bottom of the **Editor View** discards the changes made in the **Modify Parameters** pane.

- Command completion and help text are available by pressing the CTRL+SPACE key combination.
An inline drop-down is displayed with the available commands or parameters within commands. To insert a command or parameter, select an option and press TAB.
- Syntax errors are marked (in red) directly under the incorrect text.
- If a command line is not inserted in the correct position, the line is automatically moved to the correct position in the configuration.

For example, if the configuration contains information for VLAN IDs 1 to 3, and you are adding VLAN 4 after VLAN 1 in the configuration, the editor moves the VLAN 4 command line after VLAN 3.

- **Diff View**—Displays the difference between changes made in the **Editor View** and the running configuration on a switch. In this view, two panes, **Running** and **Candidate**, are displayed. When viewing details of multiple switches, select a switch from the drop-down.
 - The **Running** pane displays the running configuration on the switch.
 - The **Candidate** pane highlights the changes made in the **Editor View** in addition to displaying the running configuration on the switch. You cannot edit the switch configuration in this view.

6. Edit the configuration in the **Editor View**, and click **Save**.

Configuration Drift Warning in Edit Config

When you edit the configuration of the same AOS-CX switch, in the MultiEdit mode, in two different browser tab sessions, and try to save the configuration one after the other, the following events occur:

1. The configuration that you save first in the editor in any of the two browser tabs is saved on the switch.
2. When you try to save the configuration in the editor in the other browser tab, Aruba Central (on-premises) displays a warning that the configuration has been changed outside the current editor.
3. If you ignore the warning and continue to save the configuration, Aruba Central (on-premises) overwrites the changes saved earlier with the current changes.

If you save any changes in the MultiEdit mode and the changes do not reflect on the switch, check the Audit Trail details for any errors in the configuration sync.

Commands Not Supported in the MultiEdit Mode

The following table lists the AOS-CX switch commands that are not supported and details about how they function in the MultiEdit mode in Aruba Central (on-premises). It is recommended to use these commands in the MultiEdit **Edit Config** page with caution.

Table 122: AOS-CX Commands Not Supported in The MultiEdit Mode

Command	Caution When Editing or Deleting Command
<code>configuration-lockout</code>	Users must not delete this command. If this line is deleted in Aruba Central (on-premises), then: <ul style="list-style-type: none"> ■ Aruba Central (on-premises) Managed mode is disabled and changes can be made outside of Aruba Central (on-premises). ■ Changes made using NAE, REST APIs, or the switch CLI will be absorbed into Aruba Central (on-premises), hence causing a local override. The switch template will be deleted and replaced by the switch configuration.
<code>vsx</code> in switches running AOS-CX 10.06 or earlier versions	Users can add, edit, delete this command . However, VSX peer switch must be managed as a separate device in Aruba Central (on-premises).
<code>vsx-sync</code> in sub-contexts	Users must not add, edit, or delete this command in Aruba Central (on-premises). <ul style="list-style-type: none"> ■ Aruba Central (on-premises) Managed mode is disabled and chanAruba Central (on-premises)ges can be made outside of Aruba Central (on-premises).

Command	Caution When Editing or Deleting Command
	<ul style="list-style-type: none"> Configuration on the peer switch is modified.
<code>vsf member <n></code> if all switches are running AOS-CX 10.07 or later versions	<p>Users must not delete this command.</p> <ul style="list-style-type: none"> In case this command is deleted from the member, the member restarts and resets the configuration. In case this command is deleted from the conductor, then Aruba Central (on-premises) loses connectivity with the stack.
<code>type <jnumber></code>	<p>Users must not delete or edit this command.</p> <ul style="list-style-type: none"> In case this command is deleted or edited on the member, the member restarts and resets the configuration. In case this command is deleted or edited on the conductor, then Aruba Central (on-premises) loses connectivity with the stack.
Show commands (for example, <code>show running-config</code> , <code>show interface brief</code>)	<p>N/A These commands do not appear in the running configuration of a switch and hence will not be visible in the MultiEdit mode (View Config or Edit Config).</p>
Action commands (for example, <code>ping</code> , <code>boot system</code> , <code>erase</code>)	<p>N/A These commands do not appear in the running configuration of a switch and hence will not be visible in the MultiEdit mode (View Config or Edit Config).</p>
Commands used to reset entities to defaults (for example, <code>no bfd</code> , <code>no vrf</code> , <code>no router ospf</code> , <code>default interface <IFRANGE></code>)	<p>N/A These commands do not appear in the running configuration of a switch and hence will not be visible in the MultiEdit mode (View Config or Edit Config).</p>
Configuration context switching commands (for example, <code>interface 1/1/1-1/1/5</code>)	<p>N/A These commands do not appear in the running configuration of a switch and hence will not be visible in the MultiEdit mode (View Config or Edit Config).</p>

Express Configuration Using MultiEdit on AOS-CX

Express configuration provides a way to efficiently apply a predefined set of configuration settings to switches. Each set of configuration settings can contain settings for Network Analytics Engine (NAE) or device profile features.

To apply express configuration, complete the following steps:

- In the **Network Operations** app, select one of the following options:
 - To select a group in the filter:
 - Set the filter to a group.
The dashboard context for the group is displayed.
 - Under **Manage**, click **Devices > Switches**.
 - Click the **AOS-CX** or **Config** icon to view the AOS-CX switch configuration dashboard.

- To select a switch:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click an AOS-CX switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The AOS-CX UI configuration page is displayed.
- 2. To enable MultiEdit mode, move the **MultiEdit** toggle switch to the on position.
The **Device-Level Configuration** page is displayed with the list of devices displayed in the **Devices** table.



At the device level, the **Devices** table lists only the switch that you have selected. Also, a pop-up is displayed on the bottom-right corner of the page with the options **View Config**, **Edit Config**, and **Express Config**. Go to step 6.

3. Search for a switch by entering a search query in the **Contextual Search Engine** field.
For more information about search queries, see [Using Device Search on AOS-CX](#).
4. In the **Devices** table, select one or more switches by clicking the corresponding rows.
A pop-up is displayed on the bottom-right corner of the page with options **View Config**, **Edit Config**, or **Express Config**.
5. Click **Express Config**.
The Express Config (N) window is displayed. Where N represents the number of switches selected.
6. Select the required feature from the drop-down. The following features are supported:
 - Device Profile
 - Network Analytics Engine
7. Configure the following parameters corresponding to the selected feature:

Table 123: *Device Profile Parameters*

Name	Description	Value
Enable	Enables or disables the device profile configuration on the switches.	Select or clear the check box.
Profile Name	Name of the device profile.	This field is pre-configured and cannot be edited.
VLAN Mode	VLAN mode for the device profile. Depending on the VLAN mode, configure one of the following: <ul style="list-style-type: none"> ■ Access: <ul style="list-style-type: none"> ○ Access vlan—ID of the access VLAN. ■ Trunk: <ul style="list-style-type: none"> ○ Native vlan—ID of the native VLAN. ○ Allowed vlan list—Single or a range of allowed VLAN IDs. 	Integer in the range 1 to 4094.

Name	Description	Value
PoE Priority	PoE priority for the device.	Low, High, Critical
Allow Jumbo frames	Enables or disables processing of jumbo frames by the switches.	Select or clear the check box.

Table 124: *Network Analytics Engine Parameters*

Name	Description
NAE Script Name	<p>Name of the NAE script. You can also configure the agent parameters. The following NAE scripts are supported:</p> <ul style="list-style-type: none"> ■ software_device_health_monitor.1.6—Monitors overall software device health. ■ hardware_device_health_monitor.1.6—Monitors overall hardware device health. ■ application_health_monitor.1.1—Monitors application health using TCP SYN and ACK packets, and VoIP IP SLA sessions. ■ network_health_monitor.1.3—Monitors overall network health of device. ■ stp_health_monitor.3.1—Monitors health of ports that are involved in spanning tree protocol.

8. Click **Save**.

You can view the express configuration that you apply in the **Configuration Status** page if the **Auto-Commit** state is off, or in the **View Config** page if the **Auto-Commit** state is on. For more information on viewing the pending changes, local overrides, and the configuration status, see [Using Configuration Status on AOS-CX](#).

Using Configuration Status on AOS-CX

Aruba Central (on-premises) provides an audit dashboard for reviewing configuration changes for the AOS-CX switches provisioned in UI groups. The Configuration Status page displays the configuration status of the switches, pending changes, and local overrides present in the AOS-CX switches. It also provides options to push uncommitted changes to the switches.

To view and commit the configuration changes, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a group in the filter:
 - a. Set the filter to a group.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-CX** or **Config** icon to view the AOS-CX switch configuration dashboard.
 - To select a switch:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click an AOS-CX switch under **Device Name**.
The dashboard context for the switch is displayed.

- d. Under **Manage**, click **Device**.

The AOS-CX UI configuration page is displayed.

2. Click **Configuration Status**.

The Configuration Status page is displayed with details about the configuration status of AOS-CX switches.

The page displays the following information at the group and device levels:

- At the group level:
 - **Auto-commit Changes State** section—Click a number to view corresponding results filtered in the **Auto Commit State** column in the **Switches** table.
 - **Devices auto-commit state**—Count of switches that have the auto-commit state on and off.
 - **Configuration Issues** section—Click a number to view corresponding results filtered in the **Config Status** column in the **Switches** table.
 - **Pending changes**—Count of switches that have configuration changes that are pending commitment to the switch.
 - **Configuration errors**—Count of switches for which errors in the pending configuration caused an attempted commit to fail.In the **Config Status** column, click the link corresponding to the status to view the pending changes in a configuration or the **Error - Configuration conflicts** link to view any issues in a pending configuration. For more information, see [Viewing and Committing Configuration Issues and Pending Changes at the Group Level](#).
 - **Local Overrides** section—Click a number to view corresponding results filtered in the **Local Overrides** column in the **Switches** table.
 - **Switches with overrides**—Count of switches that have device level configuration changes.
 - **Switches without overrides**—Count of switches that do not have device level configuration changes.
- At the device level:
 - **Auto-commit Changes State** section—Enable or disable the auto-commit mode by moving the toggle switch to the on or off position.
 - Toggle switch in the on position—Displays a message that the configuration changes will be committed to the device immediately.
 - Toggle switch in the off position—Displays a message that the configuration changes will not be committed to the device immediately.
 - **Configuration State Issues** section—Displays a message defining the status of configuration on the switch. For a list of all status messages, see the description of the **Config Status** column in [Table 125](#).
Click the **Pending Changes** link to view the pending changes in a configuration or the **Error - Configuration conflicts** link to view any issues in a pending configuration. For more information, see [Viewing and Committing Configuration Issues and Pending Changes at the Group Level](#).
 - **Overrides** section—Displays a message to indicate whether there are any overrides in the switch configuration at the device level or not.

3. Click the number in the sections to apply the corresponding filter in the **Switches** table.

The **Switches** table displays the following information:



The **Switches** table appears only at the group level.

Table 125: *Details in the Switches Tables*

Column	Description	Value
Name	Name of the switch.	
Auto Commit State	Status of the auto commit option for the switch.	On, Off
Config Status	Status of switch configuration between the device and Aruba Central (on-premises). The following statuses are available: <ul style="list-style-type: none">■ Error - Configuration conflicts■ Error - Internal error■ Error - Login pending■ Error - Modified outside Central■ Offline■ Pending changes■ Pending changes - Offline■ Pending group configuration■ Synchronized■ Synchronizing	
Local Overrides	Indicates whether any overrides exist in the switches.	Yes, No

Viewing and Committing Configuration Issues and Pending Changes at the Group Level

To view and commit configuration issues and pending changes in AOS-CX switches at the group level, complete the following steps:

1. To view the pending changes in a configuration click the link corresponding to the following statuses in the **Config Status** column for the switch:
 - **Error - Internal error**
 - **Error - Modified outside Central**
 - **Pending changes**
 - **Pending changes - Offline**
 - **Synchronizing**

The Pending Configuration Changes window is displayed for that switch. This window displays the running and pending configurations of the switch and lets you review the changes made in configuration.

2. Click one of the following buttons depending on the status:
 - Click **Commit Now**—Displayed only when the user has modify permissions for the group, and when auto-commit state is off and there are pending changes but no errors.
Click this button to push the pending changes to the switch.
 - Click **Close**—Click this button to close the Pending Configuration Changes window without modifying the switch configuration.

3. To view issues with a pending configuration, click the **Error - Configuration conflicts** link in the **Config Status** column for the switch.

The Configuration Conflicts window is displayed for that switch. This window displays a description for each error and the line number in the configuration file where the error has occurred.



The line number displayed in the Configuration Conflicts window might not be same as in the configuration editor. You must look for the correct line in the editor by searching the command where the error occurs.

4. Click **Close**.

Viewing and Committing Configuration Issues and Pending Changes at the Device Level

To view and commit configuration issues and pending changes in AOS-CX switches at the device level, complete the following steps:

1. To view the pending changes in a configuration click the **Pending Changes** link in the **Configuration State Issues** section.

The Pending Configuration Changes window is displayed for that switch. This window displays the running and pending configurations of the switch and lets you review the changes made in configuration.

If the pending changes do not have any errors, the **Commit Now** button is displayed, both in the **Configuration State Issues** section and in the Pending Configuration Changes window.

2. Click **Commit Now** to push the pending changes to the switch.
3. To view issues with a pending configuration, click the **Error - Configuration conflicts** link in the **Configuration State Issues** section.

The Configuration Conflicts window is displayed for that switch. This window displays a description for each error and the line number in the configuration file where the error has occurred.



The line number displayed in the Configuration Conflicts window might not be same as in the configuration editor. You must look for the correct line in the editor by searching the command where the error occurs.

4. Click **Close**.

Managing an AOS-CX VSF Stack

A switch stack is a set of switches that are interconnected through stacking ports. By default, the first member in a stack becomes conductor. You must configure the standby conductor manually and there is no default standby conductor. All the switches in the stack other than the conductor and standby conductor become members.

The following table lists the AOS-CX switches that support stacking.

Table 126: AOS-CX Switch Stacking Support

Switch Platform	Maximum Number of Stack Members	Minimum Supported Version	Recommended Version	Supported Stack Type	Supported Configuration Group Type for Stacking (UI / Template)
AOS-CX 6200 Switch Series	8	10.05.0060	10.07.0030	VSF	UI and Template
AOS-CX 6300 Switch Series	10	10.05.0060	10.07.0030	VSF	UI and Template
AOS-CX 6300 Switch Series [JL762A] Back 2 Front Power Supply SKU only	10	10.06.0001	10.07.0030	VSF	UI and Template

For more information on topology and configuration of switch stacks, see the *AOS-CX Virtual Switching Framework (VSF) Guide* for the respective switch series.

Supported Switch Stacking Functions

The following table lists the functions supported in Aruba Central (on-premises), using UI and template configurations, based on the switch firmware versions.

Table 127: Supported Stacking Functions

Firmware Versions	Functions Supported in Aruba Central
10.06 and earlier	<ul style="list-style-type: none"> ■ Onboarding pre-configured AOS-CX stack ■ Pushing switch configuration from Aruba Central using UI options, MultiEdit, or templates ■ Rebooting a conductor <p>NOTE: This will reboot the entire stack.</p>
10.07 and later	<ul style="list-style-type: none"> ■ Onboarding pre-configured AOS-CX stack ■ Pushing switch configuration from Aruba Central using UI options, MultiEdit, or templates ■ Creating a stack ■ Adding a stack member ■ Removing a stack member ■ Modifying VSF links ■ Changing the secondary member ■ Rebooting a conductor <p>NOTE: This will reboot the entire stack.</p>

The other stacking related configurations such as replacing a conductor, replacing a standby conductor, and replacing a stack member must be performed offline, that is, outside Aruba Central. The changes are reflected in Aruba Central.

For information on these configurations, see the *AOS-CX Virtual Switching Framework (VSF) Guide* for the respective switch series and the [ArubaOS-CX VSF Best Practices](#) document.

General Recommendations

The following are the general recommendations to note when configuring an AOS-CX switch stack:

- To maximize available VSF link bandwidth, use the following Direct Attach Copper (DAC) cables for VSF links:
 - AOS-CX 6300 Switch Series: 50G
 - AOS-CX 6200 Switch Series: 10G
- All VSF link ports in a stack must operate at the same speed (10G, 25G, or 50G).
- For maximum stack resiliency, the conductor and secondary conductor should be the same switch models with redundant power supplies connected to different circuits. This is required to minimize the probability that a single-source power failure will disable both the stack conductor and standby.
- A secondary member must always be defined to assume the VSF standby role.
- The out-of-band management (OOBM) ports on the conductor and secondary conductor must be connected to each other, either directly or through a dedicated management network. This is required to utilize the VSF split detection, which must always be enabled.

Monitoring AOS-CX Switch Stacks

See [Monitoring Switches and Switch Stacks](#).

Viewing AOS-CX Switch Stacks in Site Topology

See [Monitoring Sites in the Topology Tab](#).

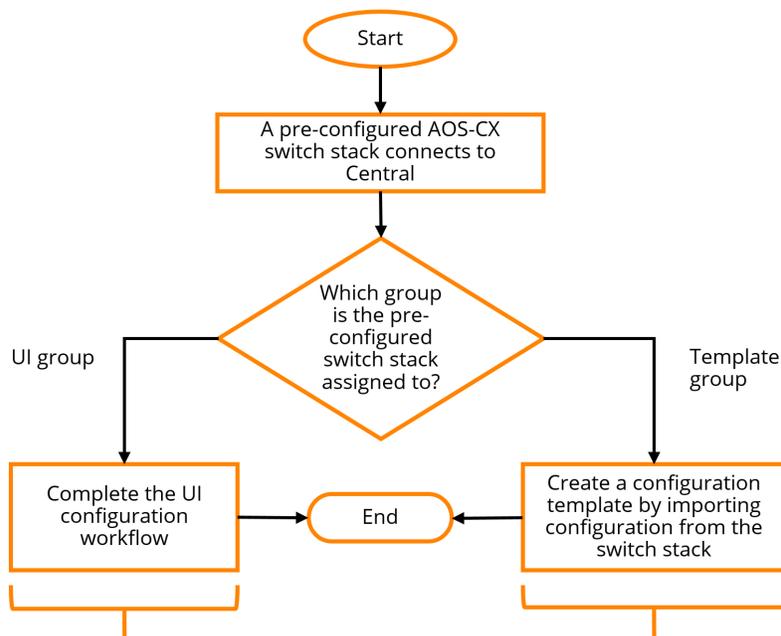
This section contains the following topics:

- [Onboarding AOS-CX VSF Stack to Aruba Central \(on-premises\)](#)
- [Configuring AOS-CX VSF Stacks Using UI Groups](#)
- [Configuring AOS-CX VSF Stacks Using Template Groups](#)
- [Replacing an AOS-CX VSF Stack Member](#)
- [Removing an AOS-CX VSF Stack Member Using UI](#)
- [Changing an AOS-CX VSF Stack to Standalone Switches on page 487](#)
- [Monitoring AOS-CX Switch Stacks](#)

Onboarding AOS-CX VSF Stack to Aruba Central (on-premises)

The following figure illustrates the provisioning steps for each group type for a VSF stack.

Figure 37 Stack Provisioning Steps Per Group Type



CAUTION: Moving a stack to a UI group will overwrite only those configuration that can be managed by Central at the group level—**SNMP, Logging, Administrator, Access Control, and VLANs**

CAUTION: - Configuration is retained only for the stack from which template is created.
- To apply the same template to multiple stacks without overwriting the stack configurations, customize the template by adding variables.

When moving a pre-configured stack to a UI group, Aruba Central configuration at the group level will overwrite configuration on the switch. Before moving a pre-configured stack to a UI group in Aruba Central, if you want to preserve any group-level configuration that is present on the stack, you must configure them at the group level in Aruba Central. However, since multiple stacks can be managed using the same UI group, if you do not want any particular configuration on some stacks, you must delete them at the device level in Aruba Central.

For example, if you want to preserve the VLANs 20, 30 on stack1 and VLANs 40, 50 on stack2, then you must configure VLANs 20, 30, 40, and 50 at the group level in Aruba Central. After moving the stacks to the UI group, you must delete VLANs 40, 50 on stack1 and VLANs 20, 30 on stack2.

- Configurations supported at the group level for a stack—**SNMP, Logging, Administrator, Access Control, VLANs**, and other features available at the group level
- Configurations supported only at the device level for a stack—**Ports & Link Aggregations, Authentication Servers, Authentication, Access Control, VLANs, Loop Prevention, and Static Routing**

To onboard an AOS-CX VSF stack to Aruba Central (on-premises), complete the following steps:

1. Setup the switch stack using the Aruba CX mobile application or the CLI.
This step must be performed outside Aruba Central (on-premises).
For information, see [ArubaOS-CX VSF Best Practices](#). Although this document is created for Aruba CX 6300 switches, it is also applicable to Aruba 6200 switches.



If you want to create a new stack with devices that are already present in Aruba Central (on-premises), you must first disconnect and delete all these devices from Aruba Central (on-premises) and then convert them as conductor, standby, and members. For information about deleting offline switches from Aruba Central (on-premises), see [Deleting an Offline Switch](#).

2. Add and subscribe the conductor, standby conductor, and all members in the AOS-CX stack to Aruba Central (on-premises). The other members are optional to be added to Aruba Central (on-premises). For information on adding and subscribing devices, see [Onboarding Devices](#).
3. Create a template group or UI group for the AOS-CX VSF stack in Aruba Central (on-premises).



In the template group, all user-defined template variables for the conductor and standby devices should contain the same values, to ensure template consistency after a stack failover event. For information on variables for template-based configuration, see [Managing Variable Files](#).

4. Assign the stack members to the template group from any of the following pages:
 - **Device Inventory** page under **Global Settings** in **Account Home**.
 - **Groups** page under **Maintain > Organization** in the **Network Operations** app.For more information on assigning a stack, see [Assigning Devices to Groups](#).



You can move a stack across different UI groups or template groups.

5. To push switch configurations to the conductor and members in the AOS-CX VSF stack from Aruba Central (on-premises), use one of the following ways:
 - **Template group**—Create a configuration template in the template group for the AOS-CX VSF stack in one of the following ways:
 - Copy the details of the `show running config` command of the AOS-CX VSF stack from the conductor and paste it in the template. Ensure to update the password in plaintext.
 - Use the **Import Configuration As Template** option. The switches must be running AOS-CX 10.06 or a later version.
 - **UI group**—Use UI options and MultiEdit mode in the AOS-CX switch configuration dashboard. Before moving the stack to a UI group in Aruba Central (on-premises), save the output of the `show running config` command from the conductor. This is required to restore or apply any configuration that might be lost because of group-level overwrite of configuration. You can apply this configuration after moving the stack to the UI group using the **Edit Config** option in the MultiEdit mode.

The UI options and MultiEdit mode are available only when the AOS-CX VSF stacks are added to a UI group. For more information, see [Configuring AOS-CX Switches in UI Groups](#).



-
- In Aruba Central (on-premises), select the serial number of the conductor switch to push switch configuration to the conductor, standby conductor, and all members in the stack.
 - Port-specific configurations such as **Ports & Link Aggregations, Authentication Servers, Authentication, Access Control, VLANs, Loop Prevention, and Static Routing** can be configured on stack members only at the device level.
 - It is not recommended to perform any stacking-related configurations, such as setting up a stack, using the MultiEdit mode.
-

6. To make stack-topology changes, use one of the following ways:
 - Template group—Update the configuration template in the template group for the AOS-CX VSF stack.
 - UI group—Use the **VSF Stacking** page in the AOS-CX configuration dashboard.
The UI options are available only at the group-level.

This step is applicable only for the switches running AOS-CX 10.07 or later firmware versions.

Configuring AOS-CX VSF Stacks Using UI Groups

You can create VSF stacks, add stack members, modify VSF links, change standby conductor and remove stack members through the UI.



Stacks can be configured only at the group-level.

To create and manage stacks through the UI, ensure that the following prerequisites are met:

- All switches in the VSF stack are added to the device inventory and assigned with a license.
- All switches in the VSF stack are set to the factory default configuration.
- All switches in the VSF stack are running 10.07 or later firmware versions.
- All switches in the VSF stack are of the same switch series. Stacks cannot be created with a mixed set of switches. The stacks must be made up of either only 6200 or only 6300 switches.
- Members in the VSF stack other than the conductor should not have an uplink connectivity. Otherwise, auto-stacking will not work.
- Before creating a stack, only the conductor must be moved to the UI group. All other stack members will be automatically moved to the UI group once the stack is created.
- For auto-stacking to work, the switches should be connected in the direction of the higher denomination port to the lower denomination port.

The following ports are reserved for auto-stacking:

- 24-port switch models— Ports 25 and 26
- 48-port switch models— Ports 49 and 50

For more information on auto-stacking configuration, refer to the *AOS-CX Virtual Switching Framework (VSF) Guide*.

For more information, see the following topics:

- [Creating an AOS-CX VSF Stack Using UI](#)
- [Adding a Stack Member Using UI](#)
- [Modifying VSF Links Using UI](#)

- [Changing the Standby Conductor Using UI](#)
- [Removing an AOS-CX VSF Stack Member Using UI](#)

Creating an AOS-CX VSF Stack Using UI

In Aruba Central (on-premises), you can create a VSF stack by selecting and configuring the conductor switch through the UI.

Before creating a stack, you must physically connect the members of the stack in the chain or ring topology on the ports reserved for auto-stacking. For auto-stacking to work, the members should be connected in the direction of the higher denomination port to the lower denomination port.

The following ports are reserved for auto-stacking:

- 24-port switch models— Ports 25 and 26
- 48-port switch models— Ports 49 and 50

Auto-stacking peer discovery is a uni-directional process. It starts with the VSF link containing the higher denomination VSF port. Member discovery starts on the higher-numbered port for each member in line. For a three-member stack in the ring topology, use the following connection example for auto-stacking to work:

- Connect port 50 of member 1 to port 49 of member 2
- Connect port 50 of member 2 to port 25 of member 3
- Connect port 26 of member 3 to port 49 of member 1

For more information on auto-stacking configuration, refer to the *AOS-CX Virtual Switching Framework (VSF) Guide*.



The stack can be created only at the group-level.

To create an AOS-CX VSF stack, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one switch.
2. Under **Manage**, click **Devices > Switches**.
3. Click the **AOS-CX** or **Config** icon to view the switch configuration dashboard.
4. Click **System > Stacking**.

The VSF Stacking page is displayed with a list of stacks.

5. In the **VSF Stacking** table, click **+** to create a stack.
The Create VSF Stack page is displayed.

6. Configure the following parameters:

Table 128: *Create VSF Stack*

Parameters	Description	Value
Switch Series	The switch platform for the VSF Stack.	6200 or 6300
Conductor	The Conductor switch in a Stack,	Select the switch from the drop-down.

Parameters	Description	Value
Link 1 port (s)	One or more port numbers for the first VSF link separated by commas.	Following are the default port values: <ul style="list-style-type: none"> ■ 24-port switch models—25 ■ 48-port switch models—49
Link 2 port (s)	One or more port numbers for the second VSF link separated by commas.	Following are the default port values: <ul style="list-style-type: none"> ■ 24-port switch models—26 ■ 48-port switch models—50
Split Mode detect	Indicates whether VSF split detection mode is enabled. If this is enabled, during a split, the fragment that has the conductor becomes the active fragment and keeps its front plane (non-VSF) interfaces up and running. The other fragment becomes inactive and all non-VSF interfaces on the inactive fragment are brought down to avoid network disruption. NOTE: It is recommended to enable this field during the stack creation. Also, ensure that the conductor and standby conductor are connected to the management interface.	Select the check box to enable or disable.

7. Click **Save**.

The new stack is displayed in the Stacking table with the conductor switch. The stack creation may take up to 10 minutes. You can use the **Configuration Audit** page to verify the status of a stack formation.

To monitor switch stacks and troubleshoot any stack-related errors, select the conductor switch of stack from the **Devices** list and navigate to the **LAN > Ports** tab. For more information, see [Monitoring AOS-CX Switch Stacks](#).

Editing the Conductor

To edit the conductor, point to the row for the conductor, and click the  edit icon. You can only edit the following parameters:

- **Split Mode detect**

This parameter is available only for the conductor.

- **Link 1 Port(s)** and **Link 2 Port(s)**

For more information on changing the VSF links, see [Modifying VSF Links Using UI](#).

Removing a Stack

To remove a stack, point to the stack you want to remove and click the  delete icon. In the **VSF Stacking** page, you can delete a stack only in the following scenarios:

- If there is only one member in a stack.
- If all other stack members except conductor are down.



Stacks cannot be deleted when the status of members are online.

To remove a stack with more than one member, it is recommended to remove individual members, one at a time, starting from the last member in the stack. For more information, see [Removing an AOS-CX VSF Stack Member Using UI](#).



-
- Deleting the stack from the **VSF Stacking** page will remove the VSF stacking configuration from the conductor. Once the stack is deleted, the conductor will reboot and move to the unprovisioned group as a standalone device.
 - Conductor member cannot be deleted as an individual member.
-

Adding a Stack Member Using UI

In Aruba Central (on-premises), you can add and configure the members through the UI. Before adding a stack member, it is recommended to navigate to the **Switch > LAN > Ports** tab in the switch dashboard, to see whether there are any errors in the stack. For more information, see [Monitoring AOS-CX Switch Stacks](#).



If you are onboarding a pre-configured stack or if the stack is formed through auto-stacking, then you do not need to add the stack through the UI. Aruba Central (on-premises) will automatically sync the configuration done on the switch and display the members in the **VSF Stacking** table.

To add a switch to stack as a new member, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one switch.
2. Under **Manage**, click **Devices > Switches**.
3. Click the **AOS-CX** or **Config** icon to view the switch configuration dashboard.
4. Click **System > Stacking**.
The VSF Stacking page is displayed with a list of stacks.
5. Expand the stack for which you want to add a member.
The table is displayed with the list of members for that particular stack.
6. To add a stack member, point to the row for the stack and click **+** in the **VSF Stacking** table.
The Add Stack Member page is displayed.
7. Configure the following parameters:

Table 129: *Add member*

Parameters	Description	Value
Member ID	The identification number of the member in the stack. This field is auto-generated and the value is incremented by 1.	Integer

Parameters	Description	Value
Standby conductor	The standby conductor of the stack.	By default, secondary member will be selected as the Standby conductor.
Switch Series	The switch platform of the member. This field is auto-generated and switch mode is displayed based on the selection of conductor. The stacking cannot be done with a mixed set of switches. The stack must be made up of only 6200 or only 6300 switches.	6200 or 6300
Device	The device model of the switch.	Select from the drop-down.
Link 1 Port(s)	One or more port numbers for the first VSF link separated by commas.	Following are the default port values: <ul style="list-style-type: none"> ■ 24-port switch models— 25 ■ 48-port switch models— 49
Link 2 Port(s)	One or more port numbers for the second VSF link separated by commas.	Following are the default port values: <ul style="list-style-type: none"> ■ 24-port switch models— 26 ■ 48-port switch models— 50

8. Click **Save**.

The newly added member is displayed in the VSF Stacking table. It may take up to 10 minutes for the new member to join the stack. Expand the stack to see the member and its status. You can use the **Configuration Audit** page to verify the status of stack formation and the **Ports** tab in the switch dashboard to monitor and troubleshoot switch stacks. For more information, see [Monitoring AOS-CX Switch Stacks](#).

Editing a Stack Member

To edit a stack member, point to row for the member you want to edit and click the edit icon.

You can only edit the following parameters:

- **Standby conductor**
- **Link 1 Port(s)** and **Link 2 Port(s)**

For more information, see [Changing the Standby Conductor Using UI](#) and [Modifying VSF Links Using UI](#).

Modifying VSF Links Using UI

You can modify VSF ports in the VSF links through the UI only when the admin status in the **Ports & Link Aggregations** page and operational status in the switch details page for the VSF link ports are down.

To change the VSF links in the VSF stack, complete the following steps:

1. Set the filter to **Global** or the group containing the stack.
2. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
3. Select the conductor switch of the stack for which you want to modify the links and navigate to the **Ports & Link Aggregations** page.
4. Select the VSF ports that you want to modify and click the  edit icon.
5. In the **Edit Ports** page, clear the **Admin Up** check box to shut down the port.
6. Remove the physical VSF links from the port that need to be modified.
7. Reconnect the physical links to the port as required.
8. At the group level, navigate to the **VSF Stacking** page and expand the stack and point to the member for which you want to modify the links, and click the  edit icon.
9. In the **Edit Stack Member** window, modify the VSF links as required. You cannot edit the VSF links when the ports are up. Both **Link 1 port(s)** and **Link 2 port(s)** should not be modified at the same time. Otherwise, the stack might break.



Before modifying VSF links, power down all non-standby members that are connected to the member you are going to modify. This prevents the members from getting into the recovery mode, after multiple reboots, when they get disconnected.

Changing the Standby Conductor Using UI

You can change the standby conductor in the stack through the UI.

To change the standby conductor in the VSF stack, complete the following steps:

1. In the **VSF Stacking** page, expand the stack for which you want to change the secondary conductor.
2. Point to the row for the member for which you want to select as Standby conductor and click the edit icon.
3. In the **Edit Stack Member** page, select the standby conductor check box.
A confirmation window is displayed.
4. Click **OK**.
Both the existing standby conductor and the new standby conductor will go for a reboot. After rebooting, the selected member will join the stack as the new standby conductor.
5. Click **Save**.

Removing an AOS-CX VSF Stack Member Using UI

You can remove a member from the AOS-CX VSF stack in Aruba Central (on-premises) only when the member is offline. It involves completing procedures both inside and outside Aruba Central (on-premises). The procedure will vary based on the switches firmware versions.

Switches running AOS-CX 10.07 or later versions

If your switches running AOS-CX 10.07 or later versions, complete the following procedure:

1. Shut down the member in the stack.
2. Disconnect the physical VSF links for the member. Otherwise, the switch will reboot and join the stack again through auto-stacking.

3. Reconnect the physical links as desired.
4. In Aruba Central (on-premises), navigate to the **VSF Stacking** page and complete the following steps:
 - a. Expand the stack for which you want to delete the member.
 - b. Point to the row for the member you want to delete and click the delete icon.
A confirmation window is displayed.
 - c. Click **Delete**.
The member will be removed from the VSF Stacking table.



-
- The removed member must be reset to the factory-default configuration before connecting back to Aruba Central (on-premises) again.
 - Conductor member cannot be deleted as an individual member.
-

Switches running AOS-CX 10.6 or earlier versions

If your switches running AOS-CX 10.06 or earlier versions, complete the following procedure:

1. Disable Aruba Central (on-premises) from the switch CLI.
You must execute these commands only on the conductor of the stack.

```
switch# configure
switch(config)# aruba-central
switch(config-aruba-central)# disable
```

2. Wait for the stack to display as offline in the List view.
It may take up to five minutes for the stack to appear offline in Aruba Central (on-premises).
3. Delete the stack from the template group or UI group in Aruba Central (on-premises).
See [Deleting an Offline Switch](#).
4. Remove the member from the VSF stack in the switch CLI by running the following commands:
For example, in a three-member stack, run the following commands to remove member 3.

```
switch# configure
switch(config)# no vsf member 3
The specified switch will be unconfigured and rebooted
Do you want to continue (y/n)? y
```

-
- When a member (other than the conductor) is removed from the stack, then the member reboots as a standalone switch and the configuration resets to factory default. The stack will remain with the conductor and other remaining members.
 - However, when the conductor itself is removed from the stack, then the conductor reboots as a standalone switch and its configuration resets to factory default, and the standby takes the role of the conductor in the stack.
-



5. Disconnect the physical VSF links for the member.

6. In the case of template group, update the template in template group Aruba Central (on-premises) with the configuration from the remaining stack.
7. Enable Aruba Central (on-premises) from the switch CLI.

If this does not work, run the `https-server session close all` command.

```
switch(config-aruba-central)# enable
```

OR

```
switch# https-server session close all
```

8. In the case of UI group, after enabling Aruba Central, complete the following steps:



Before moving the stack to a UI group in Aruba Central, save the output of the `show running config` command from the conductor. This is required to restore or apply any configuration that might be lost because of group-level overwrite of configuration. You can apply this configuration after moving the stack to the UI group using the **Edit Config** option in the MultiEdit mode.

- a. Move the stack to the UI group.
 - b. Paste the running configuration of the conductor, which you copied before moving the stack to the UI group, in the MultiEdit mode using the **Edit Config** option.
 - c. Save the running configuration.
9. Add and subscribe the remaining members in the AOS-CX stack to Aruba Central (on-premises).

Configuring AOS-CX VSF Stacks Using Template Groups

You can create VSF stacks, add stack members, remove stack members, modify VSF links, and change standby conductor through the template.

To create and manage stacks through the UI, ensure that the following prerequisites are met:

- All the switches in the VSF stack are added to the device inventory and assigned with a valid subscription.
- All the switches in the VSF stack are set to the factory default configuration.
- All the switches in the VSF stack are running 10.07 or later firmware versions.
- All the switches in the VSF stack are of the same switch series.
- Members in the VSF stack other than the conductor should not have uplink connectivity. Otherwise, auto-stacking will not work.
- The `vsf member 1` line must be present in the configuration template for stackable AOS-CX switches running 10.07 or later versions. This is required to apply configuration to the switches. Also, the `vsf member 1` line cannot be removed from the template.

For more information, see the following topics:

- [Creating an AOS-CX Stack Using Template](#)
- [Adding a Stack Member Using Template](#)
- [Modifying VSF Links Using Template](#)
- [Changing the Standby Conductor Using Template](#)

- [Removing a Stack Member Using Template](#)
- [Removing a Stack Using Template](#)

Creating an AOS-CX Stack Using Template

In Aruba Central (on-premises), you can create stacks through the template. Before creating a stack, you must physically connect the members of the stack in the chain or ring topology on the ports reserved for auto-stacking. For auto-stacking to work, the members should be connected in the direction of the higher denomination port to the lower denomination port.

The following ports are reserved for auto-stacking:

- 24-port switch models— Ports 25 and 26
- 48-port switch models— Ports 49 and 50

Auto-stacking peer discovery is a uni-directional process. It starts with the VSF link containing the higher denomination VSF port. Member discovery starts on the higher-numbered port for each member in line. For a three-member stack in the ring topology, use the following connection example for auto-stacking to work:

- Connect port 50 of member 1 to port 49 of member 2
- Connect port 50 of member 2 to port 25 of member 3
- Connect port 26 of member 3 to port 49 of member 1

For more information on VSF configuration, refer to the *AOS-CX Virtual Switching Framework (VSF) Guide*.

To create a stack using the template, complete the following steps:

1. In Aruba Central (on-premises), assign the switches to the template from any of the following pages:
 - **Device Inventory** page under **Global Settings** in **Account Home**.
 - **Groups** page under **Maintain > Organization**, in the **Network Operations** app.

For more information on assigning a stack, see [Assigning Devices to Groups](#).

2. Create a configuration template in the template group for the AOS-CX VSF stack.

The following example shows the sample VSF configuration template snippet for a three-member stack.

It is recommended to configure the VSF split-detection method in the template during stack creation. Also, ensure that the conductor and standby conductor are connected to the management interface. If the split-detection method is configured, during a split, the fragment that has the conductor becomes the active fragment and keeps its front plane (non-VSF) interfaces up and running. The other fragment becomes inactive and all non-VSF interfaces on the inactive fragment are brought down to avoid network disruption.



```
vsf split-detect mgmt
vsf secondary-member 2
vsf member 1
  type j1660a
  link 1 1/1/26
  link 2 1/1/25
vsf member 2
  type j1664a
  link 1 2/1/25
```

```
link 2 2/1/26
vsf member 3
type j1664a
link 1 3/1/25
link 2 3/1/26
```

3. Save the template.
4. Connect the uplink to the switch that should act as the conductor. The switch will connect to Aruba Central (on-premises) as a standalone device and will be added to the assigned template group. Once the switch is added to the template group, Aruba Central (on-premises) pushes the template group configuration to the switch. After the configuration is pushed, starting with the second switch, each switch in the stack reboots automatically and joins the stack one after another. Each member may take up to 10 minutes to join the stack.



If the switch is not assigned to any group, then the switch will be added to the **default** group or unprovisioned group. The factory default switch is added to the default group and non-factory default switch will be added to the unprovisioned group. You can verify the serial number of the switch once it is onboarded and move the switch to the template group as required.

5. Verify the status of the stack formation using switch monitoring pages. For more information, see [Switch > Overview > Summary](#) and [Monitoring AOS-CX Switch Stacks](#).

Adding a Stack Member Using Template

In Aruba Central (on-premises), you can add and configure the members through the template. Before adding a stack member, it is recommended to navigate to the stack faceplate in the **Switch > LAN > Ports** tab of the switch dashboard, to see whether there are any errors in the stack. For more information, see [Monitoring AOS-CX Switch Stacks](#).

To add a stack member through the template, complete the following steps:

1. In Aruba Central (on-premises), add the member to the device inventory and assign a valid license. Make sure that the new member does not have an uplink connectivity to Aruba Central (on-premises).
2. In Aruba Central (on-premises), update the template with the VSF configuration and interface configurations of the new member. For example, if you want to add the third member to a two-member VSF stack, add the third-member VSF configuration to the template, as shown in the following snippet:

```
vsf member 3
type j1664a
link 1 3/1/25
link 2 3/1/26
```

3. Save the template. Once the configuration is pushed to the conductor, the new member will go for a reboot and join the stack.
4. Physically connect the members to the ports reserved for auto-stacking on the switch interfaces. The member should be connected in the direction of the higher denomination port to the lower denomination port. The member may take up to 10 minutes to join the stack.

5. Verify the status of the member addition using switch monitoring pages. For more information, see [Switch > Overview > Summary](#) and [Monitoring AOS-CX Switch Stacks](#).

Modifying VSF Links Using Template

You can modify VSF links through the template only when the VSF interfaces of all the switches in the stack are in the shutdown state.

To modify VSF links using the template, complete the following steps:

1. In the Aruba Central (on-premises) template, use a variable to hold the shutdown state of the VSF interfaces for all switches in the stack.
2. Push the template with the interfaces state variables changed to shutdown for the device and wait for the links to go down.
3. Change the links in the template as required.
4. Change the state to `no shutdown` in the template variable for the switches in the stack and save the template.

Changing the Standby Conductor Using Template

To change the standby conductor using the template, update `vsf secondary-member <ID>` line in the Aruba Central (on-premises) template. For example, if you want to change the standby conductor from member 2 to member 3 in the stack, update member ID in the line from `vsf secondary-member 2` to `vsf secondary-member 3` and save the template. Both the existing standby conductor and the new standby conductor are rebooted. After rebooting, member 3 joins the stack as the new standby conductor. The earlier standby conductor becomes a member of the stack.

Removing a Stack Member Using Template

You can remove a stack member using the template. It involves completing procedures both in Aruba Central (on-premises) and on the switch directly.

To remove a stack member using the template, complete the following steps:

1. Shut down the member in the stack.
2. Disconnect the physical VSF links from the member you want to remove.
3. Reconnect the physical links of remaining members in the stack in the ring or chain topology.
4. In the Aruba Central (on-premises) template, delete the VSF configuration and interface configurations of the member.
5. Save the template. Once the configuration is pushed to the conductor, the member will be removed from the stack.
6. Verify the status of the member deletion using switch monitoring pages. For more information, see [Switch > Overview > Summary](#) and [Monitoring AOS-CX Switch Stacks](#).



Member 1 in the stack cannot be removed from the template.

Removing a Stack Using Template

You can remove a stack member using the template. It involves completing procedures both in Aruba Central (on-premises) and on the switch directly.

To remove a stack using the template, complete the following steps:

1. In Aruba Central (on-premises), set the **Auto Commit State** to **OFF** in the **Configuration Audit** page.
2. Shut down all the members in the stack.
3. Remove all the physical VSF links from the members of the stack.
4. Run the `erase all zeroize` command on the switch CLI for all the switches in the stack. This causes the switches to reboot, rollback to factory defaults, and connect back to Aruba Central (on-premises) as standalone devices.
5. In Aruba Central (on-premises), set the **Auto Commit State** to **ON** in the **Configuration Audit** page. Once the configuration is pushed, the stack will be removed from Aruba Central (on-premises).

Replacing an AOS-CX VSF Stack Member

You can replace either the conductor, standby, or any other member of the stack with the same part number or different part number. These configurations must be performed directly on the switch and switch CLI, outside Aruba Central (on-premises). The configurations performed directly on the switch are synced in Aruba Central (on-premises).

- [Switches Running AOS-CX 10.07 or Later Versions](#)
 - [Same Part number](#)
 - [Replacing the Conductor](#)
 - [Replacing the Standby or Other Members](#)
 - [Different Part Number](#)
 - [Replacing the Conductor](#)
 - [Replacing the Standby or Other Members](#)
- [Switches running AOS-CX 10.06 or earlier versions](#)
 - [Replacing the Conductor](#)
 - [Replacing the Standby or Other Members](#)

Switches Running AOS-CX 10.07 or Later Versions



The new replacement switch must be in the factory-default configuration and running the same firmware version. Also, ensure that the new switch is added and licensed in Aruba Central (on-premises).

Same Part number

The following section describes the procedures for replacing the conductor, standby, or any other member with the same part number:

Replacing the Conductor

To replace the conductor in the VSF stack, complete the following steps:

1. Shut down the conductor member in the stack.
2. Wait for the standby member to become the conductor.
3. Replace the conductor switch.
4. Move the VSF link from the old conductor to the new conductor.
5. Power up the new conductor switch.
6. Switchover to the new conductor in the switch CLI.

7. Verify the status of the stack in the switch monitoring pages. For more information, see [Switch > Overview > Summary](#) and [Monitoring AOS-CX Switch Stacks](#).

Replacing the Standby or Other Members

To replace the standby or any other member of the VSF stack, complete the following procedure:

1. Shut down the member in the stack.
2. Replace the old member and renumber the new member using the `vsf renumber-to` command. For example, if the member ID of the old member was 2, renumber the new VSF member to 2.
3. Move the VSF link DAC cable from the old member to the new member.
4. Verify the status of the stack in the switch monitoring pages. For more information, see [Switch > Overview > Summary](#) and [Monitoring AOS-CX Switch Stacks](#).

Different Part Number

The following section describes the procedures for replacing the conductor, standby, or any other member with the different part number:

In case of template groups, the following actions are required:

- Before replacing any stack member, set the **Auto Commit State** to **OFF** in the **Configuration Audit** page.
- After replacing any stack member:
 1. In Aruba Central (on-premises), update the template with the new VSF configuration.
 2. Set the **Auto Commit State** to **ON** in the **Configuration Audit** page.



Replacing the Conductor

To replace the conductor in the VSF stack, complete the following steps:

1. If Aruba Central (on-premises) support mode is disabled, run the following command in the switch console to enable Aruba Central (on-premises) support mode:

```
aruba-central support-mode
```

2. Power off the conductor. The standby conductor will take over as conductor. Make sure Aruba Central (on-premises) is updated with this failover change.
3. Remove the VSF links from the old conductor.
4. Delete the old conductor from the VSF stack in the switch CLI using the `no vsf member <MEMBER-ID>`. All configuration associated with the member, as well as the subsystems and interfaces of the member will also be removed.
5. Replace the conductor and wait for the member to come up.
6. Configure the new conductor in the switch CLI using the `vsf member <MEMBER-ID>` command.
7. Connect the VSF links to the new conductor.
8. Switchover to the new conductor in the switch CLI.

9. In the case of template group, update the template in Aruba Central (on-premises) with the new part number and interface configurations of the new conductor.
10. In the switch console, run the following command to disable Aruba Central support mode:

```
no aruba-central support-mode
```

11. Verify the status of the stack in the switch monitoring pages. For more information, see [Switch > Overview > Summary](#) and [Monitoring AOS-CX Switch Stacks](#).

Replacing the Standby or Other Members

To replace the standby or any other member of the VSF stack, complete the following procedure:

1. If Aruba Central (on-premises) support mode is disabled, run the following command in the switch console to enable Aruba Central (on-premises) support mode:

```
aruba-central support-mode
```

2. Reset the replacement member with the factory-default configuration.
3. Shut down the member in the stack.
4. Delete the member from the VSF stack in the switch CLI using the `no vsf member <MEMBER-ID>`. All configuration associated with the member, as well as the subsystems and interfaces of the member will also be removed.
5. Renumber the VSF member using the `vsf renumber-to` command.
For example, if the member ID of the old member was 2, renumber the new VSF member to 2.
6. Move the VSF link DAC cable from the old member to the new member.
7. In the case of template group, update the template in Aruba Central (on-premises) with the new part number and interface configurations of the new member.
8. In the switch console, run the following command to disable Aruba Central support mode:

```
no aruba-central support-mode
```

9. Verify the status of the stack in the switch monitoring pages. For more information, see [Switch > Overview > Summary](#) and [Monitoring AOS-CX Switch Stacks](#).

Switches running AOS-CX 10.06 or earlier versions

The following section describes the procedures for replacing the conductor, standby, or any other member with the same or different part number:

Replacing the Conductor

To replace the conductor in the VSF stack, complete the following steps:

1. Power off the conductor. The standby conductor will take over as conductor. Make sure Aruba Central (on-premises) is updated with this failover change.
2. Remove the VSF links from the old conductor.

3. Disable Aruba Central (on-premises) from the switch CLI.

```
switch# configure
switch(config)# aruba-central
switch(config-aruba-central)# disable
```

4. Wait for the standby member to become the conductor.
5. If you are replacing the conductor with a different part number, delete the old conductor from the VSF stack in the switch CLI using the `no vsf member <MEMBER-ID>`. All configuration associated with the member, as well as the subsystems and interfaces of the member will also be removed.
6. Replace the member and wait for the member to come up.
7. Configure the new member and the VSF links to the new member.
8. In the case of template groups, update the template in Aruba Central (on-premises) with the new part number and the interface configurations of the new conductor.
9. Enable Aruba Central (on-premises) from the switch CLI.

If this does not work, run the `https-server session close all` command.

```
switch(config-aruba-central)# enable
```

OR

```
switch# https-server session close all
```

10. Switchover to the new conductor in the switch CLI.
11. Verify the status of the stack in the switch monitoring pages. For more information, see [Switch > Overview > Summary](#) and [Monitoring AOS-CX Switch Stacks](#).

Replacing the Standby or Other Members

To replace the standby or any other member of the VSF stack, complete the following procedure:

1. Reset the replacement member with the factory-default configuration.
2. Disable Aruba Central (on-premises) from the switch CLI.

```
switch# configure
switch(config)# aruba-central
switch(config-aruba-central)# disable
```

3. Shut down the member in the stack.
4. If you are replacing the member with a different part number, delete the member from the VSF stack in the switch CLI using the `no vsf member <MEMBER-ID>`. All configuration associated with the member, as well as the subsystems and interfaces of the member will also be removed.
5. Configure the new member and the VSF links to the new member.
6. Renumber the VSF member using the `vsf renumber-to` command.
For example, if the member ID of the old member was 2, renumber the new VSF member to 2.
7. Move the VSF link DAC cable from the old member to the new member.

8. In the case of template groups, update the template in Aruba Central (on-premises) with the new part number and the interface configurations of the new member.
9. Enable Aruba Central (on-premises) from the switch CLI.

If this does not work, run the `https-server session close all` command.

```
switch(config-aruba-central)# enable
```

OR

```
switch# https-server session close all
```

10. Verify the status of the stack in the switch monitoring pages. For more information, see [Switch > Overview > Summary](#) and [Monitoring AOS-CX Switch Stacks](#).

Changing an AOS-CX VSF Stack to Standalone Switches

You can change an AOS-CX VSF stack in Aruba Central (on-premises) to standalone switches. It involves completing procedures both in Aruba Central (on-premises) and the switch CLI.



Using the **VSF Stacking** page UI, you can only change the conductor switch to standalone switch.

To change an AOS-CX VSF stack in Aruba Central (on-premises) to standalone switches, complete the following procedure:

1. Make a note of the serial numbers of switches that are part of the stack.
2. Disable Aruba Central (on-premises) from the switch CLI.

```
switch# configure
switch(config)# aruba-central
switch(config-aruba-central)# disable
```

3. Wait for the stack to display as offline in the List view.
4. Delete the stack from Aruba Central (on-premises).
See [Deleting an Offline Switch](#).
5. Run the `erase all zeroize` command on the switch CLI of the conductor.

This causes the switches to will reboot, rollback to factory defaults, and function as standalone switches. The switches will be added to the **default** group. You can verify the serial number of the switches once they are onboarded and move the switches to template or UI group as required.

The password for AOS-CX switch will be `SERIALNUM_central`, until the switches are moved to template or UI group and custom password is set. For more information on passwords, see the Password Requirements for Template-Based Configuration section in the [Using Configuration Templates for AOS-CX Switch Management](#) topic.



Monitoring AOS-CX Switch Stacks

In the switch dashboard, the **Ports** tab for a switch stack displays the faceplate of all the switches that are part of the stack. This allows you to manage, configure, monitor, and troubleshoot switch stacks that are provisioned and managed through Aruba Central (on-premises).

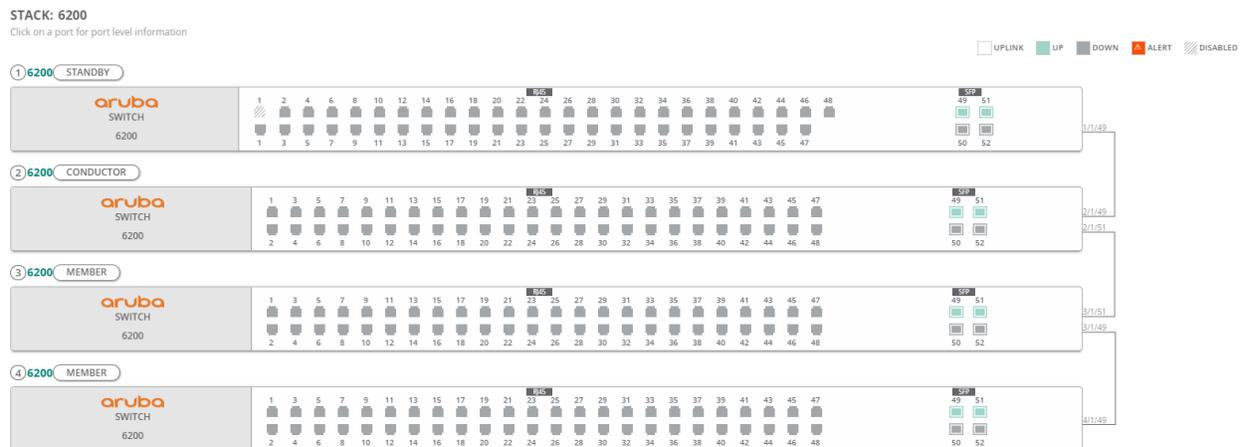
To navigate to the **Ports** tab in the Switch dashboard, complete the following steps:

1. Set the filter to **Global** or the group containing the stack.
2. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
3. Select the conductor switch of the stack from the devices list and navigate to the **LAN > Ports** tab.
The **Ports** tab is displayed with the faceplate of all the switches that are part of the stack.

For more information, see [Switch > LAN > Ports](#).

The following figure shows a four-member stack with the conductor, standby, and members with their corresponding ports and connections:

Figure 38 Switch Stack Faceplate



Stack-Related Errors

The switch stack faceplate displays the following configuration and connection errors related to the stack. You can monitor and troubleshoot these errors from the **Ports** tab:

- Auto-join eligibility error
- VSF link errors
- Cabling error
- Incompatible switch firmware error

In some cases, there can be multiple VSF errors associated with one VSF link. However, the faceplate displays only one error at a time. In such cases, you need to fix one error to see another error. For example, if the VSF link has both auto-join eligibility error and cabling error, only the auto-join eligibility error is displayed first. Once the auto-join eligibility error is resolved, the cabling error is displayed.



The faceplate will not be displayed when an auto-join eligibility or cabling error occurs on any interface connected to an existing member. The only exception is the peer-timeout error. This is because there is no peer MAC for peer-timeout error. Hence, it cannot be determined whether the peer connected to the interface is already a member of the stack.

Auto-Join Eligibility Error

The auto-join eligibility error is displayed in the **Ports** faceplate when the conductor or any of the member switches running AOS-CX 10.07 or later firmware versions in the stack do not have a factory default configuration.

Member connected to Aruba Central (on-premises)

If the member is connected to Aruba Central (on-premises), then click the  reset icon in the faceplate. The **RESOLVE AUTO-JOIN** window is displayed with a message to reboot the non-factory switch with the default configuration and join the stack. Click **Continue**. The switch reboots and joins the stack.

The following error and recommendation are displayed in the faceplate.

Error

Invalid stack configuration/connection

Recommendation

Reset the switch configuration and reboot

Member not connected to Aruba Central (on-premises)

If the member is not connected to Aruba Central (on-premises), then the  reset icon in the faceplate is disabled. In this case, execute `vsf force-autojoin` command through the switch CLI to resolve this error.

The following error and recommendation are displayed in the faceplate.

Error

Invalid stack configuration/connection

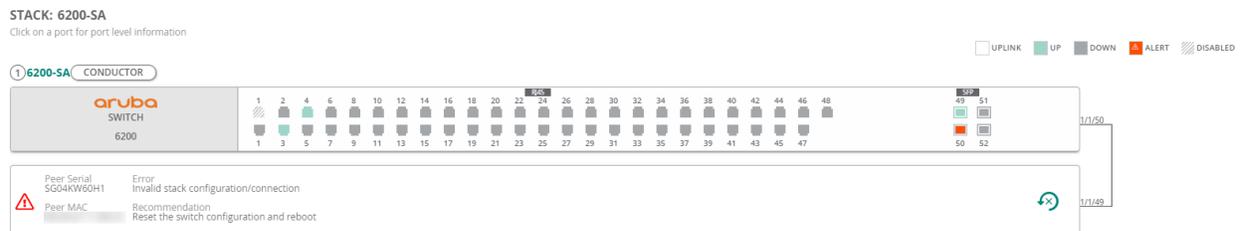
Recommendation

Configure vsf force-auto-join on the switch



The force auto-join will not work if the switch contains any existing VSF configuration. In this case, execute the `erase all zeroize` command from the switch CLI. This causes the switch to reboot, rollback to factory-default configuration and join the stack if there is no other auto-join error. For more information, refer to the *AOS-CX Virtual Switching Framework (VSF) Guide*.

Figure 39 Auto-Join Eligibility Error

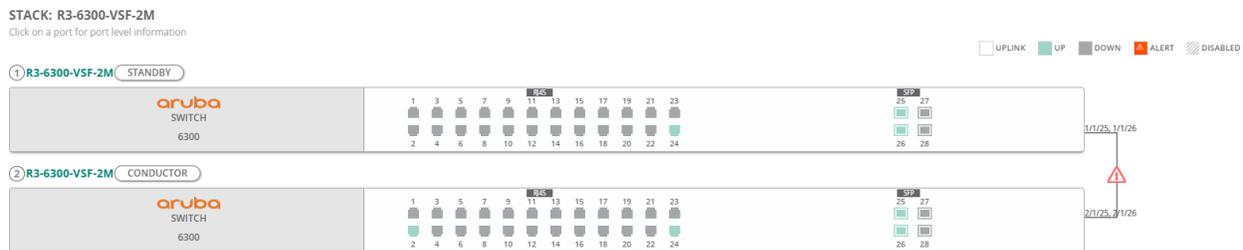


VSF Link Errors

The VSF link errors are displayed in the switch stack faceplate when there are any issues between VSF links. The faceplate displays a red-warning symbol to help you identify the type of link error in the switch stacks. You can hover over the warning symbol to identify the interfaces that are disconnected. The following VSF link errors can be identified from the face plate:

- **Broken Link**—The broken link error is displayed when a link between the two VSF members is down.
- **No peer interface**—The no peer interface error is displayed when there is connection issue between some of interfaces between the two members.

Figure 40 VSF Link Errors



Cabling Error

The cabling error is displayed in the switch stack faceplate when stack cables are connected incorrectly. For auto-stacking to work, all the stack members must be connected using the following auto-stacking reserved VSF link ports:

- 24-port switch models— Ports 25 and 26
- 48-port switch models— Ports 49 and 50

Auto-stacking peer discovery is a uni-directional process. It starts with the VSF link containing the higher denomination VSF port. Member discovery starts on the higher-numbered port for each member in line. For a three-member stack in the ring topology, use the following connection example for auto-stacking to work:

- Connect port 50 of member 1 to port 49 of member 2
- Connect port 50 of member 2 to port 25 of member 3
- Connect port 26 of member 3 to port 49 of member 1

The following error and recommendation are displayed in the faceplate:

Error

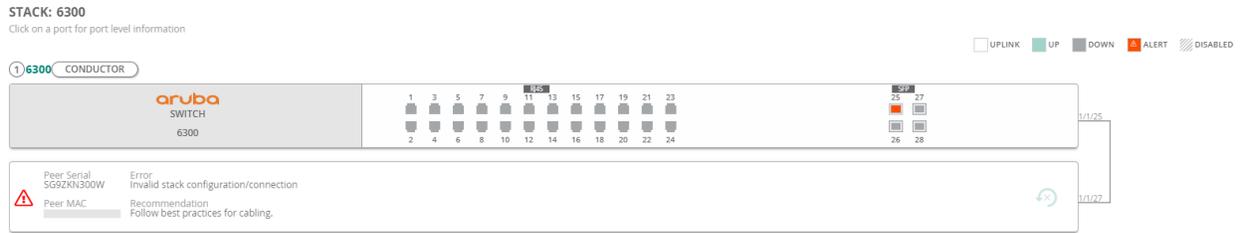
Invalid stack configuration/connection

Recommendation

Follow best practices for cabling

For more information on cabling, see the *AOS-CX Virtual Switching Framework (VSF) Guide*

Figure 41 *Cabling Error*



Incompatible Switch Firmware Error

The incompatible switch firmware error is displayed in the faceplate when the switch trying to join the stack is running the firmware prior to AOS-CX 10.07 version. To resolve this error, you need to upgrade the switch to a compatible firmware offline, outside Aruba Central (on-premises).

The following error and recommendation are displayed in the faceplate:

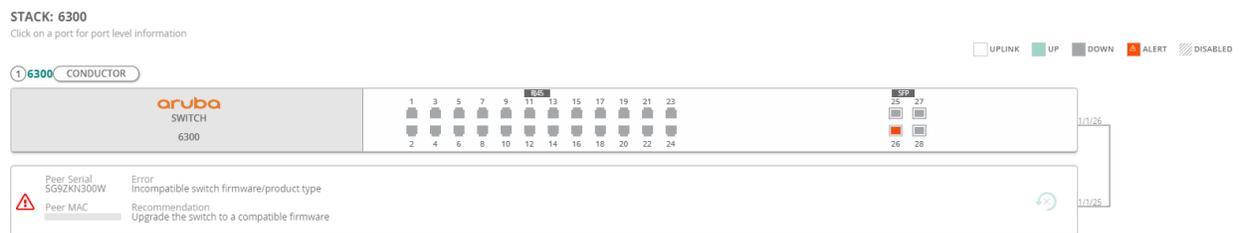
Error

Incompatible switch firmware/product type

Recommendation

Upgrade the switch to a compatible firmware

Figure 42 *Incompatible Switch Firmware Error*



AOS-Switches enable secure, role-based network access for wired users and devices, independent of their location or application.

AOS-Switches can also operate as a wired access point when deployed with an Aruba Mobility Controller. As a wired access point, users and their devices are authenticated and assigned a unique role by the Mobility Controller. These roles are applied irrespective of whether the user is a Wi-Fi client, or is connected to a port on the switch. The use of switches allows an enterprise workforce to have consistent and secure access to network resources based on the type of users, client devices, and connection method used.



Local firmware upgrade is not supported for switches due to a known issue.

Aruba Central (on-premises) supports provisioning switches in UI and template groups. Aruba Central (on-premises) supports basic configuration options in the UI. The users can also assign switches to template groups and use configuration templates and variables to manage switches from Aruba Central (on-premises).

See the following topics for more information on managing AOS-Switches in Aruba Central (on-premises):

- [Using Configuration Templates for AOS-Switch Management](#)
- [Configuring AOS-Switches in UI Groups](#)
- [AOS-Switch Stack](#)

Getting Started with AOS-Switch Deployments

Before you get started with your onboarding and provisioning operations, browse through the list of [AOS-Switches supported](#) in Aruba Central (on-premises).

Provisioning Workflow

The following sections list the steps required for provisioning switches in Aruba Central (on-premises).

Provisioning a Factory Default AOS-Switch

Like most Aruba devices, AOS-Switches support ZTP. Switches with factory default configuration have very basic configuration for all ports in VLAN-1. You must manually add either the serial number, MAC address, or part number of the new factory default switch in Aruba Central (on-premises). When the switch identifies Aruba Central (on-premises) as its management entity, it connects to Aruba Central (on-premises).

To manage switches from Aruba Central (on-premises), you must onboard the switches to the device inventory and assign a valid subscription.

For step-by-step instructions, see [Provisioning Factory Default AOS-Switches](#).

Provisioning a Pre-configured or Locally-Managed Switch

Pre-configured switches have customized configuration; for example, an additional VLAN or static IP address configured on the default.

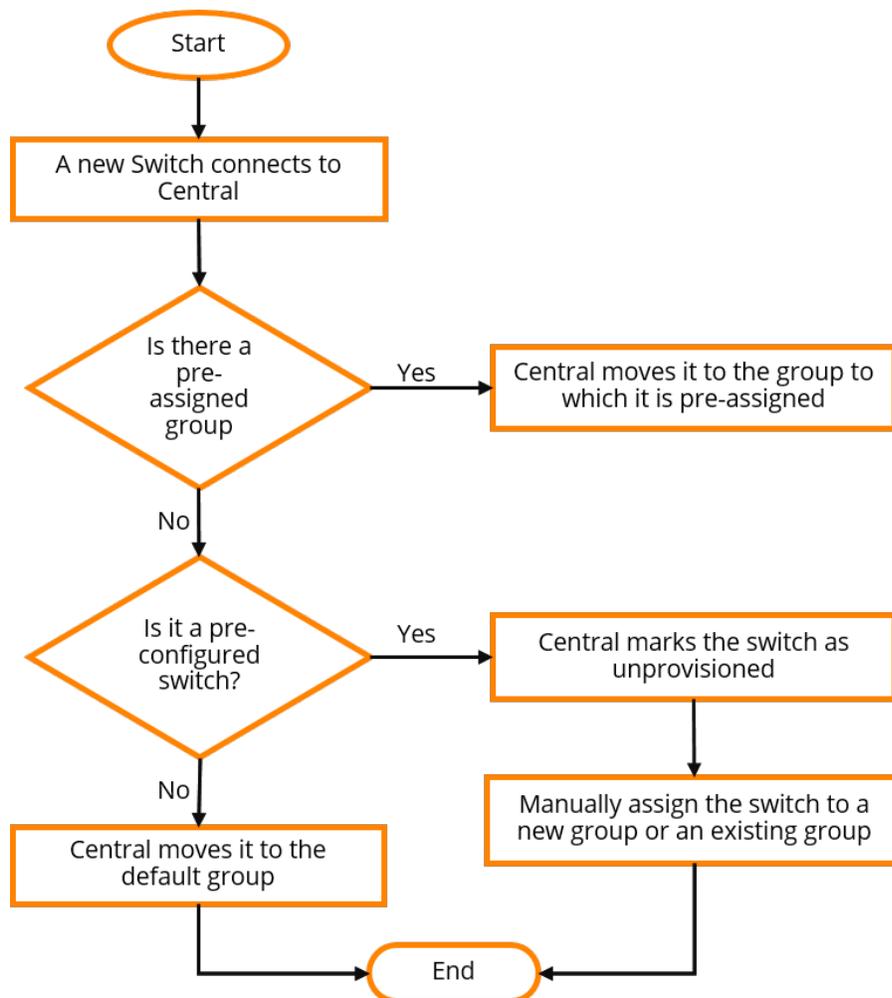
Unlike factory default switches, locally managed switches and the switches with custom configuration require one touch provisioning. These switches do not automatically identify Aruba Central (on-premises) as their management platform, therefore you must manually enable the Aruba Central (on-premises) management service on these switches to allow them to connect to Aruba Central (on-premises).

For step-by-step instructions, see [Provisioning Pre-Configured AOS-Switches](#).

Group Assignment

Aruba Central (on-premises) supports provisioning switches in one of the following types of groups:

- UI group—Allows you to customize and manage device parameters using the UI workflows, that is, the menu options and knobs available under **Network Operations**.
- Template Group—Allows you to configure devices using CLI-based configuration templates.



AOS-Switch Configuration and Management

Aruba Central (on-premises) supports managing switch configuration using UI workflows or configuration templates. Based on your configuration requirements, ensure that you assign switches to either UI group or template group.

For more information on managing switches in Aruba Central (on-premises), see the following topics:

- [Using Configuration Templates for AOS-Switch Management](#)
- [Configuring AOS-Switches in UI Groups](#)

AOS-Switch Switch Monitoring

To view the operation status of switches and health of wired access network:

1. In the **Network Operations** app, use the filter to select a group that has switches.
2. Under **Manage**, click **Devices** > **Switches**.

For more information, see [Monitoring Switches and Switch Stacks](#).

Troubleshooting and Diagnostics

The **Configuration Audit** page under **Network Operations** > **Device(s)** > **Switches** in the Aruba Central (on-premises) UI displays errors in configuration sync, templates, and a list of configuration overrides. For more information, see [Verifying Device Configuration Status](#).

To troubleshoot switches remotely, use the troubleshooting tool available under **Network Operations** > **Analyze** > **Tools**. For more information, see [Using Troubleshooting Tools](#).

Provisioning Factory Default AOS-Switches

Switches that run default configuration either after shipped from a factory or a factory reset are referred to as factory default switches. This topic describes the steps for provisioning factory default switches in Aruba Central (on-premises).

- [Step 1: Onboard the AOS-Switch to Aruba Central \(on-premises\)](#)
- [Step 2: Assign the AOS-Switch to a Group](#)
- [Step 3: Connect the AOS-Switch to Aruba Central \(on-premises\)](#)
- [Step 4: Provision the AOS-Switch to a Group](#)
- [Step 5: Verify the Configuration Status](#)

Step 1: Onboard the AOS-Switch to Aruba Central (on-premises)

Log in to Aruba Central (on-premises) and [onboard the switch](#).

Step 2: Assign the AOS-Switch to a Group

Before assigning a group, determine if the switch must be provisioned in a UI or template group. By default, Aruba Central (on-premises) assigns the factory default switches to the default group. You can create a new group and assign switch to the new group.

For step-by-step instructions on creating a group, see [Creating a Group](#).

To assign a device to a group from the **Account Home** page:

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.
The Device Inventory page is displayed.
2. Select the device that you want to assign to a group.
3. Click **Assign Group**.
The **Assign a Group to the Selected Devices** window is displayed.
4. Select the group to which you want to assign.
5. Click **Assign Device(s)**.

To assign a device to a group from the **Network Operations** app:

1. In the **Network Operations** app, set the filter to **Global**.
The Global dashboard is displayed.
2. Under **Maintain**, click **Organization > Groups**.
The Groups page is displayed.
3. From the devices table on the right, select the device that you want to assign to a new group.
4. Drag and drop the device to the group to which you want to assign the device.

Step 3: Connect the AOS-Switch to Aruba Central (on-premises)

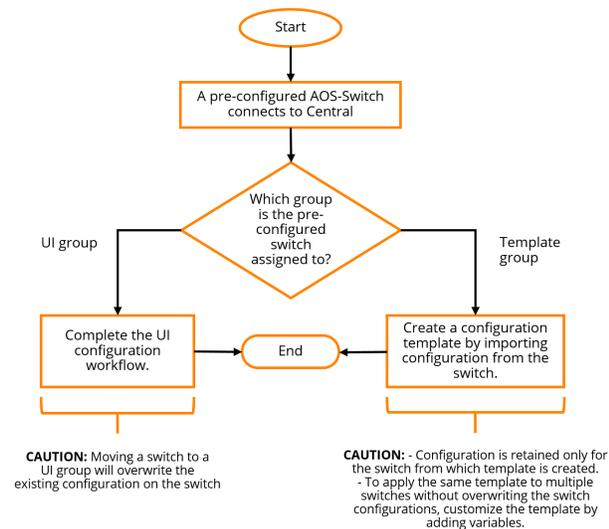
Switches with factory default configuration have very basic configuration for all ports in VLAN-1 that is required for obtaining an IP address and automatic provisioning (ZTP). For ZTP, switches must have a valid IP address, DNS, and NTP configuration. You must manually add either the serial number, MAC address, or part number of the factory default switch in Aruba Central (on-premises)

Step 4: Provision the AOS-Switch to a Group

When the switch connects to Central, if it is already added to the device inventory and is assigned a subscription in Aruba Central (on-premises), Aruba Central (on-premises) assigns it to a pre-assigned group. If there is no pre-assigned group, Aruba Central (on-premises) moves the device to **default** group. Based on your configuration requirements, you create a UI group or template group and assign the switch.

The following figure illustrates the provisioning step required for each group type.

Figure 43 Switch Provisioning Steps Per Group Type



If the switch is assigned to a new UI group, Aruba Central (on-premises) uses the current configuration of switch as base configuration and applies it to the other switches that join this group later. You can also modify the configuration of switches in a group using the UI menu options under **Network Operations** app > **Manage > Device(s) > Switches**. For more information, see [Configuring AOS-Switches in UI Groups](#).

Provisioning AOS-Switches in Template Groups

If you have assigned the switch to a template group, create a new configuration template. To create a configuration template:

1. In the **Network Operations** app, set the filter to a template group.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Switches**.
3. Click the **Config** icon.
The tabs to configure switches using templates is displayed.
4. Click the **Templates** tab. The Templates page is displayed.
5. Click **+** to add a new template. The **Add Template** window is displayed.
6. In the **Basic Info** tab, enter a name for the template in the **Template Name** field.
7. In the **Device Type** drop-down, select **Aruba Switch**.
8. Select the switch model and software version. You can specify any of the following combinations:
 - **ALL** for both **Model** and **Version**—To apply the template to all switch models and all supported switch software versions.
 - **ALL** for **Model** and a software version for **Version**—To apply the template to all switch models running the selected software version.
 - **ALL** for **Version** and a switch model for **Model**—To apply the template to a switch model and all software versions supported by the selected switch model.
 - A switch model and a software version—To apply the template to a specific switch model and the software version. The template created for a switch model and a software version takes precedence over the template that is created for all platforms and versions.
9. Select the manufacturing part number of the switch in the **Part Number** drop-down.

-
- The **Part Number** drop-down is displayed only if you select a switch model in the **Model** drop-down.
 - If you select a specific switch model and part number, you can apply the template to a standalone switch and not to a stack.
 - If you select **All** in the **Model** drop-down, or if you select a switch model and **All** in the **Part Number** drop-down, you can apply a template to both a standalone switch and stack.
-



10. Click **Next**. The **Template** tab is displayed.
11. Build a new template or import configuration information from a switch that is already provisioned in the template group.
 - To build a new template, add the switch command information in the **Template** text box. Ensure that the template text adheres to the guidelines listed in [Important Points to Note](#).
 - To import configuration text from a switch that is already provisioned in the template group:
 - a. Click **Import Configuration As Template**.
 - b. From the search box, select the switch from which you want to import the configuration. The imported configuration is displayed in the **Template** text box.



-
- Importing configuration from an existing device in the template group allows you to quickly create a basic template. However, before applying the template to other switches in the group, ensure that the template text is variabilized as per your deployment requirements. For more information on variables, see [Managing Variable Files](#).
 - All switch templates must include a password command to set a password for the device. The switch template cannot be saved without adding a password command. If the configuration that is pushed from Aruba Central to the device does not contain a password command, the configuration push is aborted for the device and a log is added to the audit trail. For example, if you add the password command in a condition block and the condition evaluates to false, the configuration that is pushed will not contain the password command. For more information, see [Managing Password in Configuration Templates](#).

For more information about using password commands, see the Configuring Username and Password Security chapter in the *ArubaOS-Switch Access Security Guide*.

- c. To view the variables present in the imported configuration template, click **Show Variables List**. The Variables in Template column is displayed.

For more information on variables, see [Managing Variable Files](#).

- d. To download the variables as a CSV or plain text file, click the download icon and select one of the following options:
 - **Download .CSV**
 - **Download plain text (.txt)**

12. Click **Save**. After you apply the configuration template, switches reboot and reconnect to Aruba Central (on-premises) with the new configuration.

Step 5: Verify the Configuration Status

To verify the configuration status:

1. In the **Network Operations** app, set the filter to a template group.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Switches**.
3. Click the **Config** icon.
The tabs to configure switches using templates is displayed.
 - To verify the configuration status for the template group, click **Configuration Audit**. The **Configuration Audit** dashboard displays the number of devices with template and configuration synchronization errors.
 - To view configuration errors for a specific device, select a switch from the filter bar. The **Configuration Audit** dashboard displays the number of template and configuration synchronization errors for the device.
4. To view template errors, click **View Template Errors**.
5. To view configuration synchronization errors, click **View Details** under **Configuration Status**.
6. To compare running configuration and pending changes, click **View** under **Config Comparison Tool**.

Provisioning Pre-Configured AOS-Switches

Unlike factory default switches, locally managed switches and the switches with custom configuration require one touch provisioning. These switches do not automatically identify Aruba Central (on-premises) as their management platform, therefore you must manually enable the Aruba Central (on-premises) management service on these switches to allow them to connect to Aruba Central (on-premises).

Aruba Central (on-premises) does not support adding pre-configured switches to a UI group. Pre-configured switches that have pre-assigned UI switch groups are added to the Unassigned Devices group. To provision a pre-configured switch to a UI group or move a switch from a template group to a UI group, complete the following steps:



1. Clear the switch configuration.
2. Delete the device from Aruba Central (on-premises).
3. Provision the switch as a new device in a UI group.

To onboard a locally-managed or a pre-configured switch to Aruba Central (on-premises), follow one of the following options:

- Manually enable Aruba Central (on-premises) management service on the switch and connect it to Aruba Central (on-premises). Aruba recommends that you use this option if you want to preserve the current configuration running on the switch. For more information on this procedure, see the workflows described in this topic.

To manually connect the switch to Aruba Central (on-premises), you must configure the Aruba Central (on-premises) URL on the switch. Execute the following commands in the switch CLI:

```
conf t
aruba-central url <Aruba Central (on-premises) URL>/ws
exit
```



Aruba does not recommend to manually provision the URL in a cloud deployment.

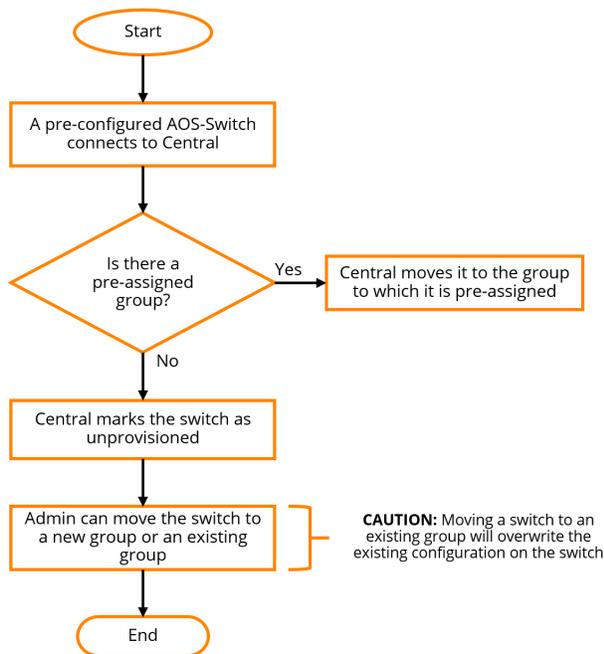
-
- Reset the switch configuration and use ZTP to provision the switch. You must first create a backup of the configuration, then reset the switch using the `erase all zeroize` command in the CLI. This initiates ZTP on the switch, enabling the switch to obtain the IP address from the option 43 sent by the DHCP server and then connect to Aruba Central (on-premises).

Aruba Central (on-premises) supports provisioning switches using one of the following methods:

- Pre-provisioning—In this workflow, a switch is added to the device inventory and assigned a group in Aruba Central (on-premises) before it connects to Aruba Central (on-premises).
See [Workflow 1—Pre-Provisioning an AOS-Switch](#).
- Onboarding connected switches—In this workflow, Aruba Central (on-premises) onboards the switch that attempts to connect and then assigns a group.
See [Workflow 2—Provisioning an AOS-Switch On-Demand](#).

The following figure illustrates provisioning procedure for a pre-configured switch.

Figure 44 Provisioning Workflow for Pre-Configured AOS-Switches



Workflow 1—Pre-Provisioning an AOS-Switch

The pre-provisioning workflow includes the following steps:

- [Step 1: Onboard the AOS-Switch to Aruba Central \(on-premises\)](#)
- [Step 2: Assign the AOS-Switch to a Group](#)
- [Step 3: Enable Aruba Central \(on-premises\) Management Service on the AOS-Switch](#)
- [Step 4: Provision the AOS-Switch to a Group](#)
- [Step 5: Verify the Configuration Status](#)

Step 1: Onboard the AOS-Switch to Aruba Central (on-premises)

To onboard switches to the device inventory in Aruba Central (on-premises), complete the following steps:

- [Add switches to Aruba Central](#)
- [Assign Subscriptions](#)

Step 2: Assign the AOS-Switch to a Group

Before assigning a group, determine if the switch must be provisioned in a UI or template group. If you want to preserve the existing configuration on the switch, Aruba recommends that you create a new group for the switch.

For more information on creating a group, see [Creating a Group](#).

To assign a device to a group from the **Account Home** page:

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.
The Device Inventory page is displayed
2. Select the device that you want to assign to a group.

3. Click **Assign Group**. The **Assign a Group to the Selected Devices** window is displayed.
4. Select the group to which you want to assign.
5. Click **Assign Device(s)**.

To assign a device to a group from the **Network Operations** app:

1. In the **Network Operations** app, set the filter to **Global**.
The dashboard context for the group is displayed.
2. Under **Maintain**, click **Organization > Groups**.
The Groups page is displayed.
3. From the devices table on the right, select the device that you want to assign to a new group.
4. Drag and drop the device to the group to which you want to assign the device.

Step 3: Enable Aruba Central (on-premises) Management Service on the AOS-Switch

A locally-managed or pre-configured switch cannot connect to Aruba Central (on-premises), unless it is configured to identify Aruba Central (on-premises) as its management entity. To manage such a device from Aruba Central (on-premises), you must manually enable the provisioning and management service on the switch.

1. To enable switches to automatically connect to Aruba Central (on-premises), enforce ZTP on the switch:

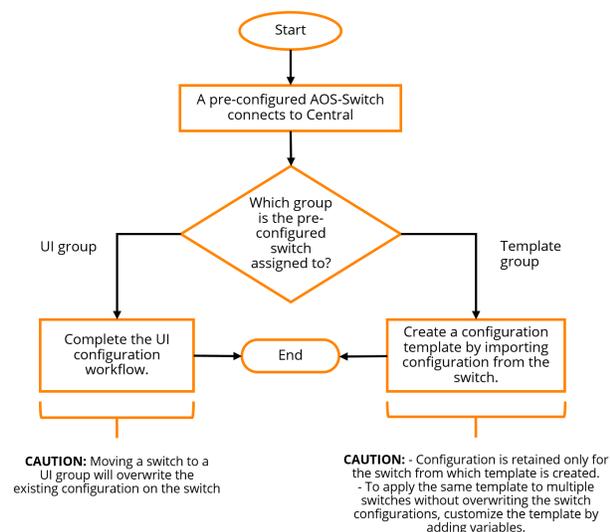
```
(switch)# erase all zeroize
```

The switch obtains the IP address from the option 43 sent by the DHCP server and then connects to Aruba Central (on-premises). If the switch is already added to the device inventory and is assigned a subscription, Aruba Central (on-premises) assigns it to a pre-assigned group.

Step 4: Provision the AOS-Switch to a Group

When the switch connects to Aruba Central (on-premises), Aruba Central (on-premises) automatically assigns it to the pre-assigned group. The following figure illustrates the provisioning steps for each group type.

Figure 45 Switch Provisioning Steps Per Group Type



If the switch is assigned to a new UI group, you can modify the configuration of switches in a group using the UI menu options under the **Network Operations** app > **Manage** > **Device(s)** > **Switches**. For more information, see [Configuring AOS-Switches in UI Groups](#).

If you have assigned the switch to a template group, you can import the existing configuration to a new configuration template and apply this template to other devices in the group. To create a configuration template using the existing configuration on the switch:

1. In the **Network Operations** app, set the filter to a template group.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Switches**.
3. Click the **Config** icon.
The tabs to configure switches using templates is displayed.
4. Click the **Templates** tab. The Templates page is displayed.
5. Click + to add a new template. The **Add Template** window is displayed.
6. In the **Basic Info** tab, enter a name for the template in the **Template Name** field.
7. In the **Device Type** drop-down, select **Aruba Switch**.
8. Select the switch model and software version. You can specify any of the following combinations:
 - **ALL** for both **Model** and **Version**—To apply the template to all switch models and all supported switch software versions.
 - **ALL** for **Model** and a software version for **Version**—To apply the template to all switch models running the selected software version.
 - **ALL** for **Version** and a switch model for **Model**—To apply the template to a switch model and all software versions supported by the selected switch model.
 - A switch model and a software version—To apply the template to a specific switch model and the software version. The template created for a switch model and a software version takes precedence over the template that is created for all platforms and versions.
9. Select the manufacturing part number of the switch in the **Part Number** drop-down.

-
- The **Part Number** drop-down is displayed only if you select a switch model in the **Model** drop-down.
 - If you select a specific switch model and part number, you can apply the template to a standalone switch and not to a stack.
 - If you select **All** in the **Model** drop-down, or if you select a switch model and **All** in the **Part Number** drop-down, you can apply a template to both a standalone switch and stack.
-



NOTE

10. Build a new template or import configuration information from a switch that is already provisioned in the template group.
 - To build a new template, add the switch command information in the **Template** text box. Ensure that the template text adheres to the guidelines listed in [Important Points to Note](#).
 - To import configuration text from a switch that is already provisioned in the template group:
 - a. Click **Import Configuration As Template**.
 - b. From the search box, select the switch from which you want to import the configuration. The imported configuration is displayed in the **Template** text box.
 - c. If required, modify the configuration parameters. Ensure that the template text adheres to the guidelines listed in [Using Configuration Templates for AOS-Switch Management](#).

11. Click **Next**. The **Template** tab is displayed.



- Importing configuration from the switch allows you to quickly create a basic configuration template that you can apply for all devices in a template group. Before applying the template to other switches in the group, ensure that the template text is variabilized based on the deployment requirements. For more information on configuration templates and variable definitions, see [Using Configuration Templates for AOS-Switch Management](#) and [Managing Variable Files](#).
- All switch templates must include a password command to set a password for the device. The template cannot be saved without adding a password command. If the configuration that is pushed from Aruba Central (on-premises) to the device does not contain a password command, the configuration push is aborted for the device and a log is added to the audit trail. For example, if you add the password command in a condition block and the condition evaluates to false, the configuration that is pushed will not contain the password command. For more information, see [Managing Password in Configuration Templates](#).
For more information about using password commands, see the Configuring Username and Password Security chapter in the *ArubaOS-Switch Access Security Guide*.

- a. To view the variables present in the imported configuration template, click **Show Variables List**. The Variables in Template column is displayed.
For more information on variables, see [Managing Variable Files](#).
 - b. To download the variables as a CSV or plain text file, click the download icon and select one of the following options:
 - **Download .CSV**
 - **Download plain text (.txt)**
12. Click **Save**. After you apply the configuration template, switches reboot and reconnect to Aruba Central (on-premises) with the new configuration.

Step 5: Verify the Configuration Status

To verify the configuration status:

1. In the **Network Operations** app, set the filter to a template group.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Switches**.
3. Click the **Config** icon.
The tabs to configure switches using templates is displayed.
 - To verify the configuration status for the template group, click **Configuration Audit**. The **Configuration Audit** dashboard displays the number of devices with template and configuration synchronization errors.
 - To view configuration errors for a specific device, select a switch from the filter bar. The **Configuration Audit** dashboard displays the number of template and configuration synchronization errors for the device.
4. To view template errors, click **View Template Errors**.
5. To view configuration synchronization errors, click **View Details** under **Configuration Status**.
6. To compare running configuration and pending changes, click **View** under **Config Comparison Tool**.

Workflow 2—Provisioning an AOS-Switch On-Demand

To dynamically provision switches on-demand, complete the following steps:

- [Step 1: Enable Aruba Central \(on-premises\) Management Service on the AOS-Switch](#)
- [Step 2: Add the AOS-Switch to Aruba Central \(on-premises\)](#)
- [Step 3: Assign a Subscription](#)
- [Step 4: Provision the AOS-Switch to a Group](#)
- [Step 5: Verify the Configuration Status](#)

Step 1: Enable Aruba Central (on-premises) Management Service on the AOS-Switch

A locally-managed or pre-configured switch cannot connect to Aruba Central (on-premises), unless it is configured to identify Aruba Central (on-premises) as its management entity. To manage such a device from Aruba Central (on-premises), you must manually enable the provisioning and management service on the switch.

1. To enable switches to automatically connect to Aruba Central (on-premises), enforce ZTP on the switch:

```
(switch)# erase all zeroize
```

The switch obtains the IP address from the option 43 sent by the DHCP server and then connects to Aruba Central (on-premises).

Step 2: Add the AOS-Switch to Aruba Central (on-premises)

Add the switch to the Aruba Central (on-premises) device inventory. For more information, see [Onboarding Devices](#).

Step 3: Assign a Subscription

To allow Aruba Central (on-premises) to manage the switch, ensure that a valid subscription is assigned to the switch.

Step 4: Provision the AOS-Switch to a Group

If the switch has a valid subscription assigned, Aruba Central (on-premises) marks the switch as **unprovisioned**. To preserve the switch configuration, move it to a new group.

To move the device to a UI group:

1. In the **Network Operations** app, set the filter to **Global**.
The dashboard context for the group is displayed.
2. Under **Maintain**, click **Organization > Groups**.
The Groups page is displayed.
3. Select the device.
4. Click **Import configuration to New Group**. The **Import configuration** window is displayed.
5. Enter a name for the group.
6. Configure a password for the group.
7. Click **Import configuration**. Aruba Central (on-premises) imports the switch configuration to the new group.

You can also modify the configuration of switches in a group using the UI menu options under the **Network Operations** app > **Manage > Devices > Switches**. For more information, see [Configuring AOS-Switches in UI Groups](#).

To move the device to a template group:

1. [Create a template group](#).
2. On the **Groups** page, select the switch.
3. Drag and drop the switch the new template group that you just created. Aruba Central (on-premises) adds the switch to the new template group.
4. To import switch configuration to a new configuration template:
 - a. In the **Network Operations** app, set the filter to a template group.

The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-S** or **Config** icon.

The tabs to configure switches using templates is displayed.
 - d. Click the **Templates** tab. The Templates page is displayed.
 - e. Click **+** to add a new template. The **Add Template** window is displayed.
 - f. In the **Basic Info** tab, enter a name for the template in the **Template Name** field.
 - g. In the **Device Type** drop-down, select **Aruba Switch**.
 - h. Select the switch model and the software version to which you want to apply the new template. You can specify any of the following combinations:
 - **ALL** for both **Model** and **Version**—To apply the template to all switch models and all supported switch software versions.
 - **ALL** for **Model** and a software version for **Version**—To apply the template to all switch models running the selected software version.
 - **ALL** for **Version** and a switch model for **Model**—To apply the template to a switch model and all software versions supported by the selected switch model.
 - A switch model and a software version—To apply the template to a specific switch model and the software version. The template created for a switch model and a software version takes precedence over the template that is created for all platforms and versions.
 - i. Select the manufacturing part number of the switch in the **Part Number** drop-down.



NOTE

 - The **Part Number** drop-down is displayed only if you select a switch model in the **Model** drop-down.
 - If you select a specific switch model and part number, you can apply the template to a standalone switch and not to a stack.
 - If you select **All** in the **Model** drop-down, or if you select a switch model and **All** in the **Part Number** drop-down, you can apply a template to both a standalone switch and stack.

 - j. Click **Next**. The **Template** tab is displayed.
 - k. Build a new template or import configuration information from a switch that is already provisioned in the template group. See [step 11](#).



-
- Importing configuration from the switch allows you to quickly create a basic configuration template that you can apply for all devices in a template group. Before applying the template to other switches in the group, ensure that the template text is variabilized based on the deployment requirements. For more information on configuration templates and variable definitions, see [Using Configuration Templates for AOS-Switch Management](#) and [Managing Variable Files](#).
 - All switch templates must include a password command to set a password for the device. The template cannot be saved without adding a password command. If the configuration that is pushed from Aruba Central (on-premises) to the device does not contain a password command, the configuration push is aborted for the device and a log is added to the audit trail. For example, if you add the password command in a condition block and the condition evaluates to false, the configuration that is pushed will not contain the password command. For more information, see [Managing Password in Configuration Templates](#).
For more information about using password commands, see the Configuring Username and Password Security chapter in the *ArubaOS-Switch Access Security Guide*.
-

- l. To view the variables present in the imported configuration template, click **Show Variables List**. The Variables in Template column is displayed.
For more information on variables, see [Managing Variable Files](#).
- m. To download the variables as a CSV or plain text file, click the download icon and select one of the following options:
 - **Download .CSV**
 - **Download plain text (.txt)**
- n. Click **Save**. After you apply the configuration template, switches reboot and reconnect to Aruba Central (on-premises) with the new configuration.

Step 5: Verify the Configuration Status

To verify the configuration status:

1. In the **Network Operations** app, set the filter to a template group.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Switches**.
3. Click the **Config** icon.
The tabs to configure switches using templates is displayed.
 - To verify the configuration status for the template group, click **Configuration Audit**. The **Configuration Audit** dashboard displays the number of devices with template and configuration synchronization errors.
 - To view configuration errors for a specific device, select a switch from the filter bar. The **Configuration Audit** dashboard displays the number of template and configuration synchronization errors for the device.
4. To view template errors, click **View Template Errors**.
5. To view configuration synchronization errors, click **View Details** under **Configuration Status**.
6. To compare running configuration and pending changes, click **View** under **Config Comparison Tool**.

Managing Switch Variable Files

The variable files consist of a set of configuration values defined for devices in the network.

Before creating or uploading a variable file, note the following points:

- The variable names must be on the left side of condition and its value must be defined on the right side. For example, `%if var=100%` is supported and `%if 100=var%` is not supported.
- The `<` or `<=` or `>` or `>=` operators should have only numeric integer value on the right side. The variables used in these 4 operations are compared as integer after flooring. For example, if any float value is set as `%if dpi_value > 2.8%`, it is converted as `%if dpi_value > 2` for comparison.
- The variable names should not include white space, and the `&` and `%` special characters. The variable names must match regular expression `[a-zA-Z0-9_]`. If the variables values with `%` are defined, ensure that the variable is surrounded by space.
- The first character of the variable name must be an alphabet. Numeric values are not accepted.
- The values defined for the variable must not include spaces. If quotes are required, they must be included as part of the variable value. For example, if the intended template and variable name is `wlan ssid-profile "emp ssid"`, the template must be defined template as `"wlan ssid-profile %ssid_name%"` and variable as `"ssid_name": "\"emp ssid\""`.
- If the configuration text has the percentile `%` in it—for example, `"url "/portal/scope.cust-5001098/Splash%20Profile%201/capture"`—Aruba Central (on-premises) treats it as a variable when you save the template. To allow the use of percentile `%` as an escape character, use `\` in the variable definition as shown in the following example:

Template text

```
wlan external-captive-portal "Splash Profile 1_#guest#_"
server naw1.cloudguest.central.arubanetworks.com
port 443
url %url%
```

Variable

```
"url": "\"/portal/scope.cust-5001098/Splash%20Profile%201/capture\""
```

Predefined Variables for Aruba Switches

Although all Aruba Switches can be configured by using common configuration templates, the configuration of these switches may need to change per device. Aruba Central (on-premises) uses the predefined variables to address the per device configuration requirements.

Aruba Central (on-premises) parses a set of predefined variables from the running configuration of the switches and identifies these as the variables per device. All the pre-defined variables are prefixed by `_sys`.

The following is the list of predefined variables used for configuring switches.

- **sys_template_header_**—Represents the first two lines of the configuration file. Ensure that this variable is the first line in the template.
- **snmpv3 engineid "%_sys_snmpv3_engineid%"**—Populates engine ID.
- **_sys_module_command**—Populates module lines.
- **ip default-gateway _sys_gateway**—Populates gateway IP address.
- **hostname _sys_hostname**—Maintains unique host name.
- **_sys_oobm_command**—Represents Out of Band Management (OOBM) block.

- **_sys_ip_address**—Indicates the IP address of the device.
- **_sys_netmask**—Netmask of the device.
- **_sys_use_dhcp**—DHCP status (true or false) of VLAN 1.
- **_sys_vlan_1_untag_command**—Untagged ports of VLAN 1.
- **_sys_vlan_1_tag_command**
- **_sys_stack_command**—Represents stack block.



The **_sys_template_header_** and **snmpv3 engineid "%_sys_snmpv3_engineid%"** are mandatory variables that must have the values populated, irrespective of their use in the template. If there is no value set for these variables, Aruba Central (on-premises) re-imports the values for these mandatory variables when it processes the running configuration of the device.

Example

The following table provides an example for the predefined variable definitions:

Table 130: Predefined Variables Example

Variable Name	Variable Value
_sys_oobm_command	oobm ip address dhcp-bootp exit
_sys_template_header	; J9729A Configuration Editor; Created on release #WB.16.03.0003+ ; Ver #0f:3f.f3.b8.ee.34.79.3c.29.eb.9f.fc.f3.ff.37.ef:91
_sys_hostname	HP-2920-48G-POEP
_sys_gateway	10.22.159.1
_sys_vlan_1_untag_command	1-28,A1-A2
_sys_ip_address	10.22.159.201
_sys_use_dhcp	0
_sys_module_command	module 1 type j9729a
_sys_stack_command	stacking member 1 type "J9729A" mac-address 5cb901-224c00 exit
_sys_vlan_1_tag_command	28-48
_sys_netmask	255.255.255.0
_sys_snmpv3_engineid	00:00:00:0b:00:00:5c:b9:01:22:4c:00

Downloading Sample Variables File

Aruba Central (on-premises) supports downloading and uploading variables in the JSON and CSV file formats.

To download a sample variables file:

1. From the app selector, click **Wired Management**.
 - To download a sample variables file for the group, select a template group to which the switches are assigned.
 - To download a sample variables file for a device, select the switch from the filter bar.
2. Select any of the following format:
 - JSON
 - CSV
3. Click **Download Sample Variables File**.

Uploading Variable Files

To upload a variable file, complete the following steps:

1. Click **Download Sample Variables File**. Save the JSON file with the sample variables.
2. Edit the variable file to customize the definitions.
3. Ensure that the **_sys_serial** and **_sys_lan_mac** variables are defined with the serial number and MAC address of the devices, respectively.
4. Click **Wired Management > Configuration > Variables**. The **Variables** page opens.
5. Click **Upload Variables File** and select the variable file to upload.
6. Click **Open**. The content of the variable file is displayed in the **Variables** table.
7. To search for a variable, specify a search term and click the Search icon.

Downloading Variable Files

To download the variable file applied for the devices, click the download icon in the **Variables** table.

Managing Password in Configuration Templates

All IAP and switch templates must include a password command to set a password for the device. The template cannot be saved without adding a password command. If the configuration that is pushed from Aruba Central (on-premises) to the switch does not contain a password command, the configuration push is aborted for the device and a log is added to the audit trail. For example, if you add the password command in a condition block and the condition evaluates to false, the configuration that is pushed will not contain the password command.



-
- When configuring a password, you must add the `include-credentials` command in the template. This command stores the password in the **running-config** file associated with the switch. Aruba Central (on-premises) automatically executes this command while reading the switch configuration.
 - For AOS-CX switches, you must configure the password only in plaintext.
-

Password for Switches

The following format of the passwords can be set on AOS-Switch series:

```
password manager plaintext <string>
password manager sha1 <string>
password manager sha256 <string>
password manager user-name <string> plaintext <string>
password manager user-name <string> sha1 <string>
password manager user-name <string> sha256 <string>
```

The following format of the passwords can be set on AOS-CX switches:

```
user manager group <string> password plaintext <string>
user manager password plaintext <string>
```

Password for APs

The following format of the passwords can be set on the APs:

```
mgmt-user <STRING:username:User_name> { <STRING:password:Password> }
hash-mgmt-user <STRING:username:User_name> password cleartext <STRING:cleartext_
password:Password>
hash-mgmt-user <STRING:username:User_name> password hash <STRING:hash_
password:Password>
```

Setting Password using Variables

User cannot enter the entire password line in a variable. The following examples show the valid and invalid format for entering password using a variable.

Valid format where the variable contains only the password (for example, `%pass_var% = Aruba@123`) for the device:

```
hostname "Aruba-2930M-24G"
password manager plaintext "%pass_var%"
include-credentials
no cwmp enable
```

Invalid format where the variable contains the password command (for example, `%pass_var% = password manager plaintext Aruba@123`) for the device:

```
hostname "Aruba-2930M-24G"
%pass_var%
include-credentials
no cwmp enable
```

Using Configuration Templates for AOS-Switch Management

Templates in Aruba Central (on-premises) refer to a set of configuration commands that can be used by the administrators for provisioning devices in a group. Configuration templates enable administrators to apply

a set of configuration parameters simultaneously to multiple switches in a group and thus automate switch deployments.



To minimize configuration errors and troubleshoot device-specific configuration issues, Aruba recommends that the device administrators familiarize themselves with the CLI configuration commands available on AOS-Switch.

For template-based provisioning, switches must be assigned to a template group.

Creating a Group for Template-Based Configuration

Unlike UI groups, template groups have minimal UI options and use the CLI commands to provision a device. Template groups allow you to automate switch deployments. For template-based provisioning, switches must be assigned to a group with template-based configuration method enabled.

To manage devices using configuration templates, you can create a template group and assign devices.

For more information, see [Creating a Group](#) and [Assigning Devices to Groups](#).

Creating a Configuration Template

To create a configuration template for switches:

1. In the **Network Operations** app, set the filter to a template group.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Switches**.
3. Click the **Config** icon.
The tabs to configure switches using templates is displayed.
4. Click the **Templates** tab. The Templates page is displayed.
5. Click **+** to add a new template. The **Add Template** window is displayed.
6. In the **Basic Info** tab, enter a name for the template in the **Template Name** field.
7. In the **Device Type** drop-down, select **Aruba Switch**.
8. Select the switch model and software version. You can specify any of the following combinations:
 - **ALL** for both **Model** and **Version**—To apply the template to all switch models and all supported switch software versions.
 - **ALL** for **Model** and a software version for **Version**—To apply the template to all switch models running the selected software version.
 - **ALL** for **Version** and a switch model for **Model**—To apply the template to a switch model and all software versions supported by the selected switch model.
 - A switch model and a software version—To apply the template to a specific switch model and the software version. The template created for a switch model and a software version takes precedence over the template that is created for all platforms and versions.
9. Select the manufacturing part number of the switch in the **Part Number** drop-down.



-
- The **Part Number** drop-down is displayed only if you select a switch model in the **Model** drop-down.
 - If you select a specific switch model and part number, you can apply the template to a standalone switch and not to a stack.
 - If you select **All** in the **Model** drop-down, or if you select a switch model and **All** in the **Part Number** drop-down, you can apply a template to both a standalone switch and stack.
-

10. Click **Next**. The Template tab is displayed.
11. Build a new template or import configuration information from a switch that is already provisioned in the template group.
 - To build a new template, add the switch command information in the **Template** text box. Ensure that the template text adheres to the guidelines listed in the [Important Points to Note](#).
 - To import configuration text from a switch that is already provisioned in the template group:
 - a. Click **Import Configuration As Template**.
 - b. From the search box, select the switch from which you want to import the configuration. The imported configuration is displayed in the **Template** text box.
 - c. If required, modify the configuration parameters. Ensure that the template text adheres to the guidelines listed in the [Important Points to Note](#).

-
- Importing configuration from an existing device in the template group allows you to quickly create a basic template. However, before applying the template to other switches in the group, ensure that the template text is variabilized as per your deployment requirements. For more information on variable definitions, see [Managing Variable Files](#).



- All switch templates must include a password command to set a password for the device. The template cannot be saved without adding a password command. If the configuration that is pushed from Aruba Central (on-premises) to the device does not contain a password command, the configuration push is aborted for the device and a log is added to the audit trail. For example, if you add the password command in a condition block and the condition evaluates to false, the configuration that is pushed will not contain the password command. For more information, see [Managing Password in Configuration Templates](#).

For more information about using password commands, see the Configuring Username and Password Security chapter in the *ArubaOS-Switch Access Security Guide*.

- d. To view the variables present in the imported configuration template, click **Show Variables List**. The Variables in Template column is displayed.
For more information on variables, see [Managing Variable Files](#).
 - e. To download the variables as a CSV or plain text file, click the download icon and select one of the following options:
 - **Download .CSV**
 - **Download plain text (.txt)**
12. Click **Save**. After you apply the configuration template, switches reboot and reconnect to Aruba Central (on-premises) with the new configuration.

Important Points to Note

Note the following points when adding configuration text to a template:

- The CLI syntax in the switch template must be accurate. Aruba recommends that you validate the configuration syntax on the switch before adding it to the template text.
- Ensure that the command text indentation matches the indentation in the running configuration.
- The commands in the template are case-sensitive.

The following example illustrates the case discrepancies that the users must avoid in templates and variable definitions.

```
trunk E1-E4 trk1 trunk
interface Trk1
  dhcp-snooping trust
  exit

trunk E1-E4 trk1 trunk
switch-interconnect trk1

trunk E5-E6 trk2 trunk
vlan 5
  name "VLAN5"
  untagged Trk2
  tagged Trk1
  isolate-list Trk1
  ip igmp forcedfastleave Trk1
  ip igmp blocked Trk1
  ip igmp forward Trk1
  forbid Trk1

loop-protect Trk2

trunk E1-E4 trk1 trunk
trunk E4-E5 trk2 trunk
spanning-tree Trk1 priority 4
spanning-tree Trk2 admin-edge-port

trunk A2-A4 trk1 trunk
igmp fastlearn Trk1

trunk E4-E5 trk2 trunk
ip source-binding 2 4.5.6.7 b05ada-96a4a0 Trk2

[no] ip source-binding trap OutOfResources

snmp-server mib hpSwitchAuthMIB ..

snmp-server mib hpicfMACsec unsecured-access ..

[no] lldp config <P-PORT-LIST> dot1TlvEnable ..

[no] lldp config <P-PORT-LIST> medTlvEnable ..

no lldp config <P-PORT-LIST> medPortLocation..

[no] lldp config <P-PORT-LIST> dot3TlvEnable ..

[no] lldp config <P-PORT-LIST> basicTlvEnable ..
```

```
[no] lldp config <P-PORT-LIST> ipAddrEnable <lldp-ip>

trunk-load-balance L4-based
trunk-load-balance L3-based
```

See also: [Managing Variable Files](#).

Best Practices

Aruba recommends you to follow the below steps to use configuration templates in managing switches:

1. Configure the switch.
2. Add the switch to Aruba Central (on-premises).
3. Create the template, You can use **Import template** option to import an existing template created for switches.
4. Modify the template based on the user requirement. For example, addition or removal of variables.
5. Save the edited template.

Configuring AOS-Switches in UI Groups

This section describes the configuration and viewing procedures for the switches in the UI groups.

Aruba Central (on-premises) does not support adding pre-configured switches to a UI group. Pre-configured switches that have pre-assigned UI switch groups are added to the Unassigned Devices group. To provision a pre-configured switch to a UI group or move a switch from a template group to a UI group, complete the following steps:

1. Clear the switch configuration.
 2. Delete the device from Aruba Central (on-premises).
 3. Provision the switch as a new device in a UI group.
-



To configure or view properties of the switches provisioned in UI groups, perform the following procedure:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-S** or **Config** icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name**.
The dashboard context for the switch is displayed.

- d. Under **Manage**, click **Device**.

The tabs to configure the switch is displayed.

2. Click the configuration icon to edit the switch properties. Tabs to access different configuration pages are displayed.

The following table describes the different configuration pages and their functions.

Table 131: *Tabs for Configuring AOS-Switches Provisioned in a UI Group*

Tab	Function
Switches	Configure or view general switch properties, such as, hostname, type of IP addressing, and so on. See Configuring or Viewing the Switch Properties .
Stacks	Create stacks, add members, or view stacking details such as stack type, stack id, topology and so on. See AOS-Switch Stack .
Ports	Assign or view port properties, such as, PoE, access policies, and trunk groups. See Configuring Switch Ports on AOS-Switches
PoE	Configure or view PoE settings for each port. See Configuring PoE Settings on AOS-Switch Ports .
Trunk Groups	Configure or view trunk groups and their associated properties, such as, members of the trunk group, type of trunk group and so on. See Configuring Trunk Groups on AOS-Switches in UI Groups .
VLANs	Configure or view VLANs and the associated ports and access policies. See Configuring VLANs on AOS-Switches .
Spanning Tree	Configure or view spanning tree protocol and its associated properties. See Enabling Spanning Tree Protocol on AOS-Switches in UI Groups .
Loop Protection	Configure or view loop protection and its associated properties. See Configuring Loop Protection on AOS-Switch Ports .
Access Policy	Add or view access policies. See Configuring Access Policies on AOS-Switches .
DHCP Snooping	Configure or view DHCP snooping, authorized DHCP servers IP addresses, and their associated properties. See Configuring DHCP Snooping on AOS-Switches .
Port Rate Limit	View or specify bandwidth to be used for inbound or outbound traffic for each port. See Configuring Port Rate Limit on AOS-Switches in UI Groups .
RADIUS	Configure or view RADIUS (Remote Authentication Dial-In User Service) server settings on switches. See Configuring RADIUS Server Settings on AOS-Switches .
Downloadable User Role	Enable Downloadable User Role option and configure ClearPass settings to download user-roles, policy, and class from the ClearPass Policy Manager server. See Configuring Downloadable User Role on AOS-Switches .

Tab	Function
Tunnel Node Server	Configure or view tunneled node on switches. See Configuring Tunnel Node Server on AOS-Switches .
Authentication	Configure or view 802.1X authentication and MAC authentication for switches. See Configuring Authentication for AOS-Switches .
Access/DNS	Configure or view the administrator and operator logins. See Configuring System Parameters for AOS-Switches .
Time	Configure time synchronization in switches. See Configuring Time Synchronization on AOS-Switches .
SNMP	Add or view SNMP community and its trap destination. See Configuring SNMP on AOS-Switches .
CDP	Configure CDP and its associated properties. See Configuring CDP on AOS-Switches .
Routing	Configure or view a specific routing path to a gateway. See Configuring Routing on AOS-Switches .
DHCP	Enable DHCP server and add DHCP pools on switches. See Configuring DHCP on AOS-Switches .
IGMP	Configure IGMP and its associated properties. See Configuring IGMP on AOS-Switches .
IP Client Tracker	Configure IP Client Tracker to access trusted and untrusted client networks. See Configuring IP Client Tracker on AOS-Switches .
QoS	Create QoS traffic policies. define QoS classes and change the priorities of traffic on switches. See Configuring QoS Settings on AOS-Switches .
Device Profile	Configure or view device profile and device identifier settings on switches. See Configuring Device Profile and Device Identifier on AOS-Switches .
Configuration Audit	View configuration sync errors and overrides. See Verifying Device Configuration Status .

Configuring or Viewing the Switch Properties

When you add a switch to a group, the switch inherits the configuration of the group.

It is not recommended to add a switch with an existing configuration to a group that already has a defined configuration. Aruba Central (on-premises) permits device-level overrides, however the overrides are resolved or preserved based on the requirements.

You can create a new group and add a pre-configured switch to that group so that the group inherits the configuration of the switch. If the switch inherits the group configuration, the configuration parameters are already defined. If required, you can edit these parameters. All factory default switches are provisioned in a new group and these parameters can also be defined at the group level.

To edit the configuration parameters for the switch in an UI group, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-S** or **Config** icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The tabs to configure the switch is displayed.
2. Click the **Switches** tab.
The **Switches** page is displayed with the following information:

Table 132: AOS-Switches Parameters

Name	Description	Value
MAC Address	MAC address of the switch.	Property inherited from the switch.
Hostname	Name of the host.	A string.
IP Assignment	Method of IP assignment as static or DHCP.	Static or DHCP .
IP Address	IP address for static IP assignment.	
Netmask	Netmask for static IP assignment.	
Default Gateway	Default gateway for static IP assignment.	
Location	Location of the switch.	For example: Portland, Oregon.
Contact	Email address or phone number.	For example: admin@xyzcompany.com.

3. To edit the switch configuration parameters, click the edit icon.
The Edit Switches window is displayed.
4. Edit the required parameters.



You can edit only Hostname, Location, and Contact information. Use the VLANs page to configure IP Assignment, IP address, Netmask and Default Gateway parameters. For more information, see [Configuring VLANs on AOS-Switches](#).

5. Click **OK**.
6. Click **Save Settings**.

Configuring Switch Ports on AOS-Switches

To view the port details of a switch, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-S** or **Config** icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The tabs to configure the switch is displayed.
2. Click **Interface > Ports**. The Ports page is displayed with the list of ports configured on the switch.

For AOS-Switches, the **Ports** page displays the following information:

Table 133: *Ports Page—AOS-Switches*

Name	Description	Value
Port Number	Indicates the number assigned to the switch port.	Dependent on the switch type.
Name	Name of the port for easy identification. You can add or edit port names. However, do not delete port names as it may cause config push to fail. The config push failure may also arise if you move a switch from a group configured with port names to a new group. This issue is only applicable to switch firmware versions earlier than 16.08.0002.	For example: UPLINK-SRVR-ROOM
Admin Status	Allows you to set the operational status of the port.	Up or Down
Speed-Duplex (Mbps)	Allows you to set the maximum bandwidth of the port traffic.	Select from drop-down. Default is Auto .
Tunneled	Indicates whether the port is tunneled or not.	Enable or Disable To configure a Tunnel Node Server, see Configuring Tunnel Node Server on AOS-Switches .

Name	Description	Value
DHCP Snooping	Status of port to filter DHCP messages received at the port.	Trust or Untrust See Configuring DHCP Snooping on AOS-Switches .
Access Policy (In)	Allows you to apply an existing access policy for the inbound traffic on the port.	Select from drop-down. See Configuring Access Policies on AOS-Switches .
Access Policy (Out)	Allows you to apply an existing access policy for the outbound traffic on the port.	Select from drop-down. See Configuring Access Policies on AOS-Switches .
Trunk Group	Displays the name of the trunk group to which the port is assigned.	To configure a Trunk Group, see Configuring Trunk Groups on AOS-Switches in UI Groups .

3. Select the port row, click **Edit**. The Edit Ports window is displayed.
4. Configure the required parameters.
5. Click **Save**.

Support for Flexible Modules and SFP Ports

In Aruba Central, you can manage Flexible modules and SFP ports using template and UI groups. Flexible modules and SFP ports are supported on both standalone switches and switch stacks. In the case of standalone switches in UI groups, the Flexible modules and SFP ports can be managed only if the AOS-Switches are running 16.10.0010 or later firmware versions. These ports are available for configuration at both group and device-levels.

At the group-level, the port numbers for Flexible modules and SFP ports are listed in the Ports page as alphanumeric characters (A1-A4 and B1-B4). At the device-level, only the ports that are listed in the Ports page can push the configuration updates to Aruba Central.

When you insert a new module, you might need to reboot or re-sync the device to detect the ports in Aruba Central (on-premises). If the Flexible modules and SFP ports are successfully detected, the audit trail displays the following message: **Additional Alphanumeric SFP ports are detected**. The Flexible modules and SFP ports will not be removed from Central even when the modules are removed physically from the device.

Configuring PoE Settings on AOS-Switch Ports

PoE is a technology that allows the switches to deliver power to the powered devices (PD). If you have switches provisioned in UI groups, you can enable or disable PoE operation on switch ports. The PoE page displays the configuration details of all PoE enabled ports.

To configure the PoE settings of a switch, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-S** or **Config** icon to view the switch configuration dashboard.

- To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The tabs to configure the switch is displayed.
- 2. Click **Interface > PoE**. The PoE page is displayed.
- 3. Select the port(s) you want to edit and click **Edit**.
The **Edit Power Over Ethernet Settings** window is displayed.
- 4. Configure the following parameters:

Table 134: PoE Parameters

Name	Description	Value
Port	The number assigned to the switch port. The port number is auto-generated and cannot be changed in the settings.	Auto-generated port number
PoE	The status of the PoE operation on the port. When PoE is enabled, the switch sends power to the powered device (PD).	Enabled or Disabled
Priority	The PoE priority level of the port. If there is not enough power available to provision all active PoE ports, then PoE ports at priority level as critical are powered first, then high and low priority at the last.	Low, High or Critical
LLDP MED TLV (PoE)	The status of the LLDP MED TLV configuration. Switches use LLDP to repeatedly query the PD to discover the power requirement and send the exact power required.	Enabled or Disabled
LLDP Dot3 TLV (PoE+)	The status of the LLDP Dot3 TLV configuration.	Enabled or Disabled
Allocation By	The PoE power allocation method used for the port. If usage is selected, then the allocation is made based on the automatic allocation by the PD. If class is selected, then the allocation is made based on class of the PD.	Usage or Class
Pre Std Detect	The status of support for pre-standard devices. When this option is enabled, switch supports some pre-802.3af devices.	Enabled or Disabled
Configured type	The user-defined identifier for the port to identify its intended use.	A string



The status of LLDP in PoE page is displayed as Enabled only if one or both LLDP settings (LLDP MED TLV (PoE) and LLDP Dot3 TLV (PoE+)) are enabled for the port.

5. Click **OK**.
6. Click **Save Settings**.

Configuring Trunk Groups on AOS-Switches in UI Groups

If you have switches provisioned in an UI group, Aruba Central (on-premises) enables you to configure port trunking on these switches using the UI workflows. The network administrator can configure a trunk group on switches to create one logical link or a trunk by aggregating multiple links. The trunk link functions as a high-speed link to provide increased bandwidth.

A trunk group is a set of up to eight ports configured as members of the same port trunk.

Table 135: *Trunk Group Configuration Support Per Switch Platform*

Aruba Switch Platform	Valid Trunk Groups
Aruba 2540 Switch Series	Trk1-Trk26
Aruba 2920 Switch Series Aruba 2930F Switch Series Aruba 2930M Switch Series	Trk1-Trk60
Aruba 3810 Switch Series	Trk1-Trk144

The following are some guidelines:

- All ports in the same trunk group must be of the same trunk type (LACP or trunk.)
- The names of the trunk groups include the prefix **Trk** followed by the numbers in a sequential order. For example, Trk1, Trk2 and so on.
- When STP is enabled on the switch, the STP configuration is applied for all ports at the trunk group level. Individual ports cannot be configured for STP or VLAN operation.

Adding Trunk Groups on AOS-Switches

To configure a trunk group on switches:

Ensure that the switches are onboarded and provisioned to a UI group in Aruba Central (on-premises).

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-S** or **Config** icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The tabs to configure the switch is displayed.

2. Click **Interface > Trunk Groups**. The Trunk Groups page is displayed.
3. In the **Trunk Groups** table, click **+** to add a trunk group and configure the following parameters:

Table 136: Ports Page—AOS-Switches

Name	Description	Value
Name	Indicates the number assigned to the switch port.	String.
Type	A name of the port for easy identification.	Trunk or LACP .
Untagged VLANs	If the switch ports are untagged, select a VLAN from the Untagged VLAN list.	Select from drop-down menu.
Tagged VLANs	If the switch ports are tagged, select the VLANs from the Tagged VLAN list.	Select from drop-down menu.
Ports	Select the ports for trunking. You can use up to eight ports for link aggregation. The ports in a trunk group need not be consecutive.	Select from drop-down menu.
DHCP Snooping	Select the status of port to filter DHCP messages received at the port.	Trust or Untrust . Default is Untrust .

4. Click **OK**.
5. Click **Save Settings**.

Editing Trunk Groups on AOS-Switches

To edit details of a trunk group, point to the row for the trunk group, and click the edit icon and configure the parameters.

Deleting Trunk Groups on AOS-Switches

To delete a trunk group, point to the row for the trunk group, and click the delete icon.

Configuring VLANs on AOS-Switches

The Aruba switches support the following types of VLANs:

- Port-based VLANs—In the case of trusted interfaces, all untagged traffic is assigned a VLAN based on the incoming port.
- Tag-based VLANs—In the case of trusted interfaces, all tagged traffic is assigned a VLAN based on the incoming tag.

Adding VLAN Details

By default, all ports in the Switches are assigned to VLAN 1. However, if the ports are assigned to different VLANs, the VLANs page displays their details.

To add a VLAN, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-S** or **Config** icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The tabs to configure the switch is displayed.
2. Click **Interface > VLANs**. The VLANs page is displayed.
3. In the **VLANs Settings** accordion, click **+** to add a VLAN and configure the following parameters.

Table 137: *Configuring and Viewing VLAN Parameters*

Name	Description	Value
Name	The name of the VLAN.	A string
IP Assignment	The method of IP assignment. The static option is displayed only at the device level. The options to assign Primary VLAN and Management VLAN are displayed only when you select Static or DHCP.	Static, DHCP, or Disabled Default: DHCP
IP Address	The IP address for static IP assignment. This field is enabled only when you select Static from the IP Assignment drop-down.	IPv4 address
Netmask	The netmask for static IP assignment. This field is enabled only when you select Static from the IP Assignment drop-down.	IPv4 address
DHCP Server	Indicates whether the switch is configured as the DHCP server on the VLAN. <ul style="list-style-type: none"> ■ This field is enabled only when you select Static from the IP Assignment drop-down. ■ You can enable DHCP Server option only when there are no DHCP Helper IP addresses configured. 	Toggle switch to the on or off position
DHCP Helper IP	IP address of the DHCP helper server for that VLAN. <ul style="list-style-type: none"> ■ You can configure a maximum of 16 DHCP helper IP addresses for each VLAN. ■ You can configure DHCP Helper IP addresses 	IPv4 address

Name	Description	Value
	only when DHCP Server option is disabled.	
Voice	Indicates whether support for voice VLANs are enabled for the VLAN interface.	Toggle switch to the on or off position
Primary VLAN	Indicates whether the VLAN is assigned as the primary VLAN for the switches. To assign primary VLAN, at least one tagged or untagged port should be configured. This is a mandatory field.	Toggle switch to the on or off position
Management VLAN	Indicates whether the VLAN is assigned as the management VLAN for the switches.	Toggle switch to the on or off position
Default Gateway	Default gateway for static IP assignment. This field is enabled only when you select Static from the IP Assignment drop-down.	IPv4 address
Jumbo	Indicates whether jumbo packet handling is enabled for the VLAN interface.	Toggle switch to the on or off position
Access Policy (In)	The security policy that you want to apply for the inbound traffic.	See Configuring Access Policies on AOS-Switches .
Access Policy (Out)	The security policy that you want to apply for the outbound traffic.	
VLAN Access Policy (In)	The security policy that you want to apply for the bridged and routed inbound packets on the VLAN.	
VLAN Access Policy (Out)	The security policy that you want to apply for the bridged and routed outbound packets on the VLAN.	

4. To configure the VLAN ports, complete the following steps:
 - a. In the **Ports** table, select the port number(s).
 - b. Select any of the following port modes:
 - **Tagged Ports**
 - **Untagged Ports**
 - **None**
5. To assign the VLAN to a trunk group, select the trunk group in the **Trunk Groups** table.
6. Click **OK**.
7. Click **Save Settings**.



When you upgrade to Aruba Central (on-premises) version 2.5.2, the static IP address configured at group level for VLANs is migrated to device level and preserved as overrides. The static IP assignment is available only at the device level.

Editing the VLAN Details

To edit the details of a VLAN, point to the row for the VLAN, and click the edit icon in the **Actions** column, and configure the parameters.

Deleting VLAN Details

To delete the VLAN details, complete the following steps:

1. Ensure that the VLANs are not tagged to any ports.
2. Point to the row for the VLAN, and click the edit icon in the **Actions** column.



VLAN 1 is the primary VLAN and cannot be deleted.

Configuring DHCP Relay Settings

You can configure a switch as a DHCP relay agent for transmitting DHCP messages between the DHCP server and client. You can also configure the option-82 feature for the switch to include DHCP relay information in the forwarded DHCP request messages.

To configure a switch as a DHCP relay agent, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-S** or **Config** icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The tabs to configure the switch is displayed.
2. Click **Interface > VLANs**. The VLANs page is displayed.
3. Expand the **DHCP Relay Settings** accordion.
4. To enable DHCP relay, move the **DHCP Relay** toggle switch to the on position.



DHCP Relay option is enabled by default.

5. To enable option-82 feature, move the **DHCP Relay Option 82** toggle switch to the on position.
6. Click **Save Settings**.

Enabling Spanning Tree Protocol on AOS-Switches in UI Groups

The Spanning Tree Protocol (STP) eliminates Layer 2 loops in networks, by selectively blocking some ports and allowing other ports to forward traffic, based on global (bridge) and local (port) parameters you can configure.

STP is always disabled by default on AOS-Switches. To configure STP for switches provisioned in the UI groups:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-S** or **Config** icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The tabs to configure the switch is displayed.
2. Click **Interface > Spanning Tree**. The Spanning Tree page is displayed.
3. Enable MSTP if you want to avoid bridge loops between network nodes and to maintain a single active path between the network nodes. MSTP will be enabled for all VLANs assigned to switch ports. If you have a trunk group configured for the switches in the group, MSTP is enabled at the trunk level.
4. Set the priority of the UI group.
5. To configure MSTP parameters for ports, select the port row(s) in **Port Settings**, click **Edit**.
6. To configure MSTP parameters for trunks, select the trunk group row(s) in **Trunk Group Settings**, click **Edit**.
7. Configure the following MSTP parameters for ports or trunks of individual switches:

Table 138: *Viewing or Configuring Port and Trunk Settings*

Name	Description	Value
Priority	<p>A number used to identify the root bridge in an STP instance. The switch with the lowest value has the highest priority and is the root bridge. A higher numerical value means a lower priority; thus, the highest priority is 0.</p> <p>When the switches in a network select their root bridge, two parameters are considered, the STP priority and the MAC address of the switch. All AOS-Switches have a default STP priority of 8. So the switch with the lowest MAC automatically gets selected as a root bridge. This is not a recommended process as it randomizes the selection of the root bridge.</p>	0 – 8 Default: 8
BPDU Protection	A security feature used to protect the active STP topology by preventing spoofed BPDU packets from entering the STP domain. In a typical implementation, BPDU protection is applied to the edge ports and access ports connected to end-user devices that do not run STP. If STP BPDU packets are received on a protected port, the port is disabled and the network manager is alerted via SNMP traps.	Enable or Disable Default: Disable

Name	Description	Value
BPDU Filter	<p>Enables control of STP participation for each port. The feature can be used to exclude specific ports from becoming part of STP operations. A port with the BPDU filter enabled ignores incoming BPDU packets and stays locked in the STP forwarding state. All other ports maintain their role.</p> <p>Recommended ports for BPDU filter: Ports or trunks connected to client devices.</p>	Enable or Disable Default: Disable
Admin-Edge	<p>When set, the port directly goes into forwarding state. This configuration is not recommended for ports which connect to infrastructure devices. A BPDU guard also assists when a port inadvertently goes into a forwarding state.</p>	Enable or Disable Default: Disable
Root Guard	<p>Sets the port to ignore superior BPDUs to prevent the switch from becoming the Root Port.</p>	Enable or Disable Default: Disable
Trunk Group	<p>Sets the trunk group to which the port is assigned.</p>	Enable or Disable Default: Disable

Configuring Loop Protection on AOS-Switch Ports



Enabling Loop Protection consumes CPU resources.

Loop protection provides protection against loops by transmitting loop protocol packets out of ports. For switches provisioned in UI groups, administrators can enable or disable loop protection on the switch ports or trunks by using the menu options available under **Network Operations** app, **Manage > Device(s) > Switches**.

Loop protection is always disabled by default on AOS-Switches. To configure loop protection for switches provisioned in the UI groups:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **Config** icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The tabs to configure the switch is displayed.
2. Click **Interface > Loop Protection**. The Loop Protection page is displayed.

3. Depending on whether you want to configure a port or trunk, complete one of the following steps:
 - In the **Port Settings** tab, select the port(s), click **Edit**.
 - In the **Trunk Group Settings** tab, select the trunk(s), click **Edit**.

Table 139: *Viewing or Configuring Port Settings*

Name	Description	Value
Port	The number assigned to the switch port.	0 – 65535
Loop Protection	Enables or disables loop protection.	Enable or Disable Default: Disable
Trunk Group	Name of the trunk group to which the port belongs.	Dependent on the switch type.

Table 140: *Viewing or Configuring Trunk Settings*

Name	Description	Value
Trunk Group	Name of the trunk group to which the port belongs.	Dependent on the switch type.
Loop Protection	Enables or disables loop protection.	Enable or Disable Default: Disable

4. Set loop protection to **Enable** in the Loop Protection drop-down.
5. Click **OK**.
6. To auto-recover ports when the switch detects a loop, configure the following parameters.
 - **Disable Timer**—Move the toggle switch to the on position to send an SNMP trap when a port detects a disabled loop and manually re-enables the loop.
 - **Time (in secs)**—Configure the time to auto-enable the **Disable Timer**. This field supports integers between 1 to 604800.
7. Click **Save Settings**.

Configuring Access Policies on AOS-Switches

To restrict certain types of traffic on physical ports of AOS-Switches, you can configure ACLs from the Aruba Central (on-premises) UI.

To create an access policy, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch.
The dashboard context for the group is displayed.
 - b. Under Manage, click **Devices** > **Switches**.
 - c. Click the **AOS-S** or **Config** icon to view the switch configuration dashboard.

- To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under Manage, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The tabs to configure the switch is displayed.
- 2. Click **Security > Access Policy**. The Access Policy page is displayed.
- 3. Click + to add a new access policy. The **New Access Policy** page is displayed.
- 4. Enter a name for the policy.
- 5. Click **Add**.
- 6. To add a rule to the access policy, click + under **Rules for test**, and configure the following parameters:

Table 141: *Configuring Rules for Access Policies*

Name	Description	Value
Source	Select a source of the traffic for which you want to an access rule.	Any, Network, or Host <ul style="list-style-type: none"> ■ For Network, specify IP address and mask ■ For Host, specify IP address
Destination	Select a destination.	Any, Network, or Host <ul style="list-style-type: none"> ■ For Network, specify IP address and mask ■ For Host, specify IP address
Protocol	Select the type of protocol from the drop-down. If you select SCTP, TCP, or UDP , the Source Port and Destination Port fields are displayed.	SCTP, TCP, UDP, AH, ESP, GRE, ICMP, IGMP, IP, IPv6_IN_IP, IP_IN_IP, OSPF, PIM, and VRRP.
Source Port	Port number of the source for SCTP, TCP, or UDP protocols.	Single or range of port numbers. <ul style="list-style-type: none"> ■ For single port number, use the same port number in the Min Port and Max Port number fields.
Destination Port	Port number of the destination for SCTP, TCP, or UDP protocols.	Single or range of port numbers. <ul style="list-style-type: none"> ■ For single port number, use the same port number in the Min Port and Max Port number fields.
Action	The action that the switch must perform on the traffic received at a port.	Permit or Deny

7. Click **OK**.
8. Click **Save Settings**.

The access policies must be applied to a switch port and the VLAN assigned to a port. For more information on access policy assignment to ports and VLANs, see the following topics:

- [Configuring Switch Ports on AOS-Switches](#)
- [Configuring VLANs on AOS-Switches](#)

Configuring DHCP Snooping on AOS-Switches

DHCP snooping provides network security by filtering untrusted DHCP messages. Filtering is performed by distinguishing trusted ports connected to a DHCP server or switch and untrusted ports connected to end-users.

When you enable DHCP snooping, DHCP packets received at untrusted ports will be dropped, because all ports are configured as untrusted by default. You must configure the ports to be trusted in the **Switches > Interface > Ports** page.

You must also configure authorized DHCP servers for the network to have a functional DHCP server that serves clients on this switch.

By default, DHCP snooping is disabled for the switch.

Enabling DHCP Snooping on a Switch

To enable DHCP snooping on a switch, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-S** or **Config** icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The tabs to configure the switch is displayed.
2. Click **Security > DHCP Snooping**. The DHCP Snooping page is displayed.
3. To enable DHCP snooping for the switch, move the **DHCP Snooping** toggle switch to the on position.
4. To enable option-82 for the switch, move the **DHCP Snooping Option-82** toggle switch to the on position.
5. When you enable both DHCP snooping and option-82, the switch drops the option-82 information from the DHCP packets.
6. Click **Save Settings**.

Adding Authorized DHCP Servers for a Switch

To add the list of IP addresses of authorized DHCP servers for a switch, complete the following steps:

1. In the **DHCP Snooping** page, click + in the **Authorized DHCP Servers IP** table. The Add Authorized DHCP Server IP window is displayed.

2. Enter the IP address in the **Authorized DHCP Servers IP** field.
3. Click **OK**.
4. Click **Save Settings**.

Deleting Authorized DHCP Servers for a Switch

To delete the authorized DHCP servers IP addresses, in the **Authorized DHCP Servers IP** table, point to IP address, and click the delete icon for the DHCP server IP you want to delete.

Enabling DHCP Snooping for a VLAN

To enable DHCP snooping for a VLAN, complete the following steps:

1. In the **DHCP Snooping Settings** table, select the VLAN row(s) for which you want to configure DHCP snooping, and click **Edit**.
2. Select **Enable** or **Disable** from the **DHCP Snooping** drop-down.
3. Click **OK**.
4. Click **Save Settings**.

Configuring Port Rate Limit on AOS-Switches in UI Groups

Rate limiting allows allocating a specific bandwidth for the incoming and outgoing traffic from each port. When traffic exceeds the configured limit, it is dropped. This effectively sets a usage level on a given port and is a tool for enforcing maximum service level commitments granted to network users. This feature operates on a per-port level and is not configurable on port trunks. Rate-limiting is designed to be applied at the network edge to limit traffic from non-critical users or to enforce service agreements such as those offered by Internet Service Providers (ISPs) to provide only the bandwidth for which a customer has paid.

Port rate limit is always disabled by default on Aruba switches. To configure port rate limit for switches provisioned in the UI groups:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-S** or **Config** icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The tabs to configure the switch is displayed.
2. Click **Security > Port Rate Limit**. The Port Rate Limit page is displayed.
3. Under **Port Rate Limit**, select the port or ports you want to modify and click **Edit**.
4. Set the value of **Limit** to **Traffic by Category** if you prefer to set individual limitations. Else, set the value of **Limit** to **All Traffic** to set a collective limitation.



Percentage limits are based on link speed. For example, if a 100 Mbps port negotiates a link at 100 Mbps and the inbound rate-limit is configured at 50%, then the traffic flow through that port is limited to no more than 50 Mbps. Similarly, if the same port negotiates a 10 Mbps link, then it allows no more than 5 Mbps of inbound traffic. Configuring a rate limit of 0 (zero) on a port blocks all traffic on that port. However, if this is the desired behavior on the port, disable the port instead of configuring a rate limit of 0.

- a. If you select **All Traffic**, rate limit is placed on all packets received from unknown sources. Move the slider to **Enable** and then enter the values for **IN** and **OUT** in percentage values.
- b. If you select **Traffic by Category**, refer to the following table to set the correct parameters.

Table 142: *Traffic by Category Parameters*

Name	Description	Value
Broadcast	Sets a rate limit on broadcast traffic.	Expressed as percentage of the total bandwidth.
Multicast	Indicates the operational status of the port.	
Unknown Unicast	Indicates the mode of operation. The port can be configured to function in Trunk or Access mode.	
ICMP	Sets a rate limit on ICMP traffic.	

Configuring RADIUS Server Settings on AOS-Switches

Aruba Central (on-premises) allows you to configure RADIUS (Remote Authentication Dial-In User Service) server settings on switches.

To configure a RADIUS server, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-S** or **Config** icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The tabs to configure the switch is displayed.
2. Click **Security > RADIUS**. The RADIUS page is displayed.
3. Click **+** to add a RADIUS server. The Add RADIUS Server window is displayed.
4. Configure the following parameters.

Table 143: RADIUS Parameters

Name	Description	Value
Server IP	The IP address of the RADIUS server.	
Port	The destination port for authentication requests to the specified RADIUS server.	Default: 1812
Shared Key	The encryption key for use during authentication sessions with the specified RADIUS server.	
Confirm Shared Key	Retype the shared key.	
Dynamic Authorization	Indicates whether the dynamic authorization is enabled. When enabled, the RADIUS server can dynamically terminate or change the authorization parameters used in an active client session on the switch.	Toggle switch to the on or off position
ClearPass Server	Indicates whether the ClearPass server is enabled on the RADIUS server.	Toggle switch to the on or off position

5. Click **Save**.

Editing a RADIUS Server Settings

To edit a RADIUS server, point to the row for the server, and click the edit icon.

Deleting a RADIUS Server Settings

To delete a RADIUS server, point to the row for the server, and click the delete icon.

Configuring Downloadable User Role on AOS-Switches

Aruba Central (on-premises) allows you to enable Downloadable User Role and configure ClearPass settings to download user-roles, policy, and class from the ClearPass Policy Manager server.



Downloadable User Role configuration is not supported on Aruba 2530 Switch Series.

To enable Downloadable User Role and configure ClearPass server settings, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch. The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-S** or **Config** icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**. A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name**. The dashboard context for the switch is displayed.

- d. Under **Manage**, click **Device**.
The tabs to configure the switch is displayed.
2. Click **Security > Downloadable User Role**. The Downloadable User Role page is displayed.
3. Slide the **Downloadable User Role** toggle switch to on position to allow switch to download user-roles.



To enable downloadable user role, ClearPass server must be configured in the **RADIUS** page. The **Downloadable User Role** toggle is disabled if ClearPass server is not enabled for any of the RADIUS settings. For more information, see [Configuring RADIUS Server Settings on AOS-Switches](#).

4. Configure the following ClearPass Settings:

Table 144: *ClearPass Settings*

Name	Description
User Name	Enter the ClearPass Policy Manager administrator username.
Password	Enter the password to access ClearPass server.
Confirm Password	Retype the password.
Retry Interval	Specify the retry interval to download TA certificate. This certificate is used to authenticate ClearPass server before downloading the user-role. Range: 0-5.

5. Click **Save Settings**.

Configuring Authentication for AOS-Switches

Aruba Central (on-premises) supports enabling 802.1X and MAC authentication for switches. You can enable and configure 802.1X authentication of clients at the switch and port level, and enable authentication of 802.1X access through a RADIUS server using either EAP or CHAP protocol. You can also enable and configure ports to authenticate clients based on MAC addresses.

See the following topics for more information on authentication:

- [Configuring 802.1X Authentication](#)
- [Configuring MAC Authentication](#)
- [Configuring Authentication Order and Priority](#)

Configuring 802.1X Authentication

802.1X is a method for authenticating the identity of a user before providing network access. Aruba Central (on-premises) supports internal RADIUS server and external RADIUS server for 802.1X authentication.

To configure 802.1X authentication for the switch, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch.
The dashboard context for the group is displayed.

- b. Under **Manage**, click **Devices > Switches**.
- c. Click the **AOS-S** or **Config** icon to view the switch configuration dashboard.
- To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The tabs to configure the switch is displayed.
- 2. Click **Security > Authentication**. The Authentication page is displayed.
- 3. Expand the **802.1X Authentication** accordion.
- 4. To enable 802.1x Authentication at group level in the group context, slide the toggle switch to on position.
- 5. In the **Authentication Method** from the drop-down, select either **EAP** or **CHAP**.



If you select EAP or CHAP, you must configure the RADIUS server.

The Port Settings table displays the number of ports and the parameters configured for the ports.

- 6. Select one or more ports for which you want to enable 802.1X authentication, and click the edit icon. The Edit Ports Selected window is displayed.
- 7. Select **Enable** from the **802.1X** drop-down.
- 8. Configure the following parameters.

Table 145: *Configuring 802.1X Authentication*

Name	Description	Value
Client Limit	The maximum number of clients to allow on the port.	Default: 0
Unauthorized VLAN ID	The VLAN to use for an unauthorized client.	Default: 0
Authorized VLAN ID	The VLAN to use for an authorized client.	Default: 0
Reauth Period	The time (in seconds) that the switch enforces on a client to re-authenticate. The client remains authenticated while the re-authentication occurs. When set to 0, re-authentication is disabled.	Default: 300 seconds
Cached Reauth Period	The time (in seconds) when cached re-authentication is allowed on the port.	Default: 0
Log off Period	The time (in seconds) that the switch enforces for an implicit logoff.	Default: 300 seconds

Name	Description	Value
Quiet Period	The time (in seconds) during which the port does not try to acquire a supplicant. The period begins after the last attempt authorized by the max-requests parameter fails.	Default: 60 seconds
Tx Period	The time (in seconds) the port waits to retransmit the next EAPOL PDU during an authentication session.	Default: 30 seconds
Server Timeout	The time (in seconds) that the switch waits for a server response to an authentication request	Default: 300 seconds
Supplicant Timeout	The time (in seconds) that the switch waits for a supplicant response to an EAP request. If the supplicant does not respond within the configured time frame, the session times out.	Default: 300 seconds

9. Click **Save Settings**.

Configuring MAC Authentication

MAC authentication is used for authenticating devices based on their physical MAC addresses. For MAC authentication, the MAC address of a machine must match an approved list of manually defined addresses on the switch.

MAC authentication can be used alone or it can be combined with 802.1X authentication.

To configure MAC authentication for the switch ports, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-S** or **Config** icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The tabs to configure the switch is displayed.
2. Click **Security > Authentication**.
3. In the **Authentication** tab, expand the MAC Authentication accordion. The Port Settings table displays the parameters configured for the port.
4. Select one or more ports for which you want to enable MAC authentication and click the edit icon. The Edit Ports Selected window is displayed.
5. Select **Enable** from the **MAC Auth** drop-down.

- Configure the following parameters.

Table 146: *Configuring MAC Authentication*

Name	Description	Value
Client Limit	The maximum number of clients to allow on the port.	Default: 0
Unauthorized VLAN ID	The VLAN to use for an unauthorized client.	Default: 0
Authorized VLAN ID	The VLAN to use for an authorized client.	Default: 0
Reauth Period	The time (in seconds) that the switch enforces on a client to re-authenticate. The client remains authenticated while the re-authentication occurs. When set to 0, re-authentication is disabled.	Default: 300 seconds
Cached Reauth Period	The time (in seconds) when cached re-authentication is allowed on the port.	Default: 0
Log off Period	The time (in seconds) that the switch enforces for an implicit logoff.	Default: 300 seconds
Quiet Period	The time (in seconds) during which the port does not try to acquire a supplicant. The period begins after the last attempt authorized by the max-requests parameter fails.	Default: 60 seconds

- Click **Save Settings**.

Configuring Authentication Order and Priority

Users can set the authentication order and priority for the 802.1X and MAC authentication methods for each port. The switch attempts to authenticate a client based on the authentication order and priority settings.

- If both 802.1X and MAC authentication are enabled on the same port without configuring authentication order and priority, then both the authentication methods are triggered in parallel and might cause issues for the clients.
- If authentication order and priority are configured, then authentication requests are processed sequentially and authentication method with high priority is used to access the client. If both 802.1X and MAC authentication are enabled on the same port, and 802.1X authentication is set as the first authentication method and MAC authentication is set as the first authentication priority, then MAC authentication is used to authenticate the clients.
- If only one authentication method is enabled on the port, then the switch will not consider authentication order and priority for authentication.



Authentication order and priority configuration is not supported on the Aruba 2920 Switch Series.

To configure the authentication order and priority, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-S** or **Config** icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The tabs to configure the switch is displayed.
2. Click **Security > Authentication**. The Authentication page is displayed.
3. Expand the **Authentication Order and Priority** accordion. The Ports Settings table displays the Authentication Order and Authentication Priority specified for the ports.
4. Click + to add ports with authentication order and priority. The Add Ports window is displayed.
5. Configure the following parameters:
 - **Ports**—Select one or more ports for setting authentication order and priority.
 - **Authentication Order**—Select either **802.1X** or **MAC** as the first method for authentication. For example, if you select **802.1X** as the first authentication method, then **802.1X** is used first for authenticating clients on the port.
 - **Authentication Priority**—Select either **802.1X** or **MAC** as the first priority for authentication. Authentication priority takes precedence over authentication order, and the authentication method with higher priority is used to access clients.
6. Click **Save**.

Editing the Authentication Order and Priority

To edit the authentication order and priority, select one or more ports for which you want to modify authentication order and priority, and click the edit icon.



When editing multiple ports, if authentication order and priority are different on ports, then the existing settings are preserved. You can override the existing settings by selecting an order or a priority.

Deleting the Authentication Order and Priority

To delete the authentication order and priority, select one or more ports for which you want to delete authentication order and priority, and click the delete icon.

Configuring Tunnel Node Server on AOS-Switches

Aruba Central (on-premises) allows you to configure tunneled node on switches. The tunneled node connects to one or more client devices at the edge of the network and then establishes a secure Generic Routing Encapsulation (GRE) tunnel to the controlling concentrator server. You can configure either Port-Based Tunnel or User-Based Tunnel using UI groups.



To modify the reserved VLAN, change the mode to **No Tunnel** and click **Save Settings**, then change the mode back to **User-Based Tunnel**.

The **Tunnel Node Server** configuration cannot be modified when tunneled clients are active.

To configure a tunneled node on the switch, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-S** or **Config** icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The tabs to configure the switch is displayed.
2. Click **Security > Tunnel Node Server**. The Tunnel Node Server page is displayed.
3. Configure the following parameters.

Name	Description	Value
Mode	The mode of tunneling from the drop-down: <ul style="list-style-type: none">■ No Tunnel—switch does not tunnel traffic.■ Port Based Tunnel—Allows the switch to tunnel traffic to an Aruba controller on a per-port basis.■ User-Based Tunnel—Allows the switch to tunnel traffic to an Aruba controller on an assigned user role basis.	Port- Based Tunnel , User-Based Tunnel, or No Tunnel
Primary Gateway IP	The IP address of the primary gateway.	A valid IPv4 address
Backup Gateway IP	The IP address of the backup gateway. This field is optional.	A valid IPv4 address
Reserved VLAN	The reserved VLAN ID to tunnel traffic to an Aruba controller. This field is available only for User-Based tunnel. The default VLAN or a VLAN that is already configured cannot be used as a reserved VLAN. To view the list of configured VLANs, navigate to Interface > VLANs .	Numeric value

4. Click **Save Settings**.

For more detailed information, refer to Dynamic Segmentation white paper at https://www.arubanetworks.com/assets/so/SO_Dynamic-Segmentation.pdf

Configuring System Parameters for AOS-Switches

The **System** menu under **Switches** allows you to configure administrator credentials and enable mode for the switch users.

Configuring Administrator and Operator Credentials for AOS-Switches

To configure administrator credentials for AOS-Switches, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-S** or **Config** icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The tabs to configure the switch is displayed.
2. Click **System > Access/DNS**. The **Access/DNS** page is displayed.
3. Enter the username for the administrator user in the **Admin Username** text box.
4. Enter the password for admin in the **Admin Password** text box and confirm the administrator password.
5. To configure the operator user credentials, complete the following steps:
 - a. Select the **Set Operator Username** check box.
 - b. Enter a username and password for the operator user.
 - c. Confirm the password.
6. Click **Save Settings**.

Configuring a Name Server

To set a static IP for switches, you must configure a name server. To configure a name server, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-S** or **Config** icon to view the switch configuration dashboard.

- To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The tabs to configure the switch is displayed.
- 2. Click **System > Access/DNS**.
The **Access/DNS** page is displayed.
- 3. From the **Name Server** drop-down, select **DHCP** or **Static**. The default option is **DHCP**.



-
- You must add at least one DNS server IP address, when you select **Static** in the drop-down.
 - You can add only a valid IPv4 address.
 - You can add a maximum of two DNS server IP addresses.
 - The first static IP address that you add is considered as priority. The second IP address that you add is considered secondary.
-

- a. Enter the static IPv4 address of the DNS server in the text box.
 - b. Click the + add icon.
 - c. To delete a static IP address, click the  delete icon.
If two IP addresses are configured, you can first delete the second priority IP address.
4. Click **Save Settings**.

Configuring Time Synchronization on AOS-Switches

Time synchronization in a switch ensures maintaining a uniform time among all interoperating devices. Aruba Central (on-premises) offers the Simple Network Time Protocol (SNTP) time synchronization protocol for switches. In SNTP, Aruba Central (on-premises) supports broadcast, unicast, and DHCP modes.

Time synchronization in a switch ensures maintaining a uniform time among all interoperating devices. Aruba Central (on-premises) offers the following time synchronization protocols for switches:

- Network Time Protocol (NTP)
- Simple Network Time Protocol (SNTP)

To configure time synchronization in a switch, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-S** or **Config** icon to view the switch configuration dashboard.

- To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The tabs to configure the switch is displayed.
- 2. Click **System > Time**. The Time page is displayed.
- 3. Configure the following parameters.

Table 147: *Configuring Time Synchronization Parameters*

Name	Description	Value
Time Sync Method	The synchronization method or protocol to use for synchronizing the time on the switch.	SNTP Default: NTP
Mode	<p>The operating mode for connecting to a time server. The following modes are supported:</p> <ul style="list-style-type: none"> ■ Broadcast—The switch acquires time updates from the data that any time server broadcasts to the network. The switch uses the time data from the first server detected and ignores others. If the poll interval expires thrice without the switch acquiring a time update from the first server detected, the switch accepts a time update from the next server broadcast. <p>NOTE: To use the Broadcast mode, the switch and the time server must be in the same subnet. Also, the time server must be configured to broadcast time updates to the network broadcast address.</p> <ul style="list-style-type: none"> ■ Unicast—The switch acquires time updates from a specific server for time synchronization. This mode requires at least one server address to be configured in the Server Address field. ■ DHCP—The switch attempts to acquire a time server IP address from the DHCP server. If the switch receives a server address, it polls the server for time updates according to the poll interval. If the switch does not receive a time server IP address, it cannot perform time synchronization updates. This mode is applicable only for SNTP. ■ Disabled—Time synchronization is disabled. You cannot disable synchronization if NTP is selected. 	<p>SNTP Supported modes: Broadcast, Unicast, DHCP, and Disabled Default mode: DHCP</p> <p>NTP Supported modes: Broadcast, Unicast Default mode: Broadcast</p> <p>Default: DHCP</p>
Server Address	IP address of the time server that the switch accesses for obtaining time synchronization updates. This field is applicable only when you select the Unicast mode for synchronization.	IPv4 address

Name	Description	Value
	<p>You can configure a maximum of three time server IP addresses. When you add more than one IP address, the priority that the switch considers in selecting the IP address is the order in which you add the IP address. Therefore, the first IP address that you add will be priority 1, second IP address will be priority 2, and so on.</p> <p>You can delete the IP addresses by clicking the delete icon corresponding to the address. When more than one IP addresses are added, you must first delete the IP address you added last.</p>	
Timezone	The time zone corresponding to the location of the switch.	Time zone selected from the drop-down.
Daylight Time Rule	<p>The rule that the switch uses to adjust the time for Daylight Saving Time (DST). For information about the predefined and user-defined times, see Predefined DST Rules.</p> <p>When you select the User-defined option, you must configure the beginning and ending months and dates for DST changes in the Begin Month and Day and End Month and Day fields. All DST rules begin and end at 2 a.m. on the configured dates.</p>	Alaska, Canada and Continental US, Middle Europe and Portugal, Southern Hemisphere, Western Europe, and User-defined.
Begin Month and Day	The beginning month and date for the user-defined DST changes. This field appears only when you select User-defined in the Daylight Time Rule field.	Month and date selected from the drop-down.
End Month and Day	The ending month and date for the user-defined DST changes. This field appears only when you select User-defined in the Daylight Time Rule field.	Month and date selected from the drop-down.

4. Click **Save Settings**.

Predefined DST Rules

Following are the details of the beginning and ending days for the predefined DST rules:

Predefined DST Rule Name	Description
Alaska	<ul style="list-style-type: none"> ■ Begin DST at 2 a.m. on March 8. ■ End DST at 2 a.m. on November 1.
Canada and Continental US	
Middle Europe and Portugal	<ul style="list-style-type: none"> ■ Begin DST at 2 a.m. on March 25. ■ End DST at 2 a.m. on September 24.
Southern Hemisphere	<ul style="list-style-type: none"> ■ Begin DST at 2 a.m. on October 25. ■ End DST at 2 a.m. on March 1.
Western Europe	<ul style="list-style-type: none"> ■ Begin DST at 2 a.m. on March 25. ■ End DST at 2 a.m. on October 25.

Configuring SNMP on AOS-Switches

Simple Network Management Protocol (SNMP) is an Internet-standard protocol used for managing and monitoring the devices connected to a network by collecting, organizing and modifying information about managed devices on IP networks.

In Aruba Central (on-premises), you can configure either SNMP versions V2C or V3 using UI groups. By default, SNMP is disabled on the AOS-Switches.



SNMP settings can be configured only when a switch is installed with the firmware version of 16.09 or later.

For more information, see the following topics:

- [Configuring SNMPv2c on AOS-Switches](#)
- [Configuring SNMPv3 on AOS-Switches](#)
- [Disabling SNMP on AOS-Switches](#)

Configuring SNMPv2c on AOS-Switches

You can configure SNMPv2c community settings and trap settings through the UI.

To enable SNMPv2c on a switch, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-S** or **Config** icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name**.
The dashboard context for the switch is displayed.
 - a. Under **Manage**, click **Device**.
The tabs to configure the switch is displayed.
2. Click **System > SNMP**. The SNMP page is displayed.
3. Select **SNMP mode** as **V2C** from the drop-down to enable SNMPv2C. Changing SNMP mode from V3 to V2C displays a confirmation message window stating that changing SNMP mode will remove existing SNMP configuration.

Changing SNMP mode from **V3** to **V2C** displays a confirmation message window stating that changing SNMP mode will remove existing SNMP configuration. Type REMOVE in the text box and click **Proceed**.

Configuring Community Settings

You can add or delete SNMP communities to restrict access to the switch.

Adding a Read Community

To add an SNMP community, complete the following steps:

1. In the **SNMP** page, expand the **Community Settings** accordion.
The **Read Community** table displays the list of communities that have read-only access.
2. To add a read community, click **+**. The Add Community window is displayed.
3. Enter the name of the community in the **Community** text box and click **OK**.

Deleting a Read Community

To delete a read community, point to the row for the trap destination, and click the delete icon.

Configuring Trap Settings

You can configure authentication, trap destination, and trap categories using trap settings.

Adding a Trap Destination

To add a trap destination, complete the following steps:

1. In the **SNMP** page, expand the **Trap Settings** accordion.
2. To add a read destination, click **+**. The Add Trap Destination window is displayed.
3. Configure the following parameters:
4. The **Trap Destination** table displays the following information:
 - **Destination IP**—The destination IP address for sending the trap.
 - **Community**—The community name used for sending the trap.
5. Click **OK**

Deleting a Trap Destination

To delete a trap destination, point to the row for the trap destination, and click the delete icon.

Enabling Trap Categories

To enable trap categories, complete the following steps:

1. In the **Trap Settings** accordion, select the authentication type used to connect to the SNMP server from the **Authentication** drop-down.
2. In the **Trap Category** table, select the checkbox for the trap category you want to enable.
3. Click **Save Settings**.



The availability of trap categories differs based on the device model.

Configuring SNMPv3 on AOS-Switches

SNMPv3 provides a secured access to SNMP management stations using authentication and privacy protocols. You can add SNMPv3 user and configure notification settings using UI groups.

To enable SNMPv3 on a switch, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-S** or **Config** icon to view the switch configuration dashboard.

- To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name**.
The dashboard context for the switch is displayed.
 - a. Under **Manage**, click **Device**.
The tabs to configure the switch is displayed.
- 2. Click **System > SNMP**. The SNMP page is displayed.
- 3. Select **SNMP mode** as **V3** from the drop-down to enable SNMPv3.
Changing SNMP mode from **V2C** to **V3** displays a confirmation message window stating that changing SNMP mode will remove existing SNMP configuration. Type REMOVE in the text box and click **Proceed**.



You must add at least one user to enable SNMPv3.

Configuring User Settings

You can add SNMPv3 users to provide secured access to SNMP management stations.

Adding an SNMPv3 User

To add an SNMPv3 user, complete the following steps:

1. In the **SNMP** page, expand the **User/Notification Settings** accordion.
The **Users** table displays the list of users with associated authentication mode and privacy mode.
2. To add an SNMPv3 user, click +. The Add User window is displayed.
3. Configure the following parameters:
 - **User Name**—Enter the user name.
 - **Authentication Mode**—Select either **MD5** (Message Digest) or **SHA** (Secure Hash Algorithm) as the authentication mode to provide secured access to the user.
 - **Password**—Enter the authentication password.
 - **Confirm Password**—Re-enter the authentication password.
 - **Privacy Mode**—Select **AES** (Advanced Encryption Standard) or **DES** (Data Encryption Standard) as the privacy mode to provide secured access to the user.
 - **Privacy Password**—Enter the privacy password.
 - **Confirm Privacy Password**—Re-enter the privacy password.
4. Click **OK**.

Editing an SNMPv3 User

To edit an SNMPv3 user, point to the row for the user, and click the edit icon.

Deleting an SNMPv3 User

To delete an SNMPv3 user, point to the row for the user, and click the delete icon.

Configuring Notification Settings

You can configure notification settings to send notifications to SNMPv3 users.

Adding an SNMPv3 Notification

To add a notification, complete the following steps:

1. In the **SNMP** page, expand the **User/Notification Settings** accordion. The **Notifications** table displays the list of users with associated IP addresses for sending notifications.
2. To add a notification, click **+**. The Add Notification window is displayed.
3. Configure the following parameters:
 - **IP address**—Enter the destination IP address for sending notifications.
 - **User Name**—Select the user to whom the notifications should be sent.
4. Click **OK**.

Editing an SNMPv3 Notification

To edit a notification, point to the row for the notification, and click the edit icon.



You can edit only the user name.

Deleting an SNMPv3 Notification

To delete an SNMPv3 user, point to the row for the notification, and click the delete icon.

Enabling Trap Categories

To enable trap categories, complete the following steps:

1. In the **Trap Settings** accordion, select the authentication type used to connect to the SNMP server from the **Authentication** drop-down.
2. In the **Trap Category** table, select the checkbox for the trap category you want to enable.
3. Click **Save Settings**.



The availability of trap categories differs based on the device model.

Disabling SNMP on AOS-Switches

You can disable SNMP on AOS-Switches. Disabling SNMP will remove all the existing SNMP configurations.

To disable SNMP, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch. The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-S** or **Config** icon to view the switch configuration dashboard.

5. Click **Save Settings**.

Configuring DHCP on AOS-Switches

Dynamic Host Configuration Protocol (DHCP) is a protocol that enables a server to automatically assign IP addresses to hosts. The server uses the configured IP address pools or ranges to assign to hosts. You can configure multiple IP pools to not have duplicate or overlapping IP subnets. You can configure the IP address pools with various options to share with the hosts. For example, network address, subnet mask, DNS server address.



In Aruba Central (on-premises) 2.5.3, **DHCP Pools** configuration is renamed to **DHCP** and moved from the **IP Settings** tab to the **System** tab.

To enable the DHCP service and to add DHCP pools on a switch, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **Config** icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The tabs to configure the switch is displayed.
2. Click **System > DHCP**. The DHCP page is displayed.



If any of the devices is running a lower version, a warning message is displayed, and the DHCP configuration changes are pushed only to the devices that support the DHCP. If the devices are upgraded to a supported version or moved out of the group, the warning message will not be displayed.

3. To activate the DHCP service, move the **Enable DHCP service** toggle switch to the on position.
The DHCP service can be enabled only if there is a valid DHCP pool.
4. To add a new DHCP pool, click + and configure the following parameters:

Table 148: *Configuring a DHCP Pool*

Name	Description	Value
Name	Name of the pool.	A string.

Name	Description	Value
Network	A valid network IP address to assigned to the DHCP pool.	IPv4 address
Netmask	Netmask of the DHCP pool.	Subnet mask
Lease Time	The lease time for the DHCP pool in days-hours-minutes format.	You can set a maximum value of 365 days 23 hours and 59 minutes in the DD-HH-MM format.
Default Router	IP address of the default router in the subnet.	You can add up to 8 IP addresses.
DNS Server	Address of the DNS server. To add multiple DNS servers, click +.	You can add up to 8 DNS servers.
Netbios Server	Address of the Netbios server. To add multiple Netbios servers, click +.	You can add up to 8 Netbios servers.
IP Address Range	IP address range within the network and network mask combination. To add multiple IP address range, click +.	You can add up to 64 IP address range.
Option	The code type, and ASCII or HEX value of the DHCP option to configure. To add multiple options, click +.	You can add up to 8 options. A value within the range of 2-254 with type as hexadecimal and ASCII is valid.

5. Click **Add**.
6. Click **Save Settings**.
7. To edit the details of a DHCP pool, point to the row for the DHCP pool, and click the edit icon in the **Edit** column, and configure the parameters.
8. To delete a DHCP pool, point to the row for the DHCP pool, and click the delete icon in the **Delete** column. Click **Yes** in the confirmation window.

Configuring IP Client Tracker on AOS-Switches

The IP Client tracker module identifies both trusted and untrusted clients that access the system. This feature is available for AOS-Switch 2930F, 2930M, and 3810 switches.



NOTE

This feature is supported on AOS-Switch version 16.10.0008 and later.

To configure IP client tracker, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-S** or **Config** icon to view the switch configuration dashboard.

- To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The tabs to configure the switch is displayed.
- 2. Click **System > IP Client Tracker**. The IP Client Tracker page is displayed.
- 3. To enable the client tracker move the **IP Client Tracker** toggle to on position.



The **IP Client Tracker** is disabled by default.

4. Select any one of the following option under **Enable IP Client Tracker for**:
 - **All clients**
 - **Trusted clients only**
 - **Untrusted clients only**
5. Move the **Probe Delay** toggle to on position.
6. Enter the **Enter probe delay** in seconds. Default value is 15, you can set a value in the range of 15 to 300 seconds.
7. Click **Save Settings**.

Configuring IGMP on AOS-Switches

In a network where IP multicast traffic is transmitted for various multimedia applications, Internet Group Management Protocol (IGMP) helps reduce bandwidth usage on a per-port basis on a switch. Enabling IGMP for a VLAN allows the ports to detect IGMP queries and report packets, and manage IP multicast traffic through the switch.

By default, IGMP is disabled for all VLANs.

To enable IGMP for a VLAN, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-S** or **Config** icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name**.
The dashboard context for the switch is displayed.

- d. Under **Manage**, click **Device**.

The tabs to configure the switch is displayed.

2. Click **IGMP**. The IGMP page is displayed with the list of existing VLANs.
3. Select the VLAN row(s) for which you want to configure IGMP, and click **Edit**.
4. Select **Enable** or **Disable** from the **IGMP** drop-down.
5. Click **OK**.
6. To configure the switch to filter unknown multicast messages, move the **Filter Unknown Multicast** toggle switch to the on position.
7. Click **Save Settings**.

Configuring Routing on AOS-Switches



In Aruba Central (on-premises) 2.5.3, **Routing** configuration is moved from the **IP Settings** tab to the **Routing** tab.

Static routes provide a means for restricting and troubleshooting routed traffic flows and in small networks can provide the simplest and most reliable configuration for routing. Static routes are manually configured in the routing table.

To enable routing and to add routes on a switch, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-S** or **Config** icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The tabs to configure the switch is displayed.
2. Click **Routing**. The Routing page is displayed.
3. You can toggle routing to **enabled** on the slider menu.
Before enabling routing, you must already have configured a path to the gateway.
4. In the **Routes** table, click **+** to add a VLAN and configure the following parameters:

Table 149: Routing Path Parameters

Name	Description	Value
Network	A valid network IP address for the destination network or host.	IPv4 address.
Netmask	Netmask of the IP address.	Netmask address.
Gateway	Default gateway IP address.	IPv4 address.
Metric	A parameter used by the routers to determine the best optimal path for routing traffic.	This is a fixed metric for static IP routes, and is set to "1".
Distance	The administrative distance helps routers determine the best route when there are multiple routes to the destination. A lower value is recommended.	The default administrative distance for static IP routes is 1, but can be configured to any value in the range of 1 - 255.

If the routing metric and administrative distance are set to a lower value for static routes, switches use the static IP routes as the best route for routing traffic.

- Click **Save**.
- To delete a route, hover over the row for the route in the **Routes** table and click the delete icon in the **Distance** column. Click **Yes** in the confirmation window.

Configuring QoS Settings on AOS-Switches

QoS is used to classify and prioritize traffic throughout a network. QoS enables you to establish an end-to-end traffic-priority policy to improve the control and throughput of important data. You can manage available bandwidth so that the most important traffic goes first.

Aruba Central (on-premises) allows you to configure QoS settings on individual or group of switches through the UI. The settings that you apply at the group level are applied to all switches in the group, except in the following conditions:

- A switch has a configuration override—That is, a QoS setting is changed at the device level. Once you update or apply a setting at the device level, any further changes that you make at the group level are not applied to the switch. A notification for the configuration override is added to the Audit Trail. If you remove local overrides on a switch, then all QoS configurations that were applied to the switch are removed, and the configurations available at the group level are applied to the switch.
For example, when a switch does not have any policies, if you add a policy for port 2 and 3 at the group level, then the policy is applied to the switch. If you add a policy for port 4 at the device level, and then add a policy for port 5 at the group level, then the policy for port 5 is not applied to the switch. You must add the same policy again at the device level to apply the policy. If you remove the local overrides on the switch, then any policies that were updated or added to the switch and the associated QoS class are replaced by the policies at the group level.
- A switch has invalid port number or VLAN ID—The port or VLAN to which the setting was applied at the group level is not available or is invalid on the switch. For example, if you apply a setting to port 15 and 16 at the group level, and a switch has only ports 1 to 10, then the settings will not be applied to that switch.

The setting that can be configured using the UI are:

- Creating QoS traffic policies on switches in your network to enable traffic-handling rules across the network.
- Defining QoS classes for a QoS Policy.
- Changing the priorities of traffic from various segments of your network as your business needs change.

Creating a QoS Traffic Policy

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-S** or **Config** icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The tabs to configure the switch is displayed.
2. Click **QoS**. The QoS page is displayed.
3. In the **QoS Traffic Policy** accordion, click **+** to add a new QoS traffic policy.
4. Configure the following parameters.

Table 150: *Configuring QoS policy*

Name	Description	Value
Policy Name	The name of the QoS policy.	A string
Target	The target where the policy is applied.	Port or VLAN
ID	The IP address for static IP assignment. This field is enabled only when you select Static from the IP Assignment drop-down.	IPv4 address

5. Click **Save**.

Editing a QoS Policy

To edit a QoS policy, point to the row for the QoS policy, and click the edit icon.

Deleting a QoS Policy

To delete a QoS policy, point to the row for the QoS policy, and click the delete icon.

Adding a QoS Class for the Policy

To define a QoS class for the a policy, complete the following steps:

1. Select a QoS policy from the New QoS Policy table. The QoS Class table is displayed below the New QoS Policy table with the configured QoS classes.
2. Click + to add a QoS classifier for the selected policy. The Add QoS classifier Classifier window is displayed.
3. Configure the following parameters.

Table 151: *Configuring QoS class*

Name	Description	Value
Class Name	The class name of the QoS policy.	A string
Packet Matching Criteria		
Source	The type of source for which you want to apply a policy.	Any, Network, or Host. If you select Network, enter the IP address and wildcard mask . If you select Host, enter the IP address.
Destination	The type of destination for which you want to apply a policy.	Any, Network, or Host. If you select Network , enter the IP address and wildcard mask . If you select Host , enter the IP address.
Protocol	Select the type of data transfer protocol from the drop-down. If you select SCTP, TCP, or UDP, the source ports and destination ports fields are displayed.	Protocol types: GRE, ESP, AH, OSPF, PIM, VRRP, ICMP, IGMP, IP, SCTP, TCP, UDP, IP_IN_IP and IPv6_IN_IP.
Source Port (s)	The port numbers of source. You can specify a comma separated list of ports or range of ports. For example: 10-12 or 10,12.	Numeric value
Destination Port(s)	The port numbers of destination. You can specify a comma separated list of ports or range of ports. For example: 10-12 or 10,12.	Numeric value
Actions		
DSCP	Select a Differentiated Service Code Point (DSCP) from the drop-down.	DSCP value range from 0 to 63. Default value is No Change. In few cases, such as 10 af11 and 10 af12
Priority	Select a priority value for the selected DSCP.	The priority range from 0 to 7. <ul style="list-style-type: none"> ■ 0 - Normal Priority ■ 1 - Low Priority ■ 7 - High Priority Default value is No Change.

Editing a QoS Class

To edit a QoS Class, point to the row for the QoS policyclass, and click the edit icon.

Deleting a QoS Class

To delete a QoS Class, point to the row for the QoS policyclass, and click the delete icon.

Configuring DSCP Map

DSCP map table displays mappings between Incoming DSCP and priority.

To change priority value associated with a DSCP code point, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-S** or **Config** icon to view the switch configuration dashboard.
2. Click **QoS**. The QoS page is displayed.
3. Expand the **DSCP Map** accordion.
4. Select the Incoming DSCP row for which you want to change the priority and click the edit icon. The Edit DSCP window is displayed.
5. Select the priority value from the drop-down.
6. Click **OK**.

Configuring Device Profile and Device Identifier on AOS-Switches

Device profile configuration allows Aruba Central to dynamically detect an Aruba AP, AOS-Switch, or other devices, which are directly connected to the switch, and apply predefined configurations to ports on which the devices are detected. The device profile configuration has default device profiles and device identifiers, which cannot be deleted. In addition to the default device profiles and device identifiers, you can create custom device profiles and device identifiers.

The following pre-configured device types under device profile are available:

- Aruba-AP—All Aruba APs
- Aruba-Switch—Aruba switches
- SCS-WAN-CPE—Swisscom WAN devices (Swiss service provider)



To apply device profiles on other device types, you must configure the devices under device identity and associate that identity with a profile, only if the device is detectable by the LLDP TLV 127 and CDP (VOIP) attributes.

To configure device profile, complete the following procedure:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-S** or **Config** icon to view the switch configuration dashboard.

- To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The tabs to configure the switch is displayed.
- 2. Click **Device Profile**. The Device Profile page is displayed.
- 3. Depending on whether you want to add a new device profile or identifier, complete one of the following steps:
 - In the Device Profile table, click + to add a device profile. For more information, see [Adding a Device Profile](#).
 - In the Device Identifier table, click + to add a device identifier. For more information, see [Adding a Device Identifier](#).



If no device profile is mapped to a device identifier, the default device profile **Default-AP-Profile** is associated with the device identifier.

Adding a Device Profile

Configuration changes made on the device profiles always takes precedence over other UI configurations on the switch. For example, the PoE Priority and PoE Allocation configuration on the device profile takes precedence over the configurations on the **Interface > PoE** page.

Configuring profiles through device CLI removes existing configurations and sets it to the default configuration, but this may not apply in some instances.

To add a device profile, complete the following steps:

1. In the **Device Profile** table, click + to add a profile. The **Add Device Profile** window is displayed.
2. Configure the following parameters.

Table 152: Device Profile Parameters

Name	Description	Value
Name	The name of the profile configured.	A unique name for the device profile. This field cannot contain tilde(~), forward slash(/), and space characters.
Class of Service (CoS)	Indicates data and voice protocols for classifying packets into different types of traffic and setting a service priority. Supported only on AOS-Switches running firmware version 16.10.0004 or later.	0,1,2,3,4,5,6,7 Default is Disabled
Tagged VLAN	The tagged member of the VLAN.	Select from the drop-down. You can configure multiple VLANs by selecting the check boxes in the drop-down.
UnTagged VLAN	The untagged member of the VLAN.	Select from the drop-down. Default value is 1.
PoE Priority	The PoE priority for the device port.	Low, High or Critical
PoE Allocation	The PoE allocation for the switch port. Not supported on Aruba 2920 Switch Series.	Usage or Class
Device Identifier Name	The device identifiers associated with the device profile.	Select from the drop-down. This field lists only the default device identifiers. To add a custom device identifier, see <>
Jumbo	Indicates whether jumbo packet handling is enabled for the VLAN interface.	Toggle switch to the on or off position

3. Click **Save**.

Editing a Device Profile

To edit a device profile, click the  edit icon.

Deleting a Device Profile

To delete a device profile, click the  delete icon. You cannot delete the default device profile or a device profile that is associated with a device identifier.



You can validate the device profiles using the `show device-profile status` and `show vlan <id>` commands.

Adding a Device Identifier

The Device Identifiers configuration allows you to configure multiple identifiers for a single device profile. Aruba-AP, Aruba-Switch, and SCS-WAN-CPE are the default device identifiers under device profile. The device

identifier allows you to identify devices based on CDP and LLDP (TLV type 127, TLV type 6, and TLV type 5) information.



Device identifiers are supported on AOS-Switches running firmware version 16.10.0004 or later.

1. In the **Device Identifier** table, click **+** to add a identifier. The Add Device Identifier window is displayed.
2. Configure the parameters in the following table.

Table 153: Device Identifiers Parameters

Name	Description	Value
Name	The name of the identifier configured.	A unique name for the device identifier. This parameter cannot contain tilde(~), forward slash(/), and space characters.
Status	Status of the device identifier is enabled or disabled.	Toggle switch to the on or off position.
Type	Type of device identity.	CDP or LLDP
VOIP VLAN query	The VOIP VLAN query name. Applicable only when you select CDP in the Type parameter. Not supported on the Aruba 2920 Switch Series.	Alphanumeric characters
MAC OUI	OUI part in the MAC address. Applicable only when you select LLDP in the Type parameter.	Hexadecimal value in the range 000001 and FFFFFFFF.
Enter subtype	Subtype associated with LLDP. Applicable only when you select LLDP in the Type parameter.	Integer value between 0 and 255.

3. Click **Save**.

Editing a Device Identifier

To edit a device identifier, click the  edit icon. You can only edit the status of the default device identifiers.

Deleting a Device Identifier

To delete a device identifier, click the  delete icon. You cannot delete the default device identifiers.

Automatic Rollback Configuration

Aruba Central (on-premises) supports auto-rollback mechanism for AOS-Switches running software version 16.10.0009 or later. The auto-rollback mechanism is triggered when the switch loses connectivity to Aruba Central (on-premises) after the configuration is applied. The switch rolls back to the last known stable configuration and reconnects to Aruba Central (on-premises) within a period of 10 minutes. After recovery, the **Auto Commit State** in the **Configuration Audit** page is set to **Off** to stop subsequent configuration

push from Aruba Central (on-premises). Before changing the **Auto Commit** state to **ON**, you must review the configuration change that resulted in the network disconnect.

When a switch rollback occurs, an event is logged in the **Audit Trail** page as shown in the following figure:

Figure 46 Example of Audit Trail Page for Automatic Rollback Configuration

AUDIT TRAIL (348)				
OCURRED ON	IP ADDRESS	USERNAME	CATEGORY	DESCRIPTION
Mar 23, 2020, 14:33		System	Configuration	Pending configuration/certificate for device
Mar 23, 2020, 14:33	-	System	Configuration	Applying template test to device
Mar 23, 2020, 14:33		System	Configuration	Auto commit is Off for the device; Config wont be pushed
Mar 23, 2020, 14:33	-	System	Configuration	Get configuration diff from the device
Mar 23, 2020, 14:33		System	Configuration	Pending configuration/certificate for device
Mar 23, 2020, 14:33	-	System	Configuration	Applying template test to device
Mar 23, 2020, 14:33		System	Configuration	Auto commit is Off for the device; Config wont be pushed
Mar 23, 2020, 14:33	-	System	Configuration	Get configuration diff from the device
Mar 23, 2020, 14:33		System	Configuration	Applying template test to device
Mar 23, 2020, 14:33	-	System	Configuration	Auto commit is Off for the device; Config wont be pushed
Mar 23, 2020, 14:33		System	Configuration	Get configuration diff from the device
Mar 23, 2020, 14:33	-	System	Configuration	Configuration rollback detected on device. Device is set to Auto commit Off mode

AOS-Switch Stack

A switch stack is a set of switches that are interconnected through stacking ports. The switches in a stack elect a primary switch called Conductor and a backup switch as Member. The following table lists the switches that support stacking:

Table 154: Switch Stacking Support

AOS-Switch Platform	Maximum Number of Stack Members	Minimum Supported Version	Supported Stack Type (Frontplane (VSF) / Backplane (BPS))	Supported Configuration Group Type for Stacking (UI / Template)
Aruba 2930F Switch Series	8	<ul style="list-style-type: none"> ■ WC.16.08.0019 or later ■ WC.16.09.0015 or later ■ WC.16.10.0012 or later 	VSF	UI and Template
Aruba 2930M Switch Series	10	<ul style="list-style-type: none"> ■ WC.16.08.0019 or later ■ WC.16.09.0015 or later ■ WC.16.10.0012 or later 	BPS	UI and Template
Aruba 3810 Switch Series	10	<ul style="list-style-type: none"> ■ KB.16.08.0019 or later ■ KB.16.09.0015 or later ■ KB.16.10.0012 	BPS	UI and Template

Table 154: *Switch Stacking Support*

AOS-Switch Platform	Maximum Number of Stack Members	Minimum Supported Version	Supported Stack Type (VSF) / Backplane (BPS))	Supported Configuration Group Type for Stacking (UI / Template)
		or later		
Aruba 5400R Switch Series	2	<ul style="list-style-type: none">KB.16.08.0019 or laterKB.16.09.0015 or laterKB.16.10.0012 or later	VSF	Template only



Provisioning and configuring of Aruba 5400R Switch Series and switch stacks is supported only through configuration templates. Aruba Central (on-premises) does not support moving Aruba 5400R Switch Series from the template group to a UI group. If an Aruba 5400R switch is preassigned to a UI group, then the device is moved to an unprovisioned group after it joins Aruba Central (on-premises).

For more information on topology and configuration of switch stacks, see the *ArubaOS-Switch Management and Configuration Guide* for the respective switch series.

Provisioning AOS-Switch Stacks in Aruba Central (on-premises)

The switch elected as the conductor establishes a WebSocket connection to Aruba Central (on-premises). The following criteria apply to provisioning and management of switch stacks in Aruba Central (on-premises):

- Switch stacks can be added only to a template group and cannot be moved to a UI group.
- If the standalone switches in a group join to form a switch stack, the switch is moved to the Unprovisioned state.
- If a switch stack in the template group joins Aruba Central (on-premises) as a stand-alone Switch, it is blocked unless it is deleted from the stack. After it is removed from the stack, the stand-alone switch is moved to the pre-provisioned group.
- If a switch stack is moved from a pre-provisioned group to an existing group in the UI, it will be moved to Unprovisioned state.
- After forming a switch stack, you can remove a member and erase its stacking configuration. However, the member can join Aruba Central (on-premises) as a standalone switch only after it is deleted from the switch stack.
- When a stack is removed, the stack members cannot join Aruba Central (on-premises) until the stack entry is deleted. For more information on deleting the stack, see [Configuring AOS-Switch Stacks Using UI Groups](#). When a stack entry is not deleted and the member tries to rejoin Aruba Central (on-premises), an event is triggered in the Audit Trail page stating that the stack association is detected.

Assigning Labels and Sites

Aruba Central (on-premises) supports organizing your devices into sites for ease of monitoring. Sites refer to physical locations in which the devices are installed. Administrators can assign switch stacks to a single site

for ease of managing installations and monitoring the overall site health. For more information on assigning devices to sites, see [Managing Sites](#).

Similarly, switch stacks can also be tagged using labels. Labels allow you to identify or tag devices installed in a specific site for ease of monitoring. For more information on assigning labels, see [Managing Labels](#).

If any one member of the switch stack is assigned to a site, Aruba Central (on-premises) automatically assigns all other members in a switch stack to the same site. Similarly, if a label is assigned to an individual member in a stack, the same label is applied to all other members of the stack.

Because all members of a switch stack must be assigned to the same site and label, Aruba Central (on-premises) automatically corrects the site and label assignment for switch stacks that were earlier assigned to different labels or sites. If you have such switch stacks in your account, you will notice that all stack members are migrated to the same site or label to which the conductor was assigned. Aruba recommends that you review the sites and labels assigned by Aruba Central (on-premises) to verify that the switch stacks in your account are assigned to sites and labels that you intended to use, and if required, assign all members of stack to a common site or label of your choice.



Configuring AOS-Switch Stacks

For information on configuring switch stacks using template groups, see [Configuring AOS-Switch Stacks Using Template Groups](#).

For information on configuring switch stacks using UI groups, see [Configuring AOS-Switch Stacks Using UI Groups](#).

Monitoring Switch Stacks

See [Monitoring Switches and Switch Stacks](#).

Viewing Switch Stacks in Site Topology

See [Monitoring Sites in the Topology Tab](#).

Configuring AOS-Switch Stacks Using Template Groups

The switch stacks are provisioned under template groups in Aruba Central (on-premises). The template groups allow you to configure and modify the settings of a switch stack using configuration templates.

When uploading a configuring template, ensure that the variables are uploaded for all the members of the stack. The template is applied with the variables of the member that is elected as the conductor.

To create a configuration template for switch stack, complete the following steps:

1. In the **Network Operations** app, set the filter to a template group.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Switches**.
3. Click the **AOS-S** or **Config** icon.
The tabs to configure switches using templates is displayed.
4. Click **+** to create a template for the Aruba switch stack.
5. Specify a name for the template.
6. Select **Aruba Switch** from the **Device Type** drop-down.
7. Select the AOS-Switch model in the **Model** drop-down.

8. Select the AOS-Switch software version in the **Version** drop-down.
9. Enter the template text in the **Template** box.



All switch templates must include a password command to set a password for the device. The switch template cannot be saved without adding a password command. If the configuration that is pushed from Aruba Central to the device does not contain a password command, the configuration push is aborted for the device and a log is added to the audit trail. For example, if you add the password command in a condition block and the condition evaluates to false, the configuration that is pushed will not contain the password command.

10. Click **Save**.



Aruba Central (on-premises) does not support the use of part number (J-number) in place of Switch model number in configuration templates for the Aruba switch stack.

The following pre-defined variables are refreshed and re-imported from a switch stack when a new stack member is added or removed, or when a failover occurs.

- `_sys_template_header`
- `_sys_module_command`
- `_sys_stack_command`
- `_sys_oobm_command`
- `_sys_vlan_1_untag_command`
- `_sys_vlan_1_tag_command`

For information about deploying VSF stacks of ArubaOS Switches using Zero Touch Provisioning (ZTP) in Aruba Central, see the [VSF Stacking Guide](#).

For information about switch stacks using UI groups, see [Configuring AOS-Switch Stacks Using UI Groups](#).

Configuring AOS-Switch Stacks Using UI Groups

Aruba Central (on-premises) supports both Backplane stacking (BPS) and Virtual Switching Framework (VSF) switch stacking. You can create switch stacks and add stack members through the UI. The stack configuration is possible only when the switches are online.



Stacks created using UI groups can only be managed in a UI group. If a device is moved to a template group, then the device cannot be managed in a UI group without rebuilding the stack.

Fiber modules / SFP ports are manageable in a UI group when the stack is created. These modules are available for configuration at the device level context.

See the following topics for more information on managing switch stacks using UI groups:

- [Onboarding Conductor and Members for VSF Stacking](#)
- [Onboarding Conductor and Members for BPS Stacking](#)
- [Creating an AOS-Switch Stack](#)
- [Adding a Stack Member](#)

Onboarding Conductor and Members for VSF Stacking

The following is a high-level process flow for configuring VSF switch stacks:

1. Add the switches to the device inventory and assign a valid subscription. All the switch members must be set to factory default and powered off.
2. Power on the switch you intend to add as a conductor. The switch comes up online in Central as a standalone switch.
3. Create a stack with the standalone switch. After stack creation, the switch will reboot and comes up as a stack conductor. For more information, see the section [Creating an AOS-Switch Stack](#).
4. Add other members to the stack when the status of the conductor switch is active. For more information, see [Adding a Stack Member](#).
5. After adding members, connect the Ethernet cables between the switches to form the desired topology.
6. Power on the switches one at a time. The second switch that is powered on will be elected as standby. The subsequent switches that get powered on will be designated as the members of the stack.

For more information on deploying a VSF stack, see [Onboarding Conductor and Members for VSF Stacking](#) section.

For more information on topology and configuration of switch stacks, see the *ArubaOS-Switch Installation and Getting Started Guide* and *ArubaOS-Switch Advanced Traffic Management Guide* for the respective switch series.



If the stack members are connected and powered on before adding to a stack, then the members might not join the stack and status of the stack members are displayed as **Inactive** in the UI. In this scenario, stack cannot be managed through the UI.

Recommended Deployment Workflow

The following procedure provides the recommended workflow for deploying three-member VSF stack (Conductor, Standby, and a Member switch).

1. Connect a staging port on the first switch in the VSF stack to a DHCP enabled network or a device that has access to the internet. After rebooting and initialization, the switch assumes its role as conductor and the LED on the VSF stack ports of the switch will turn amber.
2. Connect a VSF port of the next switch to the VSF port of the conductor switch. During initialization, the switch will act as standby and the LED on the VSF port will turn amber.
3. Connect a VSF port of the next switch to the VSF port of the standby switch. During initialization, the new switch acts as a member and the LED on the VSF port of the switch will turn amber.
4. Connect the VSF port of the conductor switch to the VSF port of the member to complete the loop.



If the stack members are connected and powered on before adding to a stack, then the members might not join the stack in Aruba Central (on-premises). In such scenarios, the status of the stack members is displayed as **Inactive** in the UI. Also, the stack cannot be managed using UI groups in Aruba Central (on-premises).

Onboarding Conductor and Members for BPS Stacking

The following is a high-level process flow for configuring BPS switch stacks:

1. Add the switches to the device inventory and assign a valid subscription. All the switch members must be set to factory default and powered off.
2. Insert the stacking module to the switch you intend to add as a conductor.
3. Power on the conductor switch. The switch comes up online in Central as one-member BPS switch stack. A one-member BPS switch stack is a single BPS switch with stacking enabled.
4. Move the one-member switch stack from the **Unassigned Devices** group to a UI group. The stacking information is displayed in the **Stacks** configuration page with switch member added as the conductor.
5. Add other members to the stack when the status of the conductor switch is active in the Members table. For more information, see [Adding a Stack Member](#).
6. After adding members, connect the stacking modules and stacking cables between the switches to form the desired topology.
7. Power on the switches one at a time. The second switch that is powered on will be elected as standby. The subsequent switches that get powered on will be designated as the members of the stack.



If the stack members are connected and powered on before adding to a stack, then the members might not join the stack in Aruba Central (on-premises). In such scenarios, the status of the stack members is displayed as **Inactive** in the UI. Also, the stack cannot be managed using UI groups in Aruba Central (on-premises).

For more information on topology and configuration of switch stacks, see the *ArubaOS-Switch Installation and Getting Started Guide* and *ArubaOS-Switch Advanced Traffic Management Guide* for the respective switch series.

Creating an AOS-Switch Stack

To create an AOS-Switch stack, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-S** or **Config** icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The tabs to configure the switch is displayed.
2. Click **Stacks**. The Stacks page is displayed.
The Stacks table displays the following information:

Table 155: *Stacks table*

Name	Description	Value
Name	The name of the switch stack.	A string
Type	The type of switch stacking.	BPS or VFS
Stack ID	The ID of the switch stack. The stack ID is auto-generated and cannot be changed in the settings.	Auto-generated String
Members	The number of members on the switch stack.	Integer
MAC Address	The MAC address of the switch stack.	Alphanumeric MAC address
Topology	The type of switch stack topology.	Chain, Ring, or unknown
Status	The status of the stack formation.	Pending, In-progress, Active, or Failed
VSF Port Speed	The port speed in the case of VSF stacking. This column is hidden by default. You must select the column from the columns list.	1G or 10G

- In the **Stacks** table, click + to add a stack.
The **Create New Stack** window is displayed.
- Select a conductor switch from the **Select Conductor Switch** drop-down list. The model number and serial number of switches are displayed in the drop-down list.



- The conductor switch must be installed with the minimum supported firmware version of 16.06 or later.

If the selected switch supports VSF Stacking, configure the following parameters:

- Link 1 Name and Port(s)**—The name of the link 1 and its corresponding ports.
- Link 2 Name and Port(s)**—The name of the link 2 and its corresponding ports.
- Domain ID**—The domain ID of the switch stack.
- Port Speed**—The VSF port speed from the drop-down.

If the selected switch supports BPS stacking, insert the stacking module in switch and continue to step 5.

- Click **Save & Reboot Stack**. When the stack reboots, the status of the stack formation is displayed in the **Stacks** table. Do not make any changes to the stack until the status changes from In Progress to Active or Failed. If stack creation fails due to some issues, delete the stack entry and retry.

Editing a Stack

To edit a stack, select the stack row you want to edit and click the edit icon.



You can edit a stack only when its status is **Active**.

Removing a Stack

To remove a stack, select the stack row that you want to remove and click the delete icon.



You can remove a stack only when its status is **Failed**.

Adding a Stack Member

Stacking allows you to add switches to the stack only when the conductor is active.

To add a switch to stack as a new member, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a switch group in the filter:
 - a. Set the filter to a group containing at least one switch.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **AOS-S** or **Config** icon to view the switch configuration dashboard.
 - To select a switch in the filter:
 - a. Set the filter to **Global** or a group containing at least one switch.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name**.
The dashboard context for the switch is displayed.
 - d. Under **Manage**, click **Device**.
The tabs to configure the switch is displayed.
2. Click **Stacks**. The Stacks page is displayed.
3. In the **Stacks** table, select the stack row for which you want to add a member. The Members table displays the list of members for that particular stack. The **Members** table displays the following information:

Table 156: *Members table*

Name	Description	Value
Name	The name of the switch stack member.	A string
MAC Address	The MAC address of the stack member.	Alphanumeric MAC address
Model	The hardware model of the switch.	A String
Priority	The priority level of the stack member.	1 to 255
Role	The role of a stack member.	Conductor, Member, or Standby
Status	The status of the switch stack member.	Active, Inactive, or Not Joined
Link1 Port	The name of the link and its corresponding port of the stack member.	A string
Link2 Port		

4. In the **Members** table, click + to add a stack member.
The **Add Stack Member For <stack name>** window is displayed. The following information is auto-

generated:

- **Member ID**—Identification number of the member.
 - **Priority**—Priority of the member.
5. Select the member using one of the following options:
 - **Same as Conductor**—Use this option when your conductor and member have the same model number.
 - **Select Model** —Use this option when your conductor and member have different model numbers.
Select the switch model from the model drop-down list.
 6. If the selected switch supports VSF Stacking, configure the following parameters:
 - **Link1 Name and Port(s)**—Specify the name of the link 1 and its corresponding port.
 - **Link2 Name and Port(s)**—Specify the name of the link 2 and its corresponding port.
 7. To add another stack member, click **Save & Add Another**.



A message is displayed above the **Members** table when the maximum number of switches in a stack has been added.

8. Click **Save**. After the stack members appear in **Members** table, connect the stacking modules and stacking cables to all switches and power on the switches.

Editing a stack member

To edit a stack member, select the member row you want to edit and click the edit icon.

Removing a stack member

To delete a stack member, select the member row that you want to delete and click the delete icon.

After removing a member, disconnect the switch from the stack. To disconnect the switch from the stack, do one of the followings:

- Turn off the power from the switch.
- Restart the switch using switch reset button.



You can remove only the stack member that has the lowest priority. For example, if there are three stack members with priority 254, 253 and 252 respectively and if you want to remove a stack member with priority 253, then first you need to remove the member with priority 252.

Priority cannot be assigned manually. Conductor switch is always assigned with priority 255. The priority of other subsequent members is decremented by 1.

This section covers the following topics:

- Aruba Central (on-premises) offers monitoring service for WLAN networks configured and managed using ArubaMobility Controllers.
- Aruba Central (on-premises) allows you to onboard and monitor controller clusters, the Mobility Conductor setup, and the conductor and local controller setup.
- When you add a conductor controller or a Mobility Conductor, Aruba Central (on-premises) discovers all the associated controllers and campus APs, and adds them to the device inventory.



Aruba Central (on-premises) does not support configuring wired clients on a controller. To configure and deploy, use the WebUI and CLI.

Before You Begin

Before adding controllers to Aruba Central (on-premises), ensure that the controller has the following parameters configured:

- Management Server profile—The Aruba Central (on-premises) server must be configured as a management server on the controller.
- Advanced Monitoring Messages—Enable AMON for communication between the Aruba Central (on-premises) server and controller. When AMON is enabled on the controller over UDP 8211, the controller periodically sends information about user sessions, AP and client association, and other such information required for managing and monitoring controllers on Aruba Central (on-premises).
- Syslog Messages and SNMP Traps—Although AMON is a preferred option for polling data from controllers, to obtain data pertaining to AP lists, you may want to enable SNMP, and configure SNMP traps and syslog server for logging system events.
- Websocket connection—To enable controller firmware upgrade and troubleshooting from Aruba Central (on-premises), ensure that the Aruba Central (on-premises) server URL and IP address are configured on the controllers running ArubaOS 6.5.3.6 or later.

For more information on configuring controllers, see *ArubaOS User Guide*.



Tools support is available for controllers that support web socket. For example, controllers running Firmware version above 8.4.x or 6.5.x.

Controllers running ArubaOS 6.5.4.8 software image do not support Websocket connection, due to which Aruba Central (on-premises) cannot onboard these controllers.

This section covers the following topics:

- [Adding Mobility Controllers](#)
- [The Controller Dashboard](#)

Supported Aruba Mobility Controllers

Aruba Central supports provisioning, management, and monitoring of the following Aruba Mobility Controllers.

Table 157: *Supported Devices and Software Versions*

Supported Device	Latest Validated Software Versions
Aruba 7000 Series Mobility Controllers	8.8.0.0
Aruba 7200 Series Mobility Controllers	8.7.1.0
Aruba 9004 non-LTE Mobility Controllers	8.6.0.7 6.5.4.16
<p>NOTE: Controllers running ArubaOS 6.5.4.8 software image do not support WebSocket connection. You must manually add these controllers to Aruba Central. The minimum software version required for monitoring controller clusters and Mobility Conductor managed networks is ArubaOS 8.2.1.0.</p>	

Adding Mobility Controllers

You can add controllers using one of the following methods:

- [Adding a Controller using Controller Management](#)
- [Adding Controllers Manually](#)
- [Adding Controllers Using a CSV File](#)

Adding a Controller using Controller Management

Configuring SNMP and HTTPS Connection Profiles

To configure connection profiles for adding controllers, complete the following steps:

1. In the **Account Home** page, under **Global Setting**, click **Device Inventory**.
The **Device Inventory** page is displayed.
2. Click **Controller Management**.
The **Controller Management** pop-up window opens.
3. Under **Connection Profile**, configure the SNMP and HTTPS connection profiles as per your requirement.
4. To add an SNMP connection profile:
 - a. Click **SNMP** and add the following details:
 - **Name**—Name of the connection profile.
 - **SNMP Version**—SNMP version, for example, V2 or V3.
 - **Community String**—Community string required for the management of controller.
 - b. Click **Save**.

5. To add an HTTPS connection profile, complete the following steps:
 - a. Click HTTPS and add the following details:
 - **Name**—Name of the connection profile.
 - **HTTPS User**—Username for HTTPS authentication.
 - **HTTPS Password** and **Confirm HTTPS Password**—Password for HTTPS authentication.
 - b. Click **Save**.

Adding a Controller

To add controllers using the **Add MM/Controllers** tab, complete the following steps:

1. In the Account Home page, under **Global Setting** click **Device Inventory**.
The **Device Inventory** page is displayed.
2. Click **Controller Management**.
The **Controller Management** pop-up window opens.
3. Click **Add MM/Controllers** tab.
4. Click **+** to add a controller.
The **Add MM/Controllers** pop-up window opens.
5. Enter a name for the Mobility Conductor.
6. Enter the IP address of the Mobility Conductor.
7. Select an SNMP or HTTPS profile.
8. Click **Save**.
This will auto-discover the managed devices associated with the Mobility Conductor and add them to Aruba Central (on-premises).
9. Return to the **Device Inventory** page and verify if your controller is added.

Adding Controllers Manually

To add the controllers manually, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.
The **Device Inventory** page is displayed.
2. Click **Add Devices**.
The **Add Devices** pop-up window is displayed.
3. Enter the **Serial Number**, **MAC Address**, and **Part Number** of each controller. You can add up to 10 devices.
4. Click **Done**.
5. To configure the controller with the SNMP or HTTPS connection profiles and IP address, click the Controller's name and enter the following information:
 - **IP Address**—IP address of the controller.
 - **SNMP or HTTPS profile**—SNMP or HTTPS profile based on your requirement.
6. Click **Save**.

Adding Controllers Using a CSV File

To import devices from a CSV file, complete the following steps:

1. Create a CSV file with the device list.
2. Ensure that the CSV file includes column headers for part number, MAC address, serial number, and other optional fields such as firmware version and IP address of the device.
3. In the Account Home page, under **Global Settings**, click **Device Inventory > Import Devices Via CSV**.
4. Browse to your local directory, select the CSV file, and then click **Open**.
5. Click **Import**.

Deleting a Controller

To delete a controller, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.
The **Device Inventory** page is displayed.
2. Click **Delete Devices**.
The **Delete Devices** window opens and displays the list of controllers provisioned in your network.
3. Select the controllers from the list.
4. Click **Delete**.

The Controller Dashboard

In the **Network Operations** app, the controller dashboard is displayed when the filter is set to a controller. To navigate to a controller dashboard, see

The following table lists all the available menu items in the **Network Operations** app for the controller dashboard.

Table 158: *Contents of the Controller Dashboard*

Left Navigation Menu	First-Level Tabs	Description
Manage > Overview	Summary	The Summary tab displays the controller device details, client count, usage, top APs, top clients, and health status. See Controller > Overview > Summary .
	Routing	Displays a summary of the IP routes configured on the controller. See Controller > Overview > Routing
Manage > LAN	Summary	Displays information about LAN port and LAN status. See Controller > LAN > Summary .
Manage > Clients	Clients	Displays a list of clients connected to a controller. See All Clients .

Left Navigation Menu	First-Level Tabs	Description
Analyze > Alerts and Events	Alerts & Events	The Alerts & Events tab displays details of the alerts and events generated for the controllers. See Controller Alerts
Analyze > Audit Trail	Audit Trail	Displays the total number of logs generated for all device management, configuration, and user management events triggered in Aruba Central (on-premises). See Viewing Audit Trail .
Analyze > Tools	Network Check	Enables network administrators and users with troubleshooting permission to perform troubleshooting or diagnostics tests on devices and networks managed by Aruba Central (on-premises). See Troubleshooting Network Issues .
	Commands	The Commands tab allows network administrators and users with troubleshooting permission to perform troubleshooting or diagnostics tests on devices and networks managed by Aruba Central. See Using Troubleshooting Tools .
Analyze > Reports	Reports	Enables network administrators to create various types of reports. You can create recurrent reports or configure the reports to run on demand. For more information, see Reports .
Maintain > Firmware	List	Provides an overview of the latest supported version of firmware for the device, details of the device, and the option to upgrade the device. For more information, see Upgrading Device Firmware .
	Config	Provides an upgrade status and compliance status for APs that are connected to the selected controller. For more information, see Upgrading Device Firmware .

Viewing the Controllers Tab

To view the Controller dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Click **Devices > Controllers**.

Controllers Dashboard

The **Controllers** dashboard page displays a complete list of offline or online controllers provisioned in Aruba Central. You can also use the following filtering options to view a specific set of controllers.

- **All**—Displays a complete list of controllers. For more information, see [Monitoring Controllers in List View](#).
- **Cluster**—Displays controller clusters deployed in Aruba Central. A controller cluster includes multiple controllers working together as a single managed entity. Controller clusters enable seamless roaming of clients between AP and ensure service continuity in the event of a failover. Controller clustering is supported only on devices running ArubaOS 8.x or later software versions. To view the cluster components, expand the cluster in the **Cluster Name** column. For more information, see [Monitoring Clusters in List View](#).

- **Mobility Conductor**—Displays a list of controllers that are functioning as Mobility Conductors. The Aruba Mobility Conductor is an advanced controller deployed as a virtual machine (VM) or installed on an x86-based hardware appliance. A single Mobility Conductor or a cluster of Mobility Conductors oversees co-located controllers. It also displays the details about the APs associated with each controller. For more information, see [Monitoring Mobility Conductors in List View](#).

Monitoring Controllers in List View

The **Controllers > All** page provides information associated with the controllers provisioned and managed in Aruba Central (on-premises).

To navigate to the **Controllers > All** page, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active controller.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Controllers**.
By default, the **All** tab is displayed.
3. Click the **All** tab.

The **Controllers > All** page displays the following information:

- **All**—Displays the total number of controllers. When you click the **All** tab, it provides information about all the controllers in the **Controllers** table.
- **Online**—Displays the total number of online controllers. When you click the **Online** tab, it provides information about the online controllers in the **Controllers** table.
- **Offline**—Displays the total number of offline controllers. When you click the **Offline** tab, it provides information about the offline controllers in the **Controllers** table.

Controllers Table

The **Controllers** table displays the following information:

- **Controller Name**—The name of the controller.
 - —Indicates that the controller is online.
 - —Indicates that the controller is offline.
- **Mobility Conductor Name**—The name of the Mobility Conductor.
- **Cluster Name**—The name of the cluster.
- **AP**—The table displays the following information related to the AP:
 - **Total**—Total number of APs.
 - **Down**—Total number of offline APs.
 - **Active**—Total number of online APs.
 - **Standby**—Total number of standby APs.
- **Client**—The number of clients connected to the controller.
- **Model**—The model number of the controller.
- **Status**—The status of the controller.
- **IP Address**—The IP address of the controller.

- **MAC Address**—The MAC address of the controller.
- **Serial**—The serial number of the controller.
- **Group**—The group to which the controller belongs.
- **Labels**—The labels associated with the controller. If multiple labels are associated with the controller, hover over the label link to view all the labels.
- **Site**—The site to which the controller belongs.
- **Version**—The version of the controller.

A search filter is provided only for the **Controller Name, Model, IP Address, MAC Address, Serial, Group, Labels, Site, and Version** columns. By default, the Controllers table sorts the offline devices and then the online devices.



Click the  icon to customize the view of Controllers table with additional columns. Click the **Reset to default** button provided in the drop-down list to reset the Controllers table with default columns only. To autofit the columns, select **Autofit columns**.

To download the **.csv** file of the Controllers table, click the  icon.

Monitoring Clusters in List View

The **Controllers > Clusters** page provides information associated with the Clusters provisioned and managed in Aruba Central (on-premises).

To navigate to the **Controllers > Clusters** page, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active controller.

The dashboard context for the selected filter is displayed.

2. Under **Manage**, click **Devices > Controllers**.
By default, the **All** tab is displayed.
3. Click the **Clusters** tab.

The **Controllers > Clusters** page displays the following information:

- **Clusters**—Displays the total number of Clusters. When you click the **Clusters** tab, it provides information about all the Clusters in the **Clusters** table.

Clusters Table

The **Clusters** table displays the following information:

- **Cluster Name**—The name of the Mobility Conductor.

Click the  icon to expand a cluster in the Clusters table. For more information, see [Monitoring Controllers in List View](#).



Click the  icon to view the **Overview > Summary** details of the cluster.

- **controller**—The table displays the following information related to the controller:
 - **Total**—Total number of controllers.
 - **Down**—Total number of offline controllers.
- **Client**—The number of clients connected to the Cluster.
- **Health Score**—The health status of the Cluster.

A search filter is provided only for the **Cluster Name** column.



Click the ☺ icon to customize the view of Clusters table with additional columns. Click the **Reset to default** button provided in the drop-down list to reset the Clusters table with default columns only. To autofit the columns, select **Autofit columns**.

To download the **.csv** file of the Clusters table, click the ↓ icon.

Monitoring Mobility Conductors in List View

The **Controllers > Mobility Conductor** page provides information associated with the Mobility Conductors provisioned and managed in Aruba Central (on-premises).

To navigate to the **Controllers > Mobility Conductor** page, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active controller.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Controllers**.
By default, the **All** tab is displayed.
3. Click the **Mobility Conductor** tab.

The **Controllers > Mobility Conductor** page displays the following information:

- **Mobility Conductor**—Displays the total number of Mobility Conductors. When you click the **Mobility Conductor** tab, it provides information about all the Mobility Conductors in the **Mobility Conductor** table.
- **Online**—Displays the total number of online Mobility Conductors. When you click the **Online** tab, it provides information about the online Mobility Conductors in the **Mobility Conductor** table.
- **Offline**—Displays the total number of offline Mobility Conductors. When you click the **Offline** tab, it provides information about the offline Mobility Conductors in the **Mobility Conductor** table.

Mobility Conductor Table

The **Mobility Conductor** table displays the following information:

- **Mobility Conductor Name**—The name of the Mobility Conductor.
 - —Indicates that the Mobility Conductor is online.
 - —Indicates that the Mobility Conductor is offline.
- **controller**—The table displays the following information related to the controller:
 - **Total**—Total number of controllers.
 - **Down**—Total number of offline controllers.

- **AP**—The table displays the following information related to the AP:
 - **Total**—Total number of APs.
 - **Down**—Total number of offline APs.
- **Role**—The role of the Mobility Conductor.
- **Client**—The number of clients connected to the Mobility Conductor.
- **Model**—The model number of the Mobility Conductor.
- **Status**—The status of the Mobility Conductor.
- **IP Address**—The IP address of the Mobility Conductor.
- **MAC Address**—The MAC address of the Mobility Conductor.
- **Serial**—The serial number of the Mobility Conductor.
- **Group**—The group to which the Mobility Conductor belongs.
- **Labels**—The labels associated with the Mobility Conductor. If multiple labels are associated with the Mobility Conductor, hover over the label link to view all the labels.
- **Site**—The site to which the Mobility Conductor belongs.
- **Version**—The version of the Mobility Conductor.

A search filter is provided only for the **Mobility Conductor Name, Role, Model, IP Address, MAC Address, Serial, Group, Labels, Site, and Version** columns. By default, the Mobility Conductor table sorts the offline devices and then the online devices.



Click the  icon to customize the view of Mobility Conductor table with additional columns. Click the **Reset to default** button provided in the drop-down list to reset the Mobility Conductor table with default columns only. To autofit the columns, select **Autofit columns**.

To download the **.csv** file of the Mobility Conductor table, click the  icon.

Controller > Overview > Summary

The **Summary** tab under **Manage > Overview** in the controller dashboard displays the following two sections:

- **Device Info**
- **Health Status**

Viewing the Overview > Summary Tab

To navigate to the **Summary** tab in the controller dashboard, complete the following steps:

- In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. Ensure that the filter selection contains at least one controller. For all devices, set the filter to **Global**. The dashboard context for the selected filter is displayed.
- Under **Manage > Devices**, click the **Controllers** tab. A list of controllers is displayed.
- Click a controller or cluster under **Device Name**. The dashboard context for the specific controller or cluster is displayed.
- Under **Manage**, click **Overview > Summary**. To exit the controller dashboard, click the back arrow on the filter.

You can change the time range for the **Summary** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

Device Info

The **Device Info** section displays the following details:

Figure 47 Device Info

CONTROLLER DETAILS					
NAME	SERIAL NUMBER	MODEL	MAC ADDRESS	SYSTEM IP ADDRESS	FIRMWARE VERSION
CHN-8x-Functional-MM1	MM7150F04	ArubaMM-VA	00:0c:29:15:0f:0e	10.27.108.195	8.9.0.0
GROUP NAME	LABELS	SITE	ROLE	CONDUCTOR	LAST REBOOT REASON
unprovisioned	--	-	Conductor	-	--
POE (DRAW/MAX)	REDUNDANCY PEER	NTP SERVER	CLUSTER NAME	4G/LTE MODEM STATUS	4G/LTE MODEM TYPE
-	CHN-8x-Functional-MM2	-	-	--	-
LOCATION	CONTACT				
controller chennai lab	mjeyakumar@arubanetworks.com				

- **Name**—The name of the controller.
- **Serial Number**—Serial number of the controller.
- **Model**—The hardware model of the controller.
- **MAC Address**—The MAC address of the controller.
- **System IP address**—The IP address of the controller.
- **Firmware Version**—The firmware version running on the controller. If a new version of the firmware is available, this information is also displayed. Clicking on the new firmware version redirects you to the Maintain > Firmware > controller page in the controller dashboard, where you can select the controller to upgrade it.
- **Group Name**—The name of the group, if the controller is configured as part of a group. Click the group name to go to the Overview > Summary page for that group.
- **Labels**—The name of the label, if the controller is configured as part of a single or multiple labels.
- **Site**—The name of the site, if the controller is configured as part of a site. Hover over the i icon to display the complete address of the site. Click the site name to go to the Overview > Site Health page for that site.
- **Role**— The role of the controller; for example, conductor or local.
- **Conductor**— The name of the conductor controller.
- **Last Reboot Reason**—The reason for the last reboot.
- **POE (DRAW/MAX)**—The amount of power that the devices connected to the controller consume and the maximum PoE power capacity. For example, if the value displayed is 6/120, the devices draw 6 watts and the maximum PoE power allocated is 120 watts.
- **Redundancy Peer**—Displays the redundant controller if it is configured.
- **NTP Server**—The name of the NTP server configured and its synchronization status.
- **Cluster Name**—The name of the cluster controller.
- **4G/LTE Modem Status**—Displays the modem connectivity status. The status shows only 'Connected' when the modem type is not internal.
- **4G/LTE Modem Type**—Displays the LTE connection type.
- **Location**—The currently configured physical location of the controller. Location details are displayed only for controllers running on firmware version ArubaOS 8.9.0.0 or later.

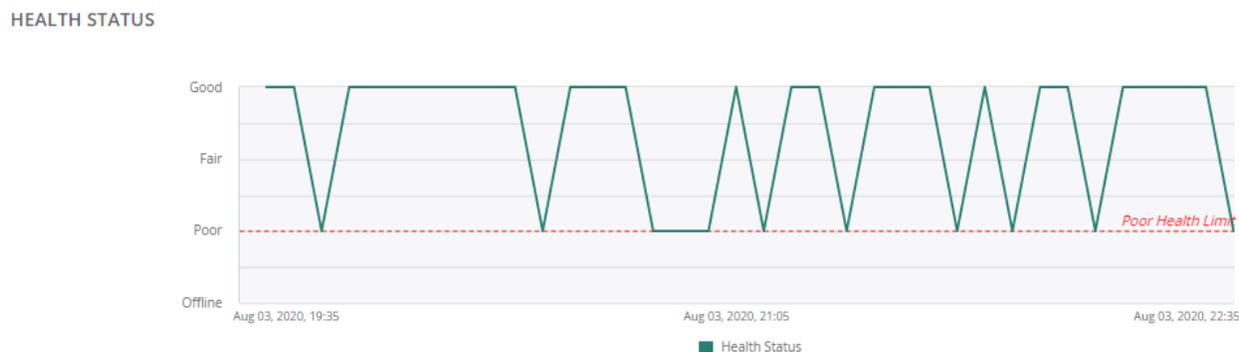
- **Contact**—The currently configured contact information of the controller. For example, E-mail ID or contact number. Contact details are displayed only for controllers running on firmware version ArubaOS 8.9.0.0 or later.

Health Status

The **Health Status** section displays the health of the controller in terms of CPU, Memory and device connectivity to Aruba Central (on-premises).

The health status is plotted using health indicators such as Good, Fair, Poor and Offline. You can hover over the chart to see the health status for a particular time frame.

Figure 48 *Health Status*



Controller > Overview > Routing

The **Routing** tab under **Manage > Overview** in the controller dashboard displays the following sections:

- **Routes Summary**
- **Routes**

Displays a summary of the IP routes configured on the controller. The following details are displayed:

- **Type**—The type of IP route.
- **Network**—IP address of the destination network.
- **VIA**—IP address through the routes are forwarded.

Viewing the Overview > Routing Tab

To navigate to the **Routing** tab in the controller dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. Ensure that the filter selection contains at least one controller. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
2. Under **Manage > Devices**, click the **Controller** tab.
A list of controllers is displayed..
3. Click a controller or cluster under **Device Name**.
The dashboard context for the specific controller is displayed.

4. Under **Manage**, click **Overview > Routing**.

To exit the controller dashboard, click the back arrow on the filter.

You can change the time range for the **Routing** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

Controller > LAN > Summary

The **Summary** tab under **Manage > LAN** page in the controller dashboard displays the following sections:

- **Port Status**
- **LAN Interfaces Summary**
- **VLAN Interfaces Summary**

Viewing the LAN > Summary Tab

To navigate to the **LAN > Summary** tab in the controller dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one controller. For all devices, set the filter to **Global**.

The dashboard context for the selected filter is displayed.

2. Under **Manage > Devices**, click the **Controller** tab.

A list of controllers is displayed.

3. Click a controller or cluster under **Device Name**.

The dashboard context for the specific controller is displayed.

4. Under **Manage**, click **LAN > Summary**.

To exit the controller dashboard, click the back arrow on the filter.

You can change the time range for the **Summary** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

Port Status

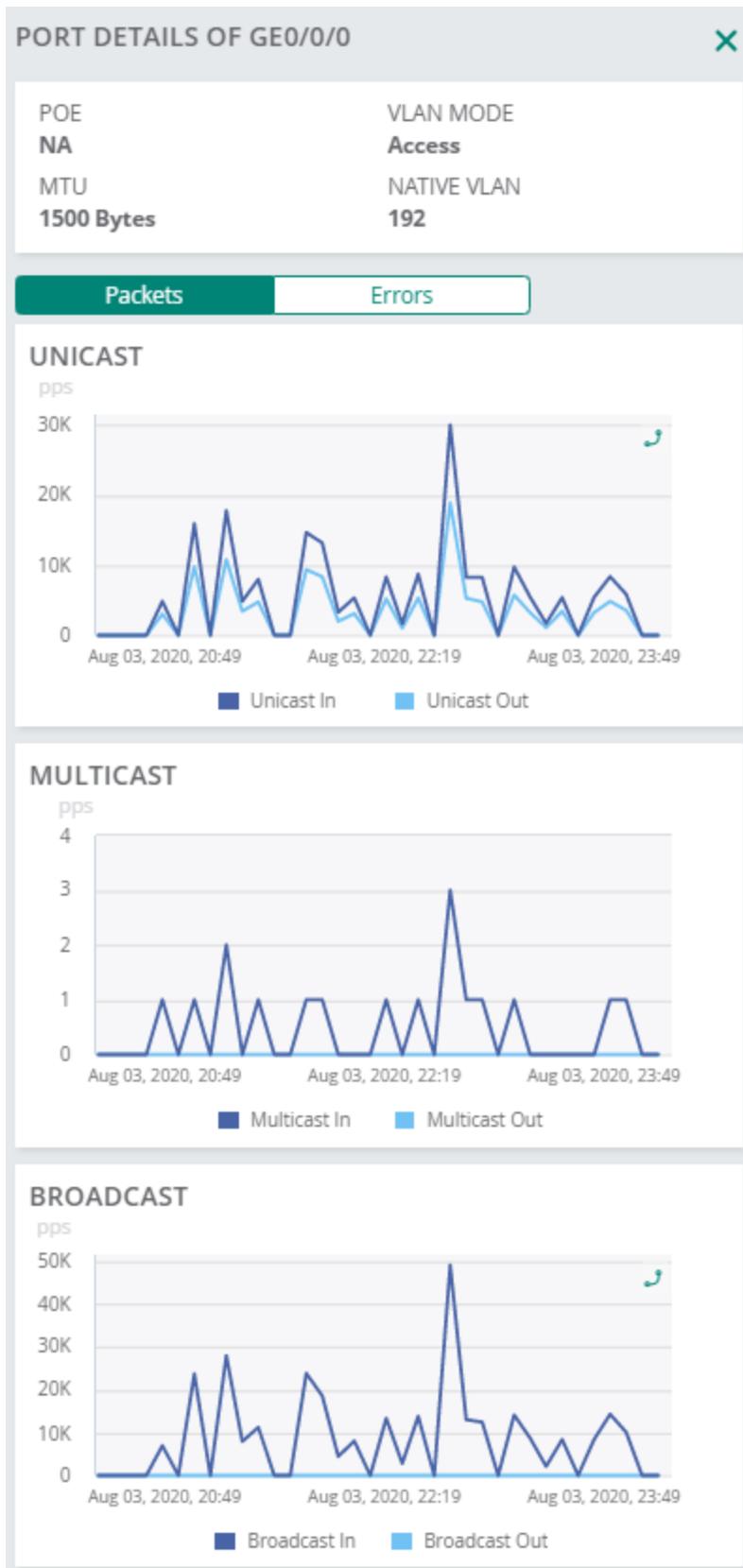
Provides a graphical representation of the Branch Gateway's LAN link availability. Also provides a quick view of the LAN port status. Click a LAN port to view the port detail graphs based on Packets or Errors.

Figure 49 *Port Status*



- The following graphs are displayed under the **Packets** tab:
- **Unicast**—The number of unicast packets per second.
- **Multicast**—The number of multicast packets per second.
- **Broadcast**—The number of broadcast packets per second.

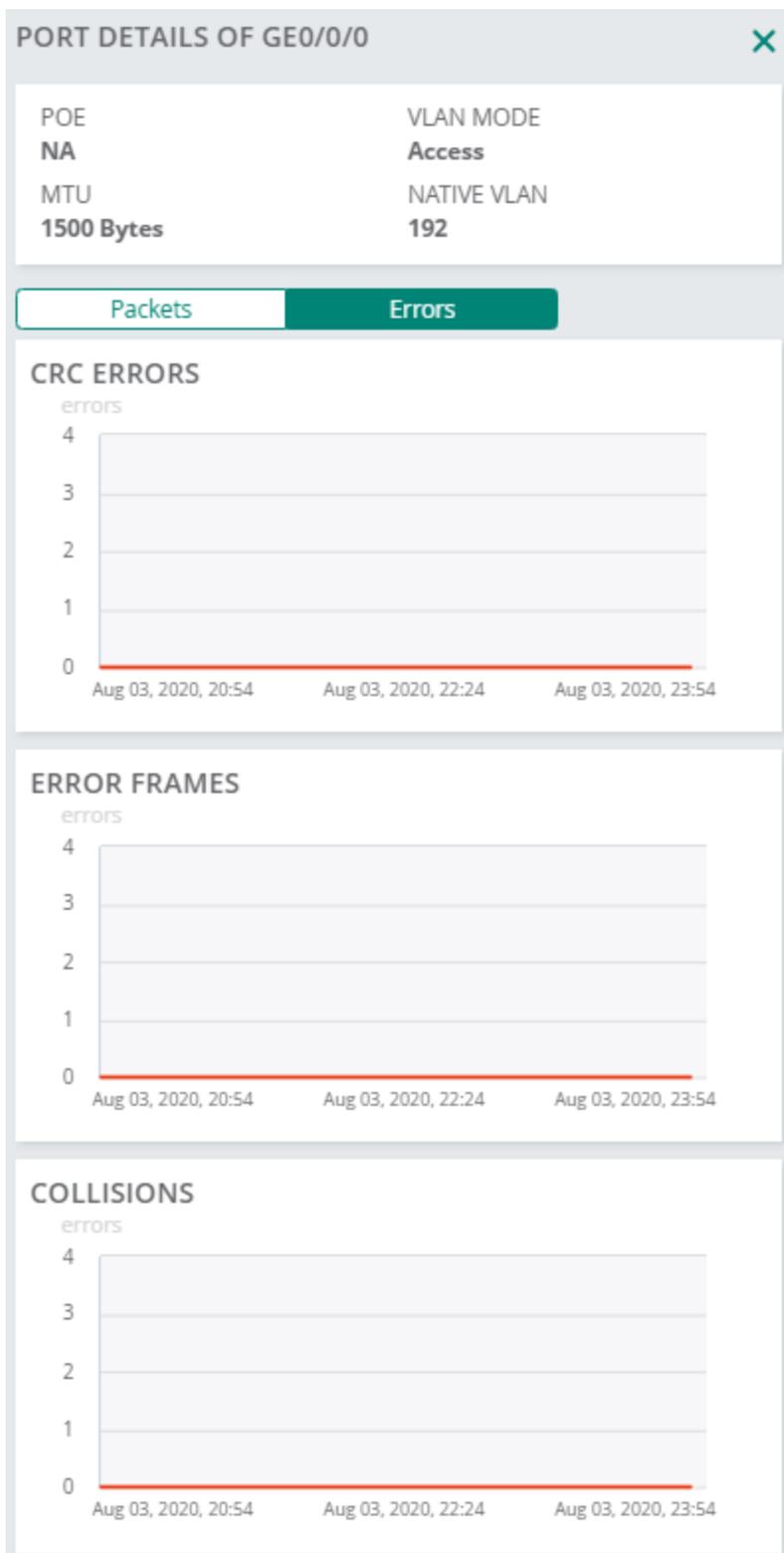
Figure 50 Port Details - Packet



- The following graphs are displayed under the **Errors** tab:

- **CRC Errors**—The number of cyclic redundancy errors logged.
- **Error Frames**—The number of error frames logged.
- **Collisions**—The number of collisions encountered.

Figure 51 *Port Details - Errors*



LAN Interfaces Summary

- The table displays the summary of LAN interfaces total number of LAN interfaces. The following details are displayed for the port:
- **Port**—Port number.
- **Admin State**—Administrative state of the LAN interface.
- **Operational State**—Operational state of the LAN interface.
- **Port Speed**—Port speed.
- **VLANs**—Range of VLANs.
- **MTU**—MTU value.

Figure 52 LAN Interface Summary

LAN INTERFACES SUMMARY (7)					
Port	Admin State	Operational State	Port Speed	VLANs	MTU
GE0/0/0	Enabled	Up	1 Gbps/Full	192	1500 Bytes
GE0/0/1	Enabled	Down	Auto/Auto	1	1500 Bytes
GE0/0/2	Enabled	Down	Auto/Auto	1	1500 Bytes
GE0/0/3	Enabled	Down	Auto/Auto	1	1500 Bytes
GE0/0/4	Enabled	Down	Auto/Auto	1	1500 Bytes
GE0/0/5	Enabled	Down	Auto/Auto	1	1500 Bytes
Gigabit-Level	Disabled	Down	Invalid/Full	--	1500 Bytes

Click a LAN port to view the port detail graphs based on Packets or Errors. For more information, see [Port Status](#).

VLAN Interface Summary

- The table displays the summary of VLAN interfaces and total number of VLAN interfaces. The following details are displayed:
- **VLAN ID**—VLAN ID number.
- **IP Address**—IP address.
- **Admin State**—Administrative state of the VLAN interface.
- **Oper. State**—Operational state of the VLAN interface.
- **Addressing Mode**—Type of addressing mode.
- **Description**—Description of the VLAN.

Figure 53 VLAN Interfaces Summary

VLAN INTERFACES SUMMARY (14)					
VLAN ID	IP Address	Admin State	Operational State	Addressing Mode	Description
1	--	--	Down	Static	--
163	21.32.54.71	--	Up	Static	--
192	192.168.10.104	--	Up	Static	--
218	71.99.84.17	--	Up	Static	--
228	95.20.84.44	--	Up	Static	--
271	25.17.85.66	--	Up	Static	--
324	79.19.27.78	--	Up	Static	--
388	14.59.23.77	--	Up	Static	--

Aruba Central users can be broadly categorized as system and external users.

- **System users**—Refer to the Aruba Central users who authenticate to the Aruba SSO server (public cloud deployments) or LocalDB servers (private cloud deployments). System users can access both the UI and API interface with their Aruba Central login credentials. Access for the system users is determined by the role to which they are mapped.

For more information on system user configuration, see **Configuring Users** in *Aruba Central Help Center*.

- **Network Administrators**—Network administrators manage, configure, and monitor devices in their respective network or organization using the Standard Enterprise Aruba Central interface.
- **External users**—Refer to the Aruba Central users who log in to Aruba Central using an external authentication source. External user accounts are maintained by IT administrators of the respective organizations. External users are also referred to as federated users. To provide a secure and seamless sign-on experience for external users, Aruba Central supports a federation configuration module based on the SAML SSO framework.



Aruba Central supports only the Identity Provider (IdP) SSO systems that support SAML 2.0.

The following table lists the tasks that you can perform from the **Users and Roles** page:

Table 159: *Users and Roles—Tasks*

Task	For more information...
Create, modify, or delete users	Configuring System Users
Create, modify, or delete user roles	Configuring User Roles
Resend email invitation to users	Resend Email Invite
Enable Two-Factor Authentication (2FA)	Two-Factor Authentication
Enable support access to debug issues	Support Access

Configuring System Users

In the **Account Home** page, the **Users and Roles** option under **Global Settings** allows you to create, modify, and delete users.

Adding a System User

To add a user, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**.
The **Users and Roles** page is displayed.
2. Click **Add User**.
The **New User** window is displayed.
3. Configure the following parameters:
 - **Username**—Email ID of the user. Enter a valid email address.
 - **Description**—Description of the user role. You can enter up to a maximum of 32 characters including alphabets, numbers, and special characters in the text field.
 - **Language**—Select a language. The Aruba Central web interface is available in English, French, Spanish, German, Brazilian Portuguese, Chinese, and Japanese languages.
 - **Account Home**—Select a user role for the **Account Home** page.
If there are common modules between **Account Home** and other app(s), the **Account Home** user role has higher precedence. For example, the **Devices and Subscription** module in the **Network Operations** app.



If an application is not provisioned, that application is not listed in the **New User** pop-up window.

- **Network Operations**—Select a user role for the **Network Operations** application. If you assign the user role **guestoperator**, **readonly**, or **readwrite**, from the **Select Groups** drop-down list, select group(s). By default, the **admin** user role has access to all groups.
4. Click **Save**. An email invite is sent to the user with a registration link. Users can use this link to access Aruba Central.

Resend Email Invite

If any user has not received the email invite, complete the following steps to resend the invite:

1. Click **Actions** and slide the **Resend Invitation To Users** toggle button to the right.
2. Enter the email ID and click **Resend Invite**.

Viewing User Details

In the **Account Home** page, under **Global Settings**, click **Users and Roles**. The **Users** tab opens. The **List of Users** table displays the following information:

- Email ID of the user.
- Type of user. The user can be system user or external user.
- Description of the user.
- Role assigned for the **Network Operations** application.
- Role assigned for the **Account Home** page.
- Allowed groups for the user.
- Last active time of the user. If the last active time cell is blank, the user has not logged in after the product upgrade.

Editing a User

To edit a user account, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**.
The **Users** tab opens.
2. In the **List of Users** table, select the user and click the edit icon.
3. In the **Edit User <"Username">** window, modify description, role, or allowed groups.
4. Click **Save**.

Deleting a User

To delete a user account:

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**.
The **Users** tab opens.
2. In the **List of Users** table, select the user and click the delete icon.
3. Confirm user deletion in the **Confirm Action** dialog box.

Viewing Audit Trail Logs for Users

Audit logs are generated when a new user is created and an existing user is modified or deleted from the Aruba Central account. It also records the login and logout activities of users.

To view audit logs for Aruba Central users:

1. In the **Account Home** page, under **Global Settings**, click **Audit Trail**.
The **Audit Trail** page opens.
2. To view audit logs for user addition, modification, or deletion, click the filter in the **Classification** column, and select **User Management**.
3. To filter audit logs about user activity, click the filter in the **Classification** column, and select **User Activity**.

Configuring User Roles

A role refers to a logical entity used for determining user access to devices and application services in Aruba Central. Users are always tagged to roles that govern the level of user access to the Aruba Central applications and services.



Access control for federated users is determined by the attributes set in the IdP.

Aruba Central supports a set of predefined roles with different privileges and access permissions. You can also configure custom roles.

Predefined User Roles

The **Users and Roles** page allows you to configure the following types of users with system-defined roles:

Table 160: *Predefined User Roles*

Application	User Role	Privilege
Account Home	admin	Administrator for the Account Home page. If there are common modules between Account Home and other app(s), the Account Home user role has higher precedence and the user is granted permission if the operation is initiated from the Account Home page.
	readwrite	Can view and modify settings in the Account Home page and all Global Settings pages.
	readonly	Can view the Account Home page and all Global Settings pages.
Network Operations	admin	Administrator for the Network Operations application. Has access to Account Home > Global Settings . This is applicable only if the Account Home role is not set or is not conflicting.
	deny-access	Cannot view the Network Operations application.
	guestoperator	Has guest operator access for the Network Operations application. User does not have access to Account Home > Global Settings .
	readonly	Has read-only access to Account Home > Global Settings and the Network Operations application.
	readwrite	Has read-write access to Account Home > Global Settings and the Network Operations application. Has access to view and modify data using the Aruba Central UI or APIs. However, the user cannot execute APIs to: Perform operations in the following pages: <ul style="list-style-type: none"> ■ Account Home > Users & Roles ■ Network Operations application > Organization > Labels and Sites

Custom Roles

Along with the predefined user roles, Aruba Central also allows you to create custom roles with specific security requirements and access control. However, only users with the administrator role and privileges can create, modify, clone, or delete a custom role in Aruba Central.

With custom roles, you can configure access control at the application level and specify access rights to view or modify specific application services or modules. For example, you can create a custom role that allows access to a specific applications like **Group Management** or **Network Management** and assign it to a user.



MSP tenant account users cannot add, edit, or delete roles.

Adding a Custom Role

The following are the permissions that you can associate with a custom role:

- User roles with **Modify** permission can perform add, edit, or delete actions within the specific module.
- User roles with **View Only** permission can only view the specific module.
- User roles with **Block** permission cannot view that particular module.

To add a custom role, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**.
2. Click the **Roles** tab.
3. Click **Add Role**. The **New Role** window is displayed.
4. Specify a name for the role.
5. From the drop-down list, select one of the following:
 - **Account Home**—To manage access to devices and subscriptions in Aruba Central.**Network Operations**—To set permissions at the module level in the **Network Operations** application.
6. For Network Management, you can set access rights at the module level. To set view or edit permissions or block the users from accessing a specific module, complete the following steps:
 - a. Click **Customize**.
 - b. Select one of the following options for each module as required:
 - **View Only**
 - **Modify**
 - **Block**
7. Click **Save**.
8. Assign the role to a user account as required.

Module Permissions

Aruba Central allows you to define user roles with **view** or **modify** permissions. You can also block user access to some modules. For example, if the **Guest Access** module is blocked for a specific user role, the corresponding pages are not displayed in the UI.

Aruba Central supports setting permissions for the following modules:

Table 161: *Permissions*

Application	Module	Description
Account Home	Devices and Subscription	Allows users to add devices and assign keys and subscriptions to devices.

Application	Module	Description
Network Operations	Group Management	Allows users to create, view, modify, and delete groups and assign devices to groups.
	Devices and Subscription	Allows users to add devices and assign subscriptions to devices.
	Network Management	Allows users to configure, troubleshoot, and monitor Aruba Central-managed networks.
	VisualRF	Allows user to access VisualRF and RF heatmaps.
	Unified Communications	Allows users to access the Unified Communications pages.
	Reports	Allows users to view and create reports.
	Other Applications	Allows users to access other applications modules such as notifications and Virtual Gateway deployment service.

Viewing User Role Details

To view the details of a user role, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**.
2. Click the **Roles** tab. The **Roles** tab displays the following information:
 - **Role Name**—Name of the user role.
 - **Allowed Applications**—The applications to which the users have access.
 - **Assigned Users**—Number of users assigned to a role.

Editing a User Role

To edit a user role, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**.
2. Click the **Roles** tab.
3. In the **List of Roles** table, select the role and click the edit icon.
4. In the **Edit Role <"Rolename">** window, modify the permissions set for module(s).
5. Click **Save**.

Deleting a User Role

To delete a user role, ensure that the role is not associated to any user and complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**.
2. Click the **Roles** tab.
3. In the **List of Roles** table, select the role and click the delete icon.
4. Confirm role deletion in the **Confirm Action** dialog box.

Two-Factor Authentication

Aruba Central (on-premises) supports two-factor authentication for both computers and mobile phones to offer a second layer of security to your login, in addition to password. When two-factor authentication is enabled on a user account, the users can sign in to their Aruba Central (on-premises) account either through the mobile app or the web application, only after providing their password and the six-digit verification code displayed on their trusted devices.

When two-factor authentication is enabled at the customer account level, all the users belonging to the customer account are required to complete the authentication procedure when logging in to Aruba Central (on-premises). If a user account is associated with multiple customer accounts and if two-factor authentication is enabled on one of these accounts, the user must complete the two-factor authentication during the login procedure.

If two-factor authentication is enabled on your accounts, you must install the Google Authenticator app on your devices such as mobile phones to access the Aruba Central (on-premises) application. When the users attempt to log in to Aruba Central (on-premises) with their credentials, the Google Authenticator app provides a six-digit verification code to complete the login procedure.

Installing the Google Authenticator App

For two-factor authentication, ensure that the Google Authenticator app is installed on your mobile device.

During the registration process, the Aruba Central (on-premises) application shares a secret key with the mobile device of the user over a secure channel when the user logs in to Aruba Central (on-premises). The key is stored in the Google Authenticator app and used for future logins to the application. This prevents unauthorized access to a user account as this authentication procedure involves two-levels for secure transaction.

When you register your mobile device successfully, the Google Authenticator app generates a six-digit token for the second level authentication. The token is generated every thirty seconds.

Enabling Two-factor Authentication for User Accounts

To enable two-factor authentication, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**.
The **Users and Roles** page is displayed.
2. From the **Actions** menu, slide the **Two-Factor Authentication (2FA)** toggle button to the right.
The two-factor authentication is enabled for all the users associated with the account.

Two-factor Authentication for Aruba Central (on-premises) Web Application

When two-factor authentication is enabled for a customer account, the users associated with that customer account are prompted for two-factor authentication when they log in to Aruba Central (on-premises).

To complete two-factor authentication, perform the following actions:

1. Access the Aruba Central (on-premises) website.
2. Log in with your credentials. If two-factor authentication is enforced on your account, the two-factor authentication page opens.
3. Install the Google Authenticator app on your mobile device if not already installed.
4. Click **Next**.

5. If this is your first login since two-factor authentication is enforced on your account, open Google Authenticator on your mobile device.
6. Scan the QR Code. If you are unable to scan the QR code, perform the following actions:
 - a. Click the **Problem in Reading QR Code** link. The secret key is displayed.
 - b. Enter this secret key in the Google Authenticator app.
 - c. Ensure that the **Time-Based** parameter is set. Aruba Central is added to the list of supported clients and a six-digit token is generated.
7. Click **Next**.
8. Enter the six-digit token.
9. Select the **Remember 2FA for 30 Days** check box if you want the authentication to expire only after 30 days.
10. Click **Finish**.

Two-factor Authentication for the Aruba Central (on-premises) Mobile App

Two-factor authentication must first be enabled for your account. If two-factor authentication is not enabled, you log in to the application directly after a successful SSO authentication.

To log in to Aruba Central (on-premises) app on your mobile device, perform the following actions:

1. Open the Aruba Central (on-premises) app on your mobile device.
2. Enter your username and password and click **Log in**. If the registration process is pending, an error message is displayed:

Please register for two-factor authentication in our web app to ensure secured authentication.
3. Enter the token. On successful authentication, the Aruba Central (on-premises) app opens.

Registering a New Mobile Device

If you have changed your mobile device, you need to install Google Authenticator app on your new device and register again using a web browser on your Desktop for two-factor authentication.

To register your new mobile device, complete the following steps:

1. Log in to Aruba Central (on-premises) web application. The two-factor authentication page is displayed.
2. Click the **Changed Your Mobile Device?** link.
3. To register your new device and receive a reset email with instructions, click **Send 2FA Reset Email**. A reset email with instructions will be sent to your registered email address.
4. Follow the instructions in the email and complete the registration.

Support Access

Aruba technical support may ask you to enable **Support Access** to debug issues. After you enable **Support Access**, the Aruba support team can access your Aruba Central account remotely. Only users with administrator role can enable **Support Access**.

Enabling Support Access

To enable **Support Access**, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**.
The **Users and Roles** page is displayed.
2. From the **Actions** menu, slide the **Support Access** toggle button to the right.
3. Set password expiry by selecting the number of days and click **Get Password**. A new password is generated.
4. Copy the password and share it with the Aruba technical support representative.

Disabling Support Access

After the remote support session is complete, do the following to disable **Support Access**:

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**.
The **Users and Roles** page is displayed.
2. From the **Actions** menu, slide the **Support Access** toggle button to the left.

Managing Sites

The **Sites** page allows you to create sites, view the list of sites configured in your setup, and assign devices to sites. The **Sites** page includes the following functions:

Table 162: *Sites Page*

Name	Contents of the Table
Convert Labels to Sites	Allows you to convert existing labels to sites. To convert labels, download the CSV file with the list of labels configured in your setup, add the site information, and upload the CSV file. For more information, see Managing Sites and Labels .
Sites table	<p>Displays a list of sites configured. It provides the following information:</p> <ul style="list-style-type: none"> ■ Site Name—Name of the site. ■ Address—Physical address of the site. ■ Device Count—Number of devices assigned to a site. <p>The table also includes the following sorting options to reset the table view on the right:</p> <ul style="list-style-type: none"> ■ All Devices—Displays all the devices provisioned in Aruba Central. ■ Unassigned—Displays the list of devices that are not assigned to any site. <p>You can also use the filter and sort icons on the Sites and Address columns to filter and sort sites respectively.</p>
New Site	Allows you to create a new site.
Bulk upload	Allows you to add sites in bulk from a CSV file.
Devices table	<p>Displays a list of devices provisioned. It provides the following information:</p> <ul style="list-style-type: none"> ■ Name—Name of the device ■ Group—Group to which the device is assigned. ■ Type—Type of the device.

Creating a Site

To create a label, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Sites** tile.
The **Manage Sites** page is displayed.
4. To add a new site, click **(+) New Site**. The **Create New Site** pop-up window opens.

5. In the **Create New Site** pop-up window, enter the following details:
 - a. **Site Name**—Name of the site. The site name can be a maximum of 255 single byte characters. Special characters are allowed.
 - b. **Street Address**—Address of the site.
 - c. **City**—City in which the site is located.
 - d. **Country**—Country in which the site is located.
 - e. **State/Province**—State or province in which the site is located.
 - f. **ZIP/Postal Code**—(Optional) ZIP or postal code of the site.
6. Click **Add**. The new site is added to the **Sites** table.

Adding Multiple Sites in Bulk

To import site information from a CSV file in bulk, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Sites** tile.
The **Manage Sites** page is displayed.
4. Click **(+) Bulk upload**. The **Bulk Upload** pop-up opens.
5. Download a sample file.
6. Fill the site information and save the CSV file in your local directory.



The CSV file for bulk upload of sites must include the mandatory information such as the name, address, city, state, and country details.

7. In the Aruba Central UI, click **Browse** and add the file from your local directory.
8. Click **Upload**. The sites from the CSV file are added to the site table.

Assigning a Device to a site

To assign a device to a site, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Sites** tile.
The **Manage Sites** page is displayed.
4. Select **Unassigned**. The list of devices that are not assigned to any site is displayed.
5. Select device(s) from the list of devices.
6. Drag and drop the devices to the site on the left. A pop-up window opens and prompts you to confirm the site assignment.
7. Click **Yes**.

Convert Existing Labels to Sites

To convert existing labels to sites, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Sites** tile.
The **Manage Sites** page is displayed.
4. Click **Convert Labels to Sites**. The **Confirm Conversion** pop-up window opens.
5. To download a CSV file with the list of labels configured in your setup, click **Download a File**. A CSV file with a list of all the labels in your setup is downloaded to your local directory.
6. Enter address, city, state, country, and ZIP code details for the labels that you want to convert to sites.



In the CSV file, you must enter the following details: address, city, state, and country.

7. Save the CSV file.
8. On the **Confirm Conversion** pop-up window, click **Browse** and select the CSV file with the list of labels to convert.
9. Click **Upload**.
10. Click **Convert**. The labels are converted to sites.

Points to Note

- If the conversion process fails for some labels, Aruba Central generates and opens an Excel file showing a list of labels that could not be converted to sites. Verify the reason for the errors, update the CSV file, and re-upload the file.
- Aruba Central does not allow conversion of sites to labels. If the existing labels are converted to sites, you cannot revert these sites to labels.
- When the existing labels are converted to sites, Aruba Central retains only the historical data for these labels. Aruba Central displays the historical data for these labels only in reports and on the monitoring dashboard.

Editing a Site

To edit a site, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Sites** tile.
The **Manage Sites** page is displayed.
4. Select the site to edit and click the edit icon.
5. Modify the site information and click **Update**.

Deleting a Site

To delete a site, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Sites** tile.
The **Manage Sites** page is displayed.
4. Select the site to delete and click the delete icon.
5. Confirm deletion.

Managing Labels

Labels are tags attached to a device provisioned in the network. Labels determine the ownership, departments, and functions of the devices. You can use labels for creating a logical set of devices and use these labels as filters when monitoring devices and generating reports.

Table 163: *Labels*

Name	Contents of the Table
Labels	<p>Displays a list of labels configured. The table provides the following information:</p> <ul style="list-style-type: none">■ Name of the label■ Number of devices assigned to a label <p>The table also includes the following sorting options to reset the table view on the right:</p> <ul style="list-style-type: none">■ All Devices—Displays all the devices provisioned in Aruba Central.■ Unassigned—Displays the list of devices that are not assigned to any label.
Devices	<p>Displays a list of devices provisioned. The table provides the following information about the devices:</p> <ul style="list-style-type: none">■ Name—Name of the device■ Group—Group to which the device is assigned■ Type—Type of the device■ Labels—Number of labels assigned to a device

Device Classification

The devices can also be classified using **Groups** and **Sites**.

- The group classification can be used for role-based access to a device, while labels can be used for tagging a device to a location or a specific area at a physical site. However, if a device is already assigned to a group and has a label associated with it, it is classified based on both groups and labels.
- The site classification is used for logically grouping devices deployed at a given physical location. You can also convert labels to sites.

Creating a Label

To create a label, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Labels** tile.
The **Manage Labels** page is displayed.
4. To add a new label, click **(+) Add Label**. The **Create New Label** pop-up window opens.
5. Enter a name for the label. The label name can be a maximum of 255 single byte characters. Special characters are allowed.
6. Click **Add**. The new label is added to the **All Labels** table.

Assigning a Device to a Label

To assign a device to a label, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Labels** tile.
The **Manage Labels** page is displayed.
4. Locate the label to which you want to assign a device.
5. In the table that lists the labels, you can perform one of the following actions:
 - Click **All Devices** to view all devices.
 - Click **Unassigned** to view all the devices that are not assigned to any labels.
6. Select **Unassigned**. The list of devices that are not assigned to any label is displayed.
7. Select device(s) from the list of devices.
8. Drag and drop the selected device(s) to a specific label. A pop-up window asking you to confirm the label assignment opens.
9. Click **Yes**.



Aruba Central (on-premises) allows you to assign up to five label tags per device.

Detaching a Device from a Label

To remove a label assigned to a device, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Labels** tile.
The **Manage Labels** page is displayed.
4. Select the device from the table on the right.

5. Click the delete icon.
6. To detach labels from the multiple devices at once, select the devices, and click **Batch Remove Labels**.
7. Confirm deletion.

Editing a label

To edit a label, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Labels** tile.
The **Manage Labels** page is displayed.
4. Select the label to edit.
5. Click the edit icon.
6. Edit the label and click **Update**.

Deleting a label

To delete a label, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Labels** tile.
The **Manage Labels** page is displayed.
4. Select the label to delete.
5. Click the delete icon.
6. Confirm deletion.

Managing Sites

The **Sites** page allows you to create sites, view the list of sites configured in your setup, and assign devices to sites. The **Sites** page includes the following functions:

Table 164: *Sites Page*

Name	Contents of the Table
Convert Labels to Sites	Allows you to convert existing labels to sites. To convert labels, download the CSV file with the list of labels configured in your setup, add the site information, and upload the CSV file. For more information, see Managing Sites .
Sites table	Displays a list of sites configured. It provides the following information: <ul style="list-style-type: none"> ■ Site Name—Name of the site. ■ Address—Physical address of the site. ■ Device Count—Number of devices assigned to a site.

Name	Contents of the Table
	<p>The table also includes the following sorting options to reset the table view on the right:</p> <ul style="list-style-type: none"> ■ All Devices—Displays all the devices provisioned in Aruba Central. ■ Unassigned—Displays the list of devices that are not assigned to any site. <p>You can also use the filter and sort icons on the Sites and Address columns to filter and sort sites respectively.</p>
New Site	Allows you to create a new site.
Bulk upload	Allows you to add sites in bulk from a CSV file.
Devices table	<p>Displays a list of devices provisioned. It provides the following information:</p> <ul style="list-style-type: none"> ■ Name—Name of the device ■ Group—Group to which the device is assigned. ■ Type—Type of the device.

Creating a Site

To create a site, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Sites** tile.
The **Manage Sites** page is displayed.
4. To add a new site, click **(+) New Site**. The **Create New Site** pop-up window opens.
5. In the **Create New Site** pop-up window, enter the following details:
 - a. **Site Name**—Name of the site. The site name can be a maximum of 255 single byte characters. Special characters are allowed.
 - b. **Street Address**—Address of the site.
 - c. **City**—City in which the site is located.
 - d. **Country**—Country in which the site is located.
 - e. **State/Province**—State or province in which the site is located.
 - f. **ZIP/Postal Code**—(Optional) ZIP or postal code of the site.
6. Click **Add**. The new site is added to the **Sites** table.

Adding Multiple Sites in Bulk

To import site information from a CSV file in bulk, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Sites** tile.
The **Manage Sites** page is displayed.
4. Click **(+) Bulk upload**. The **Bulk Upload** pop-up opens.
5. Download a sample file.
6. Fill the site information and save the CSV file in your local directory.



The CSV file for bulk upload of sites must include the mandatory information such as the name, address, city, state, and country details.

7. In the Aruba Central UI, click **Browse** and add the file from your local directory.
8. Click **Upload**. The sites from the CSV file are added to the site table.

Assigning a Device to a site

To assign a device to a site, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Sites** tile.
The **Manage Sites** page is displayed.
4. Select **Unassigned**. The list of devices that are not assigned to any site is displayed.
5. Select device(s) from the list of devices.
6. Drag and drop the devices to the site on the left. A pop-up window opens and prompts you to confirm the site assignment.
7. Click **Yes**.

Convert Existing Labels to Sites

To convert existing labels to sites, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Sites** tile.
The **Manage Sites** page is displayed.
4. Click the **Sites and Labels** tab.
5. Set the toggle switch to **Site(s)**.
6. Click **Convert Labels to Sites**. The **Confirm Conversion** pop-up window opens.
7. To download a CSV file with the list of labels configured in your setup, click **Download a File**. A CSV file with a list of all the labels in your setup is downloaded to your local directory.
8. Enter address, city, state, country, and ZIP code details for the labels that you want to convert to sites.



In the CSV file, you must enter the following details: address, city, state, and country.

9. Save the CSV file.
10. On the **Confirm Conversion** pop-up window, click **Browse** and select the CSV file with the list of labels to convert.
11. Click **Upload**.
12. Click **Convert**. The labels are converted to sites.

Points to Note

- If the conversion process fails for some labels, Aruba Central generates and opens an Excel file showing a list of labels that could not be converted to sites. Verify the reason for the errors, update the CSV file, and re-upload the file.
- Aruba Central does not allow conversion of sites to labels. If the existing labels are converted to sites, you cannot revert these sites to labels.
- When the existing labels are converted to sites, Aruba Central retains only the historical data for these labels. Aruba Central displays the historical data for these labels only in reports and on the monitoring dashboard.

Editing a Site

You can edit a site to modify the site details such as site name, street address, city, county, state, or zip or postal code.

To modify a site details, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Sites** tile.
The **Manage Sites** page is displayed.
4. Select the site to edit and click the  edit icon.
5. Modify the site information and click **Update**.

Deleting a Site

If you no longer need a site, you can delete it.

To delete a site, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Sites** tile.
The **Manage Sites** page is displayed.
4. Select the site to be deleted and click the  delete icon.
A confirmation window is displayed.



Deleting a site disassociates all devices that are associated with it. However, your network and devices will continue to operate normally.

5. Click **Yes** to confirm.
The site is deleted and devices associated with the site are moved to the unassigned devices list.

Site Search Terms

The search bar helps you to search a site's information in the **Network Operation** app.

Using the search bar you can perform the following tasks:

- Hover over a client search card to view the monitoring summary for the site.
- Click the client name to open the **Site Details** page.

Following is an example for the site search:

Figure 54 Search Card for a Site



Managing Labels

Labels are tags attached to a device provisioned in the network. Labels determine the ownership, departments, and functions of the devices. You can use labels for creating a logical set of devices and use these labels as filters when monitoring devices and generating reports.

Table 165: Labels

Name	Contents of the Table
Labels	<p>Displays a list of labels configured. The table provides the following information:</p> <ul style="list-style-type: none"> ■ Name of the label ■ Number of devices assigned to a label <p>The table also includes the following sorting options to reset the table view on the right:</p> <ul style="list-style-type: none"> ■ All Devices—Displays all the devices provisioned in Aruba Central. ■ Unassigned—Displays the list of devices that are not assigned to any label.
Devices	<p>Displays a list of devices provisioned. The table provides the following information about the devices:</p> <ul style="list-style-type: none"> ■ Name—Name of the device ■ Group—Group to which the device is assigned ■ Type—Type of the device ■ Labels—Number of labels assigned to a device

Device Classification

The devices can also be classified using **Groups** and **Sites**.

- The group classification can be used for role-based access to a device, while labels can be used for tagging a device to a location or a specific area at a physical site. However, if a device is already assigned to a group and has a label associated with it, it is classified based on both groups and labels.
- The site classification is used for logically grouping devices deployed at a given physical location. You can also convert labels to sites.

Creating a Label

To create a label, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Labels** tile.
The **Manage Labels** page is displayed.
4. To add a new label, click **(+) Add Label**. The **Create New Label** pop-up window opens.
5. Enter a name for the label. The label name can be a maximum of 255 single byte characters. Special characters are allowed.
6. Click **Add**. The new label is added to the **All Labels** table.

Assigning a Device to a Label

To assign a device to a label, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Labels** tile.
The **Manage Labels** page is displayed.
4. Locate the label to which you want to assign a device.
5. In the table that lists the labels, you can perform one of the following actions:
 - Click **All Devices** to view all devices.
 - Click **Unassigned** to view all the devices that are not assigned to any labels.
6. Select **Unassigned**. The list of devices that are not assigned to any label is displayed.
7. Select device(s) from the list of devices.
8. Drag and drop the selected device(s) to a specific label. A pop-up window asking you to confirm the label assignment opens.
9. Click **Yes**.



Aruba Central (on-premises) allows you to assign up to five label tags per device.

Detaching a Device from a Label

To remove a label assigned to a device, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Labels** tile.
The **Manage Labels** page is displayed.
4. Select the device from the table on the right.

5. Click the delete icon.
6. To detach labels from the multiple devices at once, select the devices, and click **Batch Remove Labels**.
7. Confirm deletion.

Editing a label

To edit a label, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Labels** tile.
The **Manage Labels** page is displayed.
4. Select the label to edit.
5. Click the edit icon.
6. Edit the label and click **Update**.

Deleting a label

To delete a label, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Labels** tile.
The **Manage Labels** page is displayed.
4. Select the label to delete.
5. Click the delete icon.
6. Confirm deletion.

Certificates provide a secure way of authenticating devices and eliminate the need for less secure password-based authentication. In certificate-based authentication, digital certificates are used to identify a user or device before granting access to a network or application.

Digital certificates use PKI that requires a private-public key pair. A digital certificate is associated with a private key, known only to the certificate owner and a public key. A certificate encrypted with a private key is decrypted with its public key. For example, party A encrypts its certificate with its private key and sends it to party B. Party B decrypts the certificate with the public key of party A. Server certificates and the digital certificates issued by a CA validate the identities of servers and clients. For example, when a client connects to a server for the first time, or the first time since its previous certificate has expired or been revoked, the server requests that the client transmit its authentication certificate and verifies it. Clients can also request and verify the authentication certificate of the server.

Device Certificates

Aruba devices use digital certificates for authenticating a client's access to user-centric network services. Most devices such as controllers and Instant APs include the certificate of the CA who issued the server certificate for captive portal server authentication. However, Aruba recommends that you replace the default certificate with a custom certificate issued for your site or domain by a trusted CA. Certificates can be stored locally on the devices and used for validating device or user identity during authentication.

Viewing the Certificate Store Parameters

To view the certificate store parameters, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain > Organization**
By default, the **Network Structure** tab is displayed.
3. Click the **Certificates** tile.
The **CERTIFICATES** page is displayed.
4. Expand the **Appliance Certificates** to view the **Certificate Store** table.
5. If required, expand the **Device Certificates** accordion to view the **Certificate Store** table.

Table 166: *Certificate Store Parameters*

Parameter	Description
Certificate Name	Name of the certificate.
Status	Status of the certificate.
Expiry Date	Expiry date of the certificate.

Parameter	Description
Type	Type of certificate.
MD5 Checksum	The Message Digest 5 algorithm is a widely used hash function producing a 128-bit hash value from the data input.
SHA-1 Checksum	The Secure Hash Algorithm 1 is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value.

In the **Certificate Store** table, click on the  hamburger icon to display the required columns.

Uploading Device Certificates

To upload certificates, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain > Organization**.
By default, the **Network Structure** tab is displayed.
3. Click the **Certificates** tile.
The **CERTIFICATES** page is displayed.
4. If required, expand the **Device Certificates** accordion to view the **Certificate Store** table.
5. Click the  plus icon to add the certificate to the **Certificate Store**.
6. In the **Add Certificate** dialog box, do the following:

Parameter	Description
Name	Specify the name of the Certificate.
Type	From the Type drop-down list, select of certificate type. You can select any one of the following certificates: <ul style="list-style-type: none"> ■ CA—Digital certificates issued by the CA. ■ Server—Server certificates required for communication between devices and authentication servers. ■ CRL—Certificate Revocation List that contains the serial numbers of certificates that have been revoked. This certificate is required for performing a certificate revocation check. ■ OCSP Responder Cert—OCSP responder certificates. ■ OCSP Signer Cert—OCSP Response Signing Certificate. The OCSP certificates are required for OCSP server authentication.
Format	From the Format drop-down list, select a certificate format. You can select any one of the following certificates: <ul style="list-style-type: none"> ■ PEM—Privacy Enhanced Mail is a Base64 encoded DER certificate. ■ DER—Distinguished Encoding Rules files are digital certificates in binary format. Both digital certificates and private keys can be encoded in DER format. ■ PKCS12—Public-Key Cryptography Standards 12 is an archive file format for

Parameter	Description
	storing many cryptography objects as a single file. For more information, see Viewing the Certificate Store Parameters .
Passphrase	In the Passphrase text box, enter a passphrase.
Retype Passphrase	In the Retype Passphrase text box, retype the passphrase for confirmation. The Passphrase and Retype Passphrase text boxes are displayed only when you select Server Certificate from the Type drop-down list.
Certificate File	In the Certificate File field, click Choose File and browse to the location where the certificates are stored and select the certificate files.
Click Add . The certificate is added to the Certificate Store .	

Deleting Device Certificates

To delete certificates, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain > Organization**
By default, the **Network Structure** tab is displayed.
3. Click the **Certificates** tile.
The **CERTIFICATES** page is displayed.
4. In the **Certificate Store** table, select the certificate that you want to delete and click the delete icon.
The **Confirm Action** pop-up window is displayed.
5. Click **Yes** in the **Confirm Action** pop-up window to delete the certificate.

Appliance Certificates

By default, Aruba Central includes a self-signed certificate that is available on the **Global Settings > Certificates** page.

Viewing the Certificate Store Parameters

To view the certificate store parameters, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain > Organization**
By default, the **Network Structure** tab is displayed.
3. Click the **Certificates** tile.
The **CERTIFICATES** page is displayed.
4. Expand the **Appliance Certificates** to view the **Certificate Store** table.

For viewing the certificate store parameters, refer to [Certificate Store Parameters](#)

Uploading Appliance Certificates

To view the certificate store parameters, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain > Organization**
By default, the **Network Structure** tab is displayed.
3. Click the **Certificates** tile.
The **CERTIFICATES** page is displayed.
4. Expand the **Appliance Certificates** to view the **Certificate Store** table.
5. Click the **+** plus icon to add the certificate to the **Certificate Store**.
6. In the **Add Certificate** dialog box, do the following:

Parameter	Description
Name	Specify the name of the Certificate.
Type	From the Type drop-down list, select of certificate type. You can select any one of the following certificates: <ul style="list-style-type: none"> ■ CA—Digital certificates issued by the CA. ■ Server—Server certificates required for communication between devices and authentication servers. ■ API Gateway Certificate—This is a certificate that will be presented by Aruba Central (on-premises) when the user connects to the url : apigateway-<FQDN> , and also when the user connects via a script tool.
Format	From the Format drop-down list, select a certificate format. You can select any one of the following certificates: <ul style="list-style-type: none"> ■ PEM—Privacy Enhanced Mail is a Base64 encoded DER certificate. ■ DER—Distinguished Encoding Rules files are digital certificates in binary format. Both digital certificates and private keys can be encoded in DER format. ■ PKCS12—Public-Key Cryptography Standards 12 is an archive file format for storing many cryptography objects as a single file.
Passphrase	In the Passphrase text box, enter a passphrase.
Retype Passphrase	In the Retype Passphrase text box, retype the passphrase for confirmation. The Passphrase and Retype Passphrase text boxes are displayed only when you select Server Certificate from the Type drop-down list.
Certificate File	In the Certificate File field, click Choose File and browse to the location where the certificates are stored and select the certificate files.
Click Add . The certificate is added to the Certificate Store .	

Deleting Appliance Certificates

To delete certificates, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain > Organization**
By default, the **Network Structure** tab is displayed.
3. Click the **Certificates** tile.
The **CERTIFICATES** page is displayed.
4. In the **Certificate Store** table, select the certificate that you want to delete and click the delete icon.
The **Confirm Action** pop-up window is displayed.
5. Click **Yes** in the **Confirm Action** pop-up window to delete the certificate.

Certificate Signing Request

Aruba Central also supports Certificate Signing Request (CSR) generation.

To generate CSR for certificates, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain > Organization**
By default, the **Network Structure** tab is displayed.
3. Click the **Certificates** tile.
The **CERTIFICATES** page is displayed.
4. Under **Appliance Certificate**, click **Generate and Download Certificate Signing Request (CSR)**.
5. The **Add Certificate Signing Request** is displayed.
6. Enter the following details:

Parameter	Description
Distinguished Name	Unique name
Organization	Name of your organization.
Department Name	Department name of your organization.
City	Name of the city of your organization.
State	Name of the state of your organization.
Country	Country code of your organization. See List of accepted country codes .
Email Address	Contact email address.

7. Click **Add**. A PEM file with both the public and private key is generated and downloaded automatically.
8. Remove the private key for root CA certification. After the root CA signs the certificate, add the private key, and upload the PEM file again.

Supported Certificate Formats

The following section describes the different certificate formats supported in Aruba Central (on-premises).

PEM Format

The PEM format is the most common format that Certificate Authorities issue certificates in. PEM certificates usually have extensions such as .pem, .crt, .cer, and .key. They are Base64 encoded ASCII files and contain "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" statements. Server certificates, intermediate certificates, and private keys can all be put into the PEM format.

Apache and other similar servers use PEM format certificates. Several PEM certificates, and even the private key, can be included in one file, one below the other, but most platforms, such as Apache, expect the certificates and private key to be in separate files. For more information, see [Sample PEM file](#).

DER Format

The DER format is a binary form of a certificate instead of the ASCII PEM format. It sometimes has a file extension of .der but it often has a file extension of .cer so the only way to tell the difference between a DER .cer file and a PEM .cer file is to open it in a text editor and look for the BEGIN/END statements. All types of certificates and private keys can be encoded in DER format. DER is typically used with Java platforms. The SSL Converter can only convert certificates to DER format. If you need to convert a private key to DER, use the OpenSSL commands on this page.

PKCS#12 or PFX Format

The PKCS#12 or PFX format is a binary format for storing the server certificate, any intermediate certificates, and the private key in one encryptable file. PFX files usually have extensions such as .pfx and .p12, .PFX files are typically used on Windows machines to import and export certificates and private keys.

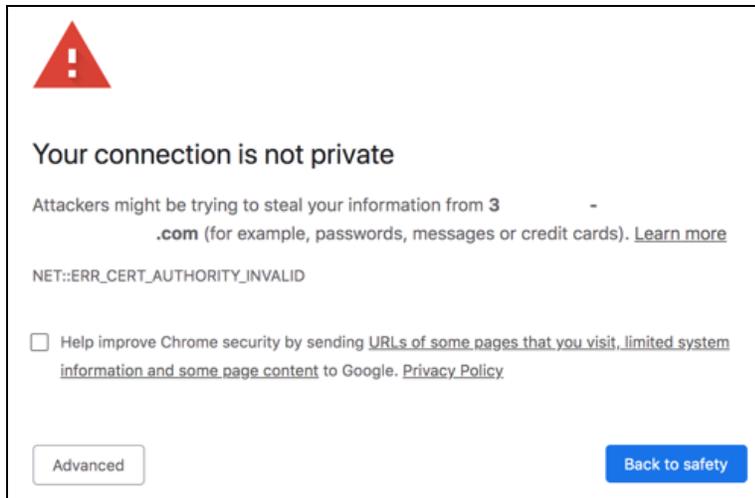
When converting a PFX file to PEM format, OpenSSL will put all the certificates and the private key into a single file. You will need to open the file in a text editor and copy each certificate and private key (including the BEGIN/END statements) to its own individual text file and save them as certificate.cer, CACert.cer, and privateKey.key respectively.

Wildcard Certificates

A wildcard certificate is a digital certificate that is applied to a domain and all its subdomains. SSL certificates use the wildcards to extend SSL encryptions to subdomains. All the wildcard certificates have a * in their common names. For example, a certificate that has *.arubathena.com in its common name, is a wildcard certificate.

Once Aruba Central (on-premises) is installed by the user, a self-signed certificate gets generated automatically and this certificate is not provided by any authorized CA providers. So, when you access the Aruba Central (on-premises) server using an FQDN, the browser displays a warning, **Your Connection is not private**, because this certificate is not trusted by the browser.

Figure 55 *Connection Status*



The following section describes how to check the status of the certificates, request for a certificate, and upload the certificate.

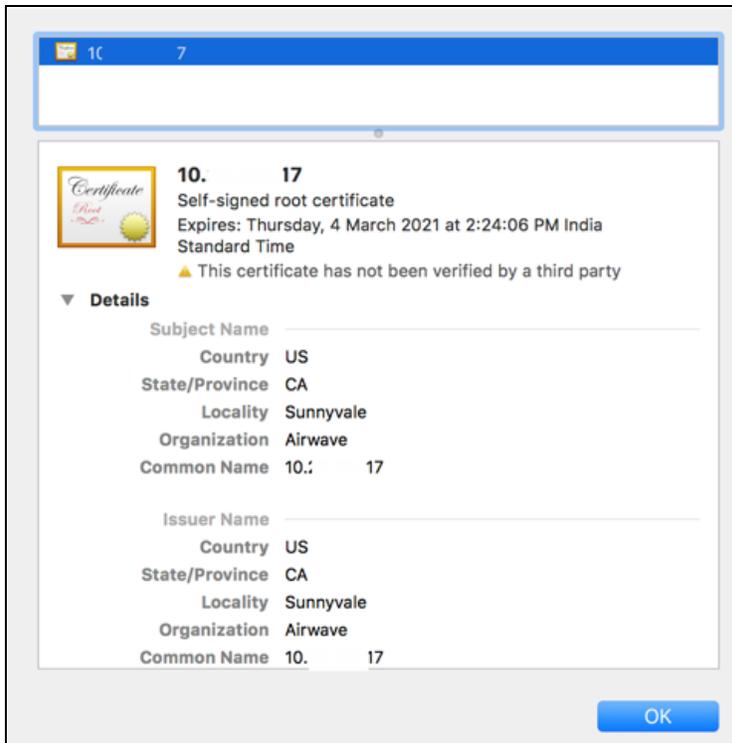
Checking the Status of the Certificate

To check the status or validity of a certificate, perform the following steps:

1. Login to the Aruba Central (on-premises) server.
2. Click the view site information icon next to the URL in the browser.
3. Click **Certificates**.

The certificate information is displayed. Here, you can check if the certificate is self-signed certificate and more details like Country, Issues Name, etc.

Figure 56 Certificate Details



Requesting for Wildcard certificate

If the certificate is not secure or invalid, ensure to request for a wildcard certificate or a certificate for the FQDN of the Aruba Central (on-premises) server from an authorized certificate provider to resolve the certificate error.

Uploading the Wildcard Certificate

Once you get the certificates required, upload the certificate in the Aruba Central (on-premises) system. Perform the following steps to add the wildcard certificate:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain > Organization**
By default, the **Network Structure** tab is displayed.
3. Click the **Certificates** tile.
The **CERTIFICATES** page is displayed.
4. Expand the **Appliance Certificates** to view the **Certificate Store table**.
5. Click the **+** plus icon to add the certificate to the **Certificate Store**.
6. In the **Add Certificate** dialog box, enter the name.
7. Select **Server Certificate** from the **Type** drop-down list.
8. Select **PEM** from the **Format** drop-down list.
9. Enter the **Passphrase** and **Retype Passphrase**.
10. In the **Certificate File** field, click **Choose File** and browse to the location where the certificates are stored and select the wildcard certificate.



The PEM file contains the certificates and the private key. The private key must be in the PEM format and appended after all the certificates. For more information, see [Sample PEM format](#).

11. Click **Add**.

The new valid certificate is successfully added.

12. Once the valid certificate is uploaded, ensure to check the status of the certificate. For the steps, see [Checking the Status of the Certificate](#)

The wildcard certificate information is displayed.



This wildcard certificate can be applied to any server where the FQDN has one hostname followed by .domainname.com. The same wildcard certificate cannot be used for servers which have other formats like *.aw.domainname.com.

Following is a sample of the certificate file in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIG2jCCBcKgAwIBAgIRAObNusiWw5M1dV3y8sEeS0cwDQYJKoZIhvcNAQELBQAw
gZaxCzAJBgNVBAYTAkdCMRswGQYDVQQIEExJHcmVhdGVyIE1hbmNoZXN0ZXIxEDA0
BgNVBAcTB1NhbGZvcmlkLWlncy4wLW9udC51LWVudC51LWVudC51LWVudC51LWVudC51
VQQDEy1DT01PRE8gUlNBIERvbWVpbiBwYXN0LWVudC51LWVudC51LWVudC51LWVudC51
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIGCDCCA/CgAwIBAgIQKy5u6t11NmWUim7bo3yMBzANBgkqhkiG9w0BAQwFADCB
hTElMAkGA1UEBHMCR0IxBGZAZBgNVBAgTEkdyZWF0ZXIgdWVudC51LWVudC51LWVudC51
A1UEBxMhU2FsZm9yZDEaMBGGA1UEChMRQ09NT0RPIENBIExpbW10ZWQxKzApBgNV
BAMTIkNPTU9ETyBSU0EgQ2VydGlmYWVhdG1vbiBBdXR0b3JpdHkwHhcNMTQwMjE1
MDAwMDAwWhcNMjkwMjE1MjM1OTU5WjCBkDELMAkGA1UEBHMCR0IxBGZAZBgNVBAgT
/qJakXz1ByjAA6quPbYzSf+AZxAeKCINT+b72x
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIFdDCCBFygAwIBAgIQJ2buVutJ846r13Ci/ITeIjANBgkqhkiG9w0BAQwFADBv
MQswCQYDVQQGEwJTRTEUMBIGA1UEChMLQWRkVHJ1c3QgQUxJjAkBgNVBAStHUFk
ZFRydXN0IEV4dGVybmFsIFRUUCBOZXR3b3JrMSIwIAYDVQQDExlBZGRUcnVzdCBF
eHRlcm5hbCBDQSBSb290MB4XDTEwMDUzMDUzMDUzMDUzMDUzMDUzMDUzMDUzMDUz
gYUxZCzAJBgNVBAYTAkdCMRswGQYDVQQIEExJHcmVhdGVyIE1hbmNoZXN0ZXN0
IxEDA0
-----END CERTIFICATE-----

-----BEGIN PRIVATE KEY-----
MIIEvwIBADANBgkqhkiG9w0BAQEFAASCBBKkwggSlAgEAAoIBAQDXApH0YGDko8W
nYWSR+k3AFxYzVoVMriJnodHEc+lYccWoBHWz1P/P8GkhRInHsPpA3RvG5idz/Jj
bi8RkKbWmNuu6DpBLPHexed8wpbmZ/O9CZAYTbe5OHNC+igzhZ5U6nk4b71xfth
mchBWAgaAKbzfmGiCQ/Gak/RTEqKtULDgBu3Em1GFzlmzE+yDRsHLqYtdGK+D2U6
v8rUXr+IGZfd2aWhTuZtCuOA+7rP9HexR2K776kqXLxj9jflj5rPH5N1VTNO1FUS
-----END PRIVATE KEY-----
```

As part of the shift to an Edge-to-Cloud Platform-as-a-Service organization, Aruba has introduced the Aruba Central (on-premises) Foundation and Advanced Licenses (Aruba Central (on-premises) Licenses). This is a uniform software subscription licensing model that will be extended to all products under the Aruba Central (on-premises)-managed portfolio. The new 1, 3, 5, 7, and 10-year fixed-term licenses offer you the flexibility to choose services and device operations that are most meaningful to the type of business that you own. This licensing model provides different licenses for APs, switches, and controllers.



The licenses for APs, switches, and controllers cannot be used interchangeably. For example, you cannot use an AP Foundation License on a controller. Similarly, if you have an Aruba 25xx Switch but the license available is for an Aruba 29xx Switch, the Aruba 29xx Switch license cannot be applied to the Aruba 25xx Switch.

All the Aruba Central (on-premises) features are available in the Foundation Licenses and have different monitoring and configuration options depending on the licensing tier.

This licensing model provides the following types of licenses depending on the devices:

- Switches:
 - **Foundation**—This license provides all the features included in the legacy Device Management tokens.



Aruba Central (on-premises) does not provide Switch Advanced Licenses.

- Access Points (APs):
 - **Foundation**—This license provides all the features included in the legacy Device Management tokens and some additional features that were available as value-added services for APs and switches in the earlier licensing model.
 - **Advanced**—This license provides all the features included in the Foundation License and in the future releases will provide support for additional features.
- Controllers:
 - **Foundation WLAN Gateway**—This license provides all features required for Controller functionality in all deployment types.



The Foundation and Advanced Licenses for APs, switches, and controllers are different and cannot be used interchangeably.

Changes to the Legacy Licensing Model

For existing Aruba Central (on-premises) customers, please note that the previous Device Management and Service Token model is changed to the new licensing model, which provides a uniform licensing structure for all types of devices such as APs, switches, and controllers.

The following list provides information about important aspects of the legacy licensing model:

- **Device Management Token**—This is a mandatory token which allows you to manage and monitor your APs and switches from Aruba Central.
- **Service Token**—This token allows you to enable value-added services for APs managed from Aruba Central.

The new Aruba Central (on-premises) Licenses simplify the existing subscription-based licensing model. With the introduction of this licensing model, the existing Device Management tokens for APs and switches are no longer available. Similarly, the Service tokens for value-added services on the APs are unavailable. Instead, APs and switches have adopted the current Foundation license model.

Supported Devices

The Aruba Central (on-premises) Licenses are supported for APs, switches, and controllers. For more information on the individual device models supported, refer to the next sections. The pricing structure for Foundation and Advanced Licenses for the hardware devices may differ based on the types of models.

APs and IAPs

All AP and IAP models that are currently being shipped are supported. See [Supported APs](#).

Switches

Aruba Central (on-premises) supports AOS-Switch and AOS-CX switches.

AOS-Switches

The following AOS-Switches are supported:

- Aruba 2540 Switch Series
- Aruba 2920 Switch Series
- Aruba 2930F Switch Series
- Aruba 2930M Switch Series
- Aruba 3810 Switch Series
- Aruba 5400R Switch Series

For more information, see [Supported AOS-Switch Platforms](#).

AOS-CX Switches

The following AOS-CX switches are supported:

- AOS-CX 4100i Switch Series
- AOS-CX 6000 Switch Series
- AOS-CX 6100 Switch Series
- AOS-CX 6200 Switch Series
- AOS-CX 6300 Switch Series
- AOS-CX 6400 Switch Series
- AOS-CX 8320 Switch Series
- AOS-CX 8325 Switch Series
- AOS-CX 8360 Switch Series
- AOS-CX 8400 Switch Series

For more information, see [Supported AOS-CX Switch Platforms](#).

Controllers

Aruba Central (on-premises) supports controllers based on the license type.

For more information, see [Supported Aruba Mobility Controllers](#).

WLAN Gateway Foundation License

The WLAN Gateway Foundation can be assigned to the following controllers:

- Aruba 70xx Series
- Aruba 72xx Series

This license does not have a capacity limit for client devices.

For more information about the **Auto-Assign Licenses** option, see [Enabling the Auto-Assign Licenses Option](#).

For an Aruba Central (on-premises) evaluation account, four licenses of each base SKU are assigned to the account. These evaluation licenses are valid for 90 days.

You can track licenses on the **Key Management** page or the **License Assignment** page available from the **Account Home** page.

Managing License Assignments

Aruba offers two tiers of device licenses as part of the Aruba Central Licenses. The two tiers are Foundation and Advanced Licenses. The devices in Aruba Central that offer Foundation and Advanced Licenses include the following:

- APs
- Switches
- Controllers

The value-added services that previously required service subscriptions are now packaged as part of either a Foundation or an Advanced License. To know more about the different types of licenses available for the devices, and the services packaged with each license, see [Managing Licenses](#).

Licensing Workflow for a New User

If you are a new user in Aruba Central and have purchased one or several licenses, ensure that all of your license keys are added to Aruba Central.

For license assignment to devices, you can avail of one of the following options:

- Use the **Auto-Assign Licenses** option
- Manually assign, update, or unassign licenses

Enabling the Auto-Assign Licenses Option

The **Auto-Assign Licenses** option in Aruba Central (on-premises) enables automatic assignment of available licenses to all of the devices available in the inventory. When you enable this option, you must specify the preferred license type as either Foundation or Advanced. You cannot manually assign licenses to devices if the **Auto-Assign Licenses** option is enabled.



The licenses for APs, switches, and controllers cannot be used interchangeably. For example, you cannot use an AP Foundation License on a controller. Similarly, if an Aruba 25xx Switch is in the inventory but the license available is for an Aruba 29xx Switch, the Aruba 29xx Switch license cannot be applied to the Aruba 25xx Switch. Before enabling the Auto-Assign License option for a specific device type, ensure that there are sufficient available licenses for the specific device type.

To enable automatic assignment of licenses from the License Assignment page:

1. On the **Account Home** page, under **Global Settings**, click **License Assignment**.
The **License Assignment** page is displayed.
2. Select the device type to assign the license.
The available tabs are Access Points, Switches, and Controllers. The total number of devices for each device type is displayed for each of the tabs.
3. On the device tab, slide the **Auto-Assign Licenses** toggle switch to the On position.
The **Manage License Assignment (Auto)** window is displayed.
4. Select the appropriate license type, **Foundation** or **Advanced**, from the drop-down menu, and then click **Update**.
All the unassigned devices of the selected type in the inventory are enabled for automatic assignment of license.

Manually Assigning, Updating, or Unassigning Licenses

The License Assignment page enables you to assign, update, or even unassign a license from a device. Aruba Central monitors devices with a valid license only.



The licenses for APs, switches, and controllers cannot be used interchangeably. For example, you cannot use an AP Foundation License on a controller. Similarly, if an Aruba 25xx Switch is in the inventory but the license available is for an Aruba 29xx Switch, the Aruba 29xx Switch license cannot be applied to the Aruba 25xx Switch.

To manually assign licenses to devices or to change the existing license assignment:

1. On the **Account Home** page, under **Global Settings**, click **License Assignment**.
The **License Assignment** page is displayed.
2. Select a device type tab.
The available tabs are **Access Points**, **Switches**, and **Controllers**. The total number of devices for each device type is displayed for each of the tabs.
3. Under **License Summary**, ensure that the **Auto-Assign Licenses** option is disabled.
You cannot manually assign licenses if the Auto-Assign Licenses option is enabled.
4. Select the device for which you want to assign or update the license.
Clicking on a device type displays two additional sub-tabs: **Licensed** and **Unlicensed**.



To manually assign or update licenses for all devices of a type, click **Select All**. You can also select devices at random.

5. Click **Manage**.
The **Manage License Assignment (Manual)** window is displayed.

6. Do one of the following:
 - a. To update or assign a license: Select the appropriate license from the drop-down menu and click **Update**.
 - b. To unassign a license: Select **Unassign** to remove the existing license from that device.

Viewing the License Assignment Details

The License Assignment page consists of three sections for the type of device selected from the tabs. The device can be **Access Points**, **Switches**, or **Controllers**.

License Summary

A summary about the type of licenses available for the selected device type, the number of licenses available, and number of licenses assigned.

The available devices for Aruba Central include APs, switches, and controllers. Clicking on a device type displays two additional sub-tabs: **Licensed** and **Unlicensed**.

Clicking on one or more license type in the License Summary section displays the details of the license type in the License Management section. To deselect the license, click the selected license type again.

License Assignment

The **License Assignment** section provides detailed information about all the devices in the inventory and license status for each of the device. This table provides following information about each device in the inventory:

- Type
- Serial Number
- MAC address
- Model
- Customer
- Assigned License

Use the sorting icon () in the table header row to arrange the rows in ascending or descending order. You can also use the row header indicated by the filter icon () to type in search queries to refine the search.

Renewing License Assignments

To renew your license, contact your Aruba Sales team.

The **Account Home > Global Settings > Authentication** page allows the administrator to manage and configure external authentication for users to have access to Aruba Central (on-premises). You can choose any one of the external authentication method to allow access to the user. By default, **None** is selected.

The **Authentication > External Authentication** page contains the following option:

- **Single-Sign-On**—Select this option to use SAML as an external authentication.
- **Radius**—Select this option to use Radius as an external authentication.
- **None**—Select this option to use none of the external authentication. In this scenario, the authentication is done internally.

Configuring SAML SSO for Aruba Central

The Single Sign On (SSO) solution simplifies user management by allowing users to access multiple applications and services with a single set of login credentials. If the applications services are offered by different vendors, IT administrators can use the SAML authentication and authorization framework to provide a seamless login experience for their users.

To provide seamless login experience for users whose identity is managed by an external authentication source, Aruba Central now offers a federated SSO solution based on the SAML 2.0 authentication and authorization framework. SAML is an XML-based open standard for exchanging authentication and authorization data between trusted partners; in particular, between an application service provider and identity management system used by an enterprise. With Aruba Central's SAML SSO solution, organizations can manage user access using a single authentication and authorization source.

Solution Overview

The SAML SSO solution consists of the following key elements:

- **Service Provider (SP)**—The provider of a business function or service; For example, Aruba Central. The service provider requests and obtains an identity assertion from the IdP. Based on this assertion, the service provider allows a user to access the service.
- **Identity Provider (IdP)**—The Identity Management system that maintains identity information of the user and authenticates the user.
- **SAML request**—The authentication request that is generated when a user tries to access the Aruba Central portal.
- **SAML Assertion**—The authentication and authorization information issued by the IdP to allow access to the service offered by the service (Aruba Central portal).
- **Relying Party**—The business service that relies on SAML assertion for authenticating a user; For example, Aruba Central.
- **Asserting Party**—The Identity management system or the IdP that creates SAML assertions for a service provider.
- **Metadata**—Data in the XML format that is exchanged between the trusted partners (IdP and Aruba Central) for establishing interoperability.

- SAML attributes—The attributes associated with the user; for example, username, customer ID, role, and group in which the devices belonging to a user account are provisioned. The SAML attributes must be configured on the IdP according to specifications associated with a user account in Aruba Central. These attributes are included in the SAML assertion when Aruba Central sends a SAML request to the IdP.
- Entity ID—A unique string to identify the service provider that issues a SAML SSO request. According to the SAML specification, the string should be a URL, although not required as a URL by all providers.
- Assertion Services Consumer URL—The URL that sends the SAML request and receives the SAML response from the IdP.
- User—User with SSO credentials.



Aruba Central SAML SSO solution supports only the HTTP Redirect POST method for sending and receiving SAML requests and response.

The SAML SSO integration allows federated users to access only the Central UI. The API Gateway access is restricted to system users that are configured and managed from Aruba Central.

How It Works

Aruba Central supports the following types of SAML SSO workflows:

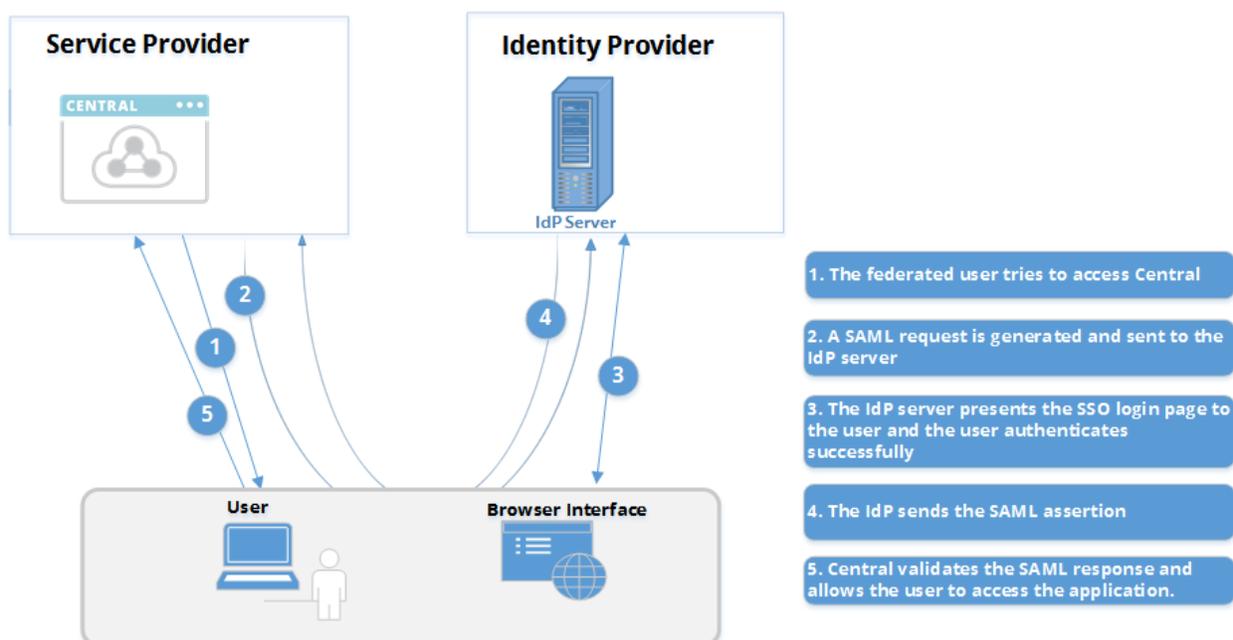
- SP-initiated SSO
- IdP-initiated SSO

SP-initiated SSO

In an SP Initiated SSO workflow, the SSO request originates from the service provider domain, that is, from Aruba Central. When a user tries to access Aruba Central, a federation authentication request is created and sent to the IdP server.

The following figure illustrates the standard SP-Initiated SAML SSO workflow:

Figure 57 *SP-Initiated SSO*



The SP-initiated SSO workflow with Aruba Central is supported only through the HTTP Redirect POST method. In other words, Aruba Central sends an HTTP redirect message with an authentication request to the IdP through the user's browser. The IdP sends a SAML response with an assertion to Aruba Central through HTTP POST.

The SP-initiated SSO workflow with HTTP Redirect POST includes the following steps:

1. The user tries to access Aruba Central and the request is redirected to the IdP.
2. Aruba Central sends an HTTP redirect message with the SAML request to the IdP for authentication through the user's browser.
3. The user logs in with the SSO credentials.
4. On successful authentication, the IdP sends a digitally signed HTML form with SAML assertion and attributes to Aruba Central through the web browser.
5. If the digital signature and the attributes in the SAML assertion are valid, Aruba Central allows access to the user.

IdP-initiated SSO

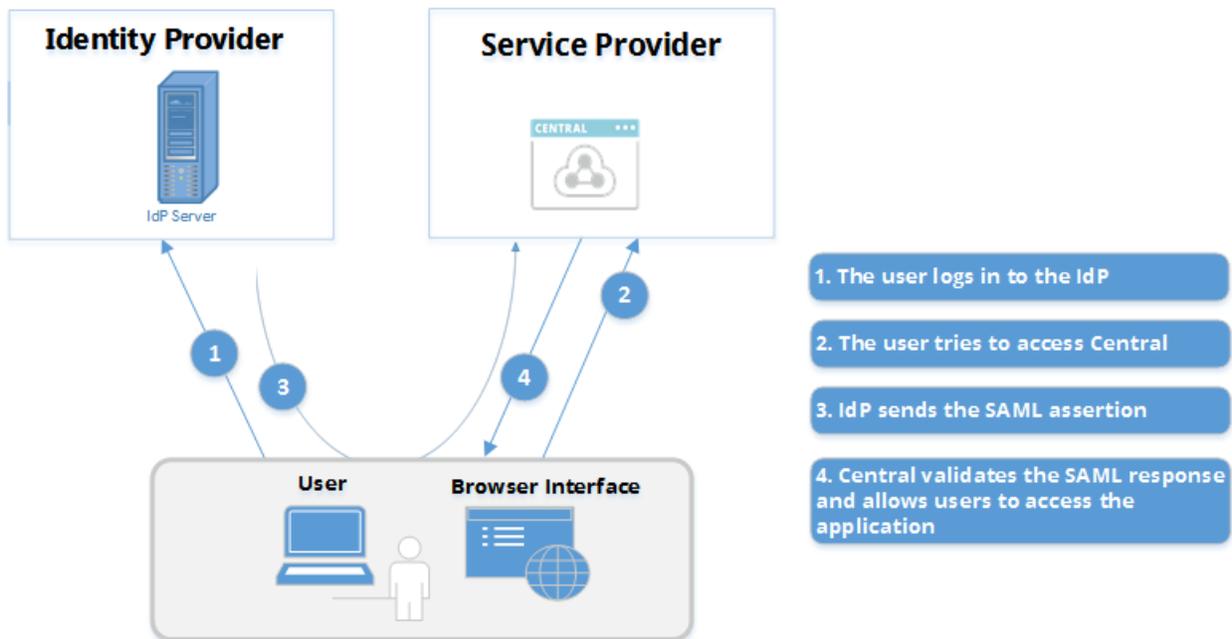
In the IdP-Initiated workflow, the SSO request originates from the IdP domain. The IdP server creates a SAML response and redirects the users to Aruba Central.

The Aruba Central SAML SSO deployments support the IdP-initiated SSO workflow through the HTTP POST method. The IdP-initiated SSO workflow consists of the following steps:

1. The user is logged in to the IdP and tries to access Aruba Central.
2. The IdP sends a digitally signed HTML form with SAML assertion and attributes to Aruba Central through the web browser.
3. If the digital signature and the attributes in the SAML assertion are valid, Aruba Central allows access to the user.

The following figure illustrates the standard IdP-Initiated SAML SSO workflow:

Figure 58 *IdP-Initiated SSO*



SAML Single Logout

Aruba Central supports Single Logout (SLO) of SAML SSO users. SLO allows users to terminate server sessions established using SAML SSO by initiating the logout process once. SAML SLO can be initiated either from the Service Provider or the IdP. However, Aruba Central supports only the IdP-initiated SLO.

IdP-initiated SAML SLO

The IdP-initiated logout workflow includes the following steps:

1. User logs out of the IdP.
2. The IdP sends a logout request to Aruba Central.
3. Aruba Central validates the logout request from the IdP, terminates the user session, and sends a logout response to the IdP.
4. User is logged out of Aruba Central.
5. After the IdP receives logout response from all service providers, the IdP logs out the user.

Configuration Steps

The SAML SSO configuration for Aruba Central includes the following steps:

1. Configuring user accounts and roles in Aruba Central. For more information, see the *Managing User Access* topic in *Aruba Central Help Center*.
2. Configure SAML authorization profile in Aruba Central. For more information, see [Configuring SAML Authorization Profiles in Aruba Central](#).
3. Configuring Service Provider metadata such as metadata URL, service consumer URL, Name and other attributes on the IdP server. For more information, see [Configuring Service Provider Metadata in IdP](#).

Configuring SAML Authorization Profiles in Aruba Central

For SAML SSO solution with Aruba Central, you must configure a valid SAML authorization profile in the Aruba Central portal.

Important Points to Note

- The SAML authorization profile configuration feature is available only for the admin users of an Aruba Central account.
- Each domain can have only one federation. There must be at least one verified user belonging to the domain in the system users' list.
- Aruba Central allows only one authorization profile per domain.
- SAML user access is determined by the role attribute included in the SAML token provided by the IdP.
- SAML users with admin privileges can configure system users in Aruba Central.
- SAML users can initiate a Single Sign On request by trying to log in to Aruba Central (SP-initiated login). However, SAML users cannot initiate a single logout request from Aruba Central.
- The following menu options in Aruba Central UI are not available for a SAML user.
 - **Change Password**—Aruba Central does not support changing the password of a SAML user account.

Before You Begin

Before you begin, ensure that you have the following information:

- Entity ID—A unique string that identifies the service provider that issues a SAML SSO request. According to the SAML specification, the string should be a URL, although not required as URL by all providers.
- Login URL—Login URL configured on the IdP server.
- Logout URL—Logout URL configured on the IdP server.
- Certificate details—SAML signing certificate in the Base64 encoded format. The SAML signing certificates are required for verifying the identity of IdP server and relying applications such as Aruba Central.
- Metadata URL—Service provider metadata URL configured on the IdP server.



SAML profiles can also be configured using NB APIs. If you want to use NB APIs for configuring SAML profiles, use the APIs available under the **SSO Configuration** category in Aruba Central API Gateway.

Configuring a SAML Authorization Profile

To configure SAML authorization profiles in Aruba Central:

1. In the **Account Home** page, under **Global Settings**, click **Single Sign On**. The **Single Sign On** page opens.
2. To add an authorization profile, enter the domain name.



Ensure that the domain has at least one verified user.

For public cloud deployments, Aruba Central does not support adding **hpe.com**, **arubanetworks.com** and other free public domain names, such as Gmail.com, Yahoo.com, or Facebook.com, for SAML authorization profiles.

3. Click **Add SAML Profile**.
4. To manually enter the metadata:
 - a. Select **Manual Setting** and enter the following information:
 - **Entity ID**—Entity ID configured on the IdP server.
 - **Login URL**—Login URL configured on the IdP server.
 - **Logout URL**—Logout URL configured on the IdP server.
 - **Certificate**—Certificate details. Ensure that the certificate content is in the Base64 encoded format. You can either upload a certificate or paste the contents of the certificate in the text box.



Ensure that the Entity ID, Login URL, and Logout URL fields have valid HTTPS URLs.

- b. Click **Save**.

The following shows an example for the manual entry of metadata:

Figure 59 Manual Addition of Metadata

FEDERATED DOMAIN
adfsaruba.com

IDENTITY PROVIDER

Configure using
 MANUAL SETTING METADATA FILE

BASIC INFO

ENTITY ID
https://adfsaruba.in

LOGIN URL
https://adfsaruba.com/adfs/ls/

LOGOUT URL
https://adfsaruba.com/adfs/ls/?wa=wsignout1.0

CERTIFICATES

UPLOAD

CERTIFICATE
205RuLjtScgUGZybDqiG8LzxsuTH8E8Fggmt6A/EhB2D7IFkAkMiB0rOo2d+o2xL
DQc7VFyivS5Nng==

Save **Cancel**

5. If you have already configured the IdP server and downloaded the metadata file, you can upload the metadata file. To upload a metadata file:
 - a. Select **Metadata File**. Ensure that the metadata file is in the XML format and it includes valid certificate content and HTTPS URLs for the Entity ID, Login URL, and Logout URL fields.
 - b. Click **Browse** and select the IdP metadata file. Aruba Central extracts the **Entity ID**, **Login URL**, **Logout URL**, and certificate contents.
 - c. Verify the details.
 - d. Click **Save**.

The following shows an example for content imported from a metadata file:

Figure 60 *Importing Information from a Metadata File*

ADD SAML PROFILE

FEDERATED DOMAIN
example.com

IDENTITY PROVIDER

Configure using

MANUAL SETTING METADATA FILE

✓ metadata.xml REMOVE

BASIC INFO

ENTITY ID
https://aruba-test-idp.com/simplesaml/saml2/idp/metadata.php

LOGIN URL
https://aruba-test-idp.com/simplesaml/saml2/idp/SSOService.php

LOGOUT URL
https://aruba-test-idp.com/simplesaml/saml2/idp/SingleLogoutService.php

CERTIFICATES

UPLOAD

CERTIFICATE
MIIDkTCCAnmgAwIBAgIJAK2BK+oUKzywMA0GCSqGSIb3DQEBCwUAMF8xCzAJ...

Save Cancel

Configuring Service Provider Metadata in IdP

Aruba Central supports SAML SSO authentication framework with various Identity Management vendors such as [ADFS](#), [PingFederate](#), [Aruba ClearPass Policy Manager](#), and so on.

Aruba recommends that you look up the instructions provided by your organization for adding service provider metadata to the IdP server in your setup.

Some of the generic and necessary attributes required to be configured on the IdP server for SAML integration with Aruba Central are described in the following list:

- **Metadata URL**—URL that provides service provider metadata.
- **Entity ID**—A unique string that identifies the service provider that issues a SAML SSO request. According to the SAML specification, the string should be a URL, although not required as URL by all providers.
- **Assertion Services Consumer URL**—The URL that sends SAML SSO login requests and receives authentication response from the IdP.
- **NameID**—The **NameID** attribute must include the email address of the user.
`<NameID>johnnyadmin1@adfsaruba.com</NameID>`
- If the **NameID** attribute does not return the email address of the user, you can use the **aruba_user_email** attribute. Ensure that you configure the **NameID** or the **aruba_user_email** attribute for each user.
- **SAML Attributes**—The following example shows the syntax structure for SAML attributes:

```
#customer 1
# appl, scope1
aruba_1_app_1 = central
aruba_1_app_1_role_1 = <readonly>

aruba_1_app_1_group_1 = [groupx, groupy]
aruba_1_app_2 = account_setting
aruba_1_app_2_role_1 = <readonly>
```

```
#customer 2
# appl, scope1
aruba_2_app_1 = central
aruba_2_app_1_role_1 = <readonly>

aruba_2_app_1_group_1 = groupx, groupy
aruba_2_app_2 = account_setting
aruba_2_app_2_role_1 = <readonly>
```

Note the following points when defining SAML attributes in the IdP server:

- **cid**—Customer ID. If you have multiple customers, define attributes separately for each customer ID.
- **app**—Application. Set the value to as per the following:
 - **Network Operations**—central
 - **Account Home**—account_setting
- **role**—User role. Specify the user role. If no role is defined, Aruba Central assigns read-only role to the user.
- **group**—Group in Aruba Central. When a group is specified in the attribute, the user is allowed to access only the devices in that group. If the attribute does not include any group, Aruba Central allows SAML SSO users to access all groups. You can also configure custom attributes to add multiple groups if the user requires access to multiple groups.



Aruba Central recommends you to configure the **Account Home**. However, if you do not return the **Account Home** application from the Idp, then the **Network Operations** role is applied by default.

See Also:

- [Configuring Service Provider Metadata in Microsoft ADFS](#)
- [Configuring Service Provider Metadata in PingFederate IdP](#)
- [Configuring Service Provider Metadata in Aruba ClearPass Policy Manager](#)

Configuring Service Provider Metadata in Microsoft ADFS

This procedure describes the steps required for configuring service provider metadata in Microsoft Active Directory Federation Services (ADFS) for SAML integration with Aruba Central.

ADFS runs on Windows Servers and provides users with SSO access to application services hosted by the trusted service providers.



This topic provides a basic set of guidelines required for setting up the ADFS instance on a Windows Server 2016 as an IdP. The images used in this procedure may change with Windows Server updates.

Before you Begin

- Go through the [SAML SSO feature description](#) to understand how SAML framework works in the context of Aruba Central.
- Ensure that the ADFS is installed and available for configuration on a Windows server. For more information, see the [ADFS Deployment Guide](#).
- Ensure that an Active Directory security group is configured and the users are added as group members. For more information, see the [ADFS Deployment Guide](#).

Steps to Configure Service Provider Metadata in ADFS

To enable SAML integration with ADFS, complete the following steps:

- [Step 1—Add a Relying Party Trust](#)
- [Step 2—Configure the Name ID Attribute](#)
- [Step 3—Configure the Customer ID Attribute](#)
- [Step 4—Configure the Application Attribute](#)
- [Step 5—Configure the Role Attribute](#)
- [Step 6—Configure the Group Attribute](#)
- [Step 7—Configure the Logout URL](#)
- [Step 8—Exporting Token-signing Certificate](#)
- [Step 9—SAML Authorization Profile in Aruba Central](#)

Step 1—Add a Relying Party Trust

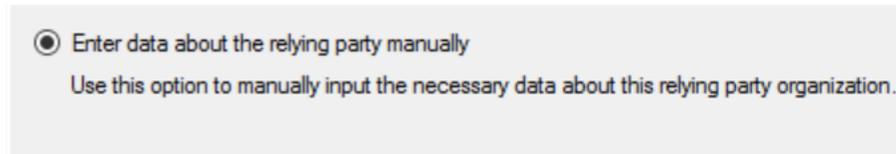
To configure Aruba Central and ADFS as trusted partners:

1. On Windows Server, click **Start > Administrative Tools > AD FS Management**. The ADFS administrative console opens.

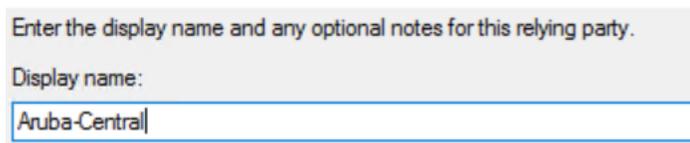
2. Click **AD FS** folder and select **Add Relying Party Trust** from the **Actions** menu.



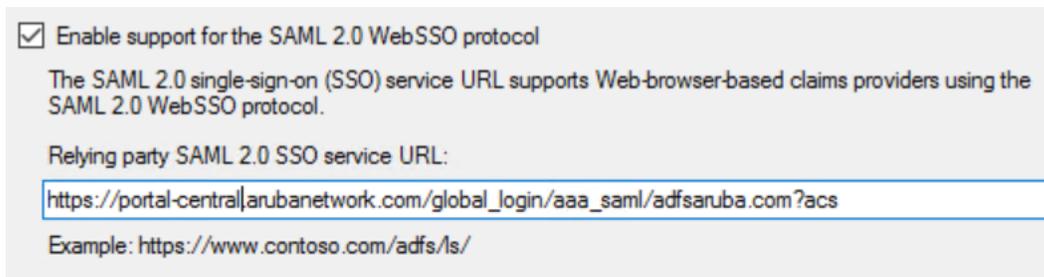
3. Select **Enter data about the relying party manually**.



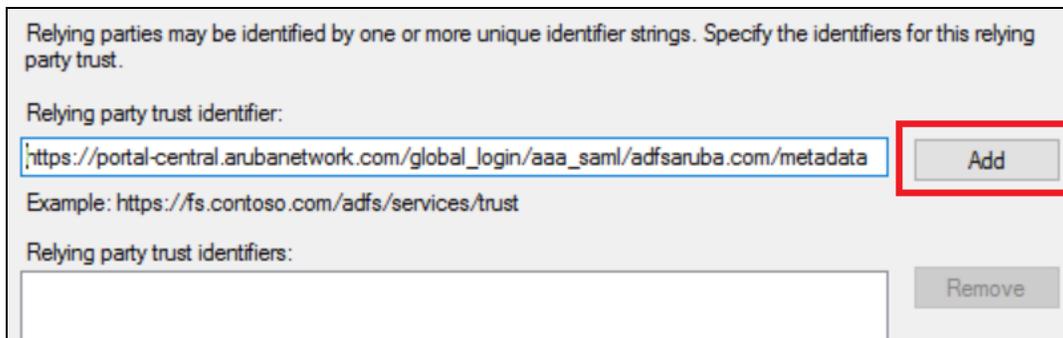
4. Click **Next**.
5. Enter a **Display Name**. The name entered here will be displayed in the management console and to the users logging in to Aruba Central.



6. Click **Next**.
7. Select **AD FS Profile** and then click **Next**.
8. Select **Enable support for the SAML 2.0 WebSSO protocol** check box and enter the consumer URL that you want to use for sending SAML SSO login requests and receiving SAML response from the IdP.



9. Click **Next**.
10. Add Aruba Central URL as the relying party trust identifier.



11. Click **Next**.
12. Select the preferred security setting. You can select **Permit all users to access this relying party** option to permit access to all users.

13. Click **Close**.
14. Verify if Aruba Central is added to the list of relying party trust.

Step 2—Configure the Name ID Attribute

The Name ID attribute is used for user identification. For SAML integration with Aruba Central, the Name ID attribute must include the email address of the user. If the Name ID attribute does not return the email address of the user, use the **aruba_user_email** attribute.

To configure the Name-ID attribute:

1. Select the display name you just added for Aruba Central and click **Edit Claim Issuance Policy**.
2. In the **Edit Claim Issuance Policy** window, click **Add Rule**.
3. Set the Claim Rule template to **Send LDAP Attributes as Claims rule**.

Claim rule template:
Send LDAP Attributes as Claims

4. Click **Next**.
5. In the **Claim rule name** text box, enter **Name-ID**.

Claim rule name:
Name-ID

Rule template: Send LDAP Attributes as Claims

Attribute store:
ldap

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	User-Principal-Name	Name ID

6. Select the LDAP as the **Attribute store**.
7. Select the **User-Principal-Name** as LDAP attribute and **Name ID** for the **Outgoing Claim Type**.
8. Click **Finish**.

Step 3—Configure the Customer ID Attribute

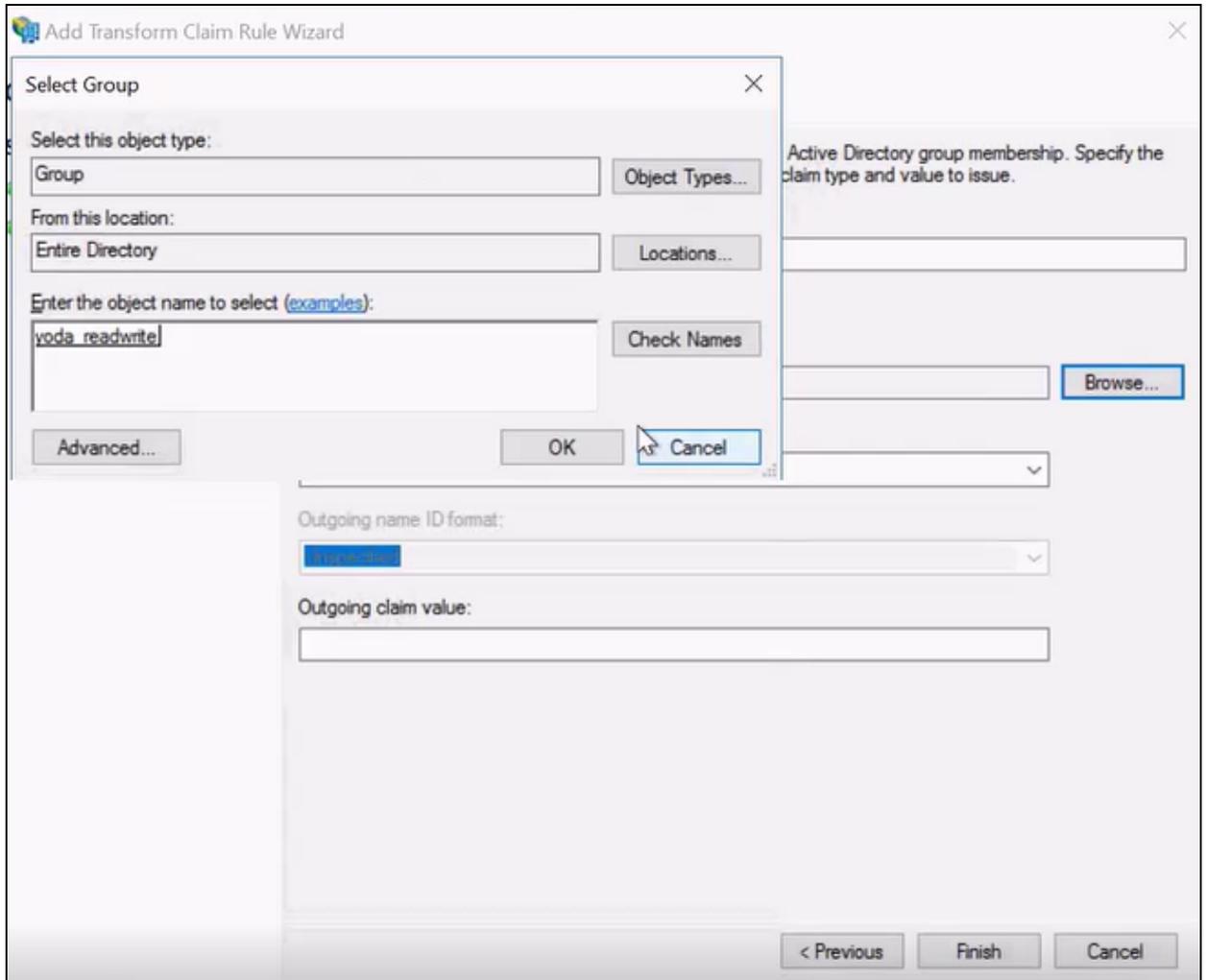
To create a rule with the customer ID attribute:

1. In the **Edit Claim Issuance Policy** window, click **Add Rule**.
2. To send a claim based on a user's Active Directory group membership, set the Claim Rule template to **Send Group Membership as a Claim**.

Claim rule template:
Send Group Membership as a Claim

3. Click **Next**.
4. In the **Claim rule name** text box, enter the customer ID attribute. For example, **aruba-cid**.

5. Select a user group.



6. Click **OK**.
7. Select a customer ID attribute for the **Outgoing claim rule** and enter a value for the **Outgoing claim value**.

Claim rule name:
Aruba-Central-Customer-ID

Rule template: Send Group Membership as a Claim

User's group:
ADFSARUBA\yoda-admin

Outgoing claim type:
aruba_1_cid

Outgoing name ID format:
Unspecified

Outgoing claim value:
12345678

8. Click **Finish**.
9. If you have multiple customers, define the customer ID attribute separately for each customer ID.

Step 4—Configure the Application Attribute

To add a rule for the application attribute:

1. In the **Edit Claim Issuance Policy** window, click **Add Rule**.
2. To send a claim based on a user's Active Directory group membership, set the Claim Rule template to **Send Group Membership as a Claim**.

Claim rule template:
Send Group Membership as a Claim

3. Click **Next**.
4. In the **Claim rule name** text box, enter the application attribute. For example, **Aruba Central App Name**.
5. Select a user group.
6. Select the application attribute for **Outgoing claim type** and enter a value for the **Outgoing claim value**.

Claim rule name:

Rule template: Send Group Membership as a Claim

User's group:

Outgoing claim type:

Outgoing name ID format:

Outgoing claim value:

7. Click **Finish**.

Step 5—Configure the Role Attribute

To add a rule for a role attribute:

1. In the **Edit Claim Issuance Policy** window, click **Add Rule**.
2. To send a claim based on a user's Active Directory group membership, set the Claim Rule template to **Send Group Membership as a Claim**.

Claim rule template:

3. Click **Next**.
4. In the **Claim rule name** text box, enter the application attribute. For example, **Aruba Central App Role**.
5. Select a user group.
6. Select the role attribute for **Outgoing claim type** and enter a value for the **Outgoing claim value**.

Claim rule name:

Rule template: Send Group Membership as a Claim

User's group:

Outgoing claim type:

Outgoing name ID format:

Outgoing claim value:

7. Click **Finish**.



If the role attribute is not configured, Aruba Central assigns a read-only role to the user.

Step 6—Configure the Group Attribute

If you want to restrict user access to a group in Aruba Central, you can configure the group attribute. If the group attribute is not configured, Aruba Central allows SAML SSO users to access all groups.

To add a rule for a group attribute:

1. In the **Edit Claim Issuance Policy** window, click **Add Rule**.
2. To send a claim based on a user's Active Directory group membership, set the Claim Rule template to **Send Group Membership as a Claim**.
3. Click **Next**.
4. In the **Claim rule name** text box, enter the application attribute. For example, **Aruba Central App Group**.
5. Select a user group.
6. Select a group attribute for **Outgoing claim type** and enter a value for the **Outgoing claim value**.
7. Click **Finish**.

Step 7—Configure the Logout URL

To enable IdP-initiated logout:

1. Select the relying party trust entry created for Aruba Central and click **Properties**.
2. Click **Endpoints**.
3. To add a logout URL, click **Add SAML**.
4. Select the endpoint type as **SAML Logout**.
5. Select **Redirect** for **Binding**.
6. Enter the Aruba Central logout URL for **Trusted URL**.

7. Enter the IdP logout URL for **Response URL**.

The screenshot shows the 'Edit Endpoint' dialog box with the following fields and values:

- Endpoint type: SAML Logout
- Binding: Redirect
- Set the trusted URL as default:
- Index: 0
- Trusted URL: https://portal-central.arubanetwork.com/global_login/aaa_saml/adfsaruba
- Example: https://sts.contoso.com/adfs/ls
- Response URL: https://adfsaruba.com/adfs/ls/?wa=wsignout1.0
- Example: https://sts.contoso.com/logout

Buttons: OK, Cancel, Apply (disabled).

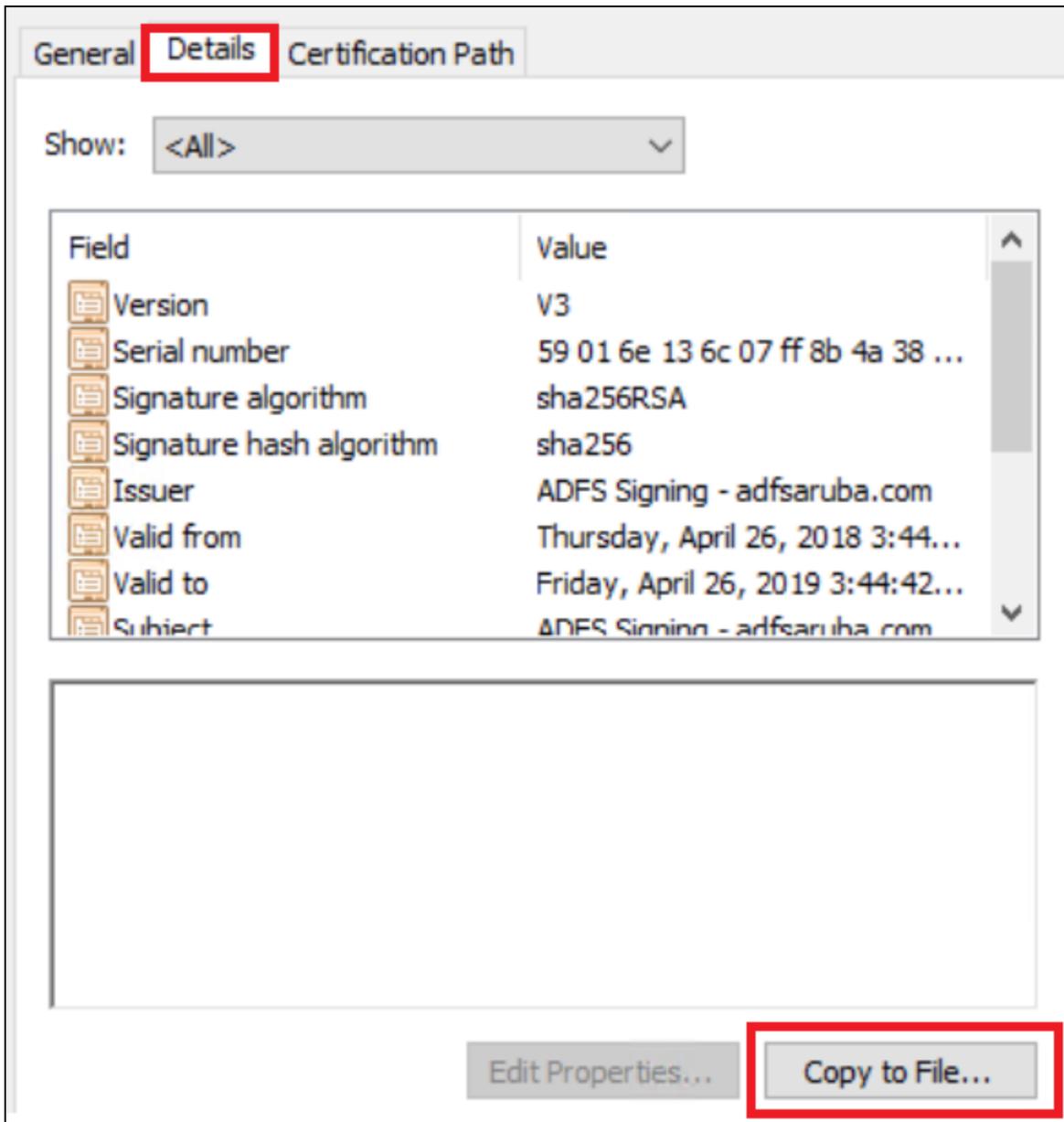
8. Click **OK**.

Step 8—Exporting Token-signing Certificate

The token-signing certificate is required SAML authentication. To export the token-signing certificate:

1. In the AD FS management console, go to **AD FS > Service > Certificates**.
2. Click the certificate under Token-signing and select **View Certificate** from the contextual menu.

3. Click **Details** > **Copy to File**.



4. Click **Next** and select **Base-64 encoded X.509 (.CER)** as the certificate format.
5. Click **Next**.
6. Save the certificate file on your local directory.

Step 9—SAML Authorization Profile in Aruba Central

For information on how to configure a SAML authorization profile, see [Configuring SAML Authorization Profiles in Aruba Central](#).

Configuring Service Provider Metadata in PingFederate IdP

This procedure describes the steps required for configuring service provider metadata in PingFederate.



This topic provides a basic set of guidelines required for service provider metadata on the PingFederate server. The images and attributes may change with PingFederate software updates.

Before you Begin

Go through the [SAML SSO feature description](#) to understand how SAML framework works in the context of Aruba Central.

Steps to Configure Service Provider Metadata in PingFederate

To configure service provider metadata in PingFederate, complete the following steps:

- [Step 1—Create an SP Connection Profile](#)
- [Step 2—Configure Browser SSO Settings](#)
- [Step 3—Configure Credentials](#)
- [Step 4—Review Configuration](#)
- [Step 5—SAML Authorization Profile in Aruba Central](#)

Step 1—Create an SP Connection Profile

1. Log in to the PingFederate administration console.
2. Click **IdP Configuration > SP Connections > Create New**. The **SP Connections** page opens.

MAIN

- Identity Provider
- Service Provider
- OAuth Server

SETTINGS

- Server Configuration

SP Connection

Connection Type	Connection Options	Metadata URL	General Info	Browser SSO	Credentials	Activation & Summary
-----------------	--------------------	--------------	--------------	-------------	-------------	----------------------

Select the type of connection needed for this SP: Browser SSO Profiles (for Browser SSO), WS-Trust STS (for access to Identity-enabled Web Services), Outbound Provisioning (for provisioning users/groups to an SP) or all.

CONNECTION TEMPLATE: No Template

BROWSER SSO PROFILES: PROTOCOL SAML 2.0

WS-TRUST STS

OUTBOUND PROVISIONING

3. In the **Connection Type** tab, select **Browser SSO Profiles**.

MAIN

- Identity Provider
- Service Provider
- OAuth Server

SETTINGS

- Server Configuration

SP Connection

Connection Type	Connection Options	Metadata URL	General Info	Browser SSO	Credentials	Activation & Summary
-----------------	--------------------	--------------	--------------	-------------	-------------	----------------------

Please select options that apply to this connection.

BROWSER SSO

IDP DISCOVERY

ATTRIBUTE QUERY

4. Click the **General Info** tab.

5. Verify the Entity ID and select the logging mode.

The screenshot shows the 'SP Connection' configuration page. On the left, there is a navigation menu with 'MAIN' at the top, followed by 'Identity Provider' (selected), 'Service Provider', and 'OAuth Server'. Below that is 'SETTINGS'. The main content area is titled 'SP Connection' and has four tabs: 'Connection Type', 'Connection Options', 'Metadata URL', and 'General Info'. Below the tabs, there is a text block explaining that the information identifies the partner's unique connection identifier (Connection ID). Below this, there are two input fields: 'PARTNER'S ENTITY ID (CONNECTION ID)' with the value 'https://asifalam.arubathena.com/global_logir' and 'CONNECTION NAME' with the value 'JohnnyCentral'. At the bottom, there is a 'LOGGING MODE' section with four radio buttons: 'NONE', 'STANDARD' (which is selected), 'ENHANCED', and 'FULL'.

6. Click **Next**. Configure the Browser SSO Settings.

Step 2—Configure Browser SSO Settings

1. On the **SP Connections** page in PingFederate administrative console, click **Browser SSO**.

The screenshot shows the 'SP Connection' configuration page with the 'Browser SSO' tab selected. The navigation menu on the left is the same as in the previous screenshot. The main content area has five tabs: 'Connection Type', 'Connection Options', 'Metadata URL', 'General Info', and 'Browser SSO' (selected). Below the tabs, there is a text block explaining that this task provides connection-endpoint and other configuration information enabling secure browser-based SSO. Below this, there is a 'BROWSER SSO CONFIGURATION' section with a 'Configure Browser SSO' button.

2. Click **Configure Browser SSO**.
3. Select the following SAML profiles:
 - Select IDP-INITIATED SSO
 - Select SP-INITIATED SSO

SP Connection | Browser SSO

SAML Profiles Assertion Lifetime Assertion Creation Protocol Settings Summary

A SAML Profile defines what kind of messages may be exchanged between an Identity Provider and a Service Provider, and I (bindings). As an IdP, you configure this information for your SP connection.

Single Sign-On (SSO) Profiles	Single Logout (SLO) Profiles
<input checked="" type="checkbox"/> IDP-INITIATED SSO	<input type="checkbox"/> IDP-INITIATED SLO
<input checked="" type="checkbox"/> SP-INITIATED SSO	<input type="checkbox"/> SP-INITIATED SLO

4. Click **Next**. The **Assertion Lifetime** tab opens.
5. Click **Next**. The **Assertion Creation** page opens.
 - a. Click **Configure Assertion Creation**. The **Assertion Creation** wizard opens.

SP Connection | Browser SSO | Assertion Creation

Identity Mapping Attribute Contract Authentication Source Mapping Summary

Identity mapping is the process in which users authenticated by the IdP are associated with user accounts local to the that you will send to the SP. Your selection may affect the way that the SP will look up and associate the user to a spe

STANDARD: Send the SP a known attribute value as the name identifier. The SP will often use account ma

PSEUDONYM: Send the SP a unique, opaque name identifier that preserves user privacy. The identifier ca identity at this IdP and may be used by the SP to make a persistent association between the user and a sp use account linking to identify the user locally.

INCLUDE ATTRIBUTES IN ADDITION TO THE PSEUDONYM.

TRANSIENT: Send the SP an opaque, temporary value as the name identifier.

INCLUDE ATTRIBUTES IN ADDITION TO THE TRANSIENT IDENTIFIER.

- b. Click **Next**. The **Attribute Contract** page opens.
- c. Add the SAML attributes in the SAML assertion. The IdP will send these attributes in the SAML Assertion.

SP Connection | Browser SSO | Assertion Creation

Identity Mapping | Attribute Contract | Authentication Source Mapping | Summary

An Attribute Contract is a set of user attributes that this server will send in the assertion.

Attribute Contract	Subject Name Format
SAML_SUBJECT	urn:oasis:names:tc:SAML:1.1:nameid-format:unspec

Extend the Contract	Attribute Name Format	Action
aruba_1_app_1	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	Edit Delete
aruba_1_app_1_role_1	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	Edit Delete
aruba_1_cid	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	Edit Delete
aruba_2_app_1	urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified	Edit Delete
aruba_2_app_1_role_1	urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified	Edit Delete
aruba_2_cid	urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified	Edit Delete

d. Click **Next**. The **Authentication Source Mapping** tab opens.

SP Connection | Browser SSO | Assertion Creation

Identity Mapping | Attribute Contract | Authentication Source Mapping | Summary

PingFederate uses IdP adapters, partner IdPs or Authentication Policies to authenticate users to your SP. Users may be authenticated by one of several different adapters or authentication policy contracts, so map an adapter instance for each IDM system or a authentication policy contract for each policy.

Adapter Instance Name	Virtual Server IDs	Action
OTKSAMLHPE		Delete

Authentication Policy Contract Name	Virtual Server IDs	Action
-------------------------------------	--------------------	--------

e. Click **Map New Adapter Instance**. The adapter configuration screen opens.

SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping

Adapter Instance | Mapping Method | Attribute Sources & User Lookup | Attribute Contract Fulfillment | Issuance Criteria

Summary

Attributes returned by the chosen adapter instance (the Adapter Contract) may be used to fulfill the Attribute Contract with your partner.

Adapter Instance	OTKSAMLHPE
------------------	------------

f. Complete the following configuration steps:

g. Click **Mapping Method** and select a mapping option.

RETRIEVE ADDITIONAL ATTRIBUTES FROM MULTIPLE DATA STORES USING ONE MAPPING

RETRIEVE ADDITIONAL ATTRIBUTES FROM A DATA STORE -- INCLUDES OPTIONS TO USE ALTERNATE DATA STORES AND/OR A FAILSAFE MAPPING

USE ONLY THE ADAPTER CONTRACT VALUES IN THE SAML ASSERTION

h. Click **Attribute Sources and User Lookup**

i. To add a data source, click **Add Attribute Store** and add the data store ID as shown in the following figure:

SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping | Attribute Sources & User Lookup

Data Store | Configure Custom Source Filters | Configure Custom Source Fields | Summary

Data stores are used to retrieve supplemental attributes. Specify the attribute store's details to use it in your configuration.

ATTRIBUTE SOURCE ID: IADHPECUSTOM

ATTRIBUTE SOURCE DESCRIPTION: IADHPECUSTOM

ACTIVE DATA STORE: IADHPE

DATA STORE TYPE: Custom

j. Click **Save**.

6. On the **SP Connections > Browser SSO Settings** page, click **Protocol Settings** to configure the Browser SSO Protocol Settings, SSO service URLs, and SAML bindings.

SP Connection | Browser SSO

SAML Profiles | Assertion Lifetime | Assertion Creation | Protocol Settings | Summary

This task provides the configuration for specific endpoints and security considerations applicable to selected profiles. revise this configuration.

Protocol Settings

OUTBOUND SSO BINDINGS: POST

INBOUND BINDINGS: POST, Redirect

SIGNATURE POLICY: SAML-standard, Authn requests over POST & Redirect

ENCRYPTION POLICY: No Encryption

Configure Protocol Settings

7. Click **Configure Protocol Settings** and complete the following steps:
 - a. Verify the **Assertion Consumer Service URL**. The endpoint URLs for Redirect and Post bindings are both automatically populated from the metadata. If not, enter the URL manually. The URL will be the same for both bindings.

SP Connection | Browser SSO | Protocol Settings

Assertion Consumer Service URL Allowable SAML Bindings Signature Policy Encryption Policy Summary

As the IdP, you send SAML assertions to the SP's Assertion Consumer Service. The SP may request that the SAML assertion be sent to one of several URLs, via different bindings. Please provide the possible assertion consumer URLs below and select one to be the default.

Default	Index	Binding	Endpoint URL	Action
default	0	POST	https://portal-yoda.arubathena.com/global_login/aaa_saml/hpe.com?acs	Edit Delete

- a. Click **Next**. The **Allowable SAML Bindings** tab opens.
- b. Select **Post** and **Redirect**.

SP Connection | Browser SSO | Protocol Settings

Assertion Consumer Service URL Allowable SAML Bindings Signature Policy Encryption Policy Summary

When the SP sends messages, what SAML bindings do you want to allow?

ARTIFACT

POST

REDIRECT

SOAP

- c. Click **Next**. The **Encryption Policy Settings** tab opens.
- d. Select **None**.

SP Connection | Browser SSO | Protocol Settings

Assertion Consumer Service URL Allowable SAML Bindings Signature Policy Encryption Policy Summary

Additional guarantees of privacy may be used between you and your partner. Specify an encryption policy for the exchange of SAML messages.

NONE

- e. Click **Next**. Review the protocol setting.
- f. Click **Done**.

Step 3—Configure Credentials

1. On the SP Connections page in the PingFederate administrative console, click **Credentials**
2. Click **Configure Credentials**.
3. Click **Digital Signature Settings**.

4. Select the certificate to use for digital signature in SAML messages.

SP Connection | Credentials

Digital Signature Settings Summary

You may need to digitally sign SAML messages or security tokens to protect against tampering. Please select a key/certificate to use from the list below.

SIGNING CERTIFICATE

INCLUDE THE CERTIFICATE IN THE SIGNATURE <KEYINFO> ELEMENT.

INCLUDE THE RAW KEY IN THE SIGNATURE <KEYVALUE> ELEMENT.

SIGNING ALGORITHM

Step 4—Review Configuration

To review the configuration, click the **Activation & Summary** tab.

Step 5—SAML Authorization Profile in Aruba Central

For information on how to configure a SAML authorization profile, see [Configuring SAML Authorization Profiles in Aruba Central](#).

Configuring Service Provider Metadata in Aruba ClearPass Policy Manager

This procedure describes the configuration steps required for setting up Aruba ClearPass Policy Manager as an IdP.



ClearPass must be synced to NTP along with any other SAML SPs and IdPs. If clocks are out of sync, SAML will not function.

Before you Begin

- Go through the [SAML SSO feature description](#) to understand how SAML framework works in the context of Aruba Central.
- Ensure that you have access to the ClearPass Policy Manager instance.
- Ensure that you have downloaded the SAML metadata from Aruba Central.

Steps to Configure ClearPass Policy Manager as an IdP

To configure ClearPass as an IdP for providing SAML authentication and authorization services to Aruba Central, complete the following steps:

- [Step 1—Configuring an IdP Service](#)
- [Step 2—Configure an Enforcement Policy](#)
- [Step 3—Upload SP Metadata](#)
- [Step 4—Add Roles](#)
- [Step 5— Map Roles and Enforcement Policies](#)

- [Step 6—Add Users](#)
- [Step 7—SAML Authorization Profile in Aruba Central](#)

Step 1—Configuring an IdP Service

To configure an IdP service:

1. Go to **Configuration > Identity > Single Sign On**.
2. Select **ClearPass Identity Provider (SAML IdP Service)**. The **Service Templates - ClearPass Identity Provider (SAML IdP Service)** page opens.
3. Click the **General** tab.
4. Enter a Name Prefix. This prefix will be used to name all of the services and enforcement policies/profiles created by the wizard.
5. Click **Next**. The **Authentication** tab opens.
6. Select an authentication source.
7. Click **Next**. The **SP Details** tab opens.
8. Click **Save**.
9. Click **Save**.

Step 2—Configure an Enforcement Policy

To configure an enforcement policy:

1. From **Configuration > Enforcement > Enforcement Policies**.
2. Click **Add** to a new enforcement policy.
3. Select the enforcement policy and click **Edit**.
4. Click the **Enforcement** tab and click **Modify** to edit the default profile.
5. In the edit enforcement profile wizard screen, click the **Attributes** tab.
6. Configure the attributes as shown in the following figure:

Configuration » Enforcement » Profiles » Edit Enforcement Profile - IDP Srv ClearPass Identity Provider (SAML IdP Service) Enforcement Profile
 Enforcement Profiles - IDP Srv ClearPass Identity Provider (SAML IdP Service) Enforcement Profile

Summary			Profile			Attributes		
Attribute Name		Attribute Value						
1.	aruba_1_cid	=	201804170039					
2.	aruba_1_app_1	=	central					
3.	aruba_1_app_1_role_1	=	admin					
4.	Click to add...							

7. Click **Save**.

- In the Edit enforcement policies wizard screen, click the **Rules** tab and add the rules.

Configuration » Enforcement » Policies » Edit - IDP Srv ClearPass Identity Provider (SAML IdP Service) Enforcement Policy

Enforcement Policies - IDP Srv ClearPass Identity Provider (SAML IdP Service) Enforcement Policy

Note: This Enforcement Policy is created by Service Template

Summary	Enforcement	Rules
Rules Evaluation Algorithm: <input checked="" type="radio"/> Select first match <input type="radio"/> Select all matches		
Enforcement Policy Rules:		
Conditions	Actions	
1. (Tips:Role EQUALS Yoda-Admin)	IDP Srv ClearPass Identity Provider (SAML IdP Service) Enforcement Profile	
2. (Tips:Role EQUALS Malshi-Admin)	malshi_IDP Srv ClearPass Identity Provider (SAML IdP Service) Enforcement Profile	
3. (Tips:Role EQUALS Yoda-ReadOnly)	yoda-readonly-enforcement-profile	
<input type="button" value="Add Rule"/> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Edit Rule"/> <input type="button" value="Remove Rule"/>		

Step 3—Upload SP Metadata

- In the **Account Home** page, under **Global Settings**, click **Single Sign On**. The **Single Sign On** page opens.
- Select the SAML authorization profile configured for the ClearPass IdP service, click **Show Metadata**, and download the metadata.
- To upload SP metadata, go to **Configuration > Identity > Single Sign-On (SSO)**.
- Click **SAML IdP Configuration** tab, and click **Add SP metadata**.
- Set the SP name as Aruba Central and select the metadata file and click **Upload**.

Configuration » Identity » Single Sign-On (SSO)

Single Sign-On (SSO)

SAML SP Configuration	SAML IdP Configuration						
Identity Provider (IdP) Metadata ClearPass supports configuration of multiple IdP Portals. To download metadata for a specific IdP, enter the IdP Portal name.							
IdP Portal Name: <input type="text"/> <input type="button" value="Download"/>							
IdP Metadata URI: <input type="text" value="http://appadmin.arubas.com/networkservices/saml2/idp/cppm-metadata.xml?page="/>							
Service Provider (SP) Metadata <input type="button" value="+ Add SP metadata"/>							
Optionally, SAML Service Providers can upload their metadata for validation during SSO flow. List of valid SAML Service Providers using ClearPass as SAML IdP.							
<table border="1"> <thead> <tr> <th>#</th> <th>Name</th> <th></th> </tr> </thead> <tbody> <tr> <td></td> <td>Central</td> <td></td> </tr> </tbody> </table>		#	Name			Central	
#	Name						
	Central						

Step 4—Add Roles

To add a user role:

1. Go to **Configuration > Identity > Roles**.
2. Add the roles and click **Save**.

Configuration » Identity » Roles

Roles

 Add
 Import
 Export All

Filter: contains Show records

#	<input type="checkbox"/>	Name ▲	Description
1.	<input type="checkbox"/>	[AirGroup v1]	Role for an AirGroup protocol version 1 request
2.	<input type="checkbox"/>	[AirGroup v2]	Role for an AirGroup protocol version 2 request
3.	<input type="checkbox"/>	[Aruba TACACS read-only Admin]	Default role for read-only access to Aruba device
4.	<input type="checkbox"/>	[Aruba TACACS root Admin]	Default role for root access to Aruba device
5.	<input type="checkbox"/>	[BYOD Operator]	Operators with this profile can view and manage their own provisioned devices
6.	<input type="checkbox"/>	[Contractor]	Default role for a contractor
7.	<input type="checkbox"/>	[Device Registration]	Operators with this profile can self-provision their devices, for use with MAC authentication and AirGroup sharing.
8.	<input type="checkbox"/>	[Employee]	Default role for an employee
9.	<input type="checkbox"/>	[Guest]	Default role for a Guest
10.	<input type="checkbox"/>	[MAC Caching]	Default role applied during MAC caching
11.	<input type="checkbox"/>	Malshi-Admin	
12.	<input type="checkbox"/>	Malshi-Readonly	

Step 5— Map Roles and Enforcement Policies

1. Go to **Configuration > Services**.
2. Select the IdP service created for Aruba Central.
3. Click **Edit**.
4. Click the **Service** tab.
5. Add a service rule.

Configuration » Services » Edit - IDP Srv ClearPass Identity Provider (SAML IdP Service)

Services - IDP Srv ClearPass Identity Provider (SAML IdP Service)

Note: This Service is created by Service Template

Name: IDP Srv ClearPass Identity Provider (SAML IdP S...

Description: Service template to provide a SAML based single sign-on service that can be

Type: Aruba Application Authentication

Status: Enabled

Monitor Mode: Enable to monitor network access without enforcement

More Options: Authorization

Service Rule

Matches ANY or ALL of the following conditions:

	Type	Name	Operator	Value	
1.	Application	Name	EQUALS	SAML	
2.	Application	SSO-SP	EQUALS	https://portal-yoda.arubathena.com/global_login/aaa_saml/abc.com/metadata	
3.	Application	SSO-SP	EQUALS	malshi-portal.arubathena.com/global_login/aaa_saml/abc.com/metadata	
4.	Click to add...				

- Click the **Authentication** tab and add the authentications source.

Configuration » Services » Edit - IDP Srv ClearPass Identity Provider (SAML IdP Service)

Services - IDP Srv ClearPass Identity Provider (SAML IdP Service)

Note: This Service is created by Service Template

Summary Service **Authentication** Roles Enforcement

Authentication Sources: [Local User Repository] [Local SQL DB] [Add new Authentication Source](#)

Move Up
Move Down
Remove
View Details
Modify

--Select to Add--

Strip Username Rules: Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

[Back to Services](#) Disable Copy Save Cancel

- Click the **Roles** tab. Add a role mapping policy.

Configuration » Services » Edit - IDP Srv ClearPass Identity Provider (SAML IdP Service)

Services - IDP Srv ClearPass Identity Provider (SAML IdP Service)

Note: This Service is created by Service Template

Summary Service Authentication **Roles** Enforcement

Role Mapping Policy: --Select-- [Add new Role Mapping Policy](#)

Role Mapping Policy Details

Description:	-
Default Role:	-
Rules Evaluation Algorithm:	-

Conditions	Role

[Back to Services](#) Disable Copy Save Cancel

8. Click the **Enforcement** tab and ensure that service name and default profile are selected.

Configuration » Enforcement » Policies » Edit - IDP Srv ClearPass Identity Provider (SAML IdP Service) Enforcement Policy

Enforcement Policies - IDP Srv ClearPass Identity Provider (SAML IdP Service) Enforcement Policy

Note: This Enforcement Policy is created by Service Template

Summary | **Enforcement** | Rules

Name:	IDP Srv ClearPass Identity Provider (SAML IdP S
Description:	
Enforcement Type:	Application
Default Profile:	IDP Srv ClearPass Identity Pr

[View Details](#) | [Modify](#) | [Add new Enforcement Profile](#)

Step 6—Add Users

To add users:

1. Go to **Configuration > Identity > User**.
2. Add users.

Step 7—SAML Authorization Profile in Aruba Central

For information on how to configure a SAML authorization profile, see [Configuring SAML Authorization Profiles in Aruba Central](#).

Configuring RADIUS Authentication and Authorization

For RADIUS capability, you must configure the IP/Hostname of the RADIUS server, the UDP port, the server shared secret and the authentication method. Perform these steps to configure RADIUS authentication:

Figure 61 Sample Figure of Radius Authentication

[GO TO ACCOUNT HOME](#)

AUTHENTICATION

Manage and configure external authentications

EXTERNAL AUTHENTICATION

Single-Sign-On RADIUS None

PRIMARY SERVER HOST NAME / IP ADDRESS

PRIMARY SERVER PORT
1812

PRIMARY SERVER SECRET

CONFIRM PRIMARY SERVER SECRET

PEAP-MSCHAPV2

Secondary Server

SECONDARY SERVER HOST NAME / IP ADDRESS

SECONDARY SERVER PORT
1812

SECONDARY SERVER SECRET

CONFIRM SECONDARY SERVER SECRET

[RESET](#) [SAVE](#)

To configure the Radius server, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Authentication**.
2. Under **External Authentication** tab, select **Radius**. The radius page is displayed.
3. Set the following fields as the shown in the table below:

Field	Default	Description
Primary Server Hostname/IP Address	N/A	Enter the IP address or the hostname of the primary RADIUS server.
Primary Server Port (1-65535)	1812	Enter the UDP port for the primary RADIUS server.
Primary Server Secret	N/A	Enter the shared secret for the primary RADIUS server.
Confirm Primary Server Secret	N/A	Re-enter the primary server secret.
Authentication Method	PEAP-MSCHAPV2	Select one of the following authentication methods: <ul style="list-style-type: none"> ■ PAP ■ PEAP-MSCHAPV2
To enable the secondary server, slide the Secondary Server toggle button to the right		
Secondary Server Hostname/IP Address	N/A	Enter the IP address or the hostname of the secondary RADIUS server.
Secondary Server Port (1-65535)	1812	Enter the UDP port for the secondary RADIUS server.
Secondary Server Secret	N/A	Enter the shared secret for the secondary RADIUS server.
Confirm Secondary Server Secret	N/A	Re-enter the secondary server secret.

4. Click **Save** to save the configuration.

Important Points to Note

1. For Radius login, the email address of the user is the username.
2. To configure Radius option, you must be an admin user of the Aruba Central account.
3. The Radius user access is determined by the role (Aruba-Admin-Role) and the group (Aruba-Admin-Device-Group) attributes configured in the Radius Server.
4. When Radius authentication fails for the User in Primary Radius Server, authentication request is not sent to Secondary Radius Server. However, if Primary Radius Server is not reachable, then authentication request is sent to Secondary Radius Server when configured.
5. Radius users with admin privileges can configure system users in Aruba Central.

- The following menu option in Aruba Central UI is not available for a Radius user:
Change Password—Aruba Central does not support changing the password of a Radius user account.
- Radius Authentication can be configured by any Radius Server which supports **PAP** and **PEAP-MSCHAPV2** protocols such as Aruba ClearPass Policy Manager.

Configuring Radius Service in Aruba ClearPass Policy Manager

For Radius Authentication, you must configure the Radius Enforcement service in Aruba ClearPass Policy Manager.

Note the following points while configuring enforcement service in ClearPass Manager:

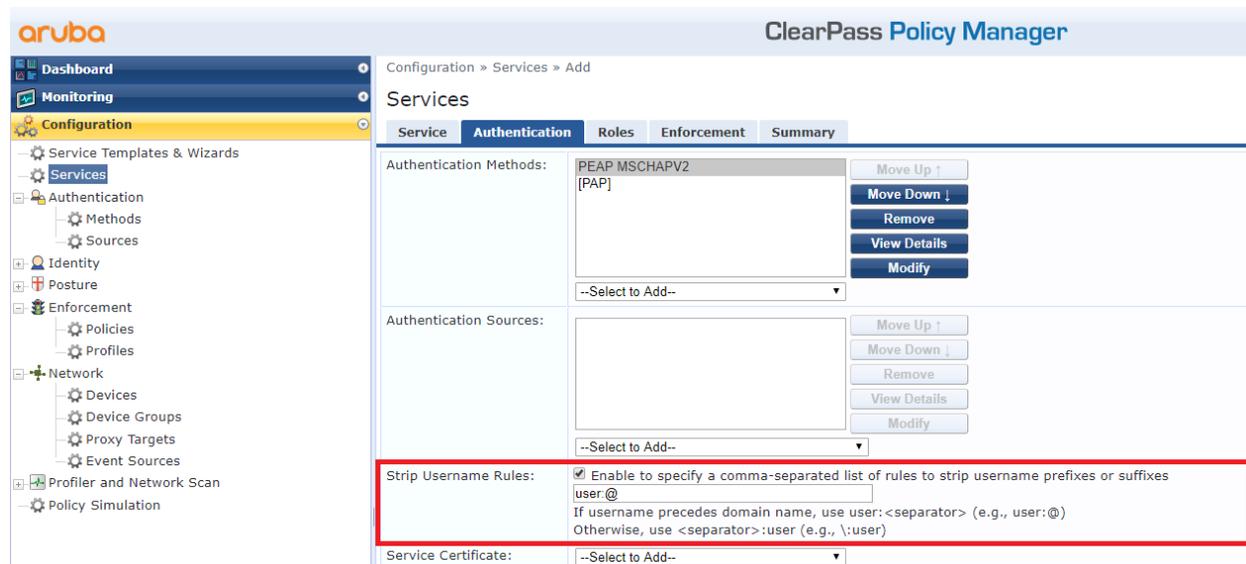
- Ensure that you have access to the ClearPass Policy Manager instance.
- Only the admin user can configure the enforcement service.
- If no role is defined in Radius response for the User, Central does not allow access to the user.
- If no group is defined in Radius response for the User, Central does not allow access to the user.

To configure the Radius enforcement service in ClearPass policy manager, follow the steps mentioned in [ClearPass Policy Manager User guide](#) available at [Aruba Support portal](#).

While configuring the enforcement service, make sure you choose the following options:

- Under **Configuration > Services > Authentication** tab, select the **Strip Username Rules** check box to preprocess the username (to remove domain suffix) before authenticating and authorizing against the authentication source.

Figure 62 Sample Figure for Services



- Under **Configuration > Enforcement > Profiles > Enforcement Profiles**, When Enforcement Profile is added for the User, click **Attributes**. The attributes tab is displayed.
 Select the options for attributes as shown in the table below:

Type	Name	Value
Radius:Aruba	Aruba-Admin-Role	Select the role assigned to the user
Radius:Aruba	Aruba-Admin-Device-Group	Select the group assigned to the user. Comma-separated option can be used when multiple groups are assigned. If the user has access to all groups, then the allgroups value can be provided.

Figure 63 Sample Figure for role and groups assignment

Viewing Audit Logs for Federated Users in Aruba Central

The federated, SAML SSO or the RADIUS user activity is logged in Aruba Central as audit trails.

To view the audit logs for federated users:

1. In the **Account Home** page, under **Global Settings**, click **Audit Trail**. The **Audit Trail** page is displayed.
2. To filter audit logs by federated user activity, click the filter in the **Category** column and select **User Activity**.



To view audit logs for the SAML authorization profiles, in the Audit Trail page, select **SAML Profile** from the **Category** filter.

Viewing Federated Users in Aruba Central

If your Aruba Central account has SAML SSO or RADIUS users, Aruba Central displays these users as federated users.

To view a list of federated users in your account:

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**. The **Users and Roles** page is displayed.
2. In the **Users** table, use the filter in **User Type** column to sort the table by federated users.

This section describes the various options available for viewing the device, client and network details.

Network Overview

In the **Network Operations** app, perform the following steps to access the overall network summary page:

1. Set the filter to **Global**.
The Global dashboard is displayed.
2. Under **Manage > Overview**, the network summary page displays the following tabs:
 - **Network Health**—Displays vital information of the network sorted by site. For more information, see [Network Health](#).
 - **Summary**—Displays details such as the bandwidth usage in the network, client counts, and cluster-specific details. For more information, see [Global—Summary](#).

Monitoring APs

The access point (AP) dashboard enables you to manage, configure, monitor and troubleshoot APs provisioned and managed through Aruba Central (on-premises).

For a list of all the available menu items in the AP dashboard, see [The Access Point Dashboard](#).

The AP Health Bar provides a snapshot of the overall health of the APs configured in Aruba Central (on-premises). For more information, see [Health Bar Dashboard for Access Point](#).

The AP Foundation license is applicable for Access Point Monitoring.

Monitoring APs in Summary View

The access point (AP) Summary page provides all the metrics about the health, status, and clients information associated with the AP provisioned and managed in Aruba Central (on-premises).

Viewing the AP Summary Page

To navigate to the AP Summary page, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click the **Summary** icon.
The AP Summary page is displayed.

The AP Summary page displays the following information:

- **Access Points**—Displays the overall usage metrics for the APs provisioned in your Aruba Central (on-premises) account. Consists of the following tabs:
 - **Usage**—Displays the incoming and outgoing data traffic detected on the APs.
 - **Clients**—Displays the number of clients connected to an AP over a specific time period.
 - **Bandwidth Usage Per Network**—Displays the incoming and outgoing traffic for all APs per SSID over a specific duration.
 - **Client Count Per Network**—Displays the number of clients connected to an AP per SSID over a specific time period.
- **Radios**—Displays the channel distribution and power distribution metrics for the AP radios. For more information on radios in the summary view, see [Monitoring Radios in Summary View](#).

You can change the time range for the AP Summary page by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

Monitoring Radios in Summary View

The **Radios** tab in the access point (AP) Summary page displays the channel distribution, power distribution, channel changes, and power changes metrics for the radios provisioned and managed in Aruba Central (on-premises). When you click the **Radios** tab, the **2.4 GHz** and **5 GHz** tabs are displayed.

Viewing the Radios Summary Page

To navigate to the Radios Summary page, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP. The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Access Points**. A list of APs is displayed in the **List** view.
3. Click the **Summary** icon. The AP Summary page is displayed.
4. Click the **Radios** tab.

When you click the **Radios** tab, it displays the following information:

- **Radios**—Click the **Radios** tab to display the graphs related to channel distribution and power distribution.
- **2.4 GHz**—Click the **2.4 GHz** tab to display the graphs related to channel distribution and power distribution for 2.4 GHz radios.
- **5 GHz**—Click the **5 GHz** tab to display the graphs related to channel distribution and power distribution for 5 GHz and 5 GHz (Secondary) radios.

The tri-radio feature is available only for AP-555. In the **5 GHz** tab, the **Radio 5 GHz (Secondary)** data is available only if the tri-radio mode is enabled. For more information, see [About Tri-Radio Mode](#).

You can change the time range for the AP Summary page by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.



When you click the **Radios**, **2.4 GHz**, and **5 GHz** tab, the **Radios** tab provides the following information:

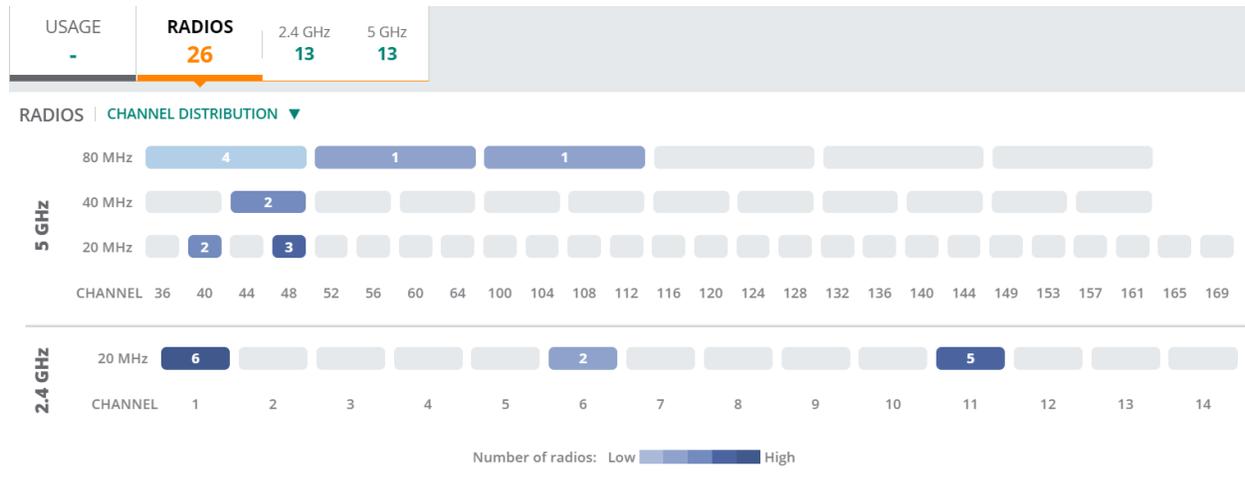
Radios

The **Radios** section displays the channel distribution and power distribution graphs for the radios.

Channel Distribution

From the drop-down list, select **Channel Distribution** to display information on the frequency, at which each of the channels of the radio operate.

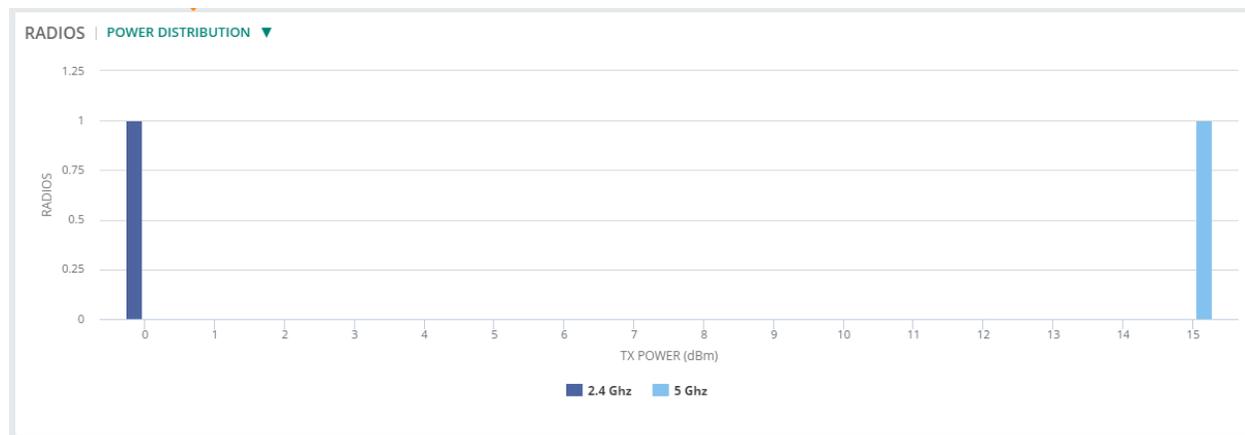
Figure 64 Channel Distribution



Power Distribution

From the drop-down list, select **Power Distribution** to display the power distributed across each of the radios.

Figure 65 Power Distribution

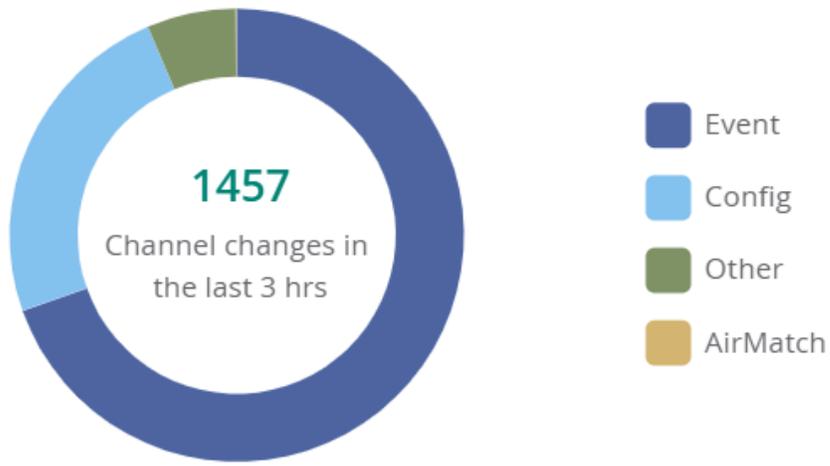


Channel Changes

The **Channel Changes** graph displays the number of channel changes that has occurred in the radios.

Figure 66 Channel Changes

CHANNEL CHANGES

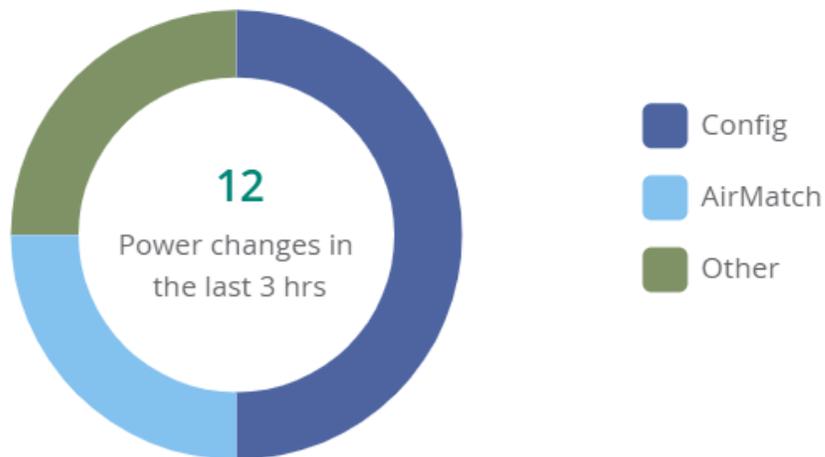


Power Changes

The **Power Changes** graph indicates the power change by each of the radios, from ARM to AirMatch EIRP.

Figure 67 Power Changes

POWER CHANGES



Monitoring APs in List View

The access point (AP) List page provides information associated with the APs and radios provisioned and managed in Aruba Central (on-premises).

The AP List page is available for Foundation and Advanced licenses for APs.

The AP List page displays the following sections:

- [Access Points Table](#)
- [Monitoring APs in List View](#)
- [Monitoring APs in List View](#)
- [Monitoring APs in List View](#)

Viewing the AP List Page

To navigate to the AP List page, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under Groups, Labels, or Sites. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP. The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.

The AP List page displays the following information:

- **Access Points**—Displays the total number of APs. When you click the **Access Points** tab, it provides information about all APs in the **Access Points** table.
- **Online**—Displays the total number of online APs. When you click the **Online** tab, it provides information about the online APs in the **Access Points** table.
- **Offline**—Displays the total number of offline APs. When you click the **Offline** tab, it provides information about the offline APs in the **Access Points** table.
- **Radios**—Displays the total number of radios. When you click the **Radios** tab, it provides information about all radios in the **Radios** table.
 - **2.4 GHz**—Displays the total number of 2.4 GHz radios. When you click the **2.4 GHz** tab, it provides information about 2.4 GHz radios in the **Radios** table.
 - **5 GHz**—Displays the total number of active 5 GHz and 5 GHz (Secondary) radios. When you click the **5 GHz** tab, it provides information about 5 GHz and 5 GHz (Secondary) radios in the **Radios** table.



The tri-radio feature is available only for AP-555. In the **5 GHz** tab, the **Radio 5 GHz (Secondary)** data is available only if the tri-radio mode is enabled. For more information, see [About Tri-Radio Mode](#).

Access Points Table

The **Access Points** table displays the following information:

- **Device Name**—Name of the AP.
- **Status**—Displays the operational status of the AP. The status is as follows:
 - **Online**—Indicates that the AP is online.
 - **Offline**—Indicates that the AP is offline.

- **Online**—Indicates that the AP is operating under thermal management. For more information, see [Thermal Shutdown Support in IAP](#).
- **IP Address**—IP address of the AP.
- **Model**—The model number of the AP.
- **Serial**—The serial number of the device.
- **Firmware Version**—The firmware version running on the AP.
- **Clients**—Clients connected to the AP.
- **Alerts**—Opens alerts related to APs.
- **MAC Address**—MAC address of the AP.
- **Controller**—The name of the controller.
- **Secondary Controller**—The name of the secondary controller.
- **Config Status**—The configuration changes associated with the AP. The **Config Status** column is not supported in the exported CSV file.
- **Group**—Group to which the AP belongs.
- **Labels**—Labels associated with the AP. If multiple labels are associated with the AP, hover over the label link to view all the labels.
- **Site**—The site to which the device belongs.
- **Uptime**—Time since when the device is operational. The **Uptime** column is not applicable for offline devices and remains blank for all the devices in the **Offline** page.
- **Last Seen**—The last active time and date of the device. The **Last Seen** column is not applicable for online devices and remains blank for all the devices in the **Online** page.
- **Public IP**—IP address logged by servers when the device is connected through internet connection.
- **Persona**—Displays the type of role of the AP. For example, CAP and IAP.
- **LLDP Neighbor**—Displays the name of the LLDP neighbor. Click the LLDP Neighbor name to view the switch details page, if the switch is managed by Aruba Central (on-premises).
- **LLDP Port**—Displays the port number of LLDP neighbor.
- **AI Insights**—The number of insights generated for the AP in the last three hours. The **AI Insights** column is not supported in the exported CSV file.
- **Note**—Displays the information captured in the **Note** parameter, in the AP Details section. The search filter allows you to search for exact and partial text search with prefix. The text search with suffix is not supported.
- **Zone**—Zone to which the AP belongs. Zone details are displayed in the column only for APs with firmware version ArubaOS 8.7.0.0 or later.



- From Aruba Central (on-premises) 2.5.4 release, **LLDP Neighbor** and **LLDP Port** details are also available for Campus APs and not only Instant APs.
- A search filter is provided only for the **Device Name, IP Address, Model, Serial, MAC Address, Controller, Secondary Controller, Group, Labels, Site, LLDP Neighbor, Note**, and **done** columns. The  and  icons allow you to sort the **Device Name, IP Address, Serial, MAC Address, Controller**, and **Zone** columns in an ascending and descending order.
- By default, the AP List table displays the **Device Name, Status, IP Address, Model, Serial**, and **Firmware Version**. You can customize the view of AP List table with additional columns such as the **Clients, Alerts, MAC Address, Controller, Secondary Controller, Config Status, Group, Labels, Site, Uptime, Last Seen, Public IP, Persona, LLDP Neighbor, LLDP Port, AI Insights, Note**, and **Zone**. These additional columns can be selected by clicking the icon provided at the right corner of the table that displays the AP list. Click the **Reset to default** button provided in the drop-down list to reset the AP List with default columns only. To autofit the columns, click the icon and select **Autofit columns**.

To download the **.csv** file of the AP list table, click the  icon. If the table contains unicode value, you must use a UTF-8 enabled software to view the contents. To view the file in Microsoft Excel 2007 spreadsheet software, perform the following steps to view table with unicode values:

1. Open the Microsoft Excel 2007 software.
2. Click on the Data menu bar option.
3. Click on the **From Text** icon.
4. Browse to the location of the file that you want to import.
5. Select the file name and click **Import**.
6. The **Text Import** wizard is displayed.
7. Select the file type. For **.csv** format, select the **Delimited** option.
8. Select the **65001: Unicode (UTF-8)** option from the drop-down list that is displayed next to the **File** origin.
9. Click **Next**. The **Text Import Wizard-Step 1 of 3** page is displayed.
10. Place a check mark next to the delimiter such as the comma or full stop that was used in the file you wish to import into Microsoft Excel 2007.
11. The **Data Preview** window displays the data based on the selected delimiter.
12. Click **Next**. The **Text Import Wizard-Step 3 of 3** page is displayed. Select the appropriate data format for each column that you want to import.



Importing one or more columns is optional.

13. Click **Finish** to import the data into Microsoft Excel 2007.

Deleting an Offline AP

To delete an offline AP, see .

Rebooting an AP

To reboot an AP, see [Rebooting an AP in the List View](#)

Radios Table

The **Radios** table displays the following information:

- **Access Point**—Name of the AP.



The online radios are displayed with a  green dot and offline radios are displayed with a  red dot.

- **Radio MAC Address**—The MAC address of the radios connected to the AP.
- **Band**—The type of radio band. For example, **2.4 GHz**, **5 GHz**, and **5 GHz (Secondary)**.



The tri-radio feature is available only for AP-555. In the **Band** column, the **Radio 5 GHz (Secondary)** data is available only if the tri-radio mode is enabled. For more information, see [About Tri-Radio Mode](#).

- **Bandwidth**—The bandwidth of data transferred through the radios.
- **Channel**—Channels assigned for the radios.
- **Utilization (%)**—The percentage of time (normalized to 255) that the channels of the radios are sensed to be busy. The AP uses either the physical or the virtual carrier sense mechanism to sense a busy channel. This percentage not only depends on the data bits transferred but also with the transmission overhead that makes use of the channel.
- **Channel Changes**—Displays the number of channel changes that has occurred in an AP. When you click the number, the **Channel Changes** pop-up window is displayed, that provides the following information:
 - **Event Time**—Displays the time period when the channel change occurred, in the format of days-hours-minutes.
 - **Reason**—Displays the reason for the channel change.
 - **From Channel**—Displays the channel number from which the channel change occurred.
 - **To Channel**—Displays the channel number to which the channel change occurred.
 - **Band**—The type of radio band. For example, **2.4 GHz**, **5 GHz**, and **5 GHz (Secondary)**.
 - **Access Point**—Name of the AP.
- **Power (dBm)**—The transmit power of the radios measured in decibels.
- **Power Changes**—Displays the number of power changes that has occurred in an AP. When you click the number, the **Power Changes** pop-up window is displayed, that provides the following information:
 - **Event Time**—Displays the time period when the power change occurred, in the format of days-hours-minutes.
 - **Reason**—Displays the reason for the power change.
 - **From Power (dBm)**—Displays the transmit power from which the power change occurred.
 - **To Power (dBm)**—Displays the transmit power to which the power change occurred.
 - **Band**—The type of radio band. For example, **2.4 GHz**, **5 GHz**, and **5 GHz (Secondary)**.
 - **Access Point**—Name of the AP.
- **Noise Floor (dBm)**—The noise at the radio receivers of the radios. Along with the thermal noise, Noise Floor may be affected by certain types of interference sources, though not all interference types result in increased noise floor. Noise Floor value may vary depending on the noise introduced by components

used in the computer or client device.



A search filter is provided only for the **Access Point** column.

Deleting an Offline AP

To delete an offline access point (AP), complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.

The dashboard context for the selected filter is displayed.

2. Under **Manage**, click **Devices > Access Points**.

A list of APs is displayed in the **List** view.

3. In the **Access Points** table, hover over the offline AP that you want to delete.

4. Click the  delete icon.



To delete multiple offline APs, select the offline APs that you want to delete and click the  delete icon.

5. Click **Delete** in the confirmation dialog box.

Thermal Shutdown Support in IAP

ArubaAP-555 and AP-535 Instant Access Point (IAP) devices are equipped with an internal thermal sensor. The sensor initiates a shutdown when the operating temperature crosses the temperature threshold recommended for an Instant AP. When an IAP operates under thermal management, all the radios are in **Disabled** mode in the AP Health Bar.

- In swarm mode, the thermal shutdown support is as follows:
 - In swarm mode, when the member IAP operates beyond the recommended temperature threshold, the Virtual AP profile is disabled. Once the member IAP attains the optimum temperature again, it reboots with the **Recovery from Thermal Management Mode** message, and then reconnects with the virtual controller. This process of reboot and reconnection is executed for five times. If the connection between the member IAP and the virtual controller does not restore after five times, the member IAP remains in the shutdown state until it is manually turned on.
 - In swarm mode, when the conductor IAP operates beyond the recommended temperature threshold, it reboots with the **Reboot due to Thermal Management** message. Once the conductor IAP attains the optimum temperature again, it turns into a member IAP, reboots with the **Recovery from Thermal Management Mode** message, and then reconnects with the virtual controller. This process of reboot and reconnection is executed for five times. If the connection between the member IAP and the virtual controller does not restore after five times, the member IAP remains in the shutdown state until it is manually turned on.
 - In swarm mode, when the conductor IAP operates beyond the recommended temperature threshold and the number of IAPs is one in the swarm scale, the Virtual AP profile is disabled. Once the conductor IAP attains the optimum temperature again, it reboots with the **Recovery from Thermal Management Mode** message. This process of reboot is executed for five times. If the conductor IAP does not reboot after five times, the conductor IAP remains in the shutdown state until it is manually turned on.

- In standalone mode, when the IAP operates beyond the recommended temperature threshold, the Virtual AP profile is disabled. Once the IAP attains the optimum temperature again, it reboots with the **Recovery from Thermal Management Mode** message. This process of reboot is executed for five times. If the IAP does not reboot after five times, it remains in the shutdown state until it is manually turned on.

Thermal Shutdown Events

To view the thermal shutdown events, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed. To select a device in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices**, and then click **Access Points**.
 - c. Click an AP listed under **Device Name**.
The dashboard context for the AP is displayed.
2. Under **Analyze**, click **Alerts & Events**.
The **Alerts & Events** page is displayed in the **List** view.
3. Click the **Events** tab.
A list of events is displayed in the **Events** table.

When the thermal shutdown feature is either enabled or disabled in an IAP, the **Events** table displays the following details:

- The **Event Type** column includes the **AP Thermal Shutdown** type which can be used to filter thermal shutdown events.
- The **Description** column includes the status of the thermal shutdown feature in the IAP. For example, **Thermal management enabled** or **Thermal management disabled**.



In Aruba Central (on-premises), the thermal shutdown feature is supported on IAPs running Aruba Instant 8.6.0.0 or later versions.

About Tri-Radio Mode

Aruba Central (on-premises) offers tri-radio mode support in ArubaAP-555, a flagship 802.11ax access point (AP). In tri-radio mode or split 5 GHz mode, the 8x8 5 GHz radio is split into two independent 4x4 5 GHz radios. In the split 5 GHz Mode, **Radio 5 GHz Secondary** operates on channels from 36 to 64 and **Radio 5 GHz** operates on channels from 100 to 165.

To enable tri-radio, go to **Access Points > Radio** in the AP configuration dashboard, and select the **Split Radio** check-box.

The split 5 GHz radio can operate in the following modes:

- Access
- Monitor
- Spectrum

Enabling Tri-Radio Mode

To enable the tri-radio mode, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a group in the filter:
 - a. Set the filter to one of the options under **Groups**. Ensure that the filter selected contains at least one active access point.
The dashboard context for the group is displayed.
 - b. Under **Manage**, click **Devices > Access Points**.
A list of access points is displayed in the **List** view.
 - To select an access point in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices > Access Points**.
A list of access points is displayed in the **List** view.
 - c. Click an access point listed under **Device Name**.
The dashboard context for the access point is displayed.
 - d. Under **Manage**, click **Devices > Access Point**.
2. Click the **Config** icon.
The tabs to configure access points are displayed.
3. Click the **Access Points** tab.
The **Access Points** page is displayed.
4. To edit an AP, select an AP in the **Access Points** table, and then click the edit icon.
5. Click **Radio**.
6. Select the **Split Radio** check-box.
7. Click **Save Settings**.

Tri-Radio Events

To view the tri-radio events, complete the following steps:

1. In the **Network Operations** app, select one of the following options:

To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.

The dashboard context for the selected filter is displayed. To select a device in the filter:

 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices**, and then click **Access Points**.
 - c. A list of APs is displayed in the **List** view.
 - d. Click an AP listed under **Device Name**. The dashboard context for the AP is displayed.
2. Under **Analyze**, click **Alerts & Events**. The **Alerts & Events** page is displayed in the **List** view.
3. Click the **Events** tab.
A list of events is displayed in the **Events** table.

When the tri-radio mode is either enabled or disabled in an AP, the **Events** table displays the following details:

- The **Event Type** column includes the **AP Tri-Radio** type which can be used to filter tri-radio events.
- The **Description** column includes the status of the tri-radio mode in AP.



In Aruba Central (on-premises), the tri-radio feature is available only on AP-555 running Aruba Instant 8.6.0.0 or later versions.

By default, the AP-555 operates in dual radio mode.

Access Point > Overview > Summary

In the access point (AP) dashboard, the **Summary** tab displays the device details, network information, radio details including the topology of clients connected to each radio, and the health status of the AP in the network. The **Summary** tab displays the following sections:

- [Device](#)
- [Network](#)
- [Radios](#)
- [Data Path](#)
- [Health Status](#)
- [WLANS](#)
- [Actions](#)
- [Go Live](#)

Viewing the Overview > Summary Tab

To navigate to the **Summary** tab in the AP dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under Groups, Labels, or Sites. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP. The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Access Points**. A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**. The **Summary** tab is displayed.
To exit the AP dashboard, click the back arrow on the filter.
You can change the time range for the **Summary** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

Device

The **Device** section displays all or some of the following details:

- **AP Model**—The AP hardware model.
- **Country Code**—Country code in which the AP operates.
- **MAC**—MAC address of the AP.

- **Serial Number**—Serial number of the AP.
- **Uptime**—Time since when the AP is operational.
- **Last Reboot Reason**—The reason for the latest rebooting of AP.
- **Firmware Version**—The firmware version running on the AP. If the device is running an older firmware version, this field prompts the user to upgrade to the latest firmware version along with the link to the **Maintenance > Firmware** page.
- **Configuration Status**—Displays the configuration status and the timestamp of the last device configuration changes.
- **Band Selection**—Displays the operating band of the AP. The supported bands are **Dual Band**, **Dual 5 GHz**, or **Tri-Radio**.
- **Power Draw**—The power utilized by the device in watts (W) or kilowatts (kW).
- **Power Negotiation**—The power in watts (W) negotiated on the ethernet port of the device in a wired network.
- **Recommended Power**—The recommended power in watts (W) negotiated on the ethernet port of the device in a wired network.
- **Controller**—The name of the controller.
- **Secondary Controller**—The name of the secondary controller.
- **Group**—The group to which the AP belongs. Click the group name to go to the **Overview > Summary** page for that group.



When an AP belongs to an unprovisioned group, the hyperlink to the unprovisioned group is disabled

- **Labels**—The labels associated with the AP. You can also add a new label to the AP by clicking the edit icon. To view all the labels associated with a device, hover your mouse over the **Labels** column.
- **LEDs on Access Point**—Enables the blinking of LEDs on the AP to identify the location. Click **Blink LED** to enable the blinking of LEDs on the AP. The default blinking time is set to 5 minutes and it stops automatically after 5 minutes. To stop the blinking, click **Stop Blinking**.
- **Site**—The site to which the AP belongs. Click the site name to go to the **Overview > Site Health** page for that site.
- **Location**—The currently configured physical location of an AP. Location detail is displayed only for APs with firmware version ArubaOS 8.9.0.0 or later.
- **Contact**—The currently configured contact of an AP. For example, E-mail ID, or contact number. Contact detail is displayed only for APs with firmware version ArubaOS 8.9.0.0 or later.
- **Note**—When you click the  edit icon, a text-box is displayed. It allows you to add information that can be used as reference. For example, AP location, and upgrade information.

Network

The **Network** section displays information of the network and interfaces to which the AP is connected. Along with the network profile name, the following fields are displayed in the **Network** section:

- **ETH0**—Displays the status of the ETH0 network.
- **Speed (Mbps)/Duplex**—The speed of the network measured in Mbps. This field also indicates whether the network has a full-duplex or half-duplex communication.
- **VLAN**—The number of VLAN connections associated with the network.
 - **LLDP Details**—Click the **LLDP Details** link to view the ETH0 LLDP details. The pop-up window displays the **Neighbor Name**, **Neighbor MAC**, **Neighbor Port**, and **Neighbor VLAN** details.

- **ETH1**—Displays the status of the ETH1 network.
- **Speed (Mbps)/Duplex**—The speed of the network measured in Mbps. This field also indicates whether the network has a full-duplex or half-duplex communication.
- **VLAN**—The number of VLAN connections associated with the network.
 - **LLDP Details**—Click the **LLDP Details** link to view the ETH1 LLDP details. The pop-up window displays the **Neighbor Name**, **Neighbor MAC**, **Neighbor Port**, and **Neighbor VLAN** details.
- **Current Uplink**—The current uplink connection on the AP.
- **Uplink connected to**—The switch name to which the AP is connected. Click this link to view the switch details page, if the switch is managed by Aruba Central (on-premises).
 - **Port**—The port number of the switch to which the AP is connected.
- **IP Address**—IP address of the AP.
- **Public IP Address**—IP address logged by servers when the AP device is connected through internet connection.
- **DNS Name Servers**—The server that has a directory of domain names and their associated IP addresses.
- **Default Gateway**—A 32 bit value that is used to uniquely identify the device on a public network.
- **NTP Server**—Displays information about the NTP Server.



From Aruba Central (on-premises) 2.5.4 release, **LLDP Details** feature is supported for Campus APs as well.

Radios

The **Radios** section displays the following information related to **Radio 2.4 GHz**, **Radio 5 GHz**, and **Radio 5 GHz Secondary**:

- **Mode**—The type of mode for the radios. For example, Client Access, Monitor, and Spectrum.
- **Status**—Displays the operational status of the radios connected to the AP. The status is as follows:
 - ● **Up**—Indicates that the radio is online.
 - ○ **Down**—Indicates that the radio is offline.
 - ○ **Down - Thermal shutdown**—Indicates that the radio is offline as the AP is operating under thermal management. For more information, see [Thermal Shutdown Support in IAP](#).
- **Radio MAC Address**—The MAC address of the radios connected to the AP.
- **Channel**—The channels assigned to the radios.
- **Power**—The transmit power of the radios.
- **Type**—The type of wireless LAN used for the radios.
- **Clients**—The number of clients connected to the AP.
- **Wireless Networks**—The number of SSIDs configured in the network.
- **Antenna**—The type of antennae. For example, internal and external.
- **Spatial Stream**—Displays the number of spatial streams. By default, the spatial stream value for **Radio 5 GHz** is 8x8. When tri-radio mode is enabled, the spatial stream values for **Radio 5 GHz** and **Radio 5 GHz (Secondary)** is 4x4.



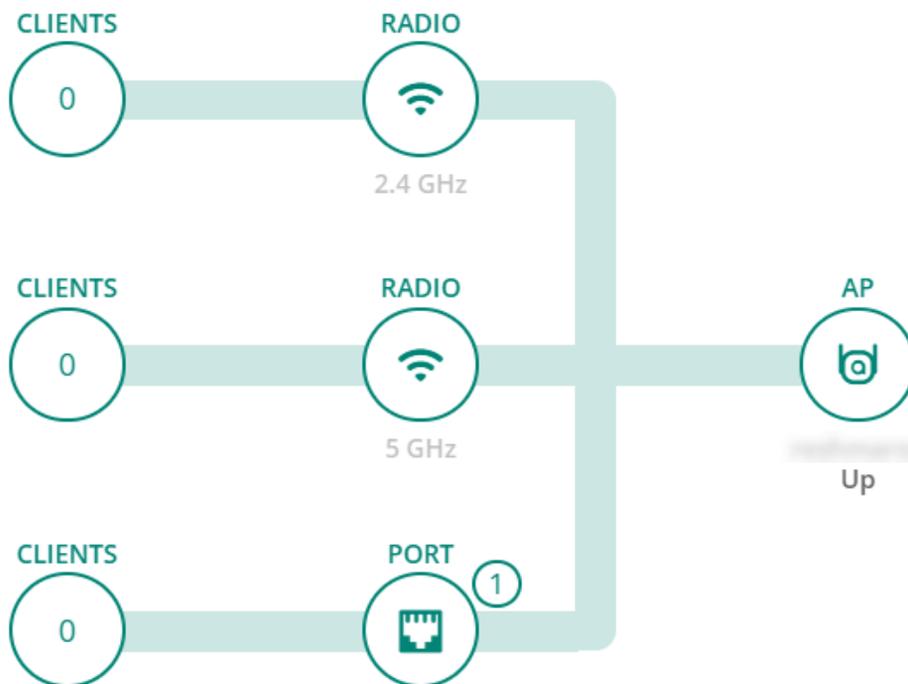
- When the Instant AP radios are set to spectrum scan mode, the **Channel** and **Power** values are empty.
- The tri-radio feature is available only for AP-555. In the **Radios** section, the **Radio 5 GHz (Secondary)** data is available only if the tri-radio mode is enabled. For more information, see [About Tri-Radio Mode](#).

Data Path

The **Data Path** section displays the topology of the clients connected to each of the radios of the AP, which in turn is connected to switches or gateways through VLAN. When you hover over the upstream device in the data path topology, a pop-up displays the **Name**, **Serial Number**, and **Port** details of the upstream devices.

PORT shows the number of ports available in the AP that also includes USB ports. **CLIENTS** connected to the **PORT** in the data path shows the number of wired clients connected to the port.

Figure 68 Data Path



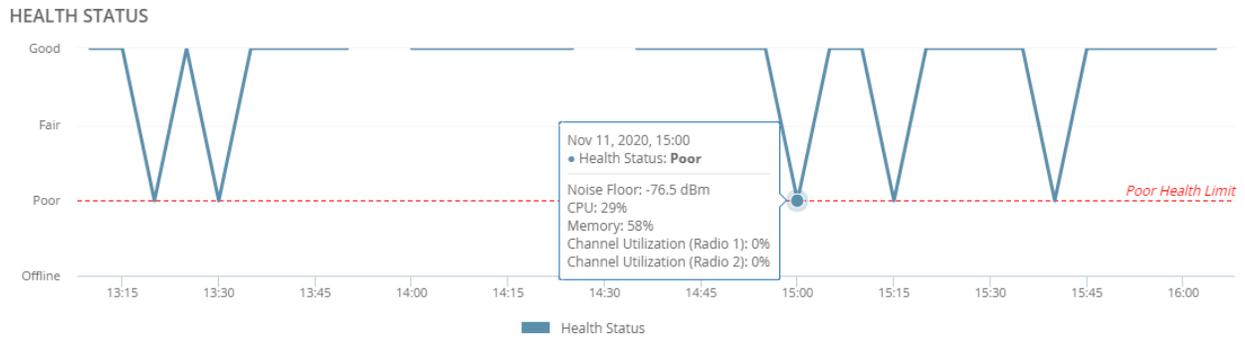
The tri-radio feature is available only for AP-555. In the **Data Path** section, the **5 GHz (Secondary)** data is available only if the tri-radio mode is enabled. For more information, see [About Tri-Radio Mode](#).

Health Status

The **Health Status** trend graph indicates the health status of the device in the network for the time selected in the time range filter. When you hover over the graph, you can view information such as date and time, Health Status, Noise Floor, CPU, Memory, Channel Utilization (Radio 1), Channel Utilization (Radio 2), and Channel Utilization (Radio 3).

In the **Health Status** graph, the **Poor Health Limit** text indicates the poor health limit of the device in the network.

Figure 69 Health Status



The tri-radio feature is available only for AP-555. In the **Health Status** section, the **Channel Utilization (Radio 3)** data is available only if the tri-radio mode is enabled. For more information, see [About Tri-Radio Mode](#).

WLANS

The **WLANS** table provides a list of all the SSIDs configured for the AP.

Figure 70 WLANS

WLANS (14) ↓												
Name	Type	VLANs	Security									
AP_555_gyu01Psk-Link05	Employee	1	WPA2 Personal									
<div style="border: 1px solid #ccc; padding: 5px;"> <p>BSSID (2)</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; border-bottom: 1px solid #ccc;">2.4 GHz</td> <td style="width: 50%; border-bottom: 1px solid #ccc;">5 GHz (Secondary)</td> </tr> <tr> <td>BSSID: 80:8d:b7:80:ce:1f</td> <td>BSSID: 80:8d:b7:80:ce:2f</td> </tr> <tr> <td>Radio Type: 802.11ax</td> <td>Radio Type: 802.11ax</td> </tr> <tr> <td>Clients: 0</td> <td>Clients: 0</td> </tr> </table> </div>					2.4 GHz	5 GHz (Secondary)	BSSID: 80:8d:b7:80:ce:1f	BSSID: 80:8d:b7:80:ce:2f	Radio Type: 802.11ax	Radio Type: 802.11ax	Clients: 0	Clients: 0
2.4 GHz	5 GHz (Secondary)											
BSSID: 80:8d:b7:80:ce:1f	BSSID: 80:8d:b7:80:ce:2f											
Radio Type: 802.11ax	Radio Type: 802.11ax											
Clients: 0	Clients: 0											
AP_555_gyu01Psk-Link06	Employee	1	WPA2 Personal									
AP_555_gyu01Psk-Link07	Employee	1	WPA2 Personal									

The **WLANS** table provides the following information:

- **Name**—Displays the name of the SSID.



In the **WLANS** table, the **Type**, **VLANs**, and **Security** values are empty.

Click > to expand an SSID in the **WLANS** table. When you expand an SSID in the **WLANS** table, you can view the following information for **2.4 GHz**, **5 GHz**, and **5 GHz (Secondary)** radios:

- **BSSID**—Displays the MAC address of the radio.
- **Radio Type**—Displays the type of radio.
- **Clients**—Displays the number of connected clients.

Click ↓ to download the **.csv** file of the **WLANS** table.



-
- The tri-radio feature is available only for AP-555. In the **WLANS** table, the **5 GHz (Secondary)** data is available only if the tri-radio mode is enabled. For more information, see [About Tri-Radio Mode](#).
 - In the **.csv** file of the **WLANS** table, the **5 GHz (Secondary)** columns are available only if the tri-radio mode is enabled.
-

Actions

The **Actions** drop-down list contains the following options:

- **Reboot AP**—Reboots the AP point. For more information, see [Rebooting an AP in the List View](#) and [Rebooting an AP in the Details Page](#).
- **Reboot Swarm**—Reboots the AP cluster. For more information, see [Rebooting an IAP Cluster](#).
- **Tech Support**—Enables the administrator to generate a tech support dump required for troubleshooting the AP. For more information, see [Tech Support for an IAP](#).

Go Live

Aruba Central (on-premises) supports live monitoring of IAPs that support Aruba Instant 8.4.0.0 firmware version and above. Aruba Central (on-premises) allows you to monitor live data of an AP updated at every 5 seconds. For more information, see [Enabling Live IAP Monitoring](#).

Access Point > Overview > AI Insights

In the access point (AP) dashboard, the **AI Insights** tab displays information on AP performance issues such as excessive channel changes, excessive reboots, airtime utilization, and memory utilization.

Viewing Access Points > AI Insights

To navigate to the **AI Insights** tab in the AP dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Access Points**. A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**.
The dashboard context for the AP is displayed.
4. In the AP dashboard context, click the **AI Insights** tab.
The **Insights** page is displayed.
5. To exit the AP dashboard, click the back arrow on the filter.

You can change the time range for the **AI Insights** tab by clicking the time range filter and selecting one of the available options: **3 hours, 1 day, 1 week, 1 month, and 3 months**.



AI Insights are displayed for the time range selected. Select the time range from the **Time Range Filter** (🔄) to filter reports.

AI Insights Categories

AI Insights are categorized in high, medium, and low priorities depending on the number of occurrences.

-  Red—High priority
-  Orange—Medium priority
-  Yellow—Low priority

AI Insights listed in the dashboard are sorted from high priority to low priority. The **AI Insights** dashboard displays a report of network events that could possibly affect the quality of the overall network performance. Each insight report provides specific details on the occurrences of these events for ease in debugging. For more information, see [The AI Insights Dashboard](#)

The **AP Insights** page displays the following insights:

- [Clients with High Wi-Fi Security Key-Exchange Failures](#)
- [Clients with High 802.1X Authentication Failures](#)
- [Clients with DHCP Server Connection Problems](#)
- [Clients with High Number of MAC Authentication Failures](#)
- [Clients with High Number of Wi-Fi Association Failures](#)
- [Clients with Captive Portal Authentication Problems](#)

Access Point > Overview > Floor Plan

In the access point (AP) dashboard, the **Floor Plan** tab provides information regarding the current location of the Instant Access Point (IAP).

Viewing the Overview > Floor Plan Tab

To navigate to the **Floor Plan** tab in the AP dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**.
The dashboard context for the AP is displayed.
4. In the AP dashboard context, click the **Floor Plan** tab. The **Floor Plan** tab is displayed.

To exit the AP dashboard, click the back arrow on the filter.

You can change the time range for the **Floor Plan** tab by clicking the time range filter and selecting one of the available options: **3 hours, 1 day, 1 week, 1 month, and 3 months**.

The **Floor Plan** tab displays a sitemap and the floor plan showing the current location of the IAP. The sitemap is derived from the Visual RF application, if Visual RF service is enabled for the Aruba Central (on-premises) account. You can also edit the location of the IAP device by clicking the edit icon provided next to the address in the **Floor Plan** tab.

Actions

The **Actions** drop-down list contains the following options:

- **Reboot AP**—Reboots the AP. For more information, see [Rebooting an AP in the Details Page](#) and [Rebooting an AP in the List View](#).

- **Reboot Swarm**—Reboots the AP cluster. For more information, see [Rebooting an IAP Cluster](#).
- **Tech Support**—Enables the administrator to generate a tech support dump required for troubleshooting the AP. For more information, see [Tech Support for an IAP](#).

Go Live

Aruba Central (on-premises) supports live monitoring of IAPs that support Aruba Instant 8.4.0.0 firmware version and above. Aruba Central (on-premises) allows you to monitor live data of an AP updated at every 5 seconds. For more information, see [Enabling Live IAP Monitoring](#).

Access Point > Overview > Performance

In the access point (AP) dashboard, the **Performance** tab displays the size of data transmitted through the AP.

Viewing the Overview > Performance Tab

To navigate to the **Performance** tab in the AP dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under groups, labels, or sites. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP. The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Access Points**. A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**. The dashboard context for the AP is displayed.
4. In the AP dashboard context, click the **Performance** tab. The **Performance** tab is displayed.

To exit the AP dashboard, click the back arrow on the filter.

You can change the time range for the **Performance** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

The **Performance** tab provides the following details:

■ **Throughput**

The **Throughput** graph indicates the size of data sent to and received by the device in bits per second for the wired or wireless networks. For example, Eth 0 or Eth 1 wired network profiles and specific SSIDs of wireless networks. You can also view data for all the wireless SSIDs by selecting **All SSIDs** from the drop-down list. You can view the overall data usage measured in bytes in the **Overall Usage** field.

■ **Clients**

The **Clients** graph indicates the number of clients connected to the device for the wired, wireless, or radio network profiles for a selected time range in the time range filter. For example, wired for wired network profile, specific SSID or All SSIDs for wireless network profile, and 2.4 GHz, 5 GHz, or 2.4 GHz&5 GHz for radio network profile. You can select a specific network profile from the drop-down list provided in the **Clients** section to view the date, time and number of clients connected.



When you hover over the **Throughput** and **Clients** graphs, it displays specific data for the selected timestamp.

Actions

The **Actions** drop-down list contains the following options:

- **Reboot AP**—Reboots the AP. For more information, see [Rebooting an AP in the Details Page on page 375](#) and [Rebooting an AP in the List View on page 356](#).
- **Reboot Swarm**—Reboots the AP cluster. For more information, see [Rebooting an IAP Cluster](#).
- **Tech Support**—Enables the administrator to generate a tech support dump required for troubleshooting the AP. For more information, see [Tech Support for an IAP](#).

Go Live

Aruba Central (on-premises) supports live monitoring of IAPs that support Aruba Instant 8.4.0.0 firmware version and above. Aruba Central (on-premises) allows you to monitor live data of an AP updated at every 5 seconds. For more information, see [Enabling Live IAP Monitoring](#).

Access Point > Overview > RF

In the access point (AP) dashboard, the **RF** tab provides details corresponding to 2.4 GHz, 5 GHz, and 5 GHz Secondary radios of the AP.

Viewing the Overview > RF Tab

To navigate to the **RF** tab in the AP dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under groups, labels, or sites. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP. The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Access Points**. A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**. The dashboard context for the AP is displayed.
4. In the AP dashboard context, click the **RF** tab. The **RF** tab is displayed.

To exit the AP dashboard, click the back arrow on the filter.

You can change the time range for the **RF** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

You can hover over the graph to view more information. You can select or clear an option in each graph to filter the data displayed on the graph. For example, if you uncheck the box corresponding to **Receiving** and **Non-Wifi interference** in the **Channel Utilization** graph, only **Transmitting** data is displayed on the graph.

The **RF** tab provides the following details corresponding to **2.4 GHz** and **5 GHz** radio channels of the AP:

Channel Utilization

The **Channel Utilization** graph indicates the percentage of channel utilization for the selected time range from the time range filter. The channel utilization information is categorized as follows:

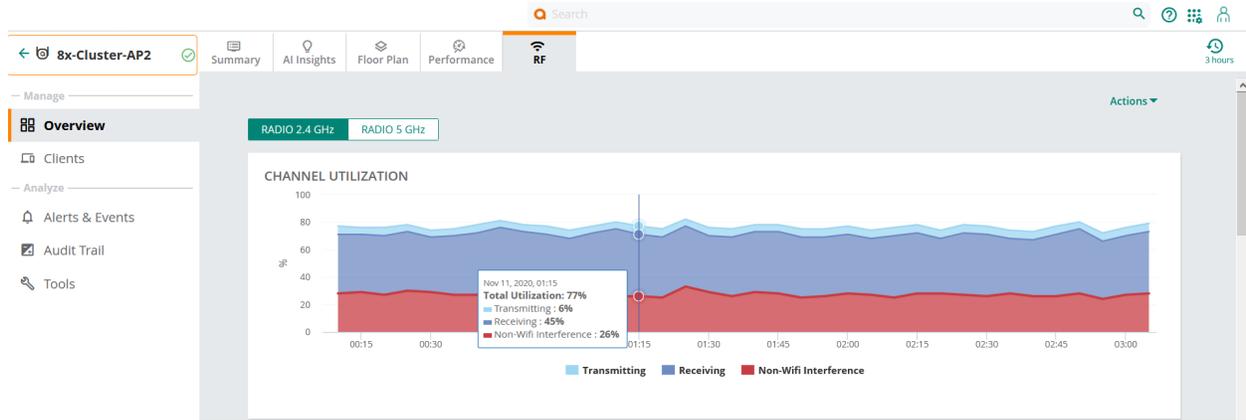
- **Transmitting**: The percentage of channel currently being transmitted.
- **Receiving**: The percentage of channel currently being received.

- **Non-Wifi Interference:** The percentage of channel currently being used by non-Wi-Fi interferers.



Total Utilization is the sum of **Transmitting**, **Receiving**, and **Non-Wifi interference**, which indicates the total percentage of channel utilization for the selected time range.

The following figure displays the channel utilization graph for 2.4 GHz radio channel:



Noise Floor

The **Noise Floor** graph indicates the noise floor detected in the network to which the device belongs.

Frames - 802.11

The **Frames - 802.11** line graph indicates the trend of frames transmitted through the network. The frames can be one of the following types: **Drops**, **Errors**, and **Retries**. The graph indicates the status of data frames that were dropped, encountered errors, retried to be transferred, in a wireless network. You can see the graph in percentage or frames/sec.



Only Campus APs and Remote APs support the **Issues & Transmitted Frames** and **Issue %** filter options.

Select one of the following option from the drop-down:

- **Issues & Transmitted Frames**—Select to view the trend value for transmitted frames along with retries, errors, and drops in frames per second
- **Issue %**—Select to view the trend value for retries, errors, and drops in percentage.

Figure 71 *Frames - 802.11 Graph*



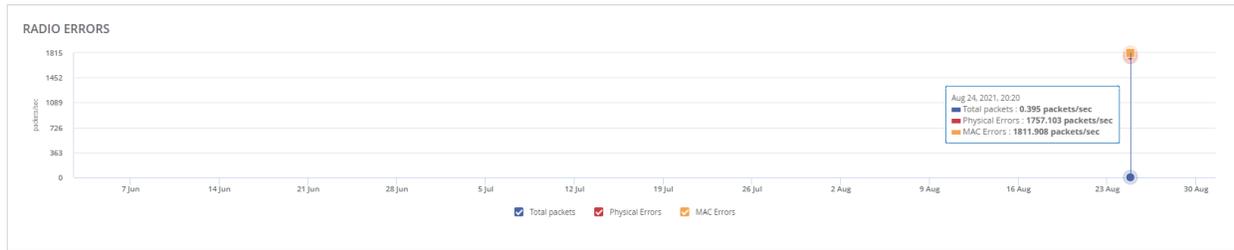
Radio Errors

The **Radio Errors** graph indicates the **Total Packets**, **Physical Errors**, and **MAC Errors** in packets per second.



Only Campus APs and Remote APs support the **Physical Errors**, and **MAC Errors** options.

Figure 72 Radio Errors Graph



Channel Quality

The **Channel Quality** graph indicates the quality of channel in percentage.

When you hover over the **Channel Utilization**, **Noise Floor**, **Frames - 802.11**, and **Channel Quality** graphs, it displays specific data for the selected timestamp.

The tri-radio feature is available only for AP-555. In the **RF** tab, the **Radio 5 GHz (Secondary)** tab is available only if the tri-radio mode is enabled. For more information, see [About Tri-Radio Mode](#).

Actions

The **Actions** drop-down list contains the following options:

- **Reboot AP**—Reboots the AP. For more information, see [Rebooting an AP in the Details Page](#).
- **Reboot Swarm**—Reboots the AP cluster. For more information, see [Rebooting an IAP Cluster](#).
- **Tech Support**—Enables the administrator to generate a tech support dump required for troubleshooting the AP. For more information, see [Tech Support for an IAP](#).

Go Live

Aruba Central (on-premises) supports live monitoring of IAPs that support Aruba Instant 8.4.0.0 firmware version and above. Aruba Central (on-premises) allows you to monitor live data of an AP updated at every 5 seconds. For more information, see [Enabling Live IAP Monitoring](#).

Access Point > Overview > Spectrum

In the access point (AP) dashboard, the **Spectrum** tab provides details for all Wifi and non-Wifi devices associated to each radio.

When the radios of Instant Access Point (IAP) are set to spectrum scan mode, the IAP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference from neighboring IAPs or interfering devices such as microwaves and cordless phones. To enable the spectrum scan feature on a specific radio of an AP, see [Access Points Configuration Parameters](#).

The spectrum scan feature is available only on IAP devices running Aruba Instant 8.5.0.1 firmware version and later.



When the spectrum scan feature is enabled, the Instant AP does not provide services to clients. The **Spectrum** tab displays the following sections:

- [Channel Utilization and Quality](#)
- [Interfering Devices](#)
- [Actions](#)
- [Go Live](#)

Viewing the Overview > Spectrum Tab

To navigate to the **Spectrum** tab in the AP dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**.
The dashboard context for the AP is displayed.
4. In the AP dashboard context, click the **Spectrum** tab. The **Spectrum** tab is displayed.

To exit the AP dashboard, click the back arrow on the filter.

You can change the time range for the **Spectrum** tab by clicking the time range filter and selecting one of the available options: **3 hours, 1 day, 1 week, 1 month, and 3 months**.

Channel Utilization and Quality

Click the **Chart** icon to view the **Channel Utilization and Quality** details corresponding to **2.4 GHz** and **5 GHz** radios of the AP. Click the **2.4 GHz** and **5 GHz** tabs on the **Channel Utilization and Quality** label to view the **Channel Utilization** and **Quality** graphs for the radios.

- **Channel Utilization**—The **Channel Utilization** graph indicates the percentage of channel utilization for the **Available, Interference, and Wi-Fi Utilization** categories associated to **2.4 GHz** and **5 GHz** radios. You can view the following channel metrics when you hover over the **Channel Utilization** bar graph:

Table 167: *Channel Utilization Metrics*

Metrics	Description
Channel	The channel number of the radio.
Available	The percentage of the channel currently available for use.
Interference	The percentage of the channel currently being used by interfering devices.

Metrics	Description
Microwave	The percentage of the channel currently being used by microwaves. Common residential microwave ovens with a single magnetron are classified as a Microwave. These types of microwave ovens may be used in cafeterias, break rooms, dormitories, and similar environments. Some industrial, healthcare, or manufacturing environments may also have other equipment that functions like a microwave and may also be classified as a Microwave device.
Bluetooth	The percentage of the channel currently being used by bluetooth devices. Any device that uses the Bluetooth protocol to communicate in the 2.4 GHz band is classified as a Bluetooth device. Bluetooth uses a frequency hopping protocol.
Cordless Phone	The percentage of the channel currently being used by cordless phones.
Wi-Fi Utilization	The percentage of the channel currently being used by Wi-Fi devices.

- **Quality**—The **Quality** graph display the channel quality corresponding to each of the WiFi and non-WiFi devices connected to the radios. When you hover over the **Quality** bar graph, the following channel metrics are displayed:

Table 168: *Channel Quality Metrics*

Metrics	Description
Channel	The channel number of the radio.
Quality	Current relative quality of the channel.
Known APs	Number of valid Instant APs identified on the radio channel.
Unknown APs	Number of invalid or rogue Instant APs identified on the radio channel.
Max AP Signal	Signal strength of the Instant AP that has the maximum signal strength on a channel in dBm.
Max Interference	Signal strength of the non-Wi-Fi device that has the highest signal strength in dBm.
Max AP SSID	The network SSID with maximum APs.
Max AP BSSID	The network SSID with maximum APs.
SNIR	The measure of SNIR detected in the network in dB.
Noise Floor	The noise at the radio receivers of the radios.

Interfering Devices

Table 169: Interfering Devices Table

Metrics	Description
Type	Device type. This parameter can be any of the following: <ul style="list-style-type: none">■ Audio FF (fixed frequency)■ Bluetooth■ Cordless base FH (frequency hopper)■ Cordless phone FF (fixed frequency)■ Cordless network FH (frequency hopper)■ Generic FF (fixed frequency)■ Generic FH (frequency hopper)■ Generic interferer■ Microwave■ Microwave inverter■ Video■ Xbox
ID	ID number assigned to the device by the spectrum monitor. Spectrum monitors assign a unique spectrum ID per device type.
Central Frequency	Center frequency of the signal sent from the device.
Bandwidth	Channel bandwidth used by the device in KHz.
Affected Channels	Radio channels affected by the wireless device.
Signal Strength	Strength of the signal sent from the device measured in dBm.
Duty Cycle	The device duty cycle. This value represents the percent of time the device broadcasts a signal.
First Seen	Time at which the device was first detected.
Last Seen	Time at which the device status was updated.

Click the **List** icon to view **Interfering Devices** details detected by the spectrum scanner. The page displays a table with following details of interfering devices:



The data displayed in the **Spectrum** tab is refreshed every 15 seconds. Aruba Central (on-premises) displays the last recorded data for 30 minutes, if the device turns offline.

Actions

The **Actions** drop-down list contains the following options:

- **Reboot AP**—Reboots the AP. For more information, see [Rebooting an AP in the Details Page on page 375](#) and [Rebooting an AP in the List View on page 356](#).
- **Reboot Swarm**—Reboots the AP cluster. For more information, see [Rebooting an IAP Cluster](#).

- **Tech Support**—Enables the administrator to generate a tech support dump required for troubleshooting the AP. For more information, see [Tech Support for an IAP](#).

Go Live

Aruba Central (on-premises) supports live monitoring of IAPs that support Aruba Instant 8.4.0.0 firmware version and above. Aruba Central (on-premises) allows you to monitor live data of an AP updated at every 5 seconds. For more information, see [Enabling Live IAP Monitoring](#).

Access Point > Security > VPN

The **VPN** tab provides information on VPN connections associated with the virtual controller along with information on the tunnels and the data usage through each of the tunnels.

Viewing the Security > VPN Tab

To navigate to the **VPN** tab, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**.
The dashboard context for the AP is displayed.
4. Under **Manage**, click **Security > VPN**.
The **VPN** tab is displayed.

You can change the time range for the **VPN** tab by clicking the time range filter and selecting one of the available options: **3 hours, 1 day, 1 week, 1 month, and 3 months**.

The **VPN** tab provides the following information:

- **VPNC Tunnels Summary**—The section displays information on tunnels with the following details:
 - **Total**—Total tunnels established.
 - **Up**—Number of tunnels currently active.
 - **Down**—Number of tunnels currently inactive.
 - **Peers**—Number of peer tunnels currently active.
The **Tunnel** table displays information on tunnels with the following columns:
 - **Tunnel**—The type of the tunnels used in the VPN. For example, primary, secondary, or backup.
 - **Status**—The status of the tunnel.
 - **Source**—The source address of the tunnel.
 - **Destination**—The destination address of the tunnel.
- **Throughput Usage Per VPN**—The **Throughput Usage Per VPN** graph indicates the successful data usage per VPN in Mbps for the primary or backup tunnel selected from the drop-down list. The **Throughput Usage Per VPN** displays a linear graph of sent and received data in the virtual private network.

- The **Gateway** tab provides information on the gateways to which the AP is connected. The tab displays the following details:
- **Tunnels Summary**—The section displays information on tunnels with the following details:

Rebooting APs

You can reboot an Instant AP or an Instant AP cluster using the Aruba Central UI.

Perform any of the following procedures:

Reboot an Instant AP

To reboot an Instant AP:

1. From the app selector, click **Monitoring & Reports** and go to **Network Overview > APs**.
2. Select **List of Up APs**. The **Access Points** table displays a list of Instant APs in the group.
3. In the **Access Points** table, select the Instant AP to reboot.
4. In the **Actions** drop-down list, click **Reboot AP**.
5. In the **Reboot** dialog box, click **Continue**.

Reboot an Instant AP cluster

To reboot an Instant AP cluster:

1. From the app selector, click **Monitoring & Reports** and go to **Network Overview > APs**.
2. In the **Access Points** table, select the master Instant AP to reboot.
3. In the **Actions** drop-down list, click **Reboot Swarm**.
4. In the **Reboot** dialog box, click **Continue**.

Rebooting an IAP Cluster

You can reboot an Instant Access Point (IAP) cluster using the Aruba Central (on-premises) UI.

To reboot an IAP cluster, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**.
The dashboard context for the AP is displayed.
4. In the **Actions** drop-down list, click **Reboot Swarm**.
A **Reboot** dialog box is displayed.
5. Click **Yes** to reboot the AP cluster.



The AP dashboard takes less than a minute to update the interface status, after the VC is rebooted and reconnected to Aruba Central (on-premises).

Resetting an AP

You can reset the system configuration of an Instant AP by erasing the existing configuration on the Instant AP. To erase the existing configuration on an Instant AP, perform any of the following procedures:

Clearing Instant AP Configuration Using Groups

To reset an Instant AP using groups, complete the following steps:

1. Create a new group. Ensure that the group has no additional configuration.
2. Move the Instant AP that you want to reset, under the new group. After the Instant AP is moved to a new group, the configuration on the Instant AP is erased and the default group configuration is pushed to the Instant AP. However, in this procedure, only the system configuration is cleared and the **Per AP Settings** on the Instant AP are retained.

Resetting an AP through the Console

To reset an Instant AP from the console, complete the following steps:

1. Log in to the Instant AP console. To access the Instant AP console:
2. Select **Monitoring & Reporting** app.
3. Click APs and select List from the APs drop-down.
4. Select the AP to reset.
5. From the **Actions** drop-down, click **Console**.
6. Execute the **write erase all** command at the command prompt.
7. Reboot the Instant AP. With this procedure, the complete configuration including the **Per AP Settings** on the Instant AP is reset.

After the reboot, the Instant AP is moved to default group and will not be present in the group to which it was previously attached.

For information on resetting an Instant AP to factory default configuration by using the reset button on the device, see *Aruba Instant User Guide*.

Tech Support for an IAP

In Aruba Central (on-premises) UI, the administrators can generate a tech support dump required for troubleshooting the Instant Access Point (IAP).

To generate a tech support dump for an IAP, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**.
The dashboard context for the AP is displayed.

4. In the **Actions** drop-down list, click **Tech Support**.
The **Commands** page is displayed. In the **Commands** page, the **Device Type** and **Available Devices** fields are automatically selected. The `AP Tech Support Dump` command is automatically selected in the **Selected Commands** pane.
5. Click **Run**. The output is displayed in the **Device Output** section.

For more information, see [Advanced Device Troubleshooting](#).

Enabling Live IAP Monitoring

Aruba Central (on-premises) supports live monitoring of Instant APs that support Aruba Instant 8.4.0.0 firmware version and above. Aruba Central (on-premises) allows you to monitor live data of an AP updated at every 5 seconds.

Enabling and Disabling Go Live

To enable and disable the live monitoring of an AP, complete the following steps:

- In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active access point. The dashboard context for the selected filter is displayed.
- Under **Manage**, click **Devices > Access Points**. A list of access points is displayed in the **List** view.
- Click an access point listed under **Device Name**. The dashboard context for the access point is displayed.
- Click the **Go Live** button to start live monitoring of the AP.
- Click the **Stop Live** button to exit live monitoring of the AP.

The **Go Live** feature is not applicable for offline Instant APs. The **Go Live** button remains grayed-out for all the APs that are not associated with Instant AP devices running Aruba Instant 8.4.0.0 firmware version and above

Aruba Central (on-premises) allows you to monitor live data for 15 minutes. After this time period, Aruba Central (on-premises) redirects to the AP dashboard in a non-live mode to display the monitoring details for the time selected in the **Time Range Filter**. For more information on AP dashboard in a non-live mode, see [Access Point > Overview > Summary](#).



AP Details in Go Live Mode

When you click the **Go Live** button, the page displays live graphs based on noise floor, frames, and channel quality of the neighboring RF devices for 15 minutes, until you select **Stop Live** button.

The page displays **Noise Floor, Frames, and Channel Quality** live graphs for **Radio 2.4 GHz, Radio 5 GHz, and Radio 5 GHz Secondary** radios.

Important Information

- The Go Live feature is not applicable for offline APs.
- Aruba Central allows you to monitor live data for 15 minutes. After this time period, Aruba Central redirects to the AP dashboard in a non-live mode to display the monitoring details for the time selected in the **Time Range Filter**. For more information on AP dashboard in a non-live mode, see [Access Point > Overview > Summary](#).
- In **Go Live** mode, AP dashboard updates and displays data at every 5 seconds.

- The tri-radio feature is available only for AP-555. In the **Go Live** page, the **Radio 5 GHz (Secondary)** tab is available only if the tri-radio mode is enabled. For more information, see [About Tri-Radio Mode](#).
- The time range selected in the **Time Range Filter** is not applicable when the **Go Live** button is enabled.
- You can monitor live data for multiple APs simultaneously on different tabs.

Access Point > Clients > Clients

In the access point (AP) dashboard, the **Clients** tab displays details of all the clients connected to a specific AP.

Viewing the Access Point > Clients > Clients Tab

To navigate to the **Clients** tab in the AP dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**.
The dashboard context for the AP is displayed.
4. Under **Manage**, click **Clients**.
The **Clients** page is displayed in the **List** view.
To exit the Clients dashboard, click the back arrow on the filter.
You can change the time range for the **Clients** tab by clicking the time range filter and selecting one of the available options: **3 hours, 1 day, 1 week, 1 month, and 3 months**.



For more information, see [All Clients](#).

Access Point > Alerts & Events > Alerts & Events

In the access point (AP) dashboard, the **Alerts & Events** tab displays details of the alerts and events generated for the AP.

Viewing the Access Point > Alerts & Events > Alerts & Events Tab

To navigate to the **Alerts & Events** tab in the AP dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**.
The dashboard context for the AP is displayed.

- Under **Analyze**, click **Alerts & Events**.

The **Alerts & Events** page is displayed in the **List** view.

To exit the Alerts & Events dashboard, click the back arrow on the filter.



For more information, see [Alerts & Events](#). You can also configure and enable certain categories of AP alerts.
For more information, see [Access Point Alerts](#).

Supported Client Events for Campus AP and Instant AP Devices

Aruba Central (on-premises) provides an **Events** dashboard for viewing the events triggered from Campus Access Point (CAP) and Instant Access Point (IAP) devices.

The following table lists the client events that are supported for IAP and CAP in Aruba Central (on-premises):

Table 170: *Client Events*

Event	Description	Campus AP	Instant AP
Client 802.11 Association Reject	802.11 Association rejected for client [<i>Client MAC</i>] to BSSID [<i>BSSID</i>] on channel [<i>Channel</i>] of AP hostname [<i>Device Hostname</i>].	Supported	Supported
Client 802.11 Disassociation to Client	802.11 Disassociation sent to client [<i>Client MAC</i>] from BSSID [<i>BSSID</i>] on channel [<i>Channel</i>] of AP hostname [<i>Device Hostname</i>].	Supported	Supported
Client 802.11 Disassociation from Client	802.11 Disassociation received from client [<i>Client MAC</i>] associated to BSSID [<i>BSSID</i>] on channel [<i>Channel</i>] of AP hostname [<i>Device Hostname</i>].	Supported	Supported

Event	Description	Campus AP	Instant AP
Client 802.11 Authentication Failure	802.11 Authentication failed for client [Client MAC] on BSSID [BSSID] on channel [Channel] of AP hostname [Device Hostname].	Supported	Supported
Client 802.11 De-authentication to Client	De-authentication sent to client [Client MAC] from BSSID [BSSID] on channel [Channel] of AP hostname [Device Hostname].	Supported	Supported
Client 802.11 De-authentication from Client	De-authentication sent from client [Client MAC] associated to BSSID [BSSID] on channel [Channel] of AP hostname [Device Hostname].	Supported	Supported
Client Roaming Success	Client [Client MAC] associated to BSSID [From BSSID (roamed from)] on channel [From Channel (roamed from)] of AP hostname [From Device Hostname (roamed from)] roamed successfully to BSSID [BSSID] on channel [Channel] of AP hostname [Device Hostname].	Supported	Supported

Event	Description	Campus AP	Instant AP
Client MAC Authentication Reject	MAC Authentication failed for client [Client MAC] to Radius Server [Radius Server IP] through BSSID [BSSID] on channel [Channel] of AP hostname [Device Hostname].	Supported	Supported
Client 802.1x Radius Reject	802.1x Radius Reject received for client [Client MAC] on BSSID [BSSID] on channel [Channel] of AP hostname [Device Hostname].	Supported	Supported
Client 802.1x Radius Timeout	802.1x Radius Timeout occurred for client [Client MAC] on BSSID [BSSID] on channel [Channel] of AP hostname [Device Hostname].	Supported	Supported
Client Captive Portal Authentication Failure	Captive Portal failure occurred for client [Client MAC] associated to BSSID [BSSID] of AP hostname [Device Hostname].	Supported	Supported
Client EAP Failure	EAP failure occurred for client [Client MAC] associated to BSSID [BSSID] on channel [Channel] of AP hostname [Device Hostname].	Supported	Supported

Event	Description	Campus AP	Instant AP
Client EAP Timeout from Client	EAP response from client [Client MAC] associated to BSSID [BSSID] on channel [Channel] of AP hostname [Device Hostname] timed out.	Not Supported	Supported
Client VoIP Call Start	VoIP call initiated from station [Source Client Name] ([Source Client IP]) to station [Destination Client Name] ([Destination Client IP]) on AP hostname [Device Hostname].	Not Supported	Supported
Client VoIP Call Stop	VoIP call terminated from station [Source Client Name] ([Source Client IP]) to station [Destination Client Name] ([Destination Client IP]) on AP hostname [Device Hostname].	Not Supported	Supported
Client DHCP Acknowledged	DHCP acknowledgment received from DHCP server [DHCP Server IP] for client [Client MAC] ([Client IP]) associated to BSSID [BSSID] on channel [Channel] of AP hostname [Device Hostname].	Supported	Supported

Event	Description	Campus AP	Instant AP
Client DHCP Not Acknowledged	DHCP NACK to DHCP server [DHCP Server IP] from client [Client MAC] ([Client IP]) associated to BSSID [BSSID] on channel [Channel] of AP hostname [Device Hostname].	Supported	Supported
Client DHCP Declined	DHCP declined from DHCP server [DHCP Server IP] for client [Client MAC] ([Client IP]) associated to BSSID [BSSID] on channel [Channel] of AP hostname [Device Hostname].	Supported	Supported
Client DNS Failure	DNS failure to [Domain Name] detected for client [BSSID] on BSSID [BSSID] of AP hostname [Device Hostname].	Not Supported	Supported
Client DHCP Timeout	DHCP request to DHCP server [DHCP Server IP] from client [Client MAC] timed out.	Supported	Supported
Client Blacklisted	Blacklisted client [Client MAC] on AP hostname [Device Hostname] for SSID [SSID name].	Not Supported	Supported

Event	Description	Campus AP	Instant AP
Client Fast Roaming Failure	Fast Roaming failed for client [Client MAC] with roaming type [Roaming Type] on AP hostname [Device Hostname].	Not Supported	Supported
Client Roaming Success	Client [Client MAC] roamed successfully to SSID [SSID name] on channel [Channel] of AP hostname [Device Hostname].	Not Supported	Supported
Client Match Steer Attempt	Client match attempted a [Steer Type] using [Steer Mode] for client [Client MAC] from radio BSSID [From BSSID] to radio BSSID [To BSSID] with result: [Steer Result].	Not Supported	Supported
Client Match Steer Reject	Client match attempted a [Steer Type] using [Steer Mode] for client [Client MAC] from radio BSSID [From BSSID] to radio BSSID [To BSSID] which was rejected by the client with reason code [802.11v Move Result].	Not Supported	Supported

Event	Description	Campus AP	Instant AP
Client Match Steer Wrong Destination	Client match attempted a <i>[Steer Type]</i> using <i>[Steer Mode]</i> for client <i>[Client MAC]</i> from radio BSSID <i>[From BSSID]</i> to radio BSSID <i>[To BSSID]</i> which resulted in the client moving to a different radio BSSID <i>[Destination Radio BSSID]</i> .	Not Supported	Supported
Client Match Success	Client match attempted a <i>[Steer Type]</i> using <i>[Steer Mode]</i> for client <i>[Client MAC]</i> from radio BSSID <i>[From BSSID]</i> to radio BSSID <i>[To BSSID]</i> with result: Success info : <11v reason if any > and steer reason [Sticky Client, Dynamic load balancing, capability mismatch, channel steering, band steering]	Supported	Not Supported

Event	Description	Campus AP	Instant AP
Client Match Steer Uncontrolled Moves	Client match attempted a <i>[Steer Type]</i> using <i>[Steer Mode]</i> for client <i>[Client MAC]</i> from radio BSSID <i>[Client MAC]</i> to radio BSSID <i>[To BSSID]</i> with result: Move result info : <11v reason if any > and steer reason <i>[Sticky Client , Dynamic load balancing, capability mismatch, channel steering, band steering]</i>	Supported	Not Supported
Client Match Steer No Move	Client match attempted a <i>[Steer Type]</i> using <i>[Steer Mode]</i> for client <i>[Client MAC]</i> from radio BSSID <i>[Client MAC]</i> to radio BSSID <i>[To BSSID]</i> with result: Move result info : <11v reason if any > and steer reason <i>[Sticky Client, Dynamic load balancing, capability mismatch, channel steering, band steering]</i>	Supported	Not Supported
Client Authentication Server Timeout	Authentication request to a Radius server <i>[Radius Server IP]</i> from a client <i>[Client MAC]</i> timed out.	Supported	Not Supported

Event	Description	Campus AP	Instant AP
Client Accounting Server Timeout	Accounting request to a Radius server [<i>Radius Server IP</i>] from a client [<i>Client MAC</i>] timed out.	Supported	Not Supported
Radius-COA Failure	Timestamp: Radius COA failure received from < <i>Server IP</i> > for a < <i>Client MAC</i> > associated to < <i>BSSID MAC/SSID</i> > on < <i>Radio Index:Channel</i> > of < <i>AP Hostname</i> > Reason Code : < <i>Description</i> >	Supported	Not Supported

Monitoring Switches and Switch Stacks

The switch dashboard enables you to manage, configure, monitor and troubleshoot AOS-Switch, AOS-CX switches, and switch stacks provisioned and managed through Aruba Central (on-premises).

To view AOS-CX switches in the monitoring and topology pages, you must create a template configuration for the switch with the password in plaintext. See [Using Configuration Templates for AOS-CX Switch Management](#).



If you are unable to view all details of the AOS-CX switch, then maybe the template configuration was not applied correctly, the password was missing in the template configuration, or the password was not in plaintext. See the audit trail to check the status of the switch. The audit trail should show the device onboarded message for the switch serial number followed by the configuration push and login successful messages. For more information on troubleshooting AOS-CX switch onboarding issues, see [Troubleshooting AOS-CX Switch Onboarding Issues](#).

Monitoring Switches in List View

The switch monitoring details are displayed on the switch dashboard and the switch details page. The switch dashboard and the switch details page are accessed from the **Network Operations** app.

The switch dashboard displays details about the health and status of switches and switch stacks. The switch details are provisioned and managed through Aruba Central (on-premises). The switch dashboard displays the details in a summary and list view.

The Switches List page provides information associated with the switches provisioned and managed in Aruba Central (on-premises). The Switches List page displays the following sections:

Viewing the Switches List Page

To navigate to the Switches List page, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.

The dashboard context for the selected filter is displayed.

2. Under **Manage**, click **Devices > Switches**.

A list of switches is displayed in the **List** view.

The Switches List page displays the following information:

- **Switches**—Displays the total number of switches, both online and offline. When you click the **Switches** tab, it provides information about all switches in the **Switches** table.
- **Online**—Displays the number of online switches. When you click the **Online** tab, it provides information about all switches that are currently online and connected to Aruba Central (on-premises) in the **Switches** table.
- **Offline**—Displays the number of offline switches. When you click the **Offline** tab, it provides information about all switches that are currently offline or not connected to Aruba Central (on-premises) in the **Switches** table.

The online switches are displayed with a green dot and offline switches are displayed with a red dot.

Even when the AOS-CX switches are displayed as online, there might be instances when the details of the switches are not displayed completely. This may be because of the following reasons:

- Template configuration is not applied correctly on the switch
- Password is not configured in the template configuration
- Password is not in plaintext format



See the audit trail to check the status of the AOS-CX switches. The audit trail should show the device onboarded message for the switch serial number followed by the configuration push and login successful messages. For more information on troubleshooting AOS-CX switch onboarding issues, see [Troubleshooting AOS-CX Switch Onboarding Issues](#).

Switches Table

The **Switches** table displays the following information:

- **Device Name**—Name of the switch or switch stack. For a switch stack, a stack icon is displayed next to the device name.
- **Type**—Type of switch. Following are the supported values:
 - **AOS**
 - **CX**
 - **AOS Stack**
- **Clients**—Number of clients connected.
- **Alerts**—Number of alerts from the switch or switch stack.
- **Model**—Model number of the switch. For a switch stack, the term **Stack** is displayed.

- **Config Status**—Configuration status of the switch or switch stack. Following are the supported values:
 - **In sync**
 - **Not in sync**
- **Last Seen**—Date and time when the switch or switch stack was last connected.
- **Usage**—Data usage on the switches.
- **IP Address**—IP address of the switch or switch stack.
- **MAC**—MAC address of the switch or switch stack.
- **Firmware Version**—Firmware version of the switch or switch stack.
- **Group**—Name of the group to which the switch or switch stack is assigned.
- **Labels**—Name of the label associated with the switch or switch stack.
- **Site**—Site in which the switch or switch stack is provisioned.
- **Uptime**—Duration for which the switch is operational.
- **Serial/Stack ID**—Serial number of the switch or switch stack.
- **Uplink Ports**—Uplink ports configured on the switch or switch stack.
- **Port Utilization**—Utilization percentage of the port.



A search filter is provided only for the **Device Name** and **Model** columns.

To download the switch details as a **.csv** file, click the **Download CSV** icon. If the table contains unicode value, you must use a UTF-8 enabled software to view the contents. To view the file, open the file in a Microsoft Excel spreadsheet software.

Assigning Uplink Ports

To assign uplink port(s):

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
3. In the **Switches** table, hover over the switch for which you want to assign uplink port(s).
4. Click **Uplinks**.



For offline switches, click **Actions > Uplinks** in the pop-up window.

5. In the **Assign Uplink Ports/Trunks** dialog box, select the ports in the **Assigned Uplink Ports/Trunks** drop-down. On selecting the ports, the uplink rates for the selected ports are displayed in the uplink trend chart. For more information, see [Uplink](#).
6. Select the port(s), and click **Assign**.

Deleting an Offline Switch

To delete an offline switch:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**. Ensure that the filter selection contains at least one

switch.

The dashboard context for the selected filter is displayed.

2. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
3. Click **Offline** to display a table with the list of offline switches.
4. In the **Switches** table, hover over the offline switch that you want to delete.
5. Click the  delete icon.



To delete multiple offline switches, select the offline switches that you want to delete, and click the  delete icon at the bottom of the page.

6. Click **Yes** in the **Confirm Action** dialog box.

Downloading Switch Details

You can download the switch details as a .csv file.

To download the switch details, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
2. Under **Manage** click **Devices > Switches**.
A list of switches is displayed in the **List** view.
3. In the **Switches** table, click the download icon to download the switches details as a .csv file.
A .csv file is downloaded.

Monitoring Switches in Summary View

The Switches Summary page provides a graphical view of all metrics about the usage and clients information associated with the switch provisioned and managed in Aruba Central (on-premises).

Viewing the Switches Summary Page

To navigate to the Switches Summary page, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
3. Click the **Summary** icon.
The Switches Summary page is displayed with the following information:
 - **Usage**—Displays aggregate client data traffic detected on the switches.
 - **Clients**—Displays the number of clients connected to a switch.

You can change the time range by clicking the time range filter and selecting one of the available options: **3 hours, 1 day, 1 week, 1 month, or 3 months**.

Switch > Overview > Summary

The **Overview** tab provides a summary of the switch device details, network details, ports, hardware, uplink graph, usage graph, and details about the stack members.

The **Summary** tab displays the following sections:

- [Switch](#)
- [Network](#)
- [Ports](#)
- [Hardware](#)
- [Uplink](#)
- [Usage](#)
- [Stack Members](#)
- [Actions](#)

Viewing the Overview > Summary Tab

To navigate to the **Summary** tab in the Switch dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active switch.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
3. Click a switch listed under **Device Name**.
The dashboard context for the specific switch is displayed.
4. Under **Manage**, click **Overview > Summary**.
The **Summary** tab is displayed.
5. To exit the Switch dashboard, click the back arrow on the filter.
You can change the time range for the **Summary** tab by clicking the time range filter and selecting one of the available options: **3 hours, 1 day, 1 week, 1 month, or 3 months**.

Switch

The **Switch** section displays the following details:

- **Model**—Hardware model of the switch.
- **J-Number**—Part number of the switch. This field is displayed only for standalone switches that are not part of switch stacks.
- **Location**—Current location of the switch.
- **Contact**—E-mail address of the contact person.
- **Conductor**—Serial number of the conductor switch in a switch stack. This field is displayed only for switch stacks.
- **Serial**—Serial number of the switch. This field is displayed only for standalone switches that are not part of switch stacks.
- **MAC Address**—MAC address of the switch. This field is displayed only for standalone switches that are not part of switch stacks.

- **Uptime**—Time duration for which the switches are operational.
- **Last Reboot**—Timestamp of when the switch was last rebooted.
- **Configuration**—Configuration status of the switch.
- **Last Sync:**—Timestamp when the configuration was last synched between the peer switches in the stack.
- **Last Stats Received**—Timestamp of when the last statistics were received.
- **Firmware Version**—Firmware version of the switch. If an updated version is available, the version number is displayed and you can click the link to navigate to the firmware management page and upgrade the firmware.
- **Last Updated**—Timestamp of when the switch firmware was last changed.
- **Firmware Status**—Displays whether a new firmware version is available.
- **Group**—Name of the group to which the switch belongs. Click the group name to view the dashboard context for the group.
- **Site**—Name of the site to which the switch belongs. Click the site name to view the dashboard context for the site.
- **Label(s)**—Name of the label to which the switch belongs.

Figure 73 *Switch Overview*

SWITCH			
MODEL HP2920-24G-PoE+ Switch	J-NUMBER J9727A	LOCATION --	CONTACT --
SERIAL SG75FLX9HM	MAC ADDRESS f4:03:43:d4:2d:00	UPTIME 46 Days 21 Hours 58 Minutes	LAST REBOOT Oct 04, 2019, 02:12:20
CONFIGURATION Not in sync Last Sync: Nov 19, 2019, 17:11:20	LAST STATS RECEIVED 20 Nov 2019 00:10:47	FIRMWARE VERSION 16.06.0006 Update Available - 16.10.0002	
GROUP Branch-2	SITE AI-Testing	LABEL(S) --	

Network

The **Network** section displays the following details:

- **IP Address**—IP address of the switch. For AOS-CX switches, a value is displayed only if the IP address is configured for the management interface of the switch. If IP address is obtained from the DHCP server, this field will appear blank for AOS-CX switches.
- **Default VLAN**—Default VLAN ID of the switch.
- **Management VLAN**—Management VLAN ID of the switch. This field is displayed only for AOS-Switches.
- **Stack/Standalone**—Indicates whether the switch is part of a stack or if it is a standalone switch.
- **Stack Members**—Total number of members in the stack. This field is displayed only for switch stacks.
- **Stack Topology**—Topology of the stack.
- **Stack ID**—Stack ID used to identify the stack. This field is displayed only for switch stacks.

Figure 74 Network Details

NETWORK		
IP ADDRESS	PRIMARY VLAN	STACK/STANDALONE
10.53.9.125	1	STANDALONE

Ports

The **Ports** section displays the following details:

- **Status**—Number of ports in Up and Down state, and number of alerts.
- **Power Over Ethernet (PoE)**—Number of PoE ports enabled and disabled, and number of alerts.

Figure 75 Port Summary

PORTS			
STATUS			
2 Up	22 Down	-- Alert	0 Uplink
POWER OVER ETHERNET (PoE)			
AVAILABLE	USED	PoE DENIED PORTS	ALERT
0W	0W	0	0

Hardware

The **Hardware** section displays the following details:

- **Power Supply**—Total number of power supplies and number of power supplies in Up state.
- **Fans**—Total number of fans and the number of fans in the Up and Down states.
- **CPU**—CPU utilization status.
- **Memory**—Memory utilization status.
- **Temperature**—Temperature status. Hover your mouse over the status to view the temperature data.

Figure 76 *Hardware Details*

HARDWARE

CPU

Good

MEMORY

Good

TEMPERATURE

Good

POWER SUPPLY

4 Total

2 Up

FANS

8 Total

8 Up

0 Down

Uplink

The **Uplink** section displays the uplink rate (bps) trend chart for the duration specified in the time range filter. Hover the mouse over the trend chart to view the uplink rate at a particular time.

Figure 77 *Uplink Trend Chart*



Usage

The **Usage** section displays the trend chart for client data traffic detected on the switch. Hover the mouse over the trend chart to view data transmitted and received at a particular time.

Stack Members

The **Stack Members** table displays the following details:

- **Name**—Name of the switch stack member.
- **Member ID**—Identification number of the member.
- **Model**—The hardware model of the switch.
- **MAC Address**—The MAC address of the stack member.
- **Serial**—The serial number of the switch.
- **Role**—The role of a stack member.
- **Status**—The status of the switch stack member.
- **Priority**—Priority of the member. This column is not displayed for AOS-CX switches.

Figure 78 Stack Members Table

STACK MEMBERS							
NAME	MEMBER ID	MODEL	MAC ADDRESS	SERIAL	ROLE	STATUS	PRIORITY
C2-2920-1-CMDR-1	1	HP2920-24G-PoE+ Swi...	14:58:d0:99:75:40	SG48FLXYV7	Commander	Down	
C2-2920-1-STBY-2	2	HP2920-24G-PoE+ Swi...	14:58:d0:99:96:80	SG48FLXYVJ	Standby	Down	

Actions

The **Actions** tab displays the various options available for remote administration of the switch. The following options are available:

- **Reboot**—Reboots the switch. See [Rebooting Switches](#).
- **Tech Support**—Allows the administrators to generate a tech support dump for troubleshooting the device. See [Troubleshooting Aruba Switches](#).
- **Console**—Opens the remote console for a CLI session through SSH. Ensure that you allow SSH over port 443. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See [Opening Remote Console for Switch](#).

For AOS-CX 8320 and 8325 switch series, you must enable SSH server on the default VRF. Add the `ssh server vrf default` code to the template.

If the Copy and Paste function from the keyboard shortcut keys (CTRL+C and CTRL+V) do not work in your web browser, use the Copy and Paste functions available under the menu options in the web browser.



Switch > Overview > Hardware

In the switch dashboard, the **Hardware** tab displays information related to power supplies, fans, utilization, and temperature.

The **Hardware** tab displays the following sections:

- [Hardware](#)
- [Power Supplies](#)
- [Fans](#)
- [CPU](#)
- [Memory](#)
- [Temperature](#)
- [Switch > Overview > Hardware](#)
- [Actions](#)

Viewing the Overview > Hardware Tab

To navigate to the **Hardware** tab in the Switch dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels,** or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active switch.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
3. Click a switch listed under **Device Name**.
The dashboard context for the specific switch is displayed.
4. Under **Manage**, click **Overview > Hardware**.
The **Hardware** tab is displayed.
5. To exit the Switch dashboard, click the back arrow on the filter.
You can change the time range for the **Routing** tab by clicking the time range filter and selecting one of the available options: **3 hours, 1 day, 1 week, 1 month,** or **3 months**.

Hardware

The **Hardware** table displays the overall hardware summary:

- **ID**—Identity of the hardware.
- **Name**—Name of the device.
- **Power Supplies**
 - **Total**—Total number of power supplies.
 - **Up**—Number of power supplies in Up state.
 - **Down**—Number of power supplies in Down state.
- **Fans**
 - **Total**—Total number of fans.
 - **Up**—Number of fans in Up state.
 - **Down**—Number of fans in Down state.
- **Utilization**
 - **CPU**—Current CPU utilization percentage.
 - **Memory**—Current memory utilization percentage.
- **Temperature**
 - **Current**—Current temperature. This column is available only for AOS-Switches.
 - **Min**—Minimum temperature. This column is available only for AOS-Switches.
 - **Max**—Maximum temperature. This column is available only for AOS-Switches.
 - **Sensors**—Number of sensors present in the switch. The number inside the brackets show the number of sensors whose status is high. This column is available only for AOS-CX switches.

Figure 79 Hardware table details for AOS-Switch

HARDWARE											
NAME	POWER SUPPLIES			FANS			UTILIZATION		TEMPERATURE		
	TOTAL	UP	DOWN	TOTAL	UP	DOWN	CPU	MEMORY	CURRENT	MIN	MAX
HP-Switch...	2	1	0	6	5	0	0%	27%	24 °C	24 °C	25 °C

Figure 80 Hardware table details for AOS-CX switch

HARDWARE										
NAME	POWER SUPPLIES			FANS			UTILIZATION		TEMPERATURE	
	TOTAL	UP	DOWN	TOTAL	UP	DOWN	CPU	MEMORY	SENSORS	
6400-VSX-Primary	4	2	0	8	8	0	11%	10%	30 (0 HIGH)	

Power Supplies

The **Power Supplies** table displays the following details:

- **Name**—Name of the power supply.
- **Status**—Current status of the power supply.

Fans

The **Fans** table displays the following details:

- **Name** —Name of the fan.
- **Status**—Current status of the fan.

CPU

The **CPU** section displays the current CPU utilization percentage and trend chart for the duration specified in the time range filter. Hover your mouse over the trend chart to view the CPU utilization at a particular time.

Memory

The **Memory** section displays the current memory utilization percentage and trend chart for the duration specified in the time range filter. Hover your mouse over the trend chart to view the memory utilization at a particular time.

Temperature



This section is available only for AOS-Switches.

The **Temperature** section displays the current, minimum, and maximum temperature and trend chart for the duration specified in the time range filter. Hover over the trend chart to view the temperature at a particular time.

Figure 81 Temperature



Thermals



This section is available only for AOS-CX switches.

The **Thermals** table displays the following details of each of the sensors that are present in the AOS-CX switches:

- **Name**—Name of the component where the sensor is present.
- **Status**—Current status of the fan.
- **Current**—Current temperature of the component.
- **Min**—Minimum temperature of the component.
- **Max**—Maximum temperature of the component.

Expand each of the rows to display the fan status, location of the fan, current, minimum, and maximum temperatures, and a temperature trend chart. Hover over the trend chart to view the temperature at a particular time.

Figure 82 *Thermals*

THERMALS (30)					
NAME	IF	STATUS	CURRENT	MIN	MAX
1-Fabric-AS...		normal	39	31	68

FAN STATUS		LOCATION	
normal		--	

CURRENT	MIN	MAX
39	31	68

Tuesday, Aug 4, 02:20
• temperature: 39 °C

Actions

The **Actions** tab displays the various options available for remote administration of the switch. The following options are available:

- **Reboot**—Reboots the switch. See [Rebooting Switches](#).
- **Tech Support**—Allows the administrators to generate a tech support dump for troubleshooting the device. See [Troubleshooting Aruba Switches](#).
- **Console**—Opens the remote console for a CLI session through SSH. Ensure that you allow SSH over port 443. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See [Opening Remote Console for Switch](#).

For AOS-CX 8320 and 8325 switch series, you must enable SSH server on the default VRF. Add the `ssh server vrf default` code to the template.



If the Copy and Paste function from the keyboard shortcut keys (CTRL+C and CTRL+V) do not work in your web browser, use the Copy and Paste functions available under the menu options in the web browser.

Switch > Overview > Routing



The **Routing** tab is displayed only for AOS-Switches that run the firmware version 16.09 or later.

In the switch dashboard, the **Routing** tab displays the following sections:

- [Overview of Routing Information](#)
- [Routing](#)
- [Actions](#)

Viewing the Overview > Routing Tab

To navigate to the **Routing** tab in the Switch dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active switch.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
3. Click a switch listed under **Device Name**.
The dashboard context for the specific switch is displayed.
4. Under **Manage**, click **Overview > Routing**.
The **Routing** tab is displayed.
5. To exit the Switch dashboard, click the back arrow on the filter.
You can change the time range for the **Routing** tab by clicking the time range filter and selecting one of the available options: **3 hours, 1 day, 1 week, 1 month, or 3 months**.

Overview of Routing Information

- This section displays the following routing information:
- **Total**—Displays the total number of routes on the switch.
- **Static**—Displays the total number of static routes on the switch.
- **Connected**—Displays the total number of connected routes on the switch.

Routing

The **Routing** table displays the following details:

- **Destination**—Displays the network address of the destination route.
- **Gateway**—Displays the IP address of the gateway.
- **VLAN**—Displays the VLAN ID of the route destination.
- **Type**—Displays the following types of routes:
 - **Static**—The routes that are manually added to the routing table in the switch.
 - **Connected**—The routes that are directly connected to the interface.
- **Sub Type**—Displays the subtype of the route as Internal or External.

- **Metric**—Displays the measure used to calculate the best path to reach the destination. A value of 1 indicates the best path, 15 indicates the worst path, and 16 indicates that the destination is unreachable on the route.
- **Distance**—Displays the administrative distance of the route. The administrative distance helps routers determine the best route when there are multiple routes to the destination.



The routing information is displayed from the Aruba 3810 Switch Series and Aruba 5400R Switch Series in the network. The details displayed on the **Routing** tab are refreshed every five minutes.

Actions

The **Actions** tab displays the various options available for remote administration of the switch. The following options are available:

- **Reboot**—Reboots the switch. See [Rebooting Switches](#).
- **Tech Support**—Allows the administrators to generate a tech support dump for troubleshooting the device. See [Troubleshooting Aruba Switches](#).
- **Console**—Opens the remote console for a CLI session through SSH. Ensure that you allow SSH over port 443. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See [Opening Remote Console for Switch](#).



For AOS-CX 8320 and 8325 switch series, you must enable SSH server on the default VRF. Add the `ssh server vrf default` code to the template.

If the Copy and Paste function from the keyboard shortcut keys (CTRL+C and CTRL+V) do not work in your web browser, use the Copy and Paste functions available under the menu options in the web browser.

Switch > Overview > AI Insights

In the switch dashboard, the **AI Insights** tab displays information on switch performance issues such as PoE issues, port errors, port flaps, airtime utilization, and memory utilization.

Viewing Switches > AI Insights

To navigate to the **AI Insights** tab in the switch dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Group, Label, or Site**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active switch.
2. The dashboard context for the selected filter is displayed.
3. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
4. Click a switch listed under **Device Name**.
The dashboard context for the switch is displayed.
5. In the switch dashboard context, click the **AI Insights** tab.
The **Insights** page is displayed.
To exit the switch dashboard, click the back arrow on the filter.

You can change the time range for the **AI Insights** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.



AI Insights are displayed for the time range selected. Select the time range from the **Time Range Filter** (🔄) to filter reports.

AI Insights Categories

AI Insights are categorized in high, medium, and low priorities depending on the number of occurrences.

-  Red—High priority
-  Orange—Medium priority
-  Yellow—Low priority

AI Insights listed in the dashboard are sorted from high priority to low priority. The **AI Insights** dashboard displays a report of network events that could possibly affect the quality of the overall network performance. Each insight report provides specific details on the occurrences of these events for ease in debugging.

Switch > Clients > Clients

In the switch dashboard, the **Clients** tab displays details about the wired clients that are connected to the switch. This tab also displays a visual representation of the switch faceplate with port details.

The **Clients** tab displays the following details:

- [Overview of Connected Devices](#)
- [Faceplate](#)
- [Client Devices](#)
- [Actions](#)

Viewing the Clients > Clients Tab

To navigate to the **Clients** tab in the Switch dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active switch.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
3. Click a switch listed under **Device Name**.
The dashboard context for the specific switch is displayed.
4. Under **Manage**, click **Clients > Clients**.
The **Clients** tab is displayed.
5. To exit the Switch dashboard, click the back arrow on the filter.
You can change the time range for the **Clients** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

Overview of Connected Devices

This section displays the following details:

- **Total**—Total number of clients connected to the switch.
- **Non-Tunneled**—Number of clients, that are not tunneled connected, to the switch.
- **User Based Tunneled (UBT)**—Number of UBT clients connected to the switch.
- **Port Based Tunneled (PBT)**—Number of PBT clients connected to the switch.



To view the details about dynamic segmentation, a controller must be licensed in Aruba Central (on-premises) and connected to the switch.

Faceplate

If the switch is a standalone switch, the faceplate of the switch is displayed. For a switch stack, faceplate of all the switches part of the stack is displayed. From the faceplate, click on a port to view port-level information. On the switch faceplate, hover over a port to view the following details:

- Port Number
- Port Name
- Speed
- Type
- Tunneled

Client Devices

The **Client Devices** tab displays the following details:



The **VLAN Type**, **Primary VLAN ID**, and **Primary VLAN Name** columns are not displayed for AOS-CX switches.

- **Name**—Displays the name of the client device.
- **Status**—Displays the status of the client as Connected, Disconnected, Failed, Connecting, or Denylisted.
- **Port**—Displays the port number of the switch the client device is connected to. If the port is part of a LAG, the LAG name is displayed.
- **MAC Address**—Displays the MAC address of the client device.
- **IP Address**—Displays the IP address of the client device. The IP address is displayed only if the client is directly connected to the switch or if the IP tracker is enabled on the switch. IP tracker is not available for AOS-CX switches.
- **VLAN ID**—Displays the VLAN ID of the client device.
- **VLAN Name**—Displays the VLAN name of the client device.
- **VLAN Type**—Displays the following VLAN types of the client device:
 - Normal—The subnetwork which can group devices on separate physical LANs.
 - Primary—The standard VLAN that is partitioned to create a private VLAN.
 - Isolated—Secondary VLAN that carries unidirectional traffic upstream from the hosts toward the promiscuous ports.

- Community—Secondary VLAN that forwards traffic between ports which belong to the same community and to the promiscuous ports.
- **Primary VLAN ID**—Displays the primary VLAN ID of the client device.
- **Primary VLAN Name**—Displays the primary VLAN name of the client device.
- **Authentication**—Displays the authentication type of the client device.
- **Usage**—Displays the total data usage by the client device for the selected time period.
- **Tunneled**—Indicates whether the client is a tunneled client or not. **Yes** or **No**.
- **Segmentation**—Displays the type of dynamic segmentation configured for the client. Supported values are **UBT**, **PBT**, **Underlay**, **Overlay**, or **None**.
- **Switch Role**—Name of the role that the switch assigns to the client.
- **Gateway Role**—Name of the role that the gateway assigns to the client.
- **Gateway Name**—Name of the gateway.



The wired client will show up in the **Client Devices** table only if the client is connected to an Aruba 2540 Switch Series, Aruba 2920 Switch Series, Aruba 2930F Switch Series, Aruba 2930M Switch Series, Aruba 3810 Switch Series, Aruba 5400R Switch Series, or any of the AOS-CX Switch Series.

Actions

The **Actions** tab displays the various options available for remote administration of the switch. The following options are available:

- **Reboot**—Reboots the switch. See [Rebooting Switches](#).
- **Tech Support**—Allows the administrators to generate a tech support dump for troubleshooting the device. See [Troubleshooting Aruba Switches](#).
- **Console**—Opens the remote console for a CLI session through SSH. Ensure that you allow SSH over port 443. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See [Opening Remote Console for Switch](#).



For AOS-CX 8320 and 8325 switch series, you must enable SSH server on the default VRF. Add the `ssh server vrf default` code to the template.

If the Copy and Paste function from the keyboard shortcut keys (CTRL+C and CTRL+V) do not work in your web browser, use the Copy and Paste functions available under the menu options in the web browser.

Switch > Clients > Neighbours

In the switch dashboard, the **Neighbours** tab displays details about the devices neighboring the switch.

Viewing the Clients > Neighbours Tab

To navigate to the **Clients** tab in the Switch dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active switch.

The dashboard context for the selected filter is displayed.

2. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
3. Click a switch listed under **Device Name**.
The dashboard context for the specific switch is displayed.
4. Under **Manage**, click **Clients > Neighbours**.
The **Neighbours** tab is displayed.
5. To exit the Switch dashboard, click the back arrow on the filter.
You can change the time range for the **Neighbours** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, or **3 months**.

Neighbour Devices

The **Neighbours** tab displays the following details:

- **MAC Address**—Displays the MAC address of the neighboring device.
- **Hostname**—Displays the hostname of the neighboring device.
- **IP Address**—Displays the IP address of the neighboring device.
- **Description**—Displays the description of the neighboring device.
- **Local Port**—Displays the local port number of the neighboring device.
- **Remote Port**—Displays the remote port number of the neighboring device.
- **Capabilities**—Displays the capabilities of the neighboring device.
- **VLAN ID(s)**—Displays the VLAN IDs of the neighboring device.

Actions

The **Actions** tab displays the various options available for remote administration of the switch. The following options are available:

- **Reboot**—Reboots the switch. See [Rebooting Switches](#).
- **Tech Support**—Allows the administrators to generate a tech support dump for troubleshooting the device. See [Troubleshooting Aruba Switches](#).
- **Console**—Opens the remote console for a CLI session through SSH. Ensure that you allow SSH over port 443. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See [Opening Remote Console for Switch](#).

For AOS-CX 8320 and 8325 switch series, you must enable SSH server on the default VRF. Add the `ssh server vrf default` code to the template.

If the Copy and Paste function from the keyboard shortcut keys (CTRL+C and CTRL+V) do not work in your web browser, use the Copy and Paste functions available under the menu options in the web browser.



Switch > LAN > Ports

In the switch dashboard, the **Ports** tab displays details about ports and the LAGs configured in the switch.

The **Ports** tab displays the following details:

- [Port Status](#)
- [Faceplate](#)

- [Ports](#)
- [LAGS](#)
- [Viewing Port-Level Information](#)
- [Actions](#)

Viewing the LAN > Ports Tab

To navigate to the **Ports** tab in the Switch dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels,** or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active switch.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
3. Click a switch listed under **Device Name**.
The dashboard context for the specific switch is displayed.
4. Under **Manage**, click **LAN > Ports**.
The **Ports** tab is displayed.
5. To exit the Switch dashboard, click the back arrow on the filter.
You can change the time range for the **Ports** tab by clicking the time range filter and selecting one of the available options: **3 hours, 1 day, 1 week, 1 month,** or **3 months**.

Port Status

The **Port Status** section displays the total number of ports for the following:

- **Up**—Ports in up state
- **Down**—Ports in down state
- **Alert**—Alerts generated
- **Uplink**—Number of uplink ports

Faceplate

If the switch is a standalone switch, the faceplate of the switch is displayed. For a switch stack, faceplate of all the switches part of the stack is displayed. From the faceplate, click on the port to drill down and view port-level information. On the switch faceplate, hover over a port to view the following details:

- Port
- Name
- Type
- Speed
- LAG
- Reason (Applicable only to AOS-CX switches)

Ports

The **Ports** table displays the following details:

- **Port**—Port number. Use the column filter to search for a particular port and use the sort option to sort the ports in ascending or descending order.
- **Name**—Name of the switch.
- **Status**—Status of the switch. Use the column filter to filter by status.
- **Type**—Type of switch port. Use the column filter to filter by type.
- **MTU (Bytes)**—MTU size of the switch.
- **Speed (Mbps)**—Port speed of the switch.
- **LAG**—If the port is part of a trunk group or LAG, the name of the trunk group or LAG is displayed.
- **Admin**—Admin status of the switch.
- **MAC Address**—MAC address of the switch.
- **VLAN**—VLAN ID of the port.
- **VLAN Mode**—VLAN mode of the port. Supported values are **Access** or **Trunk**.
- **Native VLAN**—Native VLAN ID of the port.
- **Reason**—Indicates the reason when the switch is down. This field is displayed only for AOS-CX switches.

LAGS

The LAGs table displays the list of LAGs along with the following details:

- **Name**—Name of the LAG. Use the sort option to sort the LAGs in ascending or descending order.
- **Up Ports**—Number of uplink ports in the LAG and their port numbers.
- **Down Ports**—Number of downlink ports in the LAG and their port numbers.
- **VSX**—Indicates whether VSX is enabled or disabled in the LAG. This column is displayed only for AOS-CX switches.

Viewing Port-Level Information

Use one of the following options to navigate to the port and view port-level information:

- In the switch faceplate, click on the port number.
- In the Ports table, click the port number.

The port-level information page consists of the following sections:

- **Status**—The **Status** section displays the following details:
 - Operational status
 - Admin status
 - Type of port
 - Description
 - MAC Address
 - Name
 - Untagged VLAN
 - Tagged VLAN
 - Trunk group

- Usage In
- Usage Out
- **Port Usage**—The **Port Usage** section provides a graphical representation of data received and transmitted by the port. Each line in the graph is a sum of the received and sent traffic for a given uplink port. Hover over the graph to view data for a particular time of the day.
- **Frame Counters**—The **Frame Counters** section provides a graphical representation of the interface frame counters. From the drop-down, select one of the following options:
 - **Unicast**
 - **Broadcast**
 - **Multicast**
 - **Discards**
 - **Error**

Actions

The **Actions** tab displays the various options available for remote administration of the switch. The following options are available:

- **Reboot**—Reboots the switch. See [Rebooting Switches](#).
- **Tech Support**—Allows the administrators to generate a tech support dump for troubleshooting the device. See [Troubleshooting Aruba Switches](#).
- **Console**—Opens the remote console for a CLI session through SSH. Ensure that you allow SSH over port 443. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See [Opening Remote Console for Switch](#).

For AOS-CX 8320 and 8325 switch series, you must enable SSH server on the default VRF. Add the `ssh server vrf default` code to the template.



If the Copy and Paste function from the keyboard shortcut keys (CTRL+C and CTRL+V) do not work in your web browser, use the Copy and Paste functions available under the menu options in the web browser.

Switch > LAN > PoE

In the switch dashboard, the **PoE** tab displays details, such as, PoE status summary, PoE ports, and PoE consumption.

The **PoE** tab displays the following details:

- [PoE Status](#)
- [Faceplate](#)
- [Ports PoE](#)
- [PoE Consumption](#)
- [Viewing PoE Port-Level Information](#)
- [Actions](#)

Viewing the LAN > PoE Tab

To navigate to the **PoE** tab in the Switch dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels,** or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active switch.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
3. Click a switch listed under **Device Name**.
The dashboard context for the specific switch is displayed.
4. Under **Manage**, click **LAN > PoE**.
The **PoE** tab is displayed.
5. To exit the Switch dashboard, click the back arrow on the filter.
You can change the time range for the **PoE** tab by clicking the time range filter and selecting one of the available options: **3 hours, 1 day, 1 week, 1 month,** or **3 months**.



The **PoE** tab is displayed only if the AOS-Switch or the AOS-CX switch supports PoE.

The **PoE** tab displays monitoring data only if the AOS-Switch firmware version is 16.08.0001 or later.

PoE Status

The **PoE Status** section displays the following details:

- **Available**—Power available for consumption for the switch or stack.
- **Used**—Power used by various devices.
- **Remaining**—Power remaining to be utilized in the stack or device.
- **PoE Denied Ports**—Number of ports for which power is denied.
- **Alerts**—Number of alerts generated.

Faceplate

If the switch is a standalone switch, the faceplate of the switch is displayed. For a switch stack, faceplate of all the switches part of the stack is displayed. From the faceplate, click on the port to drill down and view port-level information. On the switch faceplate, hover over a PoE port to view the following details:

- Port
- Name
- Type
- Class
- Priority

From the **Context** drop-down list, select the context:

- **POE-STATUS**—Displays the state of each port. The state can be: Uplink, Drawing, Enabled, Disabled, or Alert.

- **POE-CLASS**—Power class of the PoE port. The class can be: Class0, Class1, Class2, Class3, Class4, or Disabled.
- **POE PRIORITY**—PoE priority configured on the port. The priority can be: Critical, High, or Low.

Ports PoE

The **Ports PoE** table displays the following details:

- **Port**—Port number.
- **Name**—Name of the port.
- **PoE**—PoE state: Enabled or Disabled.
- **Priority**—PoE priority: Critical, High, or Low.
- **Status**—Current power status of the PoE port: Searching, Delivering, Disabled, or Fault.
- **Pre-STD Detect**—Displays whether PoE for pre-802.3af-standard powered devices is enabled on the switch: On or Off.
- **Alloc Actual**—Power actually being used on the port.
- **Alloc Configured**—The maximum amount of power allocated for the port.
- **PLC Class**—Power class of the PoE port.
- **PLC Type**—Physical layer classification type.

PoE Consumption

The **PoE Consumption** section displays a trend chart for the PoE power drawn from the Switch in watts. Hover your mouse over the trend chart to view the PoE power drawn at a particular time. For a stack, select the switch from the drop-down list to view the PoE consumption for the specific device.

Viewing PoE Port-Level Information

Use one of the following options to navigate to the PoE port and view port-level information:

- In the switch faceplate, click on the port number.
- In the **Ports PoE** table, click the port number.

The port-level information page consists of the following tabs:

- [Summary](#)
- [Slot Info & PoE Configuration](#)
- [LLDP Information](#)

Summary

The **Summary** tab displays the following sections:

- **Summary**—Displays the following details:
 - **PSE Reserved Power**—Power reserved for the port in the Power Sourcing Equipment (PSE).
 - **PSE Voltage**—Total voltage, in volts (V), currently being delivered to the powered device connected to the port
 - **PD Power Draw**—Power drawn by the powered device.
 - **PD Amperage Draw**—Amperage drawn by the powered device.
 - **Over Current Count**—Number of times a powered device connected to the port attempted to draw more power than was allocated to the port.

- **MPS Absent Count**—Number of times the powered device has no longer requested power from the port MPS is Maintenance Power Signature.
- **Power Denied Count**—Number of power requests from the port that were denied because sufficient power was unavailable.
- **Short Count**—Number of times the switch provided insufficient current to the powered device connected to the port.
- **PoE Consumption**—Displays the trend chart for PoE consumption and power available for the duration specified in the time range filter.

Slot Info & PoE Configuration

The **Slot Info & PoE Configuration** tab displays the following sections:

- **PoE Slot Information**—Displays the following details:
 - **Slot**—Slot where the port is located.
 - **Operation Status**—Displays PoE power is available for the slot: On, Off, or Faulty.
 - **Maximum Power**—Maximum PoE wattage available to provision active PoE ports in the slot.
 - **Power In Use**—PoE power currently being used by the slot.
 - **Usage Threshold**—Configured percentage of available PoE power provisioning the switch must exceed to generate a usage notice.
- **PoE Configuration**—Displays the following details:
 - **PoE Power**—Displays whether PoE power is enabled on the port.
 - **Pre STD Detect**—Displays whether PoE for pre-802.3af-standard powered devices is enabled on the switch: On or Off. This field is not displayed for AOS-CX switches.
 - **PoE Port Status**—Current power status of the PoE port: Searching, Delivering, Disabled, or Fault.
 - **Power Priority**—Power priority configured on ports enabled for PoE: Low, High, or Critical.
 - **Allocate by Configuration**—Maximum amount of power allocated for the port.
 - **Allocate by Actual**—Power actually being used on the port.
 - **PLC Class Type**—Physical layer classification type.
 - **DLC Class Type**—Data link layer classification type.
 - **Configured Type**—If configured, shows the user-specified identifier for the port. If not configured, this field is empty.
 - **PoE Value configuration**—PoE power value configured for the port. This field is not displayed for AOS-CX switches.

LLDP Information

The **LLDP Information** tab displays the following details:

- **UPSE Allocated Power**—Power allocated for the port in the PSE.
- **PD Requested Power**—Power requested by the powered device.
- **PD TLV Sent Type**—TLV that is actually sent from the powered device.
- **PSE TLV Configured**—TLV that is configured for the switch port to send to the powered device.
- **PSE TLV Sent Type**—TLV that is actually sent from the PSE.
- **MED LLDP Detect**—Status of the PoE LLDP detection. This field is not displayed for AOS-CX switches.

Actions

The **Actions** tab displays the various options available for remote administration of the switch. The following options are available:

- **Reboot**—Reboots the switch. See [Rebooting Switches](#).
- **Tech Support**—Allows the administrators to generate a tech support dump for troubleshooting the device. See [Troubleshooting Aruba Switches](#).
- **Console**—Opens the remote console for a CLI session through SSH. Ensure that you allow SSH over port 443. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See [Opening Remote Console for Switch](#).

For AOS-CX 8320 and 8325 switch series, you must enable SSH server on the default VRF. Add the `ssh server vrf default` code to the template.

If the Copy and Paste function from the keyboard shortcut keys (CTRL+C and CTRL+V) do not work in your web browser, use the Copy and Paste functions available under the menu options in the web browser.



Switch > LAN > VLAN

In the switch dashboard, the **VLAN** tab displays VLAN information configured on the switch and details about tagged and untagged ports.

The **VLAN** tab displays the following details:

- [VLANs](#)
- [Faceplate](#)
- [Actions](#)

Viewing the LAN > VLAN Tab

To navigate to the **VLAN** tab in the Switch dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active switch.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
3. Click a switch listed under **Device Name**.
The dashboard context for the specific switch is displayed.
4. Under **Manage**, click **LAN > VLAN**.
The **VLAN** tab is displayed.
5. To exit the Switch dashboard, click the back arrow on the filter.
You can change the time range for the **VLAN** tab by clicking the time range filter and selecting one of the available options: **3 hours, 1 day, 1 week, 1 month, or 3 months**.

VLANs

The **VLANs** table displays the following details:



The **Type**, **Primary VLAN**, **Promiscuous**, **ISL**, and **Jumbo** columns are not displayed for AOS-CX switches.

- **Name**—Displays the name of the VLAN. Click the sort icon to sort the VLAN names in the column.
- **ID**—Displays the VLAN ID associated with the VLAN.
- **Status**—Displays the status of the VLAN as Up or Down.
- **Type**—Displays the following types of VLANs:
 - **Regular VLAN**—A regular VLAN is a single broadcast domain.
 - **Private-Primary**—The regular VLAN which partitions one broadcast domain into multiple smaller broadcast sub-domains.
 - **Private-isolated**—Secondary VLAN that carries unidirectional traffic upstream from the hosts toward the promiscuous ports.
 - **Private-Community**—Secondary VLAN that forwards traffic between ports which belong to the same community and to the promiscuous ports.
- **Primary VLAN**—Displays the primary VLAN details.
- **Promiscuous**—Displays the promiscuous port value. A promiscuous port is a switch port that is connected to an uplink router, firewall, or other common gateway device, and can communicate with all ports within a private VLAN, including the ports in the isolated and community VLANs. By default, every primary VLAN port acts as a promiscuous port.
- **ISL**—Displays the Inter-switch Link (ISL) port value (range). ISL port is also called PVLAN member port. ISL port is required in multi-switch PVLAN configurations to span the switches. The ISL port will automatically become a member of all VLANs within the PVLAN and it carries traffic from the primary VLAN and all secondary VLANs.
- **Tagged Ports**—Displays the ports that have marked the VLAN as tagged.
- **Untagged Ports**—Displays the ports that have marked the VLAN as untagged.
- **IP address**—Displays the IP address of the VLAN.
- **Voice**—Displays whether the Voice is enabled or disabled for the VLAN.
- **IGMP**—Displays whether the IGMP is enabled or disabled for the VLAN.
- **Jumbo**—Displays whether the Jumbo packets are enabled or disabled for the VLAN.

Faceplate

From the **VLANs** table, select a VLAN to view the tagged and untagged ports, promiscuous port, ISL port, and the VLAN types in the faceplate.

Figure 83 VLANs tab details for AOS-Switch

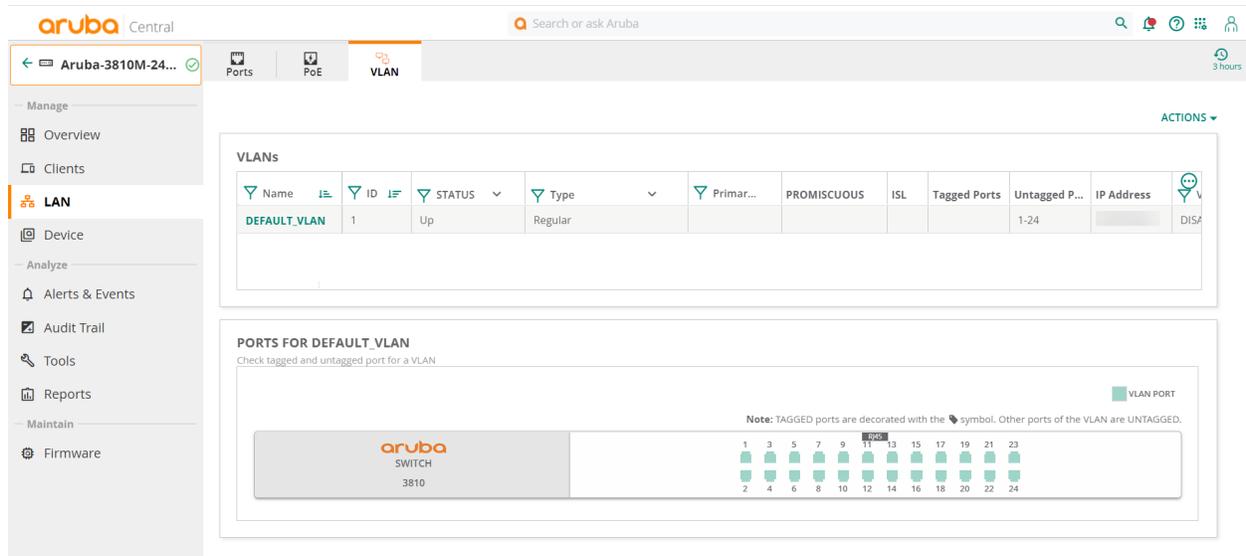
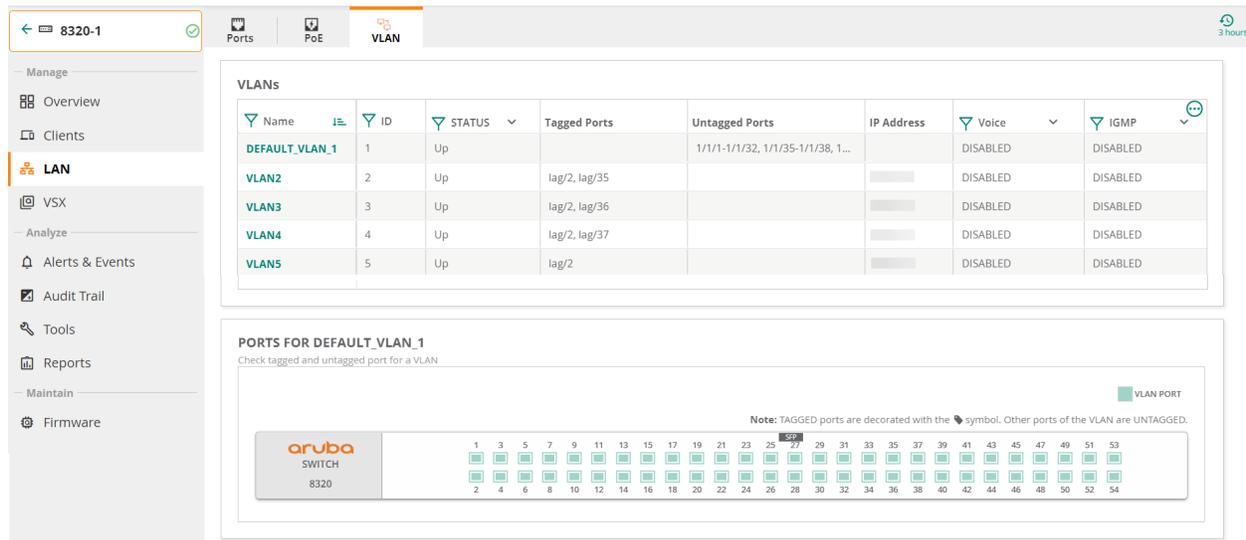


Figure 84 VLANs tab details for AOS-CX switch



Actions

The **Actions** tab displays the various options available for remote administration of the switch. The following options are available:

- **Reboot**—Reboots the switch. See [Rebooting Switches](#).
- **Tech Support**—Allows the administrators to generate a tech support dump for troubleshooting the device. See [Troubleshooting Aruba Switches](#).
- **Console**—Opens the remote console for a CLI session through SSH. Ensure that you allow SSH over port 443. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See [Opening Remote Console for Switch](#).



For AOS-CX 8320 and 8325 switch series, you must enable SSH server on the default VRF. Add the `ssh server vrf default` code to the template.

If the Copy and Paste function from the keyboard shortcut keys (CTRL+C and CTRL+V) do not work in your web browser, use the Copy and Paste functions available under the menu options in the web browser.

Switch > VSX

Aruba Virtual Switching Extension (VSX) is virtualization technology for aggregation and core AOS-CX switches. The VSX solution lets the switches present as one virtualized switch in critical areas.

VSX is supported in the AOS-CX 6400, AOS-CX 8320, and AOS-CX 8325 Switch Series.

Aruba Central (on-premises) provides support for VSX by displaying information about the configurations of the switches and the status of the inter-switch link (ISL) between the switches.

Viewing the VSX Page

To navigate to the VSX page in the Switch dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Group, Label, or Site**. Ensure that the filter selection contains at least one AOS-CX switch. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
3. Click an AOS-CX switch under **Device Name**.
The dashboard context for the switch is displayed.
4. Under **Manage**, click **VSX**.
The **VSX** page displays the following details:
 - [VSX Summary](#)
 - [Info](#)
 - [Actions](#)
5. To exit the switch dashboard, click the back arrow on the filter.

VSX Summary

Displays state information of the switch, connections to the peer switch, and the role of the switch in the VSX configuration.

Table 171: VSX Summary Details

Field	Description
ISL State	State of the ISL connection with the peer AOS-CX switch. Following are the supported values: <ul style="list-style-type: none">■ WAITING_FOR_PEER—Waiting for connectivity to the peer.■ PEER_ESTABLISHED—Steady state. VSX LAGs are up when the device is in this state.■ SPLIT_SYSTEM_PRIMARY—Lost ISL connectivity to the peer and the device is operating as primary.■ SPLIT_SYSTEM_SECONDARY—Lost ISL connectivity to the peer and the device is operating

Field	Description
	<p>as secondary.</p> <ul style="list-style-type: none"> ■ SYNC_PRIMARY—ISL connectivity to the peer restored and the device is syncing states to the peer. ■ SYNC_SECONDARY—ISL connectivity to the peer restored and the device is learning states from the peer. VSX LAGs are down when the device is in this state. ■ SYNC_SECONDARY_LINKUP_DELAY—Device has learned its states from the peer and monitoring for hardware is to be programmed. VSX LAGs are down when the device is in this state.
ISL Mgmt State	<p>Management state of the ISL. Following are the supported values:</p> <ul style="list-style-type: none"> ■ OPERATIONAL—ISL management is operational. ■ INTER_SWITCH_LINK_MGMT_INIT—ISL management is in initialization state. ■ CONFLICTING_OR_MISSING_DEVICE_ROLES—Either the role is missing on one of the VSX peers or the same role is configured on both VSX peers. ■ SW_IMAGE_VERSION_MISMATCH_ERROR—Software version on the primary device does not match with the software version on the secondary device. ■ INTER_SWITCH_LINK_DOWN—ISL is down. ■ INTERNAL_ERROR—ISL management has internal errors.
Config Sync Status	<p>Status of the configuration synchronization between the VSX switches. Following are the supported values:</p> <ul style="list-style-type: none"> ■ IN-SYNC—Configuration synchronization is operational and the VSX switches are in sync. ■ DISABLED—Configuration synchronization is disabled. ■ SW_IMAGE_VERSION_MISMATCH_ERROR—Software image version on the primary device does not match with the software image version on the secondary device. ■ CONFLICTING_OR_MISSING_DEVICE_ROLES—Either the role is missing on one of the VSX peers or the same role is configured on both VSX peers. ■ PEER_DB_CONNECTION_ERROR—Error in connecting to peer database. It involves errors due to ISL or ISL management. ■ CONFIGURATION_SYNC_CONFLICT—Configuration synchronization is operational but has conflicts synchronizing the configuration. Conflicts can occur if the configuration on the primary device is marked for sync, but the same configuration on the secondary device is not marked for sync. ■ CONFIGURATION_SYNC_MISSING_REFERENCE—Configuration synchronization is operational but has missing references in synchronizing the configuration.
NAE	Status of the NAE connection between the VSX switches.
HTTPS Server	Status of the HTTPS server connection between the VSX switches.
Last Synced	<p>Timestamp of when the configuration was synced between the peer switch. Last synced data is displayed in the Switch > VSX page only when VSX synchronization is enabled for the AOS-CX switch. However, enabling VSX synchronization using template configuration in Aruba Central (on-premises) is not recommended. By enabling VSX synchronization, the peer switch may get into an unknown configuration state.</p>
Role	Role of the AOS-CX switch in the VSX configuration. Supported values are Primary and Secondary

Info

Displays system and configuration information of the switch and its peer. The following details are displayed:

■ System

- **Local MAC**—MAC address of the selected switch.
- **Peer MAC**—MAC address of the peer switch.
- **Peer Hostname**—Hostname of the peer switch.
- **Peer IP**—IPv4 address of the peer switch.

■ Configuration

- **Config Sync**—Indicates whether the configuration synchronization between the peers are enabled or disabled.
- **ISL Port**—Inter-switch Link (ISL) port number of the selected AOS-CX switch. If the ISL is a LAG, then this field displays the LAG name.
- **Peer ISL Port**—ISL port number of the peer switch. If the ISL is a LAG, then this field displays the LAG name.
- **MC LAGs**—List of MC LAG names present in the switches.

Actions

The **Actions** tab displays the various options available for remote administration of the switch. The following options are available:

- **Reboot**—Reboots the switch. See [Rebooting Switches](#).
- **Tech Support**—Allows the administrators to generate a tech support dump for troubleshooting the device. See [Troubleshooting Aruba Switches](#).
- **Console**—Opens the remote console for a CLI session through SSH. Ensure that you allow SSH over port 443. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See [Opening Remote Console for Switch](#).

For AOS-CX 8320 and 8325 switch series, you must enable SSH server on the default VRF. Add the `ssh server vrf default` code to the template.

If the Copy and Paste function from the keyboard shortcut keys (CTRL+C and CTRL+V) do not work in your web browser, use the Copy and Paste functions available under the menu options in the web browser.



NOTE

Rebooting Switches

You can reboot a switch using the Aruba Central (on-premises) UI.

To reboot a switch, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. Ensure that the filter selection contains at least one switch. For all devices, set the filter to **Global**.

The dashboard context for the selected filter is displayed.

2. Under **Manage**, click **Devices > Switches**.

A list of switches is displayed in the **List** view.

3. Click **Online** to display a table with the list of online switches.
4. In the Switches table, click the switch to reboot.
The Switches Details page corresponding to the switch is displayed.
5. In the **Actions** drop-down, click **Reboot**.
A **Reboot Switch** dialog box is displayed.
6. Click **Continue** to reboot the switch.
All clients connected to this switch are disconnected and the switch reboots.



The Switches Details page takes less than a minute to update the interface status after the switch is rebooted and reconnected to Aruba Central (on-premises).

Opening Remote Console for Switch

In the Aruba Central (on-premises) UI, you can open the remote console for a CLI session through SSH for a switch. Ensure that you allow SSH over port 443.

For AOS-CX 8320 and 8325 switch series, you must enable SSH server on either the default VRF or the management VRF depending on the type of VRF that the switch uses to connect to Aruba Central (on-premises). You must add one of the following commands in the template:

- If the switch is connecting to Aruba Central (on-premises) using inline default VRF, add `ssh server vrf default` to the template.
- If the switch is connecting to Aruba Central (on-premises) using OOBM management VRF, add `ssh server vrf mgmt` to the template.



You can only troubleshoot switches using the Console option in Aruba Central (on-premises). You cannot configure the switches.

To open the remote console for a switch, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. Ensure that the filter selection contains at least one switch. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
3. Click **Online** to display a table with the list of online switches.
4. In the Switches table, click the switch for which you want to open the remote console.
The Switch Details page corresponding to the switch is displayed.
5. In the **Actions** drop-down, click **Open Remote Console**.
A CLI session dialog box is displayed. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device.

Troubleshooting Aruba Switches

You can troubleshoot a switch using the Aruba Central (on-premises) UI.

To troubleshoot a switch, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. Ensure that the filter selection contains at least one switch. For all devices, set the filter to **Global**.

The dashboard context for the selected filter is displayed.

2. Under **Manage**, click **Devices > Switches**.

A list of switches is displayed in the **List** view.

3. In the Switches table, click the switch to troubleshoot.

The Switch Details page corresponding to the switch is displayed.

4. In the **Actions** drop-down, click **Tech Support**.

The **Commands** page is displayed.

5. Select any command category in the **Categories** pane and the **Commands** pane displays the associated commands.



AOS-CX switches support only the `show tech` and `show running-config` commands.

6. Click **Add >** to add the selected commands to the **Selected Commands** pane.
7. If you have selected a command marked with either '*' or '+', enter the filtration parameters as displayed in the **Additional Filters** dialog box. For more information on filtering commands, see [Filtering Commands](#).
8. (Optional) Select command(s) and click **< Remove** to remove selected command(s) or click **< Remove All** to clear the **Selected Commands** pane.
9. (Optional) To set a frequency for automatically executing the troubleshooting commands:
 - a. Click the **Repeat** check box.
 - b. Specify an interval for executing the troubleshooting commands. You can also specify how frequently the commands must be executed during a given interval.
 - c. Click **Reset** to modify the values in all the fields, and **Cancel All** for canceling all the repeats. Click the stop icon to stop a particular repeat.
10. Click **Run**. The output is displayed in the **Device Output** section.

For information about viewing and downloading the output, see [Viewing the Device Output](#).

Troubleshooting AOS-CX Switch Onboarding Issues

Though an AOS-CX switch is displayed as online, there might be instances where the complete switch details are not displayed. To troubleshoot such issues, you can see the audit trail page to check the status of the switch.

To see the audit trail for a switch, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. Ensure that the filter selection contains at least one switch. For all devices, set the filter to **Global**.

The dashboard context for the selected filter is displayed.

2. Under **Manage**, click **Devices > Switches**.

A list of switches is displayed.

3. In the **Switches** table, click the switch you wish to troubleshoot.

The dashboard context for the switch is displayed.

4. Under **Analyze**, click **Audit Trail**.

The **Audit Trail** page is displayed.

If a switch is onboarded successfully, the audit trail log displays the following messages:

- a. **Device : <Device Serial Number> Onboarded**
- b. **Applying template <Template Configuration Name> to device**
- c. **Login Successful reading running configuration**
- d. **Config push successful**

If applying template configuration to the AOS-CX switch fails, the **Template/Variable Configuration Error** error message is displayed:

If any of the messages listed in step 4b, 4c, 4d, or **Template/Variable Configuration Error** is not displayed in the audit trail logs, one of the following might be the reason:



- User has not created a template group with template configuration for the AOS-CX switch.
- User has created a template group with template configuration but has not moved the AOS-CX switch to the template group.

The following image displays the audit trail log of a switch that is successfully onboarded.

Figure 85 Example audit trail log for successfully onboarded AOS-CX switch

OCURRED ON	IP ADDRESS	USERNAME	TARGET	CATEGORY	DESCRIPTION
Jul 14, 2020, 13:00	--	System	SG98KN706N	Configuration	Applying template tg_shassis to device
Jul 14, 2020, 13:00	--	System	SG98KN706N	Configuration	Login Successful reading running configuration
Jul 14, 2020, 13:00	--	System	SG98KN706N	Configuration	Applying template tg_shassis to device
Jul 14, 2020, 12:47	--	System	SG98KN706N	Configuration	Config push successful
Jul 14, 2020, 12:47	--	System	SG98KN706N	Configuration	Login Successful reading running configuration
Jul 14, 2020, 12:47	--	System	SG98KN706N	Configuration	Applying template tg_shassis to device
Jul 14, 2020, 12:45	10.28.10.86	navesh.garg@hpe.com	SG98KN706N	Device Management	Enabled services: Basic NMS
Jul 14, 2020, 12:42	10.28.10.86	navesh.garg@hpe.com	SG98KN706N	Device Management	Disabled services: Basic NMS
Jul 14, 2020, 12:41	--	System	SG98KN706N	Configuration	Config push successful
Jul 14, 2020, 12:41	--	System	SG98KN706N	Configuration	Login Successful reading running configuration
Jul 14, 2020, 12:41	--	System	SG98KN706N	Configuration	Applying template tg_shassis to device
Jul 14, 2020, 12:32	--	System	SG98KN706N	Configuration	Config push successful
Jul 14, 2020, 12:32	--	System	SG98KN706N	Configuration	Login Successful reading running configuration
Jul 14, 2020, 12:32	--	System	SG98KN706N	Configuration	Applying template tg_shassis to device
Jul 14, 2020, 12:27	10.28.10.86	navesh.garg@hpe.com	SG98KN706N	Device Management	Enabled services: Basic NMS
Jul 14, 2020, 12:22	10.28.10.86	navesh.garg@hpe.com	SG98KN706N	Device Management	Disabled services: Basic NMS
Jul 14, 2020, 12:19	--	System	SG98KN706N	Configuration	Config push successful
Jul 14, 2020, 12:19	--	System	SG98KN706N	Configuration	Login Successful reading running configuration
Jul 14, 2020, 12:19	10.28.10.86	navesh.garg@hpe.com	SG98KN706N	Configuration	Applying template tg_shassis to device
Jul 14, 2020, 12:18	16.93.60.30	System	SG98KN706N	Device Management	Device : SG98KN706N Onboarded
Jul 14, 2020, 12:18	--	System	SG98KN706N	Configuration	Assigning device to tg_chassis group
Jul 14, 2020, 12:18	--	System	SG98KN706N	Configuration	Template/Variable Configuration Error
Jul 14, 2020, 12:15	10.28.10.86	navesh.garg@hpe.com	SG98KN706N	Device Management	Assigned Preprovision group tg_chassis for device
Jul 14, 2020, 11:55	--	System	SG98KN706N	Configuration	Assigning device to UNPROVISIONED group
Jul 14, 2020, 11:55	16.93.60.30	System	SG98KN706N	Device Management	Device : SG98KN706N Onboarded
Jul 14, 2020, 11:45	10.20.15.215	navesh.garg@hpe.com	SG98KN706N	Device Management	Enabled services: Basic NMS

Controller > Overview > Summary

The **Summary** tab under **Manage > Overview** in the controller dashboard displays the following two sections:

- **Device Info**
- **Health Status**

Viewing the Overview > Summary Tab

To navigate to the **Summary** tab in the controller dashboard, complete the following steps:

- In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. Ensure that the filter selection contains at least one controller. For all devices, set the filter to **Global**. The dashboard context for the selected filter is displayed.
- Under **Manage > Devices**, click the **Controllers** tab. A list of controllers is displayed.
- Click a controller or cluster under **Device Name**. The dashboard context for the specific controller or cluster is displayed.
- Under **Manage**, click **Overview > Summary**. To exit the controller dashboard, click the back arrow on the filter. You can change the time range for the **Summary** tab by clicking the time range filter and selecting one of the available options: **3 hours, 1 day, 1 week, 1 month, and 3 months**.

Device Info

The **Device Info** section displays the following details:

Figure 86 *Device Info*



CONTROLLER DETAILS					
NAME	SERIAL NUMBER	MODEL	MAC ADDRESS	SYSTEM IP ADDRESS	FIRMWARE VERSION
CHN-8x-Functional-MM1	MM7150F04	ArubaMM-VA	00:0c:29:15:0f:0e	10.27.108.195	8.9.0.0
GROUP NAME	LABELS	SITE	ROLE	CONDUCTOR	LAST REBOOT REASON
unprovisioned	--	--	Conductor	--	--
POE (DRAW/MAK)	REDUNDANCY PEER	NTP SERVER	CLUSTER NAME	4G/LTE MODEM STATUS	4G/LTE MODEM TYPE
--	CHN-8x-Functional-MM2	--	--	--	--
LOCATION	CONTACT				
controller chennai lab	mjeyakumar@arubanetworks.com				

- **Name**—The name of the controller.
- **Serial Number**—Serial number of the controller.
- **Model**—The hardware model of the controller.
- **MAC Address**—The MAC address of the controller.
- **System IP address**—The IP address of the controller.
- **Firmware Version**—The firmware version running on the controller. If a new version of the firmware is available, this information is also displayed. Clicking on the new firmware version redirects you to the Maintain > Firmware > controller page in the controller dashboard, where you can select the controller to upgrade it.
- **Group Name**—The name of the group, if the controller is configured as part of a group. Click the group name to go to the Overview > Summary page for that group.
- **Labels**—The name of the label, if the controller is configured as part of a single or multiple labels.
- **Site**—The name of the site, if the controller is configured as part of a site. Hover over the *i* icon to display the complete address of the site. Click the site name to go to the Overview > Site Health page for that site.
- **Role**—The role of the controller; for example, conductor or local.
- **Conductor**—The name of the conductor controller.

- **Last Reboot Reason**—The reason for the last reboot.
- **POE (DRAW/MAX)**—The amount of power that the devices connected to the controller consume and the maximum PoE power capacity. For example, if the value displayed is 6/120, the devices draw 6 watts and the maximum PoE power allocated is 120 watts.
- **Redundancy Peer**—Displays the redundant controller if it is configured.
- **NTP Server**—The name of the NTP server configured and its synchronization status.
- **Cluster Name**—The name of the cluster controller.
- **4G/LTE Modem Status**—Displays the modem connectivity status. The status shows only 'Connected' when the modem type is not internal.
- **4G/LTE Modem Type**—Displays the LTE connection type.
- **Location**—The currently configured physical location of the controller. Location details are displayed only for controllers running on firmware version ArubaOS 8.9.0.0 or later.
- **Contact**—The currently configured contact information of the controller. For example, E-mail ID or contact number. Contact details are displayed only for controllers running on firmware version ArubaOS 8.9.0.0 or later.

Health Status

The **Health Status** section displays the health of the controller in terms of CPU, Memory and device connectivity to Aruba Central (on-premises).

The health status is plotted using health indicators such as Good, Fair, Poor and Offline. You can hover over the chart to see the health status for a particular time frame.

Figure 87 Health Status

HEALTH STATUS



Viewing the Controllers Tab

To view the Controller dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Click **Devices > Controllers**.

Controllers Dashboard

The **Controllers** dashboard page displays a complete list of offline or online controllers provisioned in Aruba Central. You can also use the following filtering options to view a specific set of controllers.

- **All**—Displays a complete list of controllers. For more information, see [Monitoring Controllers in List View](#).
- **Cluster**—Displays controller clusters deployed in Aruba Central. A controller cluster includes multiple controllers working together as a single managed entity. Controller clusters enable seamless roaming of clients between AP and ensure service continuity in the event of a failover. Controller clustering is supported only on devices running ArubaOS 8.x or later software versions. To view the cluster components, expand the cluster in the **Cluster Name** column. For more information, see [Monitoring Clusters in List View](#).
- **Mobility Conductor**—Displays a list of controllers that are functioning as Mobility Conductors. The Aruba Mobility Conductor is an advanced controller deployed as a virtual machine (VM) or installed on an x86-based hardware appliance. A single Mobility Conductor or a cluster of Mobility Conductors oversees co-located controllers. It also displays the details about the APs associated with each controller. For more information, see [Monitoring Mobility Conductors in List View](#).

Controller > LAN > Summary

The **Summary** tab under **Manage > LAN** page in the controller dashboard displays the following sections:

- **Port Status**
- **LAN Interfaces Summary**
- **VLAN Interfaces Summary**

Viewing the LAN > Summary Tab

To navigate to the **LAN > Summary** tab in the controller dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. Ensure that the filter selection contains at least one controller. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
2. Under **Manage > Devices**, click the **Controller** tab.
A list of controllers is displayed.
3. Click a controller or cluster under **Device Name**.
The dashboard context for the specific controller is displayed.
4. Under **Manage**, click **LAN > Summary**.
To exit the controller dashboard, click the back arrow on the filter.
You can change the time range for the **Summary** tab by clicking the time range filter and selecting one of the available options: **3 hours, 1 day, 1 week, 1 month, and 3 months**.

Port Status

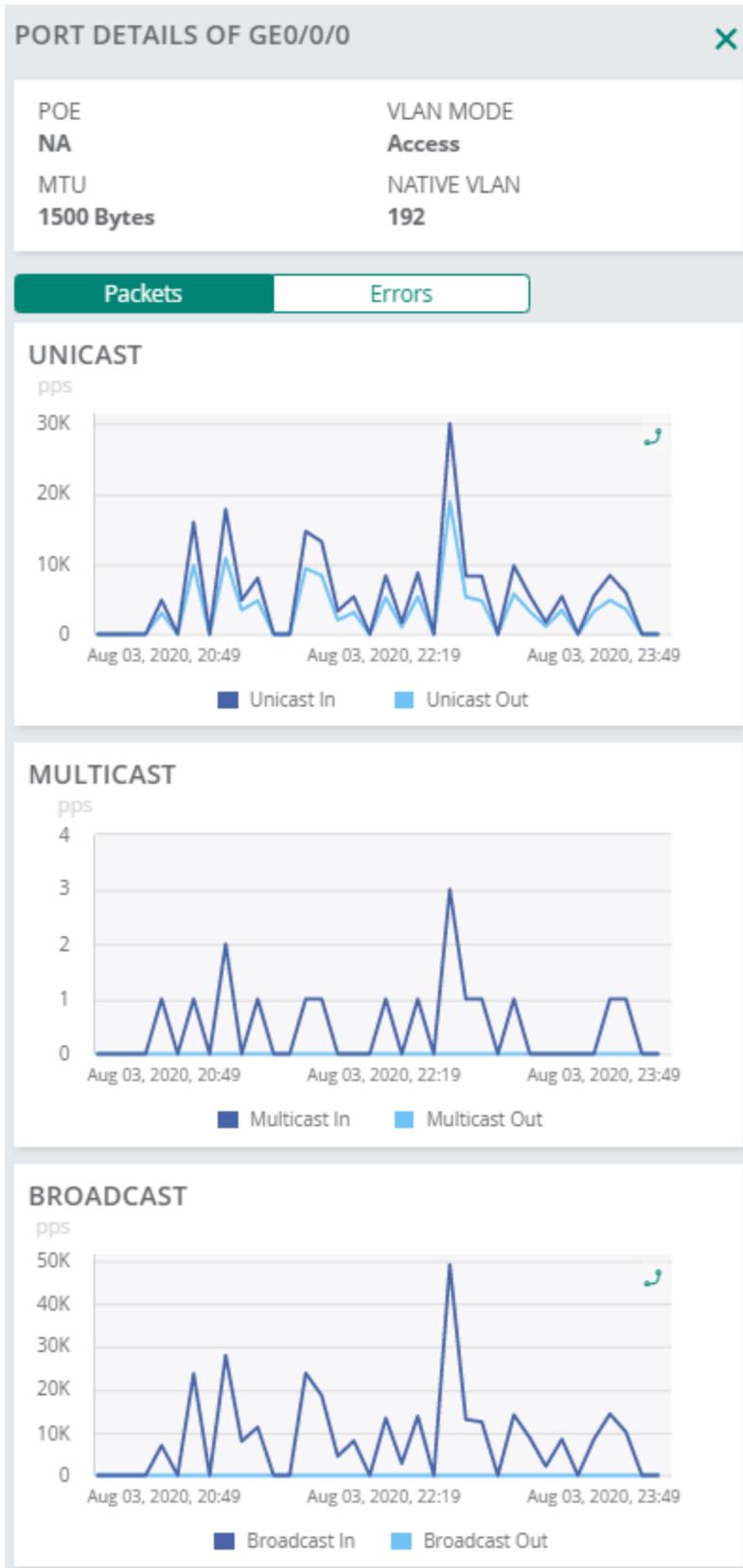
Provides a graphical representation of the Branch Gateway's LAN link availability. Also provides a quick view of the LAN port status. Click a LAN port to view the port detail graphs based on Packets or Errors.

Figure 88 *Port Status*



- The following graphs are displayed under the **Packets** tab:
- **Unicast**—The number of unicast packets per second.
- **Multicast**—The number of multicast packets per second.
- **Broadcast**—The number of broadcast packets per second.

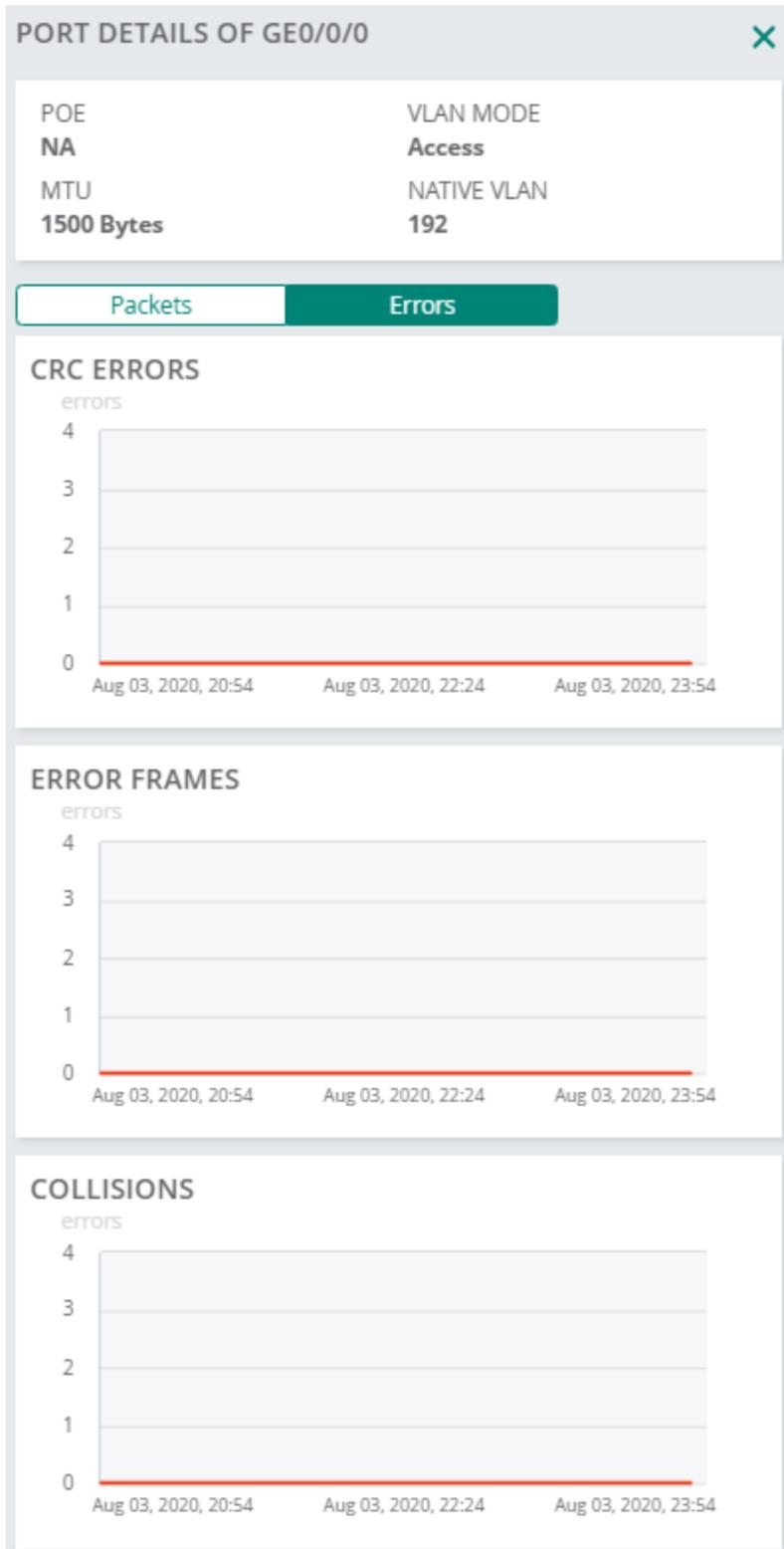
Figure 89 Port Details - Packet



- The following graphs are displayed under the **Errors** tab:

- **CRC Errors**—The number of cyclic redundancy errors logged.
- **Error Frames**—The number of error frames logged.
- **Collisions**—The number of collisions encountered.

Figure 90 *Port Details - Errors*



LAN Interfaces Summary

- The table displays the summary of LAN interfaces total number of LAN interfaces. The following details are displayed for the port:
- **Port**—Port number.
- **Admin State**—Administrative state of the LAN interface.
- **Operational State**—Operational state of the LAN interface.
- **Port Speed**—Port speed.
- **VLANs**—Range of VLANs.
- **MTU**—MTU value.

Figure 91 LAN Interface Summary

LAN INTERFACES SUMMARY (7)					
Port	Admin State	Operational State	Port Speed	VLANs	MTU
GE0/0/0	Enabled	Up	1 Gbps/Full	192	1500 Bytes
GE0/0/1	Enabled	Down	Auto/Auto	1	1500 Bytes
GE0/0/2	Enabled	Down	Auto/Auto	1	1500 Bytes
GE0/0/3	Enabled	Down	Auto/Auto	1	1500 Bytes
GE0/0/4	Enabled	Down	Auto/Auto	1	1500 Bytes
GE0/0/5	Enabled	Down	Auto/Auto	1	1500 Bytes
Gigabit-Level	Disabled	Down	Invalid/Full	--	1500 Bytes

Click a LAN port to view the port detail graphs based on Packets or Errors. For more information, see [Port Status](#).

VLAN Interface Summary

- The table displays the summary of VLAN interfaces and total number of VLAN interfaces. The following details are displayed:
- **VLAN ID**—VLAN ID number.
- **IP Address**—IP address.
- **Admin State**—Administrative state of the VLAN interface.
- **Oper. State**—Operational state of the VLAN interface.
- **Addressing Mode**—Type of addressing mode.
- **Description**—Description of the VLAN.

Figure 92 VLAN Interfaces Summary

VLAN INTERFACES SUMMARY (14)					
VLAN ID	IP Address	Admin State	Operational State	Addressing Mode	Description
1	--	--	Down	Static	--
163	21.32.54.71	--	Up	Static	--
192	192.168.10.104	--	Up	Static	--
218	71.39.84.17	--	Up	Static	--
228	95.20.84.44	--	Up	Static	--
271	25.17.85.66	--	Up	Static	--
324	79.19.27.78	--	Up	Static	--
388	14.59.23.77	--	Up	Static	--

Controller > Overview > Routing

The **Routing** tab under **Manage > Overview** in the controller dashboard displays the following sections:

- **Routes Summary**
- **Routes**

Displays a summary of the IP routes configured on the controller. The following details are displayed:

- Type—The type of IP route.
- Network—IP address of the destination network.
- VIA—IP address through the routes are forwarded.

Viewing the Overview > Routing Tab

To navigate to the **Routing** tab in the controller dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. Ensure that the filter selection contains at least one controller. For all devices, set the filter to **Global**.

The dashboard context for the selected filter is displayed.

2. Under **Manage > Devices**, click the **Controller** tab.

A list of controllers is displayed..

3. Click a controller or cluster under **Device Name**.

The dashboard context for the specific controller is displayed.

4. Under **Manage**, click **Overview > Routing**.

To exit the controller dashboard, click the back arrow on the filter.

You can change the time range for the **Routing** tab by clicking the time range filter and selecting one of the available options: **3 hours, 1 day, 1 week, 1 month, and 3 months**.

Rapids

Overview

With Aruba Central (on-premises), you can quickly identify and act on an interfering devices that can be later considered for investigation, restrictive action, or both. Once the interfering devices are discovered, Aruba Central (on-premises) sends alerts to your network administrators about the possible threat and provides essential information needed to locate and manage the threat.

Aruba Central (on-premises) supports the following features:

- Automatic detection of unauthorized wireless devices.
- Wireless detection, using authorized wireless APs to report other devices within range to calculate and display rogue location on a VisualRF map.
- Ability to make a decision based on the AP classifications and send that back to the Access Point.
- Obtaining the MAC address table from switch to identify the switch port to which the rogue device is connected.

Note the following important points:

- Users with the administrator can see all rogue AP and interfering devices.
- VisualRF uses the heard signal information to calculate the physical location of the device.
- Clicking  icon enables you to customize the **WIDS Events** table and Rogues table columns or set it to the default view.
- To view the details of each intrusion detection that is generated, click the arrow against each row in the table.

Viewing Rapids Page

To view the intrusion detail page in order to find information on interfering devices, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Group, Label, or Site**. For all devices, set the filter to **Global**.
2. Under **Manage**, click **Security > Rapids**. The **IDS** page with **WIDS Events** table is displayed.
3. Click **Rogues** tab to view the Rogues details page.

Monitoring IDS and Rogue Events

The **Manage > Security > Rapids** tab provides a summary of the rogue APs, suspected rogue APs, interfering APs, and the total number of wireless attacks detected for a given duration.

The following menu options in the **Security > Rapids** tab provide information on the potential threats discovered in the network:

- **IDS**
- **Rogues**

Intrusion Detection

The **Manage > Security > Rapids > IDS** page provides a summary of the total number of wireless attacks detected for a given duration.

The **WIDS Events** table displays the following information category:

- **Infrastructure attacks**—Displays the number of infrastructure attacks detected in the network.
- **Client attacks**—Displays the number of client attacks detected in the network.

Table 172: *WIDS Events*

Field	Description
Event Type	The type of the intrusion or attack detected. Click the drop-down arrow at the column heading to filter the event types based on your requirement.
Category	Category of the intrusion or attack, infrastructure or client attack. Click the drop-down arrow at the column heading to filter the category that you want to display.
Level	The level of the intrusion or attack detected. Click the drop-down arrow at the column heading to filter the attack level.
Time	Time of the intrusion or attack.
Station MAC	MAC address of the station under attack or BSSID of the AP under attack.
Detecting AP	The MAC address of the device that detected the intrusion or attack.
Radio Band	Radio band on which the intrusion was detected. There are two radio band signals available, 2.4 GHZ and 5 GHZ. Click the drop-down arrow at the column heading to filter the radio band where the intrusion was detected.
Description	Details of the attack or the intrusion.

EVENT TYPE	CATEGORY	LEVEL	TIME	STATION MAC	DETECTING AP
AP flood	Infrastructure	Critical	2h 45m	00:00:00:00:00:00	C8:B5:AD:C3:B2:04

INFRASTRUCTURE ATTACK DETAILS		DESCRIPTION
TIME 01 Dec 2019, 09:25:53	RADIO BAND 2.4 GHz	An AP detected that the number of potential fake APs observed across all ba...

Configuring IDS Parameters

The type and severity of Intrusion Detections raised by an AP is configurable and affects the data that is seen in the **WIDS Events** table. For more information on how to configure IDS Parameters, see Aruba Central Help Center.

Rogue Detection and Classification

Aruba Central (on-premises) employs Rogue Access Point Intrusion Detection System as a security service for detecting and classifying rogues and intruders. Central discovers unauthorized devices in your WLAN network using APs. It uses infrastructure APs routers and switches to locate, identify, and classify unknown APs. Security allows you to detect neighboring APs and classify them according to their threat level.

The access points in Aruba Central (on-premises) are classified as one of the following:

Table 173: Access Points Classification in Aruba Central (on-premises)

Classification	Description
Rogue AP	An unauthorized access point plugged into the wired side of the network.
Suspect Rogue AP	An unauthorized access point with a signal strength greater or equal to -75 that could have connected to the wired network.
Interfering AP	An access point seen in the RF environment with a signal strength lesser than -75 but is not connected to the wired network. These access points may potentially cause RF interference, but cannot be considered as a direct security threat as these devices are not connected to the wired network. For example, an interfering AP can be an access point that belongs to a neighboring office's WLAN but is not part of your WLAN network
Neighbors	A neighboring AP is when the BSSIDs are known. Once classified, a neighboring AP does not change its state.

The **Manage > Security > Rapids > Rogues** page displays the following information tabs:

- **Total**—Shows the total number of rogues classified as **Rogue**, **Suspected Rogue**, or **Interfering**, that are detected in the network.
- **Rogues**—Shows the total number of devices classified as rogue APs.
- **Suspected Rogues**— Shows the total number of devices classified as suspected rogues APs.
- **Interfering**—Shows the total number of devices classified as interfering APs.
- **Neighbors**—Shows the total number of devices classified as neighbor APs.

Click the respective tabs to display specific rogue information pertaining to each classification. By default, the **Total** information tab is selected and the **Detected Access Points** table displays all the detected rogue APs.

Table 174: Rogues

Fields	Description
BSSID	The BSSIDs broadcast by the rogue device.
Name	Name of the rogue device detected in the network.
Classification	Classification of the rogue device (monitored device) as Suspect Rogue, or Interferer. Click the drop-down arrow at the column heading to filter the rogue classification that you want to display.
SSID	The SSID broadcast by the rogue device.
Last Seen	The time relative to the current moment, for example, 6 minutes; an hour, at which the rogue device was last detected in the network.
Last Seen By	The AP name of the last device to report to have seen the monitored AP.
First Seen	The time relative to the current moment (for example, 6 minutes; an hour) at which the rogue device was detected in the network.
First Seen By	The AP name of the first AP to discover the monitored AP.
Signal	The signal strength of the AP that detected the rogue device.
Encryption	The type of encryption used by the device that detected the rogue; for example, WPA, Open, WEP, Unknown. Generally, this field alone does not provide enough information to determine if a device is a rogue, but it is a useful attribute. If a rogue is not running any encryption method, you have a wider security hole than with an AP that is using encryption.
Containment Status	Details of the containment status. Click the drop-down arrow at the column heading to filter the status that you want to display.
MAC Vendor	The vendor name associated to the MAC OUI of the rogue AP.

The screenshot displays the Aruba Central interface for monitoring detected access points. At the top, a summary bar shows the following counts: TOTAL 1627, ROGUES 596, SUSPECTED ROGUES 1015, INTERFERING 16, and NEIGHBORS 0. Below this, a table titled 'DETECTED ACCESS POINTS' lists detected devices. One device is highlighted: Atheros Comm-12:1D:1D, classified as 'Suspect Rogue', with SSID '2GHK01', last seen on 30 Jul 2020 at 13:20:42, and signal strength of -73. A detailed view for this device is shown below, divided into 'OVERVIEW' and 'LOCATION' sections.

OVERVIEW

- SSID: 2GHK01
- BSSID: 00:03:7F:12:1D:10
- FIRST SEEN: 24 Jul 2020, 23:40:37
- FIRST SEEN BY: 00:4e:35:ca:a5:6c
- LAST SEEN: 30 Jul 2020, 13:20:42
- LAST SEEN BY: 9c:8c:d8:c9:1c:da
- SWITCH PORT: --

LOCATION

ACCESS POINT NAME	SNR (DB)	BAND	BSSID	RF CHANNEL
9c:8c:d8:c9:1c:da	-73	2.4 GHz	9C:8C:D8:11:CD:A0	6

Generating Alerts for Security Events

Aruba Central (on-premises) supports configuring alerts for rogue AP detections and IDS events. To generate alerts, complete the following steps:

1. In the **Network Operations** app, use the filter to select **Global**.
2. Under **Analyze**, click **Alerts & Events**. The **Alerts & Events** page is displayed.
3. In the **Alerts & Events** page, click the **Config** icon.
The **Alert Severities & Notifications** page is displayed.
4. Select **Access Point** tab to display the AP dashboard. Aruba Central (on-premises) supports three alert types for identifying interfering devices:
 - Rogue AP Detected
 - Infrastructure Attacks Detected
 - Client Attack Detected
5. Select an alert and click **+** to enable the alert with default settings. To configure alert parameters, click on the alert tile (anywhere within the rectangular box) and do the following:
 - a. **Severity**—Set the severity. The available options are Critical, Major, Minor, and Warning.



For a few alerts, you can configure threshold value for one or more alert severities. To set the threshold value, select the alert and in the exceeds text box, enter the value. The alert is triggered when one of the threshold values exceed the duration.

- b. **Device Filter Options**—(Optional) You can restrict the scope of an alert by setting one or more of the following parameters:
 - **Group**—Select a group to limit the alert to a specific group.
 - **Label**—Select a label to limit the alert to a specific label.
 - **Sites**—Select a site to limit the alert to a specific site.
- c. **Notification Options**
 - **Email**—Select the **Email** check box and enter an email address to receive notifications when an alert is generated. You can enter multiple email addresses, separate each value with a comma.
 - **Streaming**—Select the **Streaming** check box to receive the streaming notifications when an alert is generated.
 - **Syslog**—Select the **Syslog** checkbox to receive the syslog notifications when an alert is generated.
- d. Click **Save**.
- e. **Add Rule**—(Optional) For a few alerts, the **Add Rule** option appears. For such alerts, you can add additional rule(s). The rule summaries appear at the top of the page.

Generating Reports for Security Events

Aruba Central (on-premises) supports generating reports for rogue AP detections and IDS events. To generate reports, complete the following steps:

1. In the **Network Operations** app, use the filter to select **Global**.
2. Under **Analyze**, click **Reports**.
3. In the **Reports** page, click **Create**. Aruba Central (on-premises) supports **Rapids** to display the report of all wireless intrusions. For more information on how to create Reports, see Aruba Central Help Center.

Network Health

The Network Health dashboard displays information of the network sorted by site. This dashboard displays information on network devices and WAN connectivity of individual sites.

To launch the **Network Health** dashboard, complete the following procedure:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage**, click **Overview > Network Health** to launch the **Network Health** dashboard.

The **Network Health** dashboard has two views, you can toggle between them by clicking on the view icons.

- **Summary**— This view displays the vital network information of individual sites on cards mapped by geographical location. Sites are marked with location pins- red pin for a site with potential issues and green pin for a site with no issues. To view the information card of a site, click on the location pin of a site. Hover over a site to view the Network health card.

The **Network Health** menu option in the **Manage > Overview** section provides detailed information of the network health status and usage for the sites configured in your setup.

The following table lists the information displayed in a Network health card:

Table 175: *Network Health Card*

Item	Description
Insights	Displays the number of AI Insight reports available for the site. The reports are organized by degree- High , Medium , and Low depending on the number of events in the network.
Devices	Displays the number of connected and Offline APs for the site. Clicking on one of the numbers redirects you to the Devices dashboard page of the site.
Clients	Displays the number of connected and failed clients for the site. Clicking on one of the numbers redirects you to the Clients dashboard page of the site.
RF Coverage	Provides a link to view or configure the floorplan for the site. Clicking on the Floorplan redirects you to the floor plans page of the site
Uplinks	Displays the uplink connectivity status of devices in the site. This information is displayed when there is at least one uplink in the site.
Tunnels	Displays the connectivity status of tunnels in the site. This information is displayed when there is at least one tunnel in the site.
High Mem usage	Displays the number of devices with high memory utilization in the site. This information is displayed when there is at least one device with high memory utilization in the site.
High CPU usage	Displays the number of devices with high CPU usage in the site. This information is displayed when there is at least one device with high CPU usage in the site.
High CH utilization	Displays the number of APs with a higher channel utilization in the 5 GHz and 2.4 GHz radio bands. This information is displayed when there is at least one AP with a higher channel utilization in the 5 GHz or 2.4 GHz radio bands in the site.
High noise utilization	Displays the number of APs with high RF noise in the 5 GHz and 2.4 GHz bands. This information is displayed when there is at least one AP with a higher noise utilization in the 5 GHz or 2.4 GHz radio bands in the site.

- List**—This view displays the global network report in a list sorted according to individual sites. Clicking on the site name will take you to the **Site Health** dashboard page. The data columns listed in the page can be managed by clicking on the hamburger icon (☰) on the right of the column header. The report can be filtered by clicking on the filter labels below the column name. Selecting a filter label filters the results based on the field values of the column in ascending or descending order, sites with zero issues will not be displayed. The order of the results displayed can be toggled by clicking the  or  icon beside the filter.

The **Network Health** dashboard displays the information listed in the table below.

Table 176: *Network Health Dashboard*

Header	Description
Site Name	The name of the site. Clicking on the site name will take you to the Site Health dashboard page (Site > Overview > Site Health tab). To search for a site by name, click on the Site Name label and enter the name of the site.
AI Insights	Displays the number of AI Insight reports available for the site. The reports are organized by degree- High , Medium , and Low depending on the number of events in the network.
Number of Devices	
Status	The number of devices that are in Up or Down state in a site. Click the List icon and hover your mouse over a field in the column to view the following details: <ul style="list-style-type: none"> WLAN Devices Down Wired Devices Down Branch Devices Down
High Memory Usage	The number of devices with high memory utilization in the site. Click the List icon and hover your mouse over a field in the column to view the following details: <ul style="list-style-type: none"> WLAN High Memory Wired High Memory Branch High Memory
High CPU Usage	The number of devices with high CPU usage in the site. Click the List icon and hover your mouse over a field in the column to view the following details: <ul style="list-style-type: none"> WLAN CPU High Wired CPU High Branch CPU High
High CH Utilization	The number of APs with a higher channel utilization in the 5 GHz and 2.4 GHz radio bands.
Clients	Displays the number of connected and failed clients for the site.
High Noise	The number of APs with high RF noise in the 5 GHz and 2.4 GHz bands.
WAN	
Uplink Status	Displays the uplink connectivity status of devices in the site. The data is classified into two columns: devices with no issues and devices with no uplink connectivity.
Tunnel Status	Displays the connectivity status of tunnels in the site. The data is classified into two columns: tunnels with no issues and tunnels with no connectivity.

Global—Summary

In the **Global** dashboard, the **Summary** tab displays the **Usage, Clients, Bandwidth Usage Per Network, Client Count Per Network, Top APs By Usage, Top Clients By Usage, Top IAP Clusters By Usage, Top IAP Clusters By Clients**, and **WLAN** network details.

You can change the time range for the **Summary** tab by clicking the time range filter and selecting one of the available options: **3 hours, 1 day, 1 week, 1 month**, and **3 months**.

Viewing the Global Summary Page

To navigate to the Global Summary page, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Overview > Summary**.
The Global Summary page is displayed.

The Global Summary page displays the following information:

Table 177: *Global Summary Page Parameters*

Data Pane Item	Description
Usage	Displays the incoming and outgoing data traffic detected on the APs.
Clients	Displays the number of clients connected to an AP over a specific time period.
Bandwidth Usage Per Network	Displays the incoming and outgoing traffic for all APs per SSID over a specific duration.
Client Count Per Network	Displays the number of clients connected to an AP per SSID over a specific time period.
Top APs By Usage	Displays the list of top APs that utilize the maximum bandwidth in the network. Bandwidth usage includes the sum total of data transmitted and received on the radio interfaces and wired clients connected to the AP.
Top Clients By Usage	Displays the list of top clients connected to the currently available SSIDs that utilize the maximum bandwidth in the network.
Top IAP Clusters By Usage	Displays the list of top AP clusters that utilize the maximum bandwidth in the network.
Top IAP Clusters By Clients	Displays the list of top AP clusters connected to the client that utilize the maximum bandwidth in the network.
WLAN	Displays the list of SSIDs configured. The WLANs table displays the SSID details such the Name, Clients, Type , and Security .

Site Health Dashboard

The **Site Health** dashboard displays details of wired and wireless devices deployed on the site. This page includes information on client connectivity statistics, change logs, health of devices, and RF health of the site.

To launch the **Site Health** dashboard, complete the following procedure:

1. In the **Network Operations** app, set the filter to a site.
2. Under **Manage**, click **Overview > Site Health** to launch the **Site Health** dashboard.

Alternatively, the **Site Health** dashboard can be accessed by selecting a site from the **Network Health** dashboard page.

Health Bar

The **Health Bar** provides a snapshot of the overall health of the devices configured at the site. If there are any potential issues, it is indicated by the  status icon and corresponding descriptions are displayed. When there are multiple criteria issues, only the issue criteria with the highest priority is displayed. The <+x> next to the description indicates that there are more issues. You can hover over the value to view the description of the issue in a pop-up window. For more information, see [Health Bar Dashboard for Site](#).

The descriptions displayed for the **Potential Issue** are corresponding to the issue encountered at the site. The following is a list of possible messages:

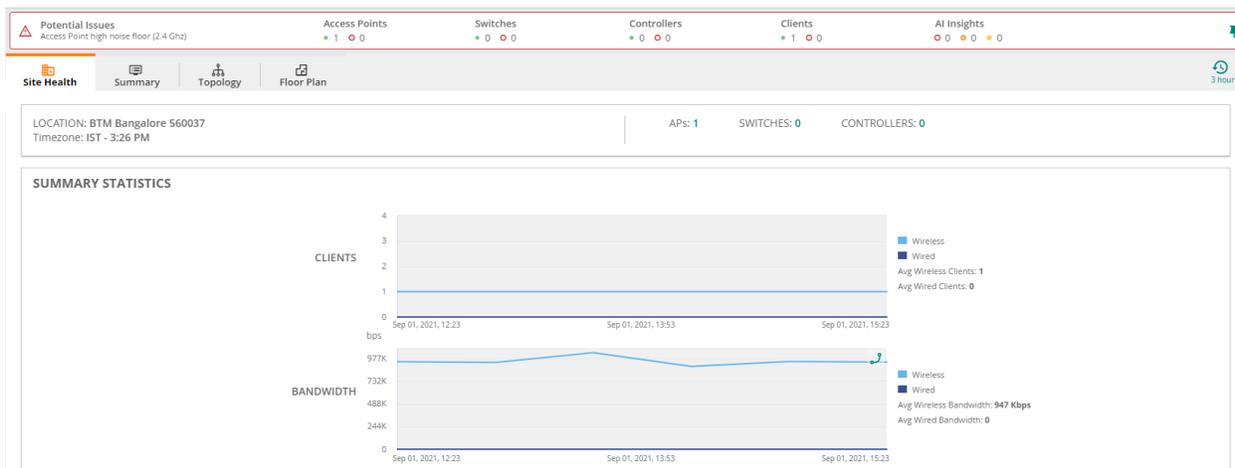
- Offline controller
- Offline switch
- Offline access point
- Access point high noise floor (2.4 GHz)
- Access point high noise floor (5 GHz)
- Controller high CPU usage
- Access point high CPU usage
- Switch high CPU usage
- Controller high memory usage
- Access Point high memory usage
- Switch high memory usage
- Access point high channel utilization (2.4 GHz)
- Access point high channel utilization (5 GHz)
- Silverpeak state <major or critical alarm>
- Cape network state <issue>
- Uplink down
- Tunnel down

To launch the **Health Bar**, complete the following steps:

1. In the **Network Operations** app, set the filter to a site.
2. Under **Manage**, click **Overview > Site Health**.
3. Click the status icon next to the site name, the **Health Bar** pop-up appears.
4. Click the  pin icon to pin the **Health Bar** to the **Site Health** page.

For information about what the status icons and the indicators denote, see [Health Bar Icons](#).

Figure 93 Site Health Bar



The **Site Health** dashboard displays the information listed in the table below:

Table 178: Site Health Dashboard

Content	
Name	Name of the site.
Location	Location of the site.
Timezone	Timezone name and local time. For example, IST-11:25 AM.
APs	Number of APs deployed on the site.
Switches	Number of switches deployed on the site.
Controllers	Number of controllers deployed on the site.
Summary Statistics	A graphical representation of the number of clients (wired and wireless) and their bandwidth usage for the selected time range.
Change Log	A visual representation of change logs for configuration, firmware, and reboot changes in the selected time range. Select a column in the graph and click on the Config Log , Firmware Log and Reboot Log button to view detailed information logs on the corresponding events in the site.
System Health Indicators	
Down Devices	This graph shows the count of devices with DOWN status. The graph displays the following information: <ul style="list-style-type: none"> ■ Total number of devices ■ Number of unique devices that were DOWN ■ Minimum and maximum device downtime.

Table 178: Site Health Dashboard

Content	
	<p>To view more details, select a time range in the graph and click on See Devices. A pop-up window displays the details of devices with DOWN status and their Up and Down time in percentage. You can also add other metrics such as CPU, Memory, 5 GHz and 2.4 GHz Channel Utilization, and 5 GHz and 2.4 GHz Noise Floor by clicking on the Add Metric button. A particular device can be filtered from the list by clicking on the  filter icon and entering the name of the device.</p>
<p>High CPU & High Memory</p>	<p>This graph shows the total count or percentage of devices with high CPU utilization and high memory utilization.</p> <ul style="list-style-type: none"> ■ High CPU Utilization—This graph displays the total number of devices, number of unique devices with high CPU utilization, and minimum and maximum number of devices with high CPU utilization. You can also view the total count or percentage of maximum and minimum number of devices with high CPU utilization for a specific time when you hover your mouse over the graph. ■ High Memory Utilization—This graph displays the total number of devices, number of unique devices, the minimum and maximum number of devices with high memory utilization. You can also view the total count or percentage of maximum and minimum number of devices with high memory utilization for specific time when you hover your mouse over the graph. ■ Threshold Setting Widget—You can also choose to view the graph details based one of the following criteria by clicking the  settings icon and selecting any of the following options: <ul style="list-style-type: none"> ○ > 70% CPU utilization. ○ > 80% CPU utilization. ○ > 90% CPU utilization. ○ > 70% memory utilization. ○ > 80% memory utilization. ○ > 90% memory utilization. <p>To view more details, select a time range in the graph and click on See Devices. A pop-up window displays the details of devices with high CPU utilization and memory utilization with their individual minimum and maximum values. You can add other metrics such as 5 GHz and 2.4 GHz Channel Utilization , 5 GHz and 2.4 GHz Noise Floor, and Device Down time for the devices by clicking on the Add Metric button. A particular device can be filtered from the list by clicking on the  filter icon and entering the name of the device.</p>
<p>RF Health Indicators</p>	
<p>5 GHz Utilization and Noise</p>	<p>This graph displays the total count or percentage of devices with high channel utilization and high noise floor levels for 5 GHz band.</p> <ul style="list-style-type: none"> ■ Device Details—The graph displays total number of devices, number of unique devices with high 5 GHz channel utilization

Table 178: Site Health Dashboard

Content	
	<p>and high noise floor levels, and the minimum and maximum number of devices with high channel utilization. You can also view the total count of maximum and minimum number of devices with high 5 GHz channel utilization and noise for a specific time when you hover your mouse over the graph.</p> <ul style="list-style-type: none"> ■ Threshold setting—You can also choose to view the graph details based one of the following criteria by clicking the  settings icon and selecting any of the following options: <ul style="list-style-type: none"> ○ > 60% 5 GHz Utilization. ○ > 70% 5 GHz Utilization. ○ > 80% 5 GHz Utilization. ○ > -75 dBm 5 GHz Noise. ○ > -80 dBm 5 GHz Noise. ○ > -85 dBm 5 GHz Noise. <p>To view more details, select a time range in the graph and click on See Devices. A pop-up window displays the details of devices with high CPU utilization and memory utilization with their individual minimum and maximum CPU utilization values. You can add other metrics such as CPU, Memory, 2.4 GHz Channel Utilization, 2.4 GHz Noise Floor, and Device Down time for the devices by clicking on the Add Metric button. A particular device can be filtered from the list by clicking on the  filter icon and entering the name of the device.</p>
<p>2.4 GHz Utilization and Noise</p>	<p>This graph displays the total count or percentage of devices with a higher channel utilization and high noise floor levels for 2.4 GHz channel.</p> <ul style="list-style-type: none"> ■ Device Details—The graph displays the total number of devices, number of unique devices with high 2.4 GHz channel utilization and noise floor levels, minimum and maximum number of devices with high channel utilization and noise levels. You can also view the total count of maximum and minimum number of devices with high 2.4 GHz Utilization and Noise for a specific time when you hover your mouse over the graph. ■ Threshold Setting widget —You can also choose to view the graph details based one of the following criteria by clicking the  settings icon and selecting any of the following options: <ul style="list-style-type: none"> ○ > 60% 2.4 GHz Utilization. ○ > 70% 2.4 GHz Utilization. ○ > 80% 2.4 GHz Utilization. ○ > -75 dBm 2.4 GHz Noise. ○ > -80 dBm 2.4 GHz Noise. ○ > -85 dBm 2.4 GHz Noise.

Table 178: *Site Health Dashboard*

Content	
	<p>To view more details, select a time range in the graph and click on See Devices. A pop-up window displays the details of devices with 2.4 GHz channel utilization and 2.4 GHz noise floor with their individual minimum and maximum values. You can add other metrics such as CPU, Memory, 5 GHz Channel Utilization, 5 GHz Noise Floor, and Device Down time for the devices by clicking on the Add Metric button. A particular device can be filtered from the list by clicking on the  filter icon and entering the name of the device.</p>
<p>NOTE: The  threshold setting icon is visible only when you bring the mouse pointer closer to its position slightly above the right-hand side of each graph.</p>	

WAN Health—Site

The **WAN Health** page displays details for the wired, wireless, and controller devices deployed on the site.

To launch the **WAN** dashboard, complete the following procedure:

1. In the **Network Operations** app, set the filter to a site.
2. Under **Manage**, click **Overview > WAN** to launch the **WAN** dashboard.
3. Click the site on the map, or the site from the **Site Name** column in the List view, to view details of that site.

The **WAN Health** dashboard displays the following information:

Table 179: *Site Health Controllers Page*

Content	Description
Site Name	Name of the site.
Time Range	Time range selection drop-down for viewing site health. You can set the time range to 3 hours, 1 day, 1 week, 1 month, or 3 months.
Summary	<p>The following details are available:</p> <ul style="list-style-type: none"> ■ Name—Name of the site. ■ Location—Location of the site. ■ APs—Number of APs deployed on the site. ■ Switches—Number of switches deployed on the site. ■ Controllers—Number of controllers deployed on the site.
Site Availability graph	Site availability metrics per provider represented in a chart. The graph displays detailed metrics for the number of sites in the down status, percentage of site availability, and the number of unknown sites.
Policy Compliance graph	Policy compliance metrics for the site. The path steering data is used to calculate this metric.
Bandwidth graph	Bandwidth utilization of the selected site. From the drop-down list, select one of the following:

Table 179: Site Health Controllers Page

Content	Description
	<ul style="list-style-type: none">■ All Traffic■ Internet vs. VPN
Bandwidth graph	Bandwidth utilization of the selected uplink. From the drop-down list, select the uplink.
Transport Health graph	Displays the transport health of the site based on active monitoring probes. Site transport health is an average of MOS score across all probes.
<p>NOTE: If you hover over any graph, a pop-up window opens and displays the data specific to that graph. Click on the graph to lock the time range. After you lock the selection, the same time range is selected across all the graphs in the Site Health page.</p> <p>NOTE: If you click on any graph, a see devices button is enabled below all the graphs. Click see details to view the list of devices. From the Add Metric drop-down list, select one or more of the following: Site Availability, Bandwidth or Internet vs. VPN.</p>	

AI Insights

Aruba AI Insights delivers actionable guidance for improving network performance and the quality of your users' mobile experience via continuous monitoring, analysis, and benchmarking. Using powerful machine learning algorithms and Aruba's extensive wireless expertise, AI Insights arms IT organizations with the intelligence needed to proactively optimize how data, voice, and video applications perform across your entire campus – including local and remote locations.

Smart analytics automate the complex task of identifying where potential problems exist. AI Insights continuously monitors the network and makes specific recommendations that can improve how the network performs. By proactively fixing potential issues, IT can stop the reactive cycle. Help desk calls are reduced, troubleshooting and problem resolution are minimized, and the IT staff is freed up for more strategic work.

AI Insights is supported on a 5-node cluster and 7-node cluster.

- 5- node cluster which supports 16,000 devices and 160000 clients
- 7-node cluster which supports 30,000 devices and 300000 clients



AI Insights is not supported on Single-node and 3-Node clusters.

AI Insights support the following features in Aruba Central (on-premises) deployment:

- [Wi-Fi Connectivity Dashboard](#) - The **Wi-Fi Connectivity** page displays an overall view of the connection details for all clients that are connected to or tried to connect to each connection phase.
- [WLAN Connectivity Insights](#) - Insights can be accessed from different contexts such as **Global**, **Site**, **Clients**, and **Device**. The following four types of AI Insights are supported in Aruba Central (on-premises):
 - DHCP Connection Failures
 - MAC Authentication Failures
 - Wi-Fi security key-exchange failures
 - 802.1x authentication Failures
 - Wi-Fi Association Failures
 - Captive Portal Authentication Failures
- [WLAN Connectivity Alerts](#) - Aruba Central (on-premises) allows you to configure and enable connectivity alerts to generate and display alerts when DNS delays, DHCP delays, authentication delays, and association failures are detected.
- [Failed Wireless Client Events or Reasons](#) - AI Insights helps populate the last seen time stamp, failure stage, and failure reason for a failed client. This information is communicated to the Aruba Central (On-premises) server and is displayed in the Failed clients list in **Global > Clients > Failed Clients**. Also, if an AI insight is associated with a failed client, the AI insight number is listed in the table and can be used to open the insight and troubleshoot the client issues.

Wi-Fi Connectivity

The **Wi-Fi Connectivity** page displays an overall view of the connection details for all clients that are connected to or tried to connect to each connection phase. The connection phases include **Association**, **Authentication**, **DHCP**, and **DNS**.

To view the connectivity details page complete the following procedure:

1. In the **Network Operations** app, select one of the following options:
To select a group, site, or all devices in the filter, set the filter to one of the options under **Group** or **Site**. For all devices, set the filter to **Global**.
2. Under **Manage > Overview**, click **Wi-Fi Connectivity**.
The dashboard context for the selected filter is displayed.

By default, the graphs on the **Wi-Fi Connectivity** page is plotted for a time range of 3 hours. To view the graphs for a different time range, click the **Time Range Filter** icon. You can choose to view graphs for a time period of 3 hours, 1 day, 1 week, 1 month and 3 months.

This section includes the following topics:

- [Connectivity Summary Bar](#)
- [Connection Experience](#)
- [AI Insights](#)
- [Connection Problems](#)
- [Connection Events](#)

Connectivity Summary Bar

The connectivity summary bar displays the details of all clients in percentage. It displays the percentage success rate of each stage for the users to know the network performance.

Figure 94 *Connectivity Summary Bar*



The following table describes the information displayed in each section:

Table 180: *Connectivity Summary Bar*

Field	Description
All	Displays the aggregated success percentage of Association, Authentication, and DHCP for all clients connected to the network.
Association	Displays the percentage of successful attempts made by a client to connect to the network.
Authentication	Displays the percentage of successful attempts of client authentication.
DHCP	Displays the percentage of successful attempts of DHCP requests and responses when onboarding a client.
DNS	Displays the percentage of successful attempts in the detected DNS resolutions, when a client is connected to the network.

Connection Experience

The **Connection Experience** tile displays the overall success percentage, total number of attempts, number of successful attempts, total delays, and the total failures for each stage based on the selected time range filter. To view the connection experience for individual stage, select the stage type from the **Connectivity Summary** bar, the **Connection Experience** displays the chart for the selected stage. Select **All** to view the success percentage for all the stages. You can hover over the time series graph to view the success percentage for a specific time. The individual stage displays the **Attempts**, **Failures**, **Success**, and **Delays** on the time series graph.

Figure 95 Connection Experience tile



AI Insights

The **AI Insights** tile provides a list of AI Insights generated for a selected time range. To view the details, click on a selected **AI Insight**. The page gets redirected to the AI Insights under the **AI Insights** page. Click each of the listed AI Insight for a detailed analysis based on the impact on the network. For more information on AI Insights, see [The AI Insights Dashboard](#).



AI-Insights is not implemented for **Association** and **DNS**. AI Insights is not implemented at a Group level also. The page displays **No AI Insights observed**.

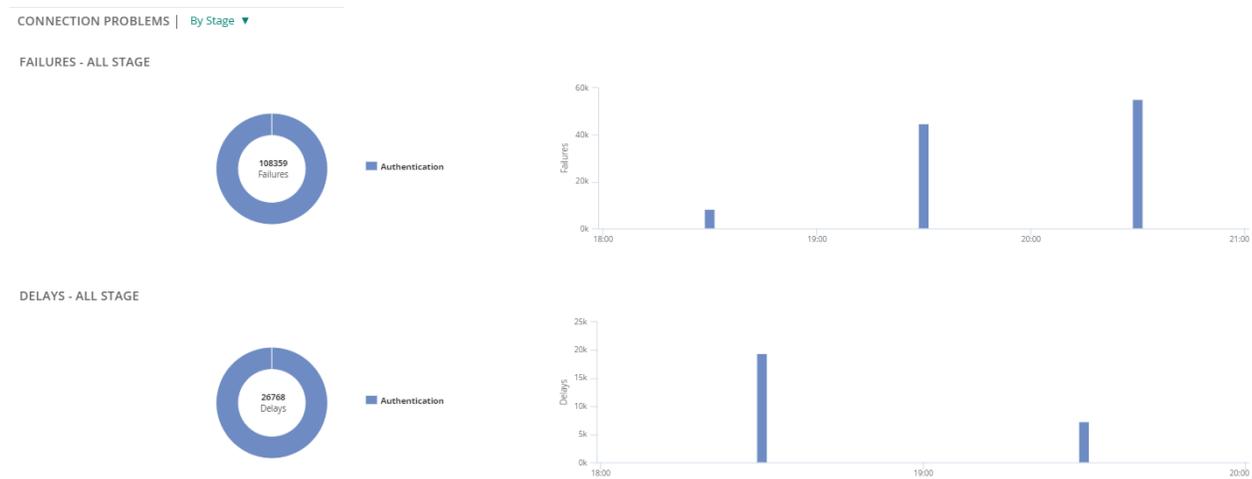
For a visual representation of viewing an AI Insight, click [here](#).

Connection Problems

The **Connection Problems** tile displays the details of **Failures** and **Delays** graphically for each of the categories from the drop-down list. Each graph displays the top five MAC addresses or SSID based on the

selected category. Each category in the **Connection Problems** drop-down lists changes based on the selected stage in the **Connectivity Summary** bar. Selecting the required category from the drop-down displays the failures and delays in a pie chart with percentage, and a bar graph with the number of failures and delays. Hover the cursor over each graph to view the number of failures or delays for each stage.

Figure 96 *Connection Problems Tile*



The following table describes the information displayed in each connection category based on the selected stage:

Table 181: *Connection Problems Rolls-ups*

Data Pane Content	Description
All	<p>Displays the details of the failures and delays that occurred during a client connection. The chart displays the failure details of Association, Authentication, and DHCP for each client. The Connection Problems drop-down list includes the following categories:</p> <ul style="list-style-type: none"> ■ By Stage ■ By Clients ■ By Access Points ■ By Band ■ By SSID
Association	<p>Charts the details of the failures and delays that occurred during a client association. The Connection Problems drop-down list includes the following categories:</p> <ul style="list-style-type: none"> ■ By Clients ■ By Access Points ■ By Band ■ By SSID ■ By Reason
Authentication	<p>Charts the details of the failures and delays that occurred during a client authentication. The Connection Problems drop-down list includes the following categories:</p> <ul style="list-style-type: none"> ■ By Type ■ By Clients ■ By Access Points ■ By Band ■ By SSID ■ By Server

Data Pane Content	Description
DHCP	Charts the details of the failures and delays that occurred during the attempts of DHCP requests and responses by a client. The Connection Problems drop-down list includes the following categories: <ul style="list-style-type: none"> ■ By Clients ■ By Access Points ■ By Reason
DNS	Charts the details of the failures and delays that occurred during the attempts in detected DNS resolutions when a client is connected to the network. The Connection Problems drop-down list includes the following categories: <ul style="list-style-type: none"> ■ By Access Points ■ By Reason ■ By Server

Connection Events

Connection Events table details out the list of delays and failures for each client based on the client MAC addresses. Click the  icon to view the connection events table. Click the **Connection Events** drop down to filter the events **By Clients** or **By Access Points**. The **Connection Events** table displays the following information:

Table 182: *Connection Events*

Data Pane Content	Description
MAC Address	Displays the MAC address of the client.
Name	Displays the name of the access point.
Delays	Displays the delays that occurred during the event.
Failures	Displays the failure details that occurred during the event.

Connectivity Alerts

Aruba Central allows network administrators and users with admin permissions to configure alerts. For more information, see [Configuring Alerts](#).

Following are the connectivity alerts that you can configure:

- **DNS Delay Detected**—Generates an alert when clients experience significant delays in response from the DNS server. Set the severity values to generate an alert if the percentage of delay from the DNS server exceeds the threshold value. The **Duration** field displays the duration after which the alert is generated. The default value is 30 minutes. You can add additional rule(s) for this alert.
- **DNS Failure Detected**—Generates an alert when wireless APs experience a high number of connection failures with the DNS server. Set the severity values to generate an alert if the DNS failure percentage exceeds the threshold value. The **Duration** field displays the duration after which the alert is generated. The default value is 30 minutes. You can add additional rule(s) for this alert.
- **DHCP Delay Detected**—Generates an alert when there is excessive DHCP delay from client to AP in the network. Set the severity values to generate an alert if the percentage of the DHCP delay exceeds the threshold value. The **Duration** field displays the duration after which the alert is generated. The default value is 30 minutes. You can add additional rule(s) for this alert.

- **DHCP Failure Detected**—Generates an alert when there is high number of DHCP failure observed from client to AP in the network. Set the severity values to generate an alert if the DHCP failure percentage exceeds the threshold value. The **Duration** field displays the duration after which the alert is generated. The default value is 30 minutes. You can add additional rule(s) for this alert.

- **Authentication Delay Detected**—Generates an alert when there is excessive delay in the client authentication process with the AP in the network. Authentication failures include the following:

- Wi-Fi security key-exchange failures
- 802.1x authentication failures
- MAC authentication failures
- Captive failures

Set the severity values to generate an alert if the percentage of the authentication delay exceeds the threshold value. The **Duration** field displays the duration after which the alert is generated. The default value is 30 minutes. You can add additional rule(s) for this alert.

- **Authentication Failure Detected**—Generates an alert when there are high number of client authentication failures in the network. Authentication failures include the following:

- Wi-Fi security key-exchange failures
- 802.1x authentication failures
- MAC authentication failures
- Captive failures

Set the severity values to generate an alert if the authentication failure percentage exceeds the threshold value. The **Duration** field displays the duration after which the alert is generated. The default value is 30 minutes. You can add additional rule(s) for this alert.

- **Association Delay Detected**—Generates an alert when client association delay is detected in the network. Set the severity values to generate an alert if the percentage of the association delay exceeds the threshold value. The **Duration** field displays the duration after which the alert is generated. The default value is 30 minutes. You can add additional rule(s) for this alert.

- **Association Failure Detected**—Generates an alert when client association failure is detected in the network. Set the severity values to generate an alert if the association failure percentage exceeds the threshold value. The **Duration** field displays the duration after which the alert is generated. The default value is 30 minutes. You can add additional rule(s) for this alert.

The AI Insights Dashboard

In an environment of rapidly changing business and user expectations driven by an explosion of connectivity requirements from the edge to the cloud, a new approach to network management is required. Aruba AI Ops (Artificial Intelligence for IT operations) is the next generation of AI-powered solutions that integrates proven Artificial Intelligence solutions with recommended and automated action to provide both fast response to identified problems, along with proactive prediction and prevention.

With data leveraged from huge network management systems, Aruba Central (on-premises) and built-in AI Insights proactively identifies and solves issues, and provides pinpoint configuration recommendations. The result of this AI based mechanism has enabled a consistent, reliable, and timely flow of information about the network performance, that helps IT work faster despite the increasing demand and complexity that a network often brings. All of this comes from Aruba advantage in accessing an enormous volume and variety of data that is factored into insights. Aruba does not collect or process personal data.

The **AI Insights** dashboard displays a report of network events that could possibly affect the quality of the overall network performance. These are anomalies observed at the access point, connectivity, and client level observed in the network for the selected time range. Each insight report provides specific details on the occurrences of these events for ease in debugging.

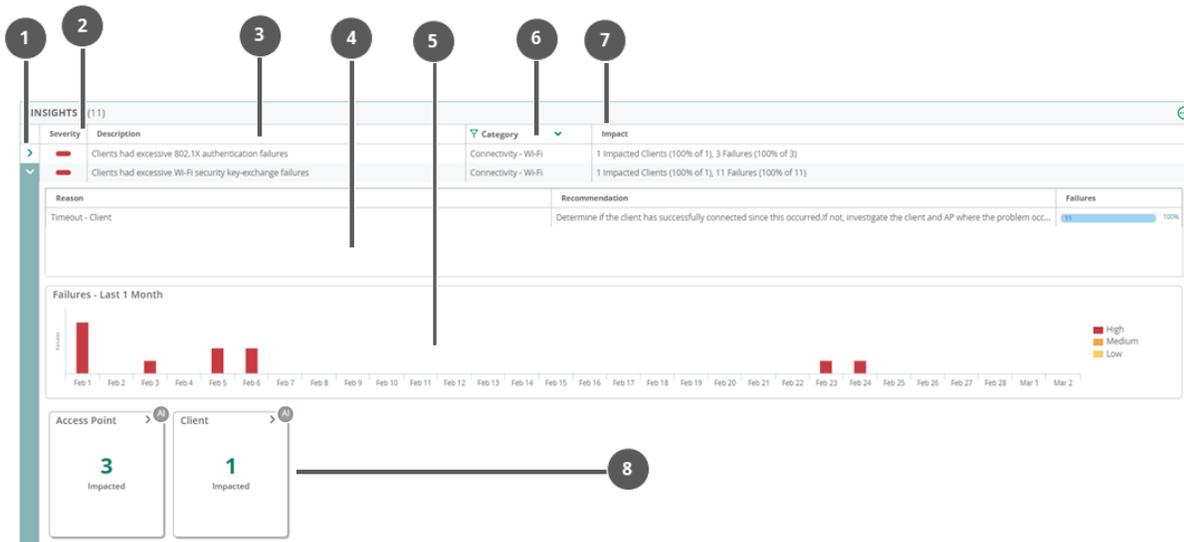
To launch the **AI Insights** dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage**, click **Overview > AI Insights**.

The **Insights** table is displayed. AI Insights listed in the dashboard are sorted from high priority to low priority.

3. Click the arrow  against each insight to view the details.

Figure 97 *Insight Anomaly*



Callout Number	Description
1	Click this arrow to expand any specific insight to view further details.
2	Displays the insight severity, using the following colors:  Red—High priority  Orange—Medium priority  Yellow—Low priority
3	Short description of the insight.
4	Insight Summary displays the reason why the insight was generated along with recommendation. It also shows the number and percentage of failures that occurred against each failure reason. <ul style="list-style-type: none"> ■ Static—These reasons rely on Aruba's domain expertise. ■ Dynamic—These reasons are generated based on error codes that is received from infrastructure devices.
5	Time Series graph is a graphical representation of the events that occurred for the selected time range.
6	Category of the insight. Insight category can be filtered by clicking the filter  icon.
7	Short description of the impact.
8	Cards display additional information specific to each insight. Cards might vary for each insight based on the context the insight is accessed from. For more information, see Cards .

All AI Insights observed for the network are listed in the **AI Insights** dashboard in the **Global** context. Alternatively, AI Insights reports for a specific site, device, or a client can be viewed by selecting the appropriate context. For more information on available insights and the context, see [Insight Context](#).



AI Insights are displayed for a selected time period based on the time selected in the Time Range Filter () . You can select one of the following: **3 Hours**, **1 Week**, **1 Day**, or **1 Month**.

Insight Context

Insights can be accessed from different contexts such as **Global**, **Site**, **Clients**, and **Device**. The following table lists the different types of insights generated by Aruba Central and the path from where it can be accessed.

Table 183: *Insight Context*

Insights	Category	Context	Navigation
Clients with High Wi-Fi Security Key-Exchange Failures	Connectivity — Wi-Fi	Global	Network Operations > Global > Overview > AI Insights
		Site	Network Operations > Sites > Overview > AI Insights
		Access Points	Network Operations > Global > Devices > Access Points > Device Name > AI Insights
		Clients	Network Operations > Global > Clients > Client Name > AI Insights Network Operations > Site > Clients > Client Name > AI Insights
Clients with High 802.1X Authentication Failures	Connectivity — Wi-Fi	Global	Network Operations > Global > Overview > AI Insights
		Site	Network Operations > Sites > Overview > AI Insights
		Access Points	Network Operations > Global > Devices > Access Points > Device Name > AI Insights
		Clients	Network Operations > Global > Clients > Client Name > AI Insights Network Operations > Site > Clients > Client Name > AI Insights

Insights	Category	Context	Navigation
Clients with DHCP Server Connection Problems	Connectivity — Wi-Fi	Global	Network Operations > Global > Overview > AI Insights
		Site	Network Operations > Sites > Overview > AI Insights
		Access Points	Network Operations > Global > Devices > Access Points > Device Name > AI Insights
		Clients	Network Operations > Global > Clients > Client Name > AI Insights Network Operations > Site > Clients > Client Name > AI Insights
Clients with High Number of MAC Authentication Failures	Connectivity — Wi-Fi	Global	Network Operations > Global > Overview > AI Insights
		Site	Network Operations > Sites > Overview > AI Insights
		Access Points	Network Operations > Global > Devices > Access Points > Device Name > AI Insights
		Clients	Network Operations > Global > Clients > Client Name > AI Insights Network Operations > Site > Clients > Client Name > AI Insights

Insights	Category	Context	Navigation
Clients with Captive Portal Authentication Problems	Connectivity — Wi-Fi	Global	Network Operations > Global > Overview > AI Insights
		Site	Network Operations > Sites > Overview > AI Insights
		Access Points	Network Operations > Global > Devices > Access Points > Device Name > AI Insights
		Clients	Network Operations > Global > Clients > Client Name > AI Insights Network Operations > Site > Clients > Client Name > AI Insights
Clients with High Number of Wi-Fi Association Failures	Connectivity — Wi-Fi	Global	Network Operations > Global > Overview > AI Insights
		Site	Network Operations > Sites > Overview > AI Insights
		Access Points	Network Operations > Global > Devices > Access Points > Device Name > AI Insights
		Clients	Network Operations > Global > Clients > Client Name > AI Insights Network Operations > Site > Clients > Client Name > AI Insights

Cards

All the insights in Aruba Central (on-premises) display certain cards with additional information specific to that insight. The top view of each card usually shows the most impacted data in a pie chart or a bar graph view. The data in a pie chart can be modified based on your requirement. To highlight specific entries in a card, click the checkbox next to each label. For few cards there is further drill down available, in the form of a drop-down. The cards might vary for each insight based on the context the insight is accessed from.

The following table displays the card details available in different insights:

Table 184: Cards

Cards	Description
Access Points	The Access Point card displays the number of APs impacted by an Insight. Click the arrow  to expand the card and view the top 5 APs where the issue occurred. You can also click the drop-down list to view further details about the impacted access points.
Site	The Site card displays the number of sites impacted by an Insight. Click the arrow  to expand the card and view the top 5 sites where the issue occurred.
Client	The Client card displays the number of clients impacted by an insight. Click the arrow  to expand the card and view the top 5 clients where the issue occurred.
Server	The Server card displays the number of servers impacted by an insight. Click the arrow  to expand the card and view the top 5 servers where the issue occurred.

If you click on the number displayed on each card, further details specific to that card is displayed in a tabular format. The  filter icon allows you to filter data in each column. The  and  icons allows you to sort the columns in ascending and descending order. Few columns are displayed by default whereas, there are few columns which does not appear in the table by default.

To customize a table, click the ellipses  icon to select the required columns, or click Reset to default to set the table to the default column. Click  to download the card details in a CSV format.

Clients with High Number of Wi-Fi Association Failures

The **Clients had a high number of Wi-Fi Association failures** insight can be accessed from the **Global**, **Site**, **Access Points**, and **Clients** context. This insight provides information on Wi-Fi association failures observed in the network. It is categorized under connectivity since the users are unable to connect to the WiFi network. This insight displays the following information:

- [Insight Summary](#)
- [Time Series Graph](#)
- [Cards](#)

Insight Summary

The insight summary provides the following details:

- **Reason**—Displays the possible causes for which the failure occurred.
- **Recommendation**—Displays the possible recommendation against each failure to resolve the same.
- **Failures**—Displays the exact number and percentage of failures that occurred against each failure reason.

Time Series Graph

The time series graph displays the number of association failures observed in the network during the selected time period. You can hover your mouse over each bar graph to see the exact number of failures.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 185: *Cards Context*

Cards	Context
Site	Global
Access Point	Global, Site, Client
Client	Global, Site, Device

Site

Lists the number of sites that experienced association authentication failures in the network. Click the arrow  to view a pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight.
- **Failures**—Number and percentage of failures occurred in each site.
- **Total**—Total number of association failures in each site.

Access Point

Lists the number and the details of APs that experienced association failures in the network. Click the arrow  to view a pictorial graph of the **Most Impacted** access points. Click the **Access Point** drop-down list to view the following:

- **SSID**—Pictorial graph of the percentage of association failures sorted by SSIDs.
- **Model**—Pictorial graph of the percentage of association failures sorted by AP models.
- **FW Version**—Pictorial graph of the percentage of association failures sorted by AP firmware version.

Click the number displayed on the **Access Point** card, to view the detailed description of the impacted access points:

- **AP Name**—Name of the access points and link to the specific insight at the AP context.
- **AP MAC**—MAC address of the AP link to the specific insight at the AP context.
- **Failures**—Number and percentage of failures occurred in each AP.
- **Total**—Total number of failures in each AP.
- **Serial**—Serial number of the AP.
- **IP**—IP address of the AP.
- **Model**—Model number of each AP.

- **FW Version**—Version of the firmware running on each AP.
- **Site**—Name of the site where the AP resides.

Client

Lists the MAC address, name, host name, and auth ID of clients that experienced association failures in the network. Click the arrow  to view the pictorial graph of the **Most Impacted** clients. Click the number displayed on the **Client** card, to view a detailed description of the impacted clients:

- **Client Name**—Name of the impacted client and link to the specific insight at the client context.
- **Client MAC**—MAC address of the client and link to the specific insight at the client context.
- **Failures**—Number and percentage of failures occurred in each client.
- **Total**—Total number of failures in each client.
- **Client OS**—OS type of the device.

Clients with High Number of MAC Authentication Failures

The **Clients had an unusual number of MAC authentication failures** insight can be accessed from the **Global, Site, Access Points, and Clients** context. This insight provides information on excessive MAC authentication failures observed in the network and is categorized under connectivity since the users are unable to connect to the Wi-Fi network. It also helps in order to identify the rogue users in a network. This insight displays the following information:

- [Insight Summary](#)
- [Time Series Graph](#)
- [Cards](#)

Insight Summary

The insight summary provides the following details:

- **Reason**—Displays the possible causes for which the failure occurred.
- **Recommendation**—Displays the recommendation against each failure to resolve the same.
- **Failures**—Displays the exact number and percentage of failures that occurred against each failure reason.

Time Series Graph

The time series graph displays the number of MAC authentication failures that occurred during the selected time period. You can hover your mouse over each bar graph to see the exact number of failures.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Cards Context

Cards	Context
Site	Global
Access Point	Global, Site, Client

Cards	Context
Client	Global, Site, Device

Site

Lists the number of sites that experienced MAC authentication failures in the network. Click the arrow  to view a pictorial graph with the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight and link to the specific insight at the site context.
- **Failures**—Number of failures occurred in each site.
- **Total**—Total number of MAC authentication in each site.

Access Point

Lists the number and the details of APs that faced the MAC authentication failures in the network. Click the arrow  to view a pictorial graph of the **Most Impacted** access points. Click the **Access Point** drop-down list to view the following:

- **SSID**—Pictorial graph of the percentage of MAC authentication failures sorted by SSIDs.
- **Model**—Pictorial graph of the percentage of MAC authentication failures sorted by AP models.
- **FW Version**—Pictorial graph of the percentage of MAC authentication failures sorted by AP firmware version.

Click the number displayed on the **Access Point** card, to view the detailed description of the impacted access points:

- **Name**—Name of the access points and link to the specific insight at the AP context.
- **MAC**—MAC address of the AP and link to the specific insight at the AP context.
- **Failures**—Number of failures occurred in each AP.
- **Total**—Total number of MAC authentication in each AP.
- **Serial**—Serial number of the AP
- **IP**—IP address of each AP.
- **Model**—Model number of each AP.
- **FW Version**—Version of the firmware running on each AP.
- **Site**—Name of the site where the AP resides.

Client

Lists the MAC address, name, host name, and auth ID of clients that failed MAC authentication. Click the arrow  to view the pictorial graph of the **Most Impacted** clients. Click the number displayed on the **Client** card, to view a detailed description of the impacted clients:

- **Name**—Name of the impacted client and link to the specific insight at the client context.
- **MAC**—MAC address of the client and link to the specific insight at the client context.
- **Failures**—Number of failures occurred in each client.
- **Client OS**—OS type of the device.

Clients with DHCP Server Connection Problems

The **Clients had DHCP server connection problems** insight can be accessed from the **Global, Site, Access Points**, and **Clients** context. This insight provides information on excessive client to AP DHCP failures observed in the network. This insight occurs when Wi-Fi clients attempt to acquire a DHCP IP address multiple times but fails to do so. **Clients had DHCP server connection problems** insight is categorized under connectivity since the users fail to get an IP address and are unable to connect to the Wi-Fi network. It displays the following information:

- [Insight Summary](#)
- [Time Series Graph](#)
- [Cards](#)

Insight Summary

The insight summary provides the following details:

- **Reason**—Displays the possible causes for which the failure occurred.
- **Recommendation**—Displays the possible recommendation against each failure to resolve the same.
- **Failures**—Displays the exact number and percentage of failures that occurred against each failure reason.

Time Series Graph

The time series graph displays the number of DHCP failures that occurred during the selected time period. You can hover your mouse over each bar graph to see the exact number of failures.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 186: *Cards Context*

Cards	Context
Site	Global
Server	Global, Site, Device, Client
Access Point	Global, Site, Client
Client	Global, Site, Device

Site

Lists the number of sites that experience DHCP server connection problems in the network. Click the arrow  to view a pictorial graph with the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight and link to the specific insight at the site context.
- **Failures**—Number and percentage of failures occurred in each site.
- **Total**—Total number of DHCP requests.

Server

Lists the number of DHCP servers involved in this insight. Click the arrow  to view the pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Server** card, to view a detailed description of the impacted servers:

- **Server IP**—IP address of the server impacted by this insight.
- **Failures**—Number of failures occurred in each server.
- **Total**—Total number of DHCP requests.

Access Point

Lists the number and the details of the DHCP server connection problems observed in an AP. Click the arrow  to view a pictorial graph of the **Most Impacted** access points. Click the **Access Point** drop-down list to view the following:

- **SSID**—Pictorial graph of the percentage of DHCP failures sorted by SSIDs.
- **Model**—Pictorial graph of the percentage of DHCP failures sorted by AP models.
- **FW Version**—Pictorial graph of the percentage of DHCP failures sorted by AP firmware version.

Click the number displayed on the **Access Point** card, to view the detailed description of the impacted access points:

- **AP Name**—Name of the access points and link to the specific insight at the AP context.
- **AP MAC**—MAC address of the AP and link to the specific insight at the AP context.
- **Failures**—Number of failures occurred in each AP.
- **Total**—Total number of DHCP requests.
- **Serial**—Serial number of the AP
- **IP**—IP address of each AP.
- **Model**—Model number of each AP.
- **FW Version**—Version of the firmware running on each AP.
- **Site**—Site name of the AP where the failure occurred.

Client

Lists the MAC address, host name, and auth ID of clients that failed DHCP handshake. Click the arrow  to view the pictorial graph of the **Most Impacted** clients. Click the number displayed on the **Client** card, to view a detailed description of the impacted clients:

- **Client Name**—Name of the impacted client and link to the specific insight at the client context.
- **Client MAC**—MAC address of the client and link to the specific insight at the client context.
- **Failures**—Number of failures occurred in each client.
- **Total**—Total number of DHCP requests.
- **Client OS**—OS type of the device.

Clients with High Wi-Fi Security Key-Exchange Failures

The **Clients had excessive Wi-Fi security key-exchange failures** insight can be accessed from the **Global, Site, Access Points, and Clients** context. This insight provides information on excessive Wi-Fi security key-exchange failures observed in the network. When this failure occurs, users connecting to Wi-Fi

using PSK or 802.1x authentication, experience higher EAPOL Key exchange failures. This insight is categorized under connectivity since the users are unable to connect to the WiFi network. This insight displays the following information:

- [Insight Summary](#)
- [Time Series Graph](#)
- [Cards](#)

Insight Summary

The insight summary provides the following details:

- **Reason**—Displays the possible causes of Wi-Fi security key-exchange failure in the network.
- **Recommendation**—Displays the possible recommendation against each failure to resolve the same.
- **Failures**—Displays the exact number and percentage of failures that occurred against each failure reason.

Time Series Graph

This time series bar graph displays the number of Wi-Fi security key-exchange failures that occurred in the network during the selected time period. You can hover your mouse on each bar graph to see the exact number of failures.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 187: *Cards Context*

Cards	Context
Site	Global
Access Point	Global, Site, Client
Client	Global, Site, Device

Site

Lists the number of sites that experienced excessive Wi-Fi security key-exchange failures in the network.

Click the arrow  to view the pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight and link to the specific insight at the site context.
- **Failures**—Number and percentage of failures occurred in each site.
- **Total**—Total number of failures in each site.

Access Point

Lists the number APs that experienced Wi-Fi security key-exchange failures in the network. Click the arrow  to view the pictorial graph of the **Most Impacted** access points. Click the **Access Point** drop-down list, to view the following:

- **SSID**: Pictorial graph of 4-way handshake authentication failures sorted by SSIDs.
- **Model**: Pictorial graph of 4-way handshake failures classified by AP models.
- **FW Version**: Pictorial graph of 4-way handshake failures classified by AP firmware versions.

Click the number displayed on the **Access Point** card to view a detailed description of the impacted access points:

- **AP Name**—Name of the access points and link to the specific insight at the AP context.
- **AP MAC**—MAC address of the AP and link to the specific insight at the AP context.
- **Failures**—Number and percentage of failures occurred in each AP.
- **Total**—Total number of failures in each AP.
- **Serial**—Serial number of the AP.
- **IP**—IP address of the AP.
- **Model**—Model number of each AP.
- **FW Version**—Version of the firmware running on each AP.
- **Site**—Name of the site where the AP resides.

Client

Lists the MAC Address, name, host name, and auth ID of clients that failed Wi-Fi security key-exchange authentication. Click the arrow  to view the pictorial graph of the **Most Impacted** clients. Click the number displayed on the **Client** card, to view a detailed description of the impacted clients:

- **Client Name**—Name of the impacted client and link to the specific insight at the client context.
- **Client MAC**—MAC address of the client and link to the specific insight at the client context.
- **Failures**—Number and percentage of failures occurred in each client.
- **Total**—Total number of failures in each client.
- **Client OS**—OS type of the device.

Clients with High 802.1X Authentication Failures

The **Clients had excessive 802.1x authentication failures** insight can be accessed from the **Global**, **Site**, **Access Points**, and **Clients** context. This insight provides information on excessive 802.1X authentication failures observed in the network. It is categorized under connectivity since the users are unable to connect to the WiFi network. This insight displays the following information:

- [Insight Summary](#)
- [Time Series Graph](#)
- [Cards](#)

Insight Summary

The insight summary provides the following details:

- **Reason**—Displays the possible causes for which the failure occurred.
- **Recommendation**—Displays the possible recommendation against each failure to resolve the same.
- **Failures**—Displays the exact number and percentage of failures that occurred against each failure reason.

Time Series Graph

The time series graph displays the number of 802.1X authentication failures observed in the network during the selected time period. You can hover your mouse over each bar graph to see the exact number of failures.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 188: *Cards Context*

Cards	Context
Site	Global
Server	Global, Site, Device, Client
Access Point	Global, Site, Client
Client	Global, Site, Device

Site

Lists the number of sites that experienced 802.1X authentication failures in the network. Click the arrow  to view a pictorial graph with the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight and link to the specific insight at the site context.
- **Failures**—Number and percentage of failures occurred in each site.
- **Total**—Total number of 802.1X authentication in each site.

Server

Lists the number of servers that failed 802.1X authentication in the network. Click the arrow  to view the pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Server** card, to view a detailed description of the impacted servers:

- **Server IP**—IP address of each server.
- **Failures**—Number of 802.1X authentication failures in each server.
- **Total**—Total number of 802.1X authentication.

Access Point

Lists the number and the details of APs that failed 802.1X authentication in the network. Click the arrow

 to view a pictorial graph of the **Most Impacted** access points. Click the **Access Point** drop-down list to view the following:

- **SSID**—Pictorial graph of the percentage of 802.1X authentication failures sorted by SSIDs.
- **Model**—Pictorial graph of the percentage of 802.1X authentication failures sorted by AP models.
- **FW Version**—Pictorial graph of the percentage of 802.1X authentication failures sorted by AP firmware version.

Click the number displayed on the **Access Point** card, to view the detailed description of the impacted access points:

- **AP Name**—Name of the access points and link to the specific insight at the AP context.
- **MAC**—MAC address of the AP and link to the specific insight at the AP context.
- **Failures**—Number and percentage of failures occurred in each AP.
- **Total**—Total number of failures in each AP.
- **Serial**—Serial number of the AP.
- **IP**—IP address of the AP.
- **Model**—Model number of each AP.
- **FW Version**—Version of the firmware running on each AP.
- **Site**—Name of the site where the AP resides.

Client

Lists the MAC address, name, host name, and auth ID of clients that failed 802.1X authentication. Click the

arrow  to view the pictorial graph of the **Most Impacted** clients. Click the number displayed on the **Client** card, to view a detailed description of the impacted clients:

- **Client Name**—Name of the impacted client and link to the specific insight at the client context.
- **Client MAC**—MAC address of the client and link to the specific insight at the client context.
- **Failures**—Number and percentage of failures occurred in each client.
- **Total**—Total number of failures in each client.
- **Client OS**—OS type of the device.

Clients with Captive Portal Authentication Problems

The **Clients had problems authenticating with the Captive Portal** insight can be accessed from the **Global, Site, Access Points, and Clients** context. This insight provides information on captive portal failures observed in the network. It is categorized under connectivity since the users are unable to connect to the WiFi network. This insight displays the following information:

- [Insight Summary](#)
- [Time Series Graph](#)
- [Cards](#)

Insight Summary

The insight summary provides the following details:

- **Reason**—Displays the possible causes for which the failure occurred.
- **Recommendation**—Displays the possible recommendation against each failure to resolve the same.
- **Failures**—Displays the exact number and percentage of failures that occurred against each failure reason.

Time Series Graph

The time series graph displays the number of client captive portal failures observed in the network during the selected time period. You can hover your mouse over each bar graph to see the exact number of failures.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 189: *Cards Context*

Cards	Context
Site	Global
Access Point	Global, Site, Client
Client	Global, Site, Device

Site

Lists the number of sites that experienced captive portal failures in the network. Click the arrow  to view a pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight.
- **Failures**—Number and percentage of failures occurred in each site.
- **Total**—Total number of captive portal authentication in each site.

Access Point

Lists the number and the details of APs that failed captive portal authentication in the network. Click the arrow  to view a pictorial graph of the **Most Impacted** access points. Click the **Access Point** drop-down list to view the following:

- **SSID**—Pictorial graph of the percentage of captive portal authentication failures sorted by SSIDs.
- **Model**—Pictorial graph of the percentage of captive portal authentication failures sorted by AP models.
- **FW Version**—Pictorial graph of the percentage of captive portal authentication failures sorted by AP firmware version.

Click the number displayed on the **Access Point** card, to view the detailed description of the impacted access points:

- **AP Name**—Name of the access points and link to the specific insight at the AP context.
- **AP MAC**—MAC address of the AP link to the specific insight at the AP context.

- **Failures**—Number and percentage of failures occurred in each AP.
- **Total**—Total number of failures in each AP.
- **Serial**—Serial number of the AP.
- **IP**—IP address of the AP.
- **Model**—Model number of each AP.
- **FW Version**—Version of the firmware running on each AP.
- **Site**—Name of the site where the AP resides.

Client

Lists the MAC address, name, host name, and auth ID of clients that failed captive portal authentication.

Click the arrow  to view the pictorial graph of the **Most Impacted** clients. Click the number displayed on the **Client** card, to view a detailed description of the impacted clients:

- **Client Name**—Name of the impacted client and link to the specific insight at the client context.
- **Client MAC**—MAC address of the client and link to the specific insight at the client context.
- **Failures**—Number and percentage of failures occurred in each client.
- **Total**—Total number of failures in each client.
- **Client OS**—OS type of the device.

AOS-CX Switch Ports with High Power-over-Ethernet Problems

The **CX Switch ports had a high number with Power-over-Ethernet problems** insight can be accessed from the **Global**, **Site**, and **Switches** context. This insight provides information on the switches that have not received required power from PoE devices connected to them. PoE issues occur in switches when power is denied, or power is demoted from the device connected to them. It is categorized under availability since the impacted switches are unable to receive sufficient power. This insight displays the following information:

- [Time Series Graph](#)
- [Cards](#)

Time Series Graph

In **Global** and **Site** context the time series graph displays the count of switches experiencing power issues in the network during the selected time period. You can hover your mouse on each bar graph to see the number of impacted switches during the selected time under each severity. In the **Device** context this graph displays the severity level of the selected switch experiencing power issues during the selected time period.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 190: *Cards Context*

Cards	Context
Site	Global

Cards	Context
Switch	Global, Site
Wired Clients	Global, Site

Site

Lists the number of sites where switches have PoE issue. Click the arrow  to view the pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site where the impacted switch resides and link to the specific insight at the site context.
- **Events**—Number of events generated pertaining to PoE failures in each site.
- **Ports**—Number of ports for which power is denied.
- **Switches**—Number of switches for which power is denied.
- **Impact (Minutes)**—Amount of time (minutes) for which power is denied in each site.

Switch

Lists the number of switches that experience PoE issues in the network. Click the arrow  to view the pictorial graph of the **Most Impacted** switches. Click the **Switch** drop-down list to view the following:

- **Switch Model**—Pictorial graph of PoE issues classified by switch models.
- **FW Version**—Pictorial graph of PoE issues classified by switch firmware versions.

Click the number displayed on the **Switch** card to view a detailed description of the impacted switches:

- **Switch Name**—Name of the switch experiencing power issues and link to the specific insight at the switch context.
- **Serial**—Serial number of the impacted switch and link to the specific insight at the switch context.
- **Events**—Number of events generated pertaining to PoE failures in each switch.
- **Wired Clients**—Number of clients impacted by the PoE failures.
- **Impact (Minutes)**—Amount of time (minutes) for which power is denied in each switch.
- **Stack ID**—Stack ID of the impacted switch.
- **Number of Events**—Number of events generated pertaining to PoE failures in each switch.
- **Model**—Model number of the impacted switch.
- **FW Version**—Version of the firmware running on each switch.
- **Site**—Name of the site where the switch exists.

Wired Clients

Lists the MAC Address, name, host name, and auth ID of the clients connected to a switch that experience PoE issues. Click the arrow  to view the pictorial graph of the **Most Impacted** clients. Click the **Wired Clients** drop-down list to view the following:

- **Model**—Pictorial graph of all the device types models connected to the impacted switch.
- **Vendor**—Pictorial graph of the device type vendors connected to the impacted switch.

Click the number displayed on the **Wired Clients** card to view a detailed description of the impacted switches:

- **Wired Client**—Name of the client.
- **Client MAC**—MAC address of the client.
- **Description**—An overview of the connected devices, including the OS type, model, and version.
- **Switch Name**—Name of the impacted switch where the client resides and link to the specific insight at the switch context.
- **Serial**—Serial number of the impacted switch and link to the specific insight at the switch context.
- **Stack ID**—Stack ID of the impacted switch where the client resides.
- **Port Number**—Port number of the switch the client device is connected to.
- **Power Requested/Offered**—PoE consumption for each client.
- **Reason**—Cause of the denied PoE power in each client.
- **Status**—Status of client.
- **Model**—Hardware model of the impacted switch where the client resides.
- **Vendor**—Vendor of the wired client.
- **Site**—Name of the site where the client resides.

AOS-Switch Ports with High Power-over-Ethernet Problems

The **PVOS Switch ports had a high number with Power-over-Ethernet problems** insight can be accessed from the **Global**, **Site**, and **Switches** context. This insight provides information on the switches that have not received required power from PoE devices connected to them. PoE issues occur in switches when power is denied, or power is demoted from the device connected to them. It is categorized under availability since the impacted switches are unable to receive sufficient power. This insight displays the following information:

- [Time Series Graph](#)
- [Cards](#)

Time Series Graph

In **Global** and **Site** context the time series graph displays the count of switches experiencing power issues in the network during the selected time period. You can hover your mouse on each bar graph to see the number of impacted switches during the selected time under each severity. In the **Device** context this graph displays the severity level of the selected switch experiencing power issues during the selected time period.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 191: *Cards Context*

Cards	Context
Site	Global
Switch	Global, Site
Wired Clients	Global, Site

Site

Lists the number of sites where switches have PoE issue. Click the arrow  to view the pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site where the impacted switch resides and link to the specific insight at the site context.
- **Events**—Number of events generated pertaining to PoE failures in each site.
- **Ports**—Number of ports for which power is denied.
- **Switches**—Number of switches for which power is denied.
- **Impact (Minutes)**—Amount of time (minutes) for which power is denied in each site.

Switch

Lists the number of switches that experience PoE issues in the network. Click the arrow  to view the pictorial graph of the **Most Impacted** switches. Click the **Switch** drop-down list to view the following:

- **Switch Model**—Pictorial graph of PoE issues classified by switch models.
- **FW Version**—Pictorial graph of PoE issues classified by switch firmware versions.

Click the number displayed on the **Switch** card to view a detailed description of the impacted switches:

- **Switch Name**—Name of the switch experiencing power issues and link to the specific insight at the switch context.
- **Serial**—Serial number of the impacted switch and link to the specific insight at the switch context.
- **Events**—Number of events generated pertaining to PoE failures in each switch.
- **Wired Clients**—Number of clients impacted by the PoE failures.
- **Impact (Minutes)**—Amount of time (minutes) for which power is denied in each switch.
- **Stack ID**—Stack ID of the impacted switch.
- **Number of Events**—Number of events generated pertaining to PoE failures in each switch.
- **Model**—Model number of the impacted switch.
- **FW Version**—Version of the firmware running on each switch.
- **Site**—Name of the site where the switch exists.

Wired Clients

Lists the MAC Address, name, host name, and auth ID of the clients connected to a switch that experience PoE issues. Click the arrow  to view the pictorial graph of the **Most Impacted** impacted clients. Click the **Wired Clients** drop-down list to view the following:

- **Model**—Pictorial graph of all the device types models connected to the impacted switch.
- **Vendor**—Pictorial graph of the device type vendors connected to the impacted switch.

Click the number displayed on the **Wired Clients** card to view a detailed description of the impacted switches:

- **Wired Client**—Name of the client.
- **Client MAC**—MAC address of the client.
- **Description**—An overview of the connected devices, including the OS type, model, and version.

- **Switch Name**—Name of the impacted switch where the client resides and link to the specific insight at the switch context.
- **Serial**—Serial number of the impacted switch and link to the specific insight at the switch context.
- **Stack ID**—Stack ID of the impacted switch where the client resides.
- **Port Number**—Port number of the switch the client device is connected to.
- **Power Requested/Offered**—PoE consumption for each client.
- **Reason**—Cause of the denied PoE power in each client.
- **Status**—Status of client.
- **Model**—Hardware model of the impacted switch where the client resides.
- **Vendor**—Vendor of the wired client.
- **Site**—Name of the site where the client resides.

All Clients

The **Clients** page provides a summary view of all the clients connected to the network. You can filter clients based on the network the clients are connected to. The page displays key client information and also allows you to view a specific client detail page.

By default, the **Clients** page displays a unified list of clients for the selected group. The list of clients is populated for a time range of 3 hours. To view the list of clients for a different time range, click the **Time Range Filter** link and select the required time period. Total data usage for the selected time period is displayed above the client summary bar.

To filter clients based on the device to which the clients are connected, select the device type from the **Clients** drop-down list:

- **All**—Displays a unified list of clients connected to the network.
- **AP**—Displays a list of clients connected to the Instant AP.
- **Switch**—Displays a list of clients connected to the switch.
- **Controller**—Displays a list of clients connected to the Aruba Controller.



The wired client will show up in the **Clients** page only if the client is connected to an Aruba 2540 Series, Aruba 2920 Series, Aruba 2930F Series, Aruba 2930M Series, Aruba 3810 Series, or Aruba 5400R Series switch.

To filter clients based on the network to which the clients are connected, click the network type from the **Client Summary** bar:

- **Wireless**—Displays a list of clients connected to the wireless network. The wireless clients are denoted by the  icon.
- **Wired**—Displays a list of clients connected to the wired network. The wired clients are denoted by the  icon.
- **Remote**—Displays a list of clients connected through VPN. The remote clients are denoted by the  icon.

The **Clients** table lists the details of each client. By default, **All** clients is selected and the table displays the following columns: **Client Name**, **Status**, **IP Address**, **Connected To**, **VLAN**, **SSID/Port**, **AP Role**, **Controller Role**, and **Health**.

The following functions are available in the table:

- Click [↓](#) to download the client details in the .csv file format.
- Click [☰](#) to select more columns or reset the table view to the default columns.
- If a filter icon appears next to the column header, click and enter the filter criteria or select a filter criteria. For example, to search a client, click the predefined filter criteria: **Connecting**, **Connected**, **Offline**, **Failed**, or **Blocked** from the **Client Summary** bar and in the **Client Name** column enter the name of the client.
- To disconnect a wireless client, hover over the corresponding wireless client and click **Disconnect from AP**. For more details, see [Disconnecting a Wireless Client from an AP](#).

Table 192: *Unified Client List View*

Column	Applicability	Description
Client Name	<ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Controller 	Username, hostname, or MAC address of the client. Click the client name to view the client details page.
Status	<ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Controller 	<p>Client connection status. Use the filter option to view the following:</p> <ul style="list-style-type: none"> ■ Connecting clients ■ Connected clients ■ Offline clients ■ Failed clients ■ Blocked clients <p>Hover your mouse over the status to view:</p> <ul style="list-style-type: none"> ■ Client name ■ IP address ■ Connected—Date and time at which the client connected. ■ Offline—Last seen time. ■ Failed—Failure reason and last seen time.
IP Address	<ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Controller 	IP address of the client.
VLAN	<ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Controller 	VLAN of the device to which the client is connected.
Connected To	All	AP name, Switch name, or Controller name. This is the first layer 2 hop for the client. If the device does not have a name, the MAC address is displayed.
SSID/Port	<ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Controller 	Displays the SSID for wireless clients and the port number for wired clients. The column title displays SSID and Port interchangeably based on the device filters. For APs, the column title displays SSID . For switch and controller, the column title displays as Port .
AP Role	AP	Role assigned by the Instant AP.

Table 192: Unified Client List View

Column	Applicability	Description
Controller Role	Controller	Role assigned by the Aruba Controller.
Health	AP	Client health. The value can be one of the following: <ul style="list-style-type: none"> ■ Good—71-100. ■ Fair—31-70. ■ Poor—0-30.
Failure Stage	AP	Stage of the connection where the client failed to connect. The failure reasons could be: <ul style="list-style-type: none"> ■ Association failure ■ MAC authentication failure ■ 802.1X authentication failure ■ Key exchange failure ■ DHCP failure ■ Captive Portal failure
Group Name	<ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Controller 	Group name of the device managed by Aruba Central.
Site Name	<ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Controller 	Name of the site in which the devices managed by Aruba Central are installed.
MAC Address	<ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Controller 	MAC address of the client. NOTE: The filter criteria supports all delimiters in the MAC address. For example, if you search a MAC address with a comma, it is automatically converted to semicolon and the corresponding result is displayed.
Hostname	<ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Controller 	Host name of the client.
User Name	<ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Controller 	Username of the client.
Key Management	AP	Security mode used by the client.
Authentication	<ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Controller 	Authentication type used by the client to connect with the device.

Table 192: Unified Client List View

Column	Applicability	Description
Global Unicast IPv6 Address	<ul style="list-style-type: none"> ■ All ■ AP ■ Controller 	When the IPv6 address is present for a client, you can view its Global Unicast IPv6 address. Click the ellipsis and select the column to view the value if the column is not displayed.
Link Local IPv6 Address	<ul style="list-style-type: none"> ■ All ■ AP ■ Controller 	When the IPv6 address is present for a client, you can view its Link Local IPv6 address. Click the ellipsis and select the column to view the value if the column is not displayed.
Capabilities	AP	Client 802.11 capabilities.
Usage	<ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Controller 	Total data usage for the selected time period.
OS	<ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Controller 	Operating system of the client.
Last Seen Time	<ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Controller 	Date and time at which the client was last seen.
Connected Since	<ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Controller 	Date and time since when the client was connected.
AP Name	AP	Name of the Instant AP.
AP Mac Address	AP	MAC address of the Instant AP.
Channel/Band	AP	Last connected channel and band.
Switch Name	<ul style="list-style-type: none"> ■ All ■ Switch 	Name of the switch.
Port	<ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Controller 	Port number of the switch.
Controller Name	<ul style="list-style-type: none"> ■ All ■ Controller 	Name of the Aruba Controller.
Tunneled	<ul style="list-style-type: none"> ■ All 	Tunnel mode applicable for the Aruba Gateway managed WLAN, UBT, or PBT client.

Table 192: Unified Client List View

Column	Applicability	Description
	<ul style="list-style-type: none"> ■ AP ■ Switch ■ Controller 	
Segmentation	<ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Controller 	<p>Type of segmentation. The type of segmentation can be:</p> <ul style="list-style-type: none"> ■ None ■ UBT ■ PBT ■ Underlay ■ Overlay <p>NOTE: To view the details about dynamic segmentation, a gateway must be licensed in Aruba Central and connected to the switch.</p>

Client Overview

The Clients page displays the details of clients connected to the devices and their connectivity status.

To view the clients overview page:

1. In the **Network Operations** app, use the filter bar to select a group, label, site, or a device.
2. Under **Manage**, click **Clients**. The All Clients overview page is displayed.
3. Click the  icon to view the client overview page.

The overview page displays the total number of clients, bandwidth usage, and the application usage by the clients connected to the wired and wireless networks. The following table describes the information displayed in each section:

Table 193: Client Overview Page

Data Pane Content	Description
Time Range Filter	By default, the graphs on the Clients page are plotted for a time range of 3 hours. To view the graphs for a different time range, click the Time Range Filter link. You can choose to view graphs for a time period of 3 hours, 1 day, 1 week, 1 month and 3 months. However, the Distribution data (Client OS) under the Distribution tab does not honor the time range you selected in the time range filter.
Total	Displays the total number of clients.
Wireless	Displays the total number of clients connected to wireless network.
Wired	Displays the total number of clients connected to the wired network.
Remote	Displays the total number of remote clients connected through VPN.

Data Pane Content	Description
Usage	Displays the Bandwidth Usage and Remote Bandwidth Usage of the incoming and outgoing throughput traffic for all clients and remote clients during a specific time range in kilobits per second (Kbps). The graph will not show any data for the clients that are connected to the network for less than two hours.
Distribution	Displays the type of client device connected to the wireless network.
Top N	Displays a list of clients connected to the currently available SSIDs that utilize the maximum bandwidth in the network. The Top Clients by Usage table displays data only for the clients that are connected to the network for a total duration of two or more hours.

Client Details

The **Clients** page displays the number of clients connected to the wireless, wired, or remote networks. By default, the **Clients** page displays a unified list of clients for the selected group.

The client details page shows a summary of the client and allows you to navigate to the corresponding device details page.



The wired client shows up in the **Clients** page only if the client is connected to an Aruba 2540 Series, Aruba 2920 Series, Aruba 2930F Series, Aruba 2930M Series, Aruba 3810 Series, or Aruba 5400R Series switch.

This section includes the following topics:

- [Wireless Client Details](#)
- [Wired Client Details](#)
- [Remote Client Details](#)

Wireless Client Details

The wireless client overview page displays the client summary details, applications, and events details for the selected client.

This section includes the following topics:

- [Viewing Clients Connected to Wireless Networks](#)
- [Summary](#)
- [Overview](#)
- [Disconnecting a Wireless Client from an AP](#)
- [Blocking a Wireless Client from an AP](#)
- [Applications](#)
- [Events](#)

Viewing Clients Connected to Wireless Networks

To view the details of a client connected to the wireless network:

1. In the **Network Operations** app, use the filter bar to select a group or a device.
2. Under **Manage**, click **Clients**. The clients overview page is displayed.

3. Click the list icon to view the client table.
4. By default, the **Clients** table displays a unified list of clients for the selected group.
5. Click the client name to view the client details page. If there are many clients connected to the network, click **Wireless** to filter the clients connected to the wireless network and enter the client name in the **Client Name** column and then click the client name. The **Summary** page is displayed.

Summary

The client summary page displays the following information:

Wireless Client Health Bar

Table 194: *Wireless Client Health Bar*

Field	Description
Connection status icon	Displays the icons with the connection status of the client. Connection status is updated immediately on state change. The available statuses are: <ul style="list-style-type: none"> ■ Connecting—Displays a list of client connections that are in progress. ■ Connected—Displays a list of clients that are successfully connected to the network. ■ Failed—Displays a list of all failed client connections. ■ Offline—Displays a list of all offline clients. ■ Blocked—Displays a list of all blocked clients.
Device Health	Signal strength of the client device. The signal strength value is displayed in percentage: 0-30—Poor 31-70—Fair >71—Good
Signal Quality	SNR for the client as measured by the AP. The SNR value is displayed in decibels: 0-20—Poor 21-35—Fair >35—Good
Tx Rx Rate	Data transmission or reception rate.
Connected To	Name of the AP that broadcasts the SSID to which the client is connected. Click the name of the AP to view the device details page.
Refresh icon	Restarts the Live Health Bar session. This icon appears only after 15 minutes of pinning the Health Bar to the Client Details page and it is called as the Live Health Bar because the data is updated every 5 seconds. For more information, see Live Health Bar .

Overview

The **Overview** tab displays information about the type of data path that the client uses, the network and connectivity details, and basic client details such as IP address of the client, type of encryption etc. The following table describes the information displayed in each section:

Table 195: *Client Details*

Section	Description
Data Path	Displays the data path of the client in the network. Click the AP icon to view the AP details page. The data path can be one of the following:

Table 195: Client Details

Section	Description
	<ul style="list-style-type: none"> ■ Client > SSID > AP ■ Client > SSID > AP > Switch ■ Client > SSID > AP > Switch > Controller ■ Client > SSID > AP > Controller
Client	<p>Displays the following information:</p> <ul style="list-style-type: none"> ■ Username—User name of the client. ■ Hostname—Hostname of the client. ■ Client Type—Type of the client device. ■ IP Address—IP address of the client. ■ MAC Address—MAC address of the client. ■ Client OS—Operating system running on the client device. ■ Connected Since—Date and time since when the client is connected. ■ Manufacturer—Manufacturer of the client device. ■ Encryption—Type of client encryption. ■ AI Insights—See AI Insights
Network	<p>Displays the following information:</p> <ul style="list-style-type: none"> ■ VLAN—Displays the VLAN ID on which the client is connected to the AP. ■ Switch Role—Displays the role assigned to the client by the Switch. ■ Role—Displays the role assigned to the client by the AP. ■ Segmentation—Displays the type of dynamic segmentation configured for the client. Supported values are UBT, PBT, Underlay, or Overlay. ■ Auth Server—Server that last authenticated the client device. The field displays the IP address of the server that performed either 802.1X or MAC authentication for the client device. If the client connects to the network through 802.1X and MAC authentication, Aruba Central displays only the IP address of the server that performed 802.1X authentication. ■ DHCP Server—DHCP server that last assigned IP address to the client. ■ Tunneled—Displays whether the client is tunneled or not. ■ Tunnel ID—Displays the tunnel ID the client is connected to.
Connection	<p>Displays the following information:</p> <ul style="list-style-type: none"> ■ Channel—Radio channel assigned to the client. ■ Band—Radio band on which the client is connected. ■ Client Capabilities—Capabilities of the client device. ■ Client Max Speed—Wireless link data transfer speed. ■ LEDs on Access Point—Enables or disables the LED indication on the corresponding AP to which the client is connected. Click Blink LED to enable the blinking of LEDs on the AP. The default blinking time is set to 5 minutes and it stops automatically after 5 minutes. To stop the blinking, click Stop.
Throughput	<p>Displays the incoming and outgoing throughput traffic for the client during a specific time range. By default, the graph on the Throughput pane is plotted for a time range of 3 hours. To view the graph for a different time range, click the Time Range Filter link. You can choose to view the graph for a time period of 3 hours, 1 day, 1 week, 1 month, or 3 months.</p>

Table 195: Client Details

Section	Description
Health	Displays the health score and status of a wireless client. By default, the graph on the Health pane is plotted for a time range of 3 hours. To view the graph for a different time range, click the Time Range Filter link. You can choose to view the graph for a time period of 3 hours, 1 day, 1 week, 1 month, or 3 months. The graph is plotted against the client health and client score, where the client health is measured as Poor , Fair , or Good and the health score ranges between 0 to 100. <ul style="list-style-type: none"> ■ 0-30—Poor ■ 31-70—Fair ■ >71—Good
Signal Quality	Displays the signal quality and the SNR for the wireless client as measured by the AP. The SNR value is displayed in decibels: <ul style="list-style-type: none"> ■ 0-20—Poor ■ 21-35—Fair ■ >35—Good
Retry Frames	Displays the percentage of Tx and Rx retries by a wireless client.
Tx/Rx Rate	Displays the data transmission and reception rate for the wireless client .

Association History

The **Association History** table is available only for Campus APs. It consists of a list of events for client association or disassociation such as when it disconnects from an AP, roams between APs, changes SSID, or change in the radio or BSSID. The table launches only the default parameters, click the **Ellipsis** icon and select all columns to view all the parameters. By default, the data is displayed for a time range of 3 hours. To change the time range, click the **Time Range Filter** link and select the required option as 3 hours, 1 day, 1 week, 1 month, or 3 months. Additionally, you can use the filter option in the **Association Time** column to set a different time range other than the given options. The maximum time range configured for the association history data is seven days.

Click the download icon  to download the association history details as a .csv file.



Fetching details for the **Avg. Speed**, **Total Data Used**, and **Avg. Signal Quality** parameters might encounter a delay of 2 to 3 minutes due to processing the messages in queue. These values are fetched from the stats message and the details are received only if the session duration is more than 5 minutes. Sometimes, these values are not available for 15 minutes if the Aruba Central (on-premises) has not received the message from the device.

Filtering Options:

- The  icon allows to filter a particular item in the column.
- The  icon allows to sort the items of a column in ascending or descending order.

The following table describes the parameters displayed in **Association History**.

Table 196: Association History

Column	Description
Username	Username of the client.
Role	Role of the client.
Association Time	Time stamp of when the client associated or roamed.
Disassociation Time	Time stamp of when the client disassociated or roamed.
Session Duration	Time duration of the connection.
Device	Device to which the client was connected.
VLAN	VLAN of the device to which the client was connected.
SSID	SSID to which the client was connected.
LAN IP Address	LAN IP address of the client.
Controller	Name of the controller.
Avg. Speed	Average speed of the data transferred.
Total Data Used	Total data received and transmitted.
Avg. Signal Quality	Average SNR in dB.
Connection Mode	Mode of connection.
Client MAC Address	MAC address.
Channel Width	Channel width while establishing the connection.
Client OS	OS of the client.
MAC Vendor	MAC address of the vendor.
Cipher	Encryption method.
Key Management	Key management information.

AI Insights

The **AI Insight** tab displays information about client performance and connectivity issues. AI Insights are displayed for a selected time period based on the time selected in **Time Range Filter**. The user can select 3 hours, 1 week, 1 day, or 1 month to view the insight data. **AI Insights** are categorized in high, medium, and low priorities depending on the number of occurrences.

-  Red—High priority
-  Orange—Medium priority
-  Yellow—Low priority

Each insight report specific details on the occurrences of these events for ease in debugging. For more information, see [The AI Insights Dashboard](#)

The client **AI Insights** page displays the following insights:

- [Clients with High Wi-Fi Security Key-Exchange Failures](#)
- [Clients with High 802.1X Authentication Failures](#)
- [Clients with DHCP Server Connection Problems](#)
- [Clients with High Number of MAC Authentication Failures](#)

Live Client Monitoring

Click **Go Live** to start live monitoring of the client. Live monitoring is supported only if the Instant AP is running 8.4.0.0 firmware version. Live monitoring stops after 15 minutes. At any point, you can click **Stop Live** to go back to the historical view.

Five seconds after you start live monitoring, the following data starts getting populated:

- **Throughput**
- **Signal to Noise Ratio (SNR)**

Live Health Bar

The Live Health Bar is present in the **Summary** page for a wireless client. It provides live data every 5 seconds for a session duration of 15 minutes.

To launch the Live Health Bar:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**. The **All Clients** page is displayed.
3. By default, the **Clients** table displays a unified list of clients.
4. Click the client name to view the client details page. If there are many clients connected to the network, click **Wireless** to filter the clients connected to the wireless network.
5. Enter the client name in the **Client Name** column and then click the client name.
The contextual dashboard for the selected client is displayed and opens the **Summary** page by default.
6. Hover over the client name, the **Health Bar** pop-up appears. The pop-up displays the latest values that is updated every 5 seconds.
The Live Health Bar session is for 15 minutes only, after that time period, the refresh icon appears. If you click the refresh icon, the **Live Health Bar** session restarts where the values are updated every 5 seconds.
7. Click the pin icon to pin the **Health Bar** to the **Summary** page for the constant view.

The parameters available in the **Live Health Bar** are:

- **Connection status icon**
- **Device Health**
- **Signal Quality**
- **Tx | Rx Rate**
- **Connected To**

Disconnecting a Wireless Client from an AP

You can disconnect a wireless client using the following pages:

- [List view](#)
- [Client Details](#)



You can disconnect the wireless client from the AP only if the AP is in the online status.

Disconnecting a Client Using the List View

To disconnect a wireless client connected to an AP on the **List** view, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under groups, labels, or sites. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**.
The clients overview page is displayed in **List** view. By default, the **Clients** table displays a unified list of clients.
3. Hover over the wireless client that you want to disconnect and click **Disconnect from AP**.
If there are many clients connected to the network, click **Wireless** to filter the clients connected to the wireless network, enter the client name in the **Client Name** column, and click the client name.
4. Click **Yes** in the dialog box.
The client is disconnected from the AP.

Disconnecting a Client using the Client Details Page

To disconnect a wireless client from an online AP:

1. In the **Network Operations** app, use the filter bar to select a group or a device.
2. Under **Manage**, click **Clients**. The clients overview page is displayed.
3. Click the list icon to view the client table.
4. By default, the **Clients** table displays a unified list of clients for the selected group.
5. Click the name of the wireless client to open the corresponding **Client Details** page. If there are many clients connected to the network, click **Wireless** to filter the clients connected to the wireless network, enter the client name in the **Client Name** column, and click the client name.
6. From the **Actions** drop-down list, click **Disconnect from AP**.

The **Actions** drop-down is disabled if the AP is offline.

To disconnect a wireless client, ensure that there is an established Websocket connection from the controller to Aruba Central.



Blocking a Wireless Client from an AP

To block a wireless client from an online AP:

1. In the **Network Operations** app, use the filter bar to select a group or a device.
2. Under **Manage**, click **Clients**. The clients overview page is displayed.
3. Click the list icon to view the clients table.
4. By default, the **Clients** table displays a unified list of clients for the selected group.
5. Click the name of the wireless client to open the corresponding **Client Details** page. If there are many clients connected to the network, click **Wireless** to filter the clients connected to the wireless network, enter the client name in the **Client Name** column, and click the client name.
6. From the **Actions** drop-down list, click **Block Client**.
The clients is unblocked from the network.



To remove a client from the blocked status, select the blocked client and click **Remove Block** from the **Actions** drop-down list in the **Client Details** page.

Applications

The **Application** page consists of the **Visibility**, **UCC** and **AirGroup** tab.

Visibility

The **Visibility** dashboard provides a summary of client traffic and their data usage to and from applications, and websites. You can also analyze the client traffic flow using the graphs displayed in the **Visibility** dashboard. The tab consists of a list view and a graph view. The **Visibility** dashboard displays metrics and graphs related to client traffic flow in the following sections:

- **Applications**
- **Websites**

For more information about enabling **Application Visibility**, list of supported Instant APs, and the data displayed on the **Applications** and **Websites** sections, see [Application Visibility](#).

UCC

The **UCC** tab displays the detailed call records for the client if any. To view this data, ensure that the **Unified Communication** application service is enabled on the APs. The following table describes the information displayed in each session:

Table 197: *UCC Tab*

Section	Description
Calls	Displays the total number of calls. The call quality is displayed as: <ul style="list-style-type: none"> ■ Good ■ Fair ■ Poor ■ Unknown
Client Health	Displays the health of the client.
Session Type	Displays the type of the call or session. For example, audio, or video, or desktop sharing.
Quality	Displays the quality of the call.

AirGroup

The **AirGroup** displays the details of the servers a client is connected to. The following table describes the information displayed in each session:

Table 198: *AirGroup Tab*

Section	Description
Hostname	Displays the host name.
MAC Address	Displays the MAC address of the server the client is connected to.
IP Address	Displays the IP address.
Role	Displays the user role assigned to the client.
Service	Displays the type of service.
VLAN	Displays the connected VLAN details.
Connected To	Displays the network the client is connected to. Name of the AP that broadcasts the SSID to which the client is connected.

Events

In the **Events** page, the table displays the following columns by default: **Occurred On**, **Event Type**, and **Description**. Click the ellipsis icon to perform additional operations:

- **Autofit columns**—Adjusts the column width of the table to fit the page evenly.
- **Reset to default**—Resets the table view to the default columns.

If a filter icon appears next to the column header, click it and enter the filter criteria or select a filter criteria. The following table describes the information displayed in each event:

Table 199: *Events Tab*

Section	Description
Occurred On	Displays the time at which the event occurred.
Event Type	Displays the type of the event.
Description	Displays the detailed description of the event.
Device MAC	Displays the MAC address of the device.
BSSID	Displays the BSSID.

To download events into a CSV format, click the download button. Aruba Central generates the CSV report of all the events for the selected client.

You can also filter the events based on the type of events, click the **Click here for Advance Filtering**. Select the type of events from the list and click **Filter**. The events under the selected categories get listed in the **Events** table.

Wired Client Details

The wired client overview page displays the client summary details, applications, and events details for the selected client.

This section includes the following topics:

- [Viewing Clients Connected to Wired Networks](#)
- [Overview](#)
- [Applications](#)
- [Events](#)
- [Tools](#)

Viewing Clients Connected to Wired Networks

To view the details of a client connected to the wired network:

1. In the **Network Operations** app, use the filter bar to select a group or a device.
2. Under **Manage**, click **Clients**. The clients overview page is displayed.
3. Click the list icon to view the clients table.
4. By default, the **Clients** table displays a unified list of clients for the selected group.
5. Click the name of the wired client to open the corresponding **Client Details** page. If there are many clients connected to the network, click **Wired** to filter the clients connected to the wired network, enter the client name in the **Client Name** column, and click the client name.

Wired Client Details

The wired client details page displays the client details summary and the client sessions information.

Summary

The client summary page displays the following information:

Wired Client Health Bar

Table 200: *Wired Client Health Bar*

Field	Description
Connection status icon	Displays the icons with the connection status of the client. Connection status is updated immediately on state change. The available statuses are: <ul style="list-style-type: none">■ Connecting—Displays a list of client connections that are in progress.■ Connected—Displays a list of clients that are successfully connected to the network.■ Failed—Displays a list of all failed client connections.■ Offline—Displays a list of all offline clients.■ Blocked—Displays a list of all blocked clients.
Connected Port	Name of the port through which the is connected.
Connected To	Name of the controller to which the client is connected. Click the name of the controller to view the device details page.
Refresh icon	Refreshes the data on the Health Bar for the wired client.

Overview

The **Overview** tab consists of the following sections.

Table 201: *Overview Tab*

Section	Description
Data Path	Displays the data path of the client in the network. Click the device icon to view the corresponding device details page. The data path can be one of the following: <ul style="list-style-type: none">■ Client > Wired Profile > AP■ Client > Wired Profile > AP > Switch■ Client > Wired Profile > AP > Switch > Controller■ Client > Wired Profile > AP > Controller■ Client > Switch■ Client > Switch > Controller■ Client > Controller
Client	Displays the following information: <ul style="list-style-type: none">■ Username—User name of the client.■ Hostname—Hostname of the client.■ Client Type—Type of the client device.■ IP Address—IP address of the client.■ MAC Address—MAC address of the client.■ Client OS—Operating system running on the client device.■ Connected Since—Date and time since when the client is connected.■ Manufacturer—Manufacturer of the client device.
Network	Displays the following information: <ul style="list-style-type: none">■ VLAN—VLAN ID on which the client is connected to the AP.■ Role—Controller role associated to the client.

Applications

To view application usage metrics for the client connected to the wired network, enable **Deep Packet Inspection**.

The **Applications** tab consists of two sections:

- **Applications**—Displays a table with details on the client traffic flow to and from various applications. Click the bar graph icon to view bar graphs indicating the traffic flow.
- **Websites**—Displays a table with details on client traffic flow and their data usage by various websites. Click the bar graph icon to view bar graphs indicating the data usage by various websites.

For more information about enabling **Application Visibility**, list of supported Instant APs, and the data displayed on the **Applications** and **Websites** sections, see [Application Visibility](#).

UCC

The **UCC** tab displays the detailed call records for the client if any. To view this data, ensure that the **Unified Communication** application service is enabled on the APs. The following table describes the information displayed in each session:

Table 202: *UCC Tab*

Section	Description
Calls	Displays the total number of calls. The call quality is displayed as: <ul style="list-style-type: none">■ Good■ Fair■ Poor■ Unknown
Client Health	Displays the health of the client.
Session Type	Displays the type of the call or session. For example, audio, or video, or desktop sharing.
Quality	Displays the quality of the call.

AirGroup

The **AirGroup** displays the details of the servers a client is connected to. The following table describes the information displayed in each session:

Table 203: *AirGroup Tab*

Section	Description
Hostname	Displays the host name.
MAC Address	Displays the MAC address of the server the client is connected to.
IP Address	Displays the IP address.
Role	Displays the user role assigned to the client.
Service	Displays the type of service.
VLAN	Displays the connected VLAN details.
Connected To	Displays the network the client is connected to. Name of the AP that broadcasts the SSID to which the client is connected.

Events

The **Events** page displays the details of events generated by the AP and client association. By default, the table displays the following columns: **Occurred On**, **Event Type**, and **Description**. Click the ellipsis icon to perform additional operations:

- **Autofit columns**—Adjusts the column width of the table to fit the page evenly.
- **Reset to default**—Resets the table view to the default columns.

If a filter icon appears next to the column header, click it and enter the filter criteria or select a filter criteria. The following table describes the information displayed in each event.

Table 204: *Events Tab*

Section	Description
Occurred On	Displays the time at which the event occurred.
Event Type	Displays the type of the event.
Description	Displays the detailed description of the event.
Device MAC	Displays the MAC address of the device.
BSSID	Displays the BSSID.

To download events into a CSV format, click the download button. Aruba Central (on-premises) generates the CSV report of all the events for the selected client.

Tools

The **Tools** page is automatically filtered based on the client you select. This enables network administrators to perform checks on the client and debug client connectivity issues. For more information, see [Using Troubleshooting Tools](#).

Remote Client Details

The remote clients are clients that are connected to the network through VPN. The in-house wireless and wired clients can also be authenticated using the VPN (VIA). The overview page displays the client summary details, applications, and events for the selected remote client.

This section includes the following topics:

- [Viewing Remote Clients Connected through VPN](#)
- [Summary](#)
- [Overview](#)
- [Applications](#)
- [Events](#)

Viewing Remote Clients Connected through VPN

To view the details of a remote client:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**. The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**. The **All Clients** page is displayed.
3. By default, the **Clients** table displays a unified list of clients for the selected group, label, site or device.
4. Click the name of the remote client to open the corresponding **Client Details** page. If there are many clients connected to the network, click **Remote** to filter the clients connected to the network.
5. Enter the client name in the **Client Name** column, and click the client name. The client **Summary** page is displayed.
6. Click the required tab name to navigate and view the details.

Summary

The client summary page displays the following information.

Health Bar

Table 205: *Health Bar*

Field	Description
Connection status icon	Displays the icons with the connection status of the client. Connection status is updated immediately on state change. The available statuses are: <ul style="list-style-type: none">■ Connecting—Displays a list of client connections that are in progress.■ Connected—Displays a list of clients that are successfully connected to the network.■ Failed—Displays a list of all failed client connections.■ Offline—Displays a list of all offline clients.■ Blocked—Displays a list of all blocked clients.
Connected To	Displays the name of the AP that broadcasts the SSID to which the client is connected. Click the name of the AP to view the device details page.

Overview

The **Overview** tab displays information about the type of data path that the client uses, the network and connectivity details, and basic client details such as IP address of the client, type of encryption etc. The following table describes the information displayed in each section:

Table 206: *Remote Client Details*

Section	Description
Data Path	Displays the data path of the client in the network. Click the controller to view the details page. The data path can be Client > Tunnel > Controller
Client	Displays the following information: <ul style="list-style-type: none">■ Username—User name of the client.■ Hostname—Hostname of the client.■ Client Type—Type of the client device.■ Local IP Address—Link local IP address of the client.■ IP Address—IP address of the client.■ MAC Address—MAC address of the client.■ Client OS—Operating system running on the client device.■ Connected Since—Date and time since when the client is connected.
Network	Displays the following information: <ul style="list-style-type: none">■ Controller Role—Displays the role assigned to the client.■ Authentication Type—Displays the authentication method as VIA VPN.
Throughput	Displays the incoming and outgoing throughput traffic for the client during a specific time range. By default, the graph on the Throughput pane is plotted for a time range of 3 hours. To view the graph for a different time range, click the Time Range Filter link. You can choose to view the graph for a time period of 3 hours, 1 day, 1 week, 1 month, or 3 months.

AI Insights

The **AI Insight** tab displays information about client performance and connectivity issues. AI Insights are displayed for a selected time period based on the time selected in **Time Range Filter**. The user can select 3 hours, 1 week, 1 day, or 1 month to view the insight data. **AI Insights** are categorized in high, medium, and low priorities depending on the number of occurrences.

-  Red—High priority
-  Orange—Medium priority
-  Yellow—Low priority

Each insight report specific details on the occurrences of these events for ease in debugging. For more information, see [The AI Insights Dashboard](#)

The client **AI Insights** page displays the following insights:

- [Clients with High Wi-Fi Security Key-Exchange Failures](#)
- [Clients with High 802.1X Authentication Failures](#)
- [Clients with DHCP Server Connection Problems](#)
- [Clients with High Number of MAC Authentication Failures](#)

Applications

The **Application** page consists of the **Visibility** , **UCC** and **AirGroup** tab.

Visibility

The **Visibility** dashboard provides a summary of client traffic and their data usage to and from applications, and websites. You can also analyze the client traffic flow using the graphs displayed in the **Visibility** dashboard. The tab consists of a list view and a graph view. The **Visibility** dashboard displays metrics and graphs related to client traffic flow in the following sections:

- **Applications**
- **Websites**

For more information about enabling **Application Visibility**, list of supported Instant APs, and the data displayed on the **Applications** and **Websites** sections, see [Application Visibility](#).

Sessions

The client sessions page consists of the firewall session details for the client connected to a Branch Gateway. The **Sessions** page displays information filtered by the IP address of the client. The **Sessions Summary** pane displays the device the client is connected to, total number of sessions, and the time stamp of when the page was last refreshed. The sessions details page refreshes automatically, to refresh the page manually, click the refresh icon after the timestamp.

The **Sessions** table lists the details of each session. By default, the table displays the following columns: **Application, Destination IP, Protocol, , Dest Port, DSCP, Flags, Packets, State** and **Action**.

Click the ellipsis icon to perform additional operations:

- **Autofit columns**—Adjusts the column width of the table to fit the page evenly.
- **Reset to default**—Resets the table view to the default columns.

If a filter icon appears next to the column header, click it and enter the filter criteria or select a filter criteria. The following table describes the information displayed in each session:

Table 207: Sessions Tab

Section	Description
Application	Displays the list of applications.
Source IP	Displays the source IP address.
Destination IP	Displays the destination IP address.
Protocol	Displays the communication protocol used.
Source Port	Displays the source port number.
Dest Port	Displays the destination port number.
DSCP	Displays the DSCP value.
Flags	Displays the active flags
Packets	Displays the number of packets.
Bytes	Displays the total number of bytes.
State	Displays the connection state of the application. The state can either be Denied, Active, or Inactive.
Action	Displays the application specific action.
VLAN	Displays the VLAN the client is connected to.
Start Time	Displays the start time.
Receive Time	Displays the receive time.
WebCC Category	Displays the WebCC category.
WebCC Reputation	Displays the WebCC reputation.
WebCC Score	Displays the WebCC score.
Application Category	Displays the application category.
Priority	Displays the priority value.

Events

In the **Events** page, the table displays the following columns by default: **Occurred On**, **Event Type**, and **Description**. Click the ellipsis icon to perform additional operations:

- **Autofit columns**—Adjusts the column width of the table to fit the page evenly.
- **Reset to default**—Resets the table view to the default columns.

If a filter icon appears next to the column header, click it and enter the filter criteria or select a filter criteria. The following table describes the information displayed in each event:

Table 208: *Events Tab*

Section	Description
Occurred On	Displays the time at which the event occurred.
Event Type	Displays the type of the event.
Description	Displays the detailed description of the event.
Device MAC	Displays the MAC address of the device.
BSSID	Displays the BSSID.

To download events into a CSV format, click the download button. Aruba Central generates the CSV report of all the events for the selected client.

You can also filter the events based on the type of events, click the **Click here for Advance Filtering**. Select the type of events from the list and click **Filter**. The events under the selected categories get listed in the **Events** table.

Client Live Events

Aruba Central (on-premises) allows you to troubleshoot issue related to client at both client device level and site level in real time for detailed analysis. Live troubleshooting is supported only if the wireless client is connected to the access point running Aruba Instant 8.4.0.0 or a later version. You can also enable packet capture during live troubleshooting and download the PCAP file if the access point is running Aruba Instant 8.6.0.5 or a later version.



The live troubleshooting can only be performed at a site level or for a specific client.

Live Events are supported only on Instant APs.

Troubleshooting a Client

To troubleshoot a client at a site level, perform the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Sites** that contains at least one device.
The dashboard context for the selected site is displayed.
2. Under **Analyze**, click **Live Events**.
The **Live Events** page is displayed.
3. Enter the MAC address of the client and click **Start Troubleshooting**.

To troubleshoot a wireless or wired client, perform the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**.
The clients overview page is displayed in **List** view.
3. By default, the **Clients** table displays a unified list of clients.

4. Click the name of the wireless or wired client to open the corresponding **Client Details** page. If there are many clients connected to the network, click **Wireless** or **Wired** to filter the clients connected to the wireless or wired client respectively.
5. Enter the client name in the **Client Name** column, and then click the client name.
6. Under **Analyze**, click **Live Events**.

The **Live Events** page is displayed.

The client live troubleshooting starts automatically for the selected client.

The status of the troubleshooting is displayed every minute. The troubleshooting session runs for a duration of 15 minutes. You can stop live troubleshooting at any point by clicking **Stop Troubleshooting** and to go back to the historical view.

After the live troubleshooting session ends, the details of the events are displayed in the live events table.

Live Events Details

The following details are captured and displayed in the **Live Events** table:

- **Occurred On**—Displays the timestamp of the event. Use the filter option to filter the events by date and time.
- **Device Name**—Displays the name of the device the client is connected to. Set the filter to select a specific device under **Site**.
- **Device Type**—Displays the type of device the client is connected to.
- **Category**—Displays the category of the event. Use the filter option to filter the events by category.
- **Description**—Displays a description of the event. Use the filter option to filter the events based on description.

You can download the list of live events to a CSV file for offline analysis. To download live events, click the

Download CSV  icon on the **Live Events** table.

Packet Capture

Aruba Central (on-premises) allows you to interact and launch a targeted packet capture on a client connected to a specific access point. Users with read-write and admin role can use live packet capture for troubleshooting devices. After you start packet capture from the UI, Aruba Central notifies the access point and the switch. The default packet capture duration is 15 minutes. After you start packet capture, use the toggle button to stop packet capture, or go back to the **Client Overview** page.

Starting Packet Capture

You can start packet capture from the wireless or wired clients page. Packet capture can be done at a site level (wireless client only) or for a selected client.

To start packet capture at a site level, perform the following steps:

1. In the **Network Operations** app, set the filter to a **Site** that contains at least one device. The dashboard context for the selected site is displayed.
2. Under **Analyze**, click **Live Events**. The **Live Events** page is displayed.
3. Enter the MAC address of the client.



At a site level, Aruba Central (on-premises) does not support packet capture for a wired client connected to a switch.

4. Enable the **Packet Capture** toggle button to start live packet capture for the selected client.
5. Click **Start Troubleshooting**.

To start packet capture for a wireless or wired client, perform the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**. The clients overview page is displayed in **List** view.
3. By default, the **Clients** table displays a unified list of clients.
4. Click the name of the wireless or wired client to open the corresponding **Client Details** page. If there are many clients connected to the network, click **Wireless** or **Wired** to filter the clients connected to the wireless or wired client respectively.
5. Enter the client name in the **Client Name** column, and click the client name.
6. Under **Analyze**, click **Live Events**. The **Live Events** page is displayed. The client live troubleshooting starts automatically for the selected client.
7. Click **Stop Troubleshooting** to stop live troubleshooting.
8. Enable the **Packet Capture** toggle button to start live packet capture for the selected client.
9. Click **Start Troubleshooting** to live troubleshoot the selected client. Live packet capture starts for the selected client.

The live troubleshooting session runs for a duration of 15 minutes. After the live troubleshooting session ends, a **Download PCAP** text appears above the live events table. Click **Download PCAP** to download the generated pcap file on your local system.



Packet capture can only be enabled or disabled before live troubleshooting is started. You cannot enable or disable packet capture while a live troubleshooting session is in progress.

Packet capture is not supported in single node deployments.

Failed Wireless Client Events or Reasons

The **Clients** page provides a summary view of all the clients connected to the network. You can filter clients based on the network the clients are connected to. The page displays key client information and also allows you to view a specific client detail page.

By default, the **Clients** page displays a unified list of clients for the selected group. The list of clients is populated for a time range of 3 hours. To view the list of clients for a different time range, click the **Time Range Filter** link and select the required time period. Total data usage for the selected time period is displayed above the client summary bar.

To filter clients based on the device to which the clients are connected, select the device type from the **Clients** drop-down list:

- **Unified**—Displays a unified list of clients connected to the network.
- **AP**—Displays a list of clients connected to the Instant AP.
- **Switch**—Displays a list of clients connected to the switch.
- **Controller**—Displays a list of clients connected to the Aruba Controller.



The wired client will show up in the **Unified Clients** page only if the client is connected to an Aruba 2540 Series, Aruba 2920 Series, Aruba 2930F Series, Aruba 2930M Series, Aruba 3810 Series, or Aruba 5400R Series switch.

To view failed clients and the reason for their failure, complete the following steps:

1. In the **Network Operations** app, use the filter bar to select a group, label, site, or a device.
2. Under **Manage**, click **Clients**. The All Clients overview page is displayed.
3. Click **Failed** from the clients summary bar to view a list of all the failed clients.
4. Hover over the status of a particular client to view the following information. This information is provided by the AI Insights feature based on algorithms and smart analytics:
 - **Last seen** - Date and time at which the client was last seen
 - **Failure Stage** - Failure status of the client that failed to connect. The failure reasons could be:
 - Association error
 - MAC authentication error
 - 802.1X authentication error
 - Key exchange error
 - DHCP error
 - Captive Portal error
 - **Failure Reason** - Based on the failure stage, failure reason is populated. For example, if it is a 802.1X authentication error, the reason for the failure could be **Authentication Server Timeout**.

CLIENT NAME	STATUS	IP ADDRESS	VLAN	CONNECTED TO	ROLE	HEALTH	LINK	AI INSIGHTS
00:d4:be:00:17:da	Failed			COP4_1670_000			AP_groupCOP403-PEAP	1
00:d4:be:00:21:a2	Failed			COP4_2360_001			AP_groupCOP401-PEAP	1
00:d4:be:00:0e:94	Failed			COP4_800_003			AP_groupCOP403-PEAP	1
00:58:c7:00:26:d1	Failed			COP4_2130_003			AP_groupCOP400-PEAP	1
00:d4:be:00:14:8b	Failed			COP4_1810_003			AP_groupCOP403-PEAP	1

5. You can also view if any AI Insight is associated with the failed client by clicking on the number under the AI Insights column. This will lead to Insights page.

Client Events

Aruba Central (on-premises) allows you to troubleshoot issues related to a wired or wireless clients connected to APs. The **Events** tab at the client context provides a capability to filter events further to identify a specific issue and troubleshoot it. It provides an aggregate view of events based on its severity level categorized under **Negative**, **Positive**, or **Neutral**

Events

To access the client event information connected to an IAP, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**. The clients overview page is displayed in **List** view.
3. By default, the **Clients** table displays a unified list of clients.

4. Click the name of the wireless or wired client to open the corresponding **Client Details** page. If there are many clients connected to the network, click **Wireless** or **Wired**.
5. Enter the client name in the **Client Name** column, and click the client name.
6. Under **Analyze**, click **Events**.

By default the **Events** tab is selected and the **Events** table is displayed with the list of events specific to the selected client. The **Events** tab categorizes the events as **Negative**, **Positive**, or **Neutral**.

Filtering Events in the List View

Aruba Central allows you to filter the events based on the event types. Perform the following steps to filter events based on event types in the **List** view:

1. In the **Events** page, click **Click here for advanced filtering** to filter the events based on event types.
2. Select the event type and click **Filter**. You can select multiple event types from the advanced filtering option.
3. The events table displays the list of events generated in each event type. The filter summary bar displays the total number of events in the selected category and the type(s) of events.
4. Optionally, to clear advanced filtering option, from the events summary bar, click **Clear All**.

The following table describes the information displayed in each column of the **Events** table:

Table 209: *Events Pane*

Data Pane Content	Description
Occurred On	Displays the timestamp of the event. Use the sort option to sort the events by date and time. Use the filter option to select a specific time range to display the events.
Device Hostname	Displays the host name of the device where the event is generated. Use the filter option to filter events by hostname.
Device MAC	Displays the MAC address of the device. Use the filter option to filter events by device MAC address.
BSSID	Displays the BSSID of the device. Use the filter option to filter events by the BSSID.
Event Type	Displays the type of the event along with the severity level represented by an icon for each event type.
Description	Displays the description of the event. Use the column filter to perform a free search and filter an event based on the description. You can type a search phrase including client MAC, reason code, or BSSID and filter the events.



The event columns allows free text search at all column levels to enhance filtration.

Additionally, it displays an event frequency bar which shows the time range of the events that occurred. This allows you to view the actual time of the failure, which helps in troubleshooting the issue. Drag and select a specific range to filter events occurred in that time range. Hover over each bar to see the proportion of

negative, positive and neutral events distributed in a specific time range. The distribution changes based on the time range selected in the **Time Range Filter** (🕒).

To clear any time range selected on the frequency bar, click **Clear**.

Filtering Events in the Summary View

Aruba Central allows you view different event types for the selected client distributed across the time line. You can filter the events based on the event types and drill down further to diagnose client's health. It gives a deep insight on the failure events that occur in the network.

Select the **Summary** view icon to display the list of events. The graphs in the **Summary** view displays the events in the following categories:

- Events by severity—Displays the event severity categorized under **Negative**, **Positive**, or **Neutral**. Click each tab to drill down to each category. The frequency bar and the event type chart changes accordingly and displays events based on the selected tab.
 - Events Frequency Bar—Displays the time range of the events that occurred. This allows you to view the actual time of the failure, which helps in troubleshooting the issue. Drag and select a specific range to filter events occurred in that time range. Hover over each bar to see the proportion of negative, positive and neutral events distributed in a specific time range. The distribution changes based on the time range selected in the **Time Range Filter** (🕒). To clear any time range selected on the frequency bar, click **Clear**.
- Events per type—Displays the different event types categorized based on severity and color codes as following:
 - Red—Indicates negative severity
 - Green—Indicates positive severity
 - Grey—Indicates neutral severity

This **Events per type** section has the following capabilities:

- Click on the event type to open a new pane which displays details regarding that event type. It shows the time range when the specific event occurred, the APs that were impacted, and a pictorial pie chart of the reason codes for that failure event. Hover your mouse to see the different reason codes differentiated with color codes. Clicking on the reason codes redirects you to the events list with appropriate reason selected.

The new pane provides advanced links to troubleshoot at the device level:

- Click on the AP name or the bar to navigate to the AP details page for that particular event. On the AP details page, you can click the **Events** tab to see the event details.
- Click on the number displayed against each bar to navigate to AP events page along with the filter for the selected client and the event type. The number displayed against each bar is the frequency of the selected event occurred on that particular AP.
- Click on the number displayed against each event type bar to go back to the event list view for that particular event. You can see the list of all the events with details within the selected time range. In this case all the details is pre-selected for the user.



The components of the **Events** summary page is displayed for a selected time period based on the time selected in the **Time Range Filter** (🕒). You can select one of the following: **3 Hours**, **1 Week**, **1 Day**, or **1 Month**.

Viewing Applications Monitored by AirSlice

To view the applications monitored by AirSlice, ensure to enable AirSlice. For more information, see [Enabling AirSlice on APs](#).

To view the applications monitored by AirSlice, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.

The dashboard context for the selected filter is displayed.

2. Under **Manage**, click **Clients**. The **Clients** page is displayed in **List** view.

By default, the **Clients** table displays a list of all clients.

3. Click a client listed under **Client Name**.

The dashboard context for the client is displayed.

4. Click **Applications**.

The **Visibility > Applications** page is displayed in **List** view. The **Applications** table provides the following information:

- **Application**—Name of the application.
- **Category**—Category to which the application belongs. The application can belong to any of the categories. For example, Unclassified, Standard, Social Networking, Streaming, Web, Cloud File Storage, Instant Messaging, and so on.
- **Usage**—The usage size by the respective application.
- **Sent**—The size of data sent from the application.
- **Received**—The size of data received by the application.



In the **Visibility > Applications** page, under the **Application** column, ★ indicates that the applications are prioritized by AirSlice.

5. Click an application listed under **Application**. The following information along with the graph of minimum, maximum, and average values are displayed:

- **Usage**
- **Loss**
- **Latency**
- **Jitter**

The above information is available only in the client dashboard.



The **Usage, Loss, Latency, and Jitter** data is available only for applications that are prioritized by AirSlice.

The **Usage, Loss, Latency, and Jitter** data are displayed only for the following applications:

- Zoom
- Slack
- Skype
- WebEx
- GoToMeeting Online Meeting
- Microsoft Office 365

- Dropbox
- Amazon Web Services/Cloudfront CDN
- GitHub
- Microsoft Teams
- ALG Wi-fi Calling

Figure 98 *AirSlice—Applications*

APPLICATIONS					
Passive Monitoring					
Total Transferred: 170.1 MB					
APPLICATION	CATEGORY	USAGE	SENT	RECEIVED	
ICP	Network Service	11.8 MB (6.92%)	65 KB	11.7 MB	
Dropbox	Dropbox SAAS	2.5 MB (1.44%)	1.5 MB	1.0 MB	
Outlook Message Block	Network Service	768 KB (0.45%)	546 KB	228 KB	
Microsoft	Office365 SAAS	369 KB (0.21%)	60 KB	309 KB	
GoToMeeting Online Meeting	GoToMeeting SAAS	213 KB (0.12%)	94 KB	119 KB	
Microsoft Office 365	Office365 SAAS	81 KB (0.05%)	11 KB	69 KB	
Google Generic	Google SAAS	71 KB (0.04%)	71 KB	0 B	
Amazon Generic Services	Amazon SAAS	60 KB (0.04%)	16 KB	44 KB	
Skype	Instant Messaging	41 KB (0.02%)	6 KB	35 KB	
Amazon Web Services/Cloudfront CDN	Amazon SAAS	18 KB (0.01%)	10 KB	9 KB	
HTTPS	Web	16 KB (0.01%)	3 KB	14 KB	
Microsoft Outlook (Office 365)	exchange_saas	16 KB (0.01%)	1 KB	14 KB	
Microsoft Skype for Business	skype_teams_saas	12 KB (0.01%)	6 KB	6 KB	
Bing.com	Web	12 KB (0.01%)	3 KB	9 KB	
Google Cloud Storage	Google SAAS	11 KB (0.01%)	1 KB	9 KB	
Microsoft Office OneNote (Office 365)	Office365 SAAS	10 KB (0.01%)	904 B	9 KB	
UDP	Network Service	9 KB (0.01%)	4 KB	6 KB	

Application Visibility

The **Manage > Applications** tab provides detailed information on data usage by the clients connected to APs and Branch Gateways in the network. Clicking the **Applications** tab displays a **Visibility** dashboard that provides a summary of client traffic and their data usage to and from applications, and websites. You can also analyze the client traffic flow using the graphs displayed in the **Visibility** dashboard.

Viewing Visibility Dashboard

To view the **Visibility** dashboard, complete the following steps:

- In the **Network Operations** app, select one of the following options:
 - To navigate to the applications tab for a site, set the filter to one of the options under **Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
 - To navigate to the applications tab for a client, set the filter to one of the options under **Groups**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
 - Under **Manage**, click **Clients**.
A list of all connected clients is displayed in the **List** view.
 - Select any one of the connected clients from the list.
- Under **Manage**, click **Applications**. The visibility dashboard is displayed.



The applications data is not displayed for campus APs at the Client and Site level.

The **Visibility** dashboard displays metrics and graphs related to client traffic flow in the following sections:

- **Applications**
- **Websites**
- **Blocked Traffic**



-
- To view the client traffic details, ensure that the DPI access rules are enabled on the AP device. For more information, see Aruba Central Help Center.
 - The **Blocked Traffic** tab is only displayed in **Global** level in the **Network Operations > Manage > Applications** page.
 - Application Visibility data is updated every 0th minute of every hour. The data population on the **Applications > Visibility** dashboard may be delayed by an hour when compared to the Application Visibility data displayed in the **Applications** pages for the Group, Global, and APs.
-

Graph View in Visibility Dashboard

Click the **Summary** icon in the **Visibility** dashboard to view both the applications and websites graphical information:

■ Applications

- **Applications**—The stacked bar graph and the pie chart in this tab displays details of the client traffic flowing to or from the top five classified applications listed in the **Applications** table. The legend below the graphs displays the list of applications to which the traffic flow is detected. Select or deselect the application check box to show or hide the traffic flow data from the pie chart and stacked bar. By hovering the mouse on pie chart and stacked bar, you can view the size of data flowing to and from the application same as displayed in legend.
- **Categories**—The stacked bar graph in this tab displays details of the client traffic flowing to or from the top five classified application categories listed in the **Applications** table. The legend below the graphs displays the list of applications categories to which the traffic flow is detected. Select or deselect the application category check box to show or hide the traffic flow data from the pie chart and stacked bar. By hovering the mouse on pie chart and stacked bar, you can view the size of data flowing to and from the application same as displayed in legend.

■ Websites

- **Reputations**—The stacked bar graph and the pie chart in this tab displays details of client traffic flow for the top three reputations listed in the **Websites** table. The legend displays the list of websites based on its reputation, to which the traffic flow is detected. Select or deselect the reputation check box to show or hide the data from the pie chart and stacked bar. By hovering the mouse on pie chart and stacked bar, you can view the size of data flowing to and from each of the websites that are categorized based on reputation.
- **Web Categories**—The stacked bar graph and the pie chart in this tab displays details of client traffic flow for the top five web categories listed in the **Websites** table. Select or deselect the web category check box to show or hide the data from the pie chart and stacked bar. You can view the size of data flowing to and from each of the web categories by hovering the mouse on both the stacked bar graph and pie chart. The legend below the graphs displays the list of websites based on its reputation, to which the traffic flow is detected.

Related Topics:

- [Application Visibility](#)
- [Websites](#)
- [Blocked Traffic](#)

Applications

The **Applications** tab includes a table view and a graph view related to the client traffic flow to and from various applications. These graphs are displayed for a specific time frame (3 Hours, 1 Day, 1 Week, 1 Month, 3 Months). By default, the graphs display real-time client traffic data or usage trend in last three hours.

Table View in Application Section

Click the **List** icon in the **Applications** tab to display a table with the following columns:

- **Application**—Name of the application.

Search Options:

- The  **filter** icon allows you to search a particular application by its name.
- The  and  **sort** icons allow you to sort the application in ascending or descending order.

- **Category**—The category to which the application belongs. The application can belong to any of the categories, such as **Unclassified, Standard, Social Networking, Streaming, Web, Cloud File Storage, Instant Messaging Network Service** and so on.

Search Options:

- The  **filter** icon allows you to search a particular category by its name.
- The  and  **sort** icons allow you to sort the category in ascending or descending order.

- **Usage**—Data consumed by an application.

Search Options:

- The  and  **sort** icons allow you to sort the usage in ascending or descending order.
- **Sent**—The size of data sent from the application.
- **Received**—The size of data received by the application.

Graph View in Visibility Dashboard

To view the application section in summary view, see [Graph View in Visibility Dashboard](#)

Websites

The **Websites** tab includes a table view and a bar graph view related to the client traffic flow and their data usage by various websites. These graphs are displayed for a specific time frame (3 Hours, 1 Day, 1 Week, 1 Month, 3 Months). By default, the graphs display real-time client traffic data or usage trend in last three hours.

Table View in Websites Section

The **Websites** tab displays the following details:

- **Reputation**—The reputation of the application categories, for example, **Trustworthy, Incomplete, Moderate Risk, Low Risk, High Risk** and so on. The reputations are set based on the risk levels exhibited by the application categories.
- **Usage**—The percentage of data usage by application categories based on their reputation.
- **Category**—The category of the client traffic that sends and receives data, for example, **Unclassified, Social Networking, Streaming, Web, Cloud File Storage, Instant Messaging** and so on.
- **Usage**—The size and percentage of data usage by the corresponding categories.

Graph View in Websites Section

To view the application section in summary view, see [Graph View in Visibility Dashboard](#).

Blocked Traffic

Based on the group selection from the **Blocked Traffic** drop-down list, the **Blocked Traffic** section of the **Application > Visibility > Blocked Traffic** dashboard allows you to view the following information:

- Blocked devices of the selected group as CSV file.
- The number of user sessions that are blocked. This information is displayed under **Blocked Sessions**.



The blocked traffic details are shown only for the APs on which the Application Visibility or DPI ACLs are enabled. For more information, see Aruba Central Help Center.

Downloading Blocked Session Details

To download the blocked session details in the CSV format, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
The global dashboard is displayed.
2. Under **Manage**, click **Applications**. The visibility dashboard is displayed.
3. Click **Blocked Traffic** tab in the visibility dashboard.
4. To download the blocked sessions report, select the device group from the **Select Group** drop-down. If the device group is already selected from the **Groups** drop-down on the filter bar, the page displays the group name and the number of sessions blocked for the clients connected to devices in that group.
5. Click **Download CSV**. Aruba Central generates the CSV report with data from the last 7 days.



The CSV file shows up to 50000 blocked sessions for a single AP cluster.

About Floorplans

Floorplans allow you to plan sites, create and manage floor plans, and provision access points. You can use Floorplans to do basic planning procedures, such as, creating a floor plan and provisioning access points. The **Floorplans** dashboard can be accessed only from a site context.

Floorplans provide a real-time picture of the radio environment of your wireless network and the ability to plan the wireless coverage of new sites. For a better understanding of your wireless network, you must know the location of your devices and users, and the RF environment of your network. Floorplans provide this information at your fingertips through integrated mapping and location data.

Floorplans use sophisticated RF fingerprinting to accurately display coverage patterns and calculate the location of every wireless device in range. Floorplans does not require dedicated RF sensors or a costly additional location appliance, because it gathers all the necessary information from your existing devices.



- Floorplans is supported only on access points running 6.5.2.0 or a later version.
- Do not use the back or front navigation. Instead, use the breadcrumbs.
- APs are removed from the floorplan and deployed device list based on the device unlicensing. For example, When you unassign a license for an AP, it gets removed from the deployed device list and floorplans, and when you assign back the license for an AP, it gets added back to the deployed device list and to the same co-ordinates of the floorplan location. Also, when your license gets auto expired, the devices gets removed from the list and floorplan location and the same gets added back on license renewal. Make sure that you check the assigned AP device licensing status before adding them to the floorplan.

Floorplans offer the following features:

- Create and import floor plans.
- Pictorial navigation that allows you to view the floor plans associated with access points, associated clients, rogues, buildings, and floors.
- Accurate calculation of the location of all associated client devices using RF data from your devices.
- Accurate calculation of the location of all rogue devices (as classified by RAPIDS) using RF data from your devices.
- A map view that shows the location of devices and heatmaps that depict the strength of RF coverage in each location.

Related Topics

- [Floor Plan Dashboard](#)
- [Planning and Provisioning Devices](#)
- [Customizing the Floor Plans View](#)

Floor Plan Dashboard

The **Floor Plan** dashboard can be accessed from a site context or an access point context. You can view the floor plan dashboard in **List** view and **Summary** view. By default, the floor plan for a site is displayed in the summary view.

The following table describes the options displayed in floor plan dashboard in the summary view.

Table 210: *Floor Plan Dashboard in Summary View*

Data Pane Content	Description
	Allows you to search the floor names and APs.
	Allows you to add a new floor.
	Allows you to edit or modify the floor plan properties.
	Allows you to delete a floor plan.

The following table describes the information displayed in each column of the **Floor** table in the list view.

Table 211: *Floor Plan Dashboard in List View*

Data Pane Content	Description
Number	Displays the floor number. Use the sort option to sort the numbers in ascending or descending order.
Name	Displays the name of floors. Use the sort option to sort the floor names in ascending or descending order. Use the filter option to select a specific floor name.
Access Points	Displays the number of APs (deployed AP, planned AP, and air monitors) associated with the floor. Use the sort option to sort the APs in ascending or descending order.
Clients	Displays the number of clients associated with the floor. Use the sort option to sort the clients in ascending or descending order.
Width (m/ft)	Displays the width of the floor in meter/feet.
Length (m/ft)	Displays the length of the floor in meter/feet.
Ceiling Height (m/ft)	Displays the ceiling height of the floor in meter/feet.
	Allows you to add a new floor.
	Allows you to edit or modify the floor plan properties.
	Allows you to delete a floor plan.

You can either navigate to a specific site to view the floor plan or view a specific site floor plan from the **Network Health** tab in the **Global** context.

To view the **Floor Plan** dashboard from the **Network Health** tab in the **Global** context, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
The global dashboard is displayed.
2. Under **Manage > Overview**, the **Network Health** page is displayed.

3. Hover over a site to view the following details:

Figure 99 Site-level Details with Floorplan Option



4. Click **FloorPlan** under **RF Coverage**. By default, the **Floor Plan** dashboard with all floors is displayed in the summary view.
5. Click any one of the floor tile under **All Floors** to navigate to the floor plan. To go back to the all floor tiles, click the back arrow next to the floor name.
6. To view all floors in a list, click the **Lists** view.
A **Floor** table with a list of floors is displayed in the list view.
7. In the **Floor** table, click any one of the floor under **Name** column or enter the floor name in the **Name** column and then click the floor name to navigate to the floor plan to navigate to the floor plan. To go back to the floor list, click the back arrow next to the floor name.

To view the **Floor Plan** dashboard from a site context, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Sites**.
The dashboard context for the selected site is displayed.
2. Under **Manage > Overview**, click **Floor Plan**. By default, the **Floor Plan** dashboard with all floors is displayed in the summary view.
3. Click any one of the floor tile under **All Floors** to navigate to the floor plan. To go back to the all floor tiles, click the back arrow next to the floor name.
4. To view all floors in a list, click the **Lists** view.
A **Floor** table with a list of floors is displayed in the list view.
5. In the **Floor** table, click any one of the floor under **Name** column or enter the floor name in the **Name** column and then click the floor name to navigate to the floor plan.
6. To download the bill of material, click **Download Bill of Material (BOM)** under **Floor Details** window.
7. To go back to the floor list, click the back arrow next to the floor name.

To view the **Floor Plan** dashboard from an access point context, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
The global dashboard is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of access points is displayed in the **List** view.
3. Click the **Access Point** name to view the **Access Point Details** page. If there are many APs connected to the network, click **Online** or **Offline** to filter the online or offline APs.
4. Additionally, enter the access point name in the **Device Name** column and then click the AP name.
The AP **Summary** page is displayed.
5. Under **Manage > Overview**, click **Floor Plan**. The floor plan details with the highlighted AP is displayed.

6. Click anywhere on the floor plan to navigate to the exact floor for a site with the AP highlighted. By default, the **Access point Details** window pops up displaying the highlighted AP details.



The floor plan details for an AP is only accessible for the devices that are assigned with license.

Planning and Provisioning Devices

Floor Plan provide the capability to plan buildings, floors, and location for device provisioning before the actual deployment. You can create a floor plan and add devices to the floor plan.

The planning and provisioning workflow includes the following procedures:

- [Creating a Floor Plan](#)
- [Importing a Floor Plan](#)
- [Modifying Floor Plan Properties](#)
- [Adding Devices to the Floor Plan](#)
- [Deleting a Floor with in a Site](#)

Creating a Floor Plan

Floor Plan allow you to add, modify, and import a floor plan background image file. When importing RF plans ensure that the devices from the device catalog are included.

To create a new floor plan, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Sites**.
The dashboard context for the selected site is displayed.
2. Under **Manage > Overview**, click **Floor Plan**. The **Floor Plan** dashboard is displayed.
3. Click **Add Floors**. The **Floor Plans** tab is displayed.
4. Click **Edit** in the slide out pane on the right.
5. Click **New Floorplan**. You can also add the floor plan by right-clicking on the center gray area and click **New Floorplan**. The **New Floorplan** pop-up window is displayed.
6. Click **Choose File** and locate a floor plan image file from your local file system. You can import the floor plan image file in the jpg, jpeg, gif, bmp, pdf, png, dwg, and svg format.
7. Assign a floor name and a floor number in the **Floor name** and **Floor number** text boxes, respectively.
8. Click **Save**.



Make sure that you add a new floor plan image within the recommended size of **2625*2625** feet or **800*800** meter. You can also use the measure tool to resize the current image to the recommended size.

9. You can define new floor by clicking the **Define New Floor** option on the top right corner.
10. The **Define New Floor** includes the following option:
 - a. **Scale**—Shows the dimensions of the floor.
 - b. **Region**—Allows you to define floor plan boundary and planning region.
 - c. **CAD Layer**—Allows you to import walls from the CAD file.
 - d. **Access Points**—Allows you to add the access point's to the floor plan.
11. Click **Next** button after you set the **Scale**, **Region**, and **CAD layer** for the floor.

12. To add a planned access point, under **Access Points > Planned APs**, select the device type from the **Type** drop-down menu.
13. In the **Count** field, enter the number of devices to add to the new floor.
14. Click and drag the **Deployment Type** slider bar to adjust data rates for a high density or low density environment.
15. Optionally, click the **Advance** link to configure the advance deployment options:
 - a. **Service Level**—Select **Speed** or **Signal** to plan coverage by adjusting the data rate requirements (speed) or AP signal strength settings. Click **Calculate AP Count** to recalculate the suggested number of APs based on these settings.
 - b. **Client Density**—In the **Max Clients** field, set the anticipated number of clients that will be stationed in the floor. In the **Clients Per AP** field, enter the maximum number of clients supported by each radio. Click **Calculate AP Count** to recalculate the suggested number of APs based on these settings.
16. Click **Add APs to Floorplan** to add the planned APs to the floor.
17. Click **Finish**.
18. To remove the planned device from the floor plan, right-click on that device and click **Remove**.

Importing a Floor Plan

To import a floor plan exported from AirWave or Aruba Central, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Sites**.
The dashboard context for the selected site is displayed.
2. Under **Manage > Overview**, click **Floor Plan**. The **Floor Plan** dashboard is displayed.
3. Click the **Import** menu option.
4. Click **Choose File** and select the floor plan zip file to import.
5. Click **Upload**. When an import is complete, the UI displays a notification to alert the user.

Modifying Floor Plan Properties

To edit the properties of an existing floor plan, complete the following steps:

1. In the **Network Operations** app, set the filter to a **Site**.
The dashboard context for the selected site is displayed.
2. Under **Manage > Overview**, click **Floorplans**. The **Floorplans** dashboard is displayed.
3. Click **Edit** to modify the properties. For more information, see [Customizing the Floor Plans View](#).
4. Click **Save**.

Adding Devices to the Floor Plan

You can add planned devices or devices available in Aruba Central, to a floor plan. Planned devices are used to simulate AP behaviors (heatmap coverage) on the floor plan, instead of real devices. You can match and replace planned devices with real devices that are available in Aruba Central.

To add the already deployed devices to the floor plan, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Sites**.
The dashboard context for the selected site is displayed.
2. Under **Manage > Overview**, click **Floor Plan**. The **Floor Plan** dashboard is displayed.
3. Click **Edit**. In case of multiple floors, select the floor from the drop-down list and click **Edit**.

4. Click the **Add Deployed Devices**. A list of devices is displayed.
5. Expand the group containing the APs which need to be provisioned on this floor plan. Note that by default, devices that have already been added to **Floor Plan** are hidden. To show them, clear the **Hide APs that are already added** check box at the bottom of the list.
6. Click and drag an AP to its proper location on the floor.
7. To remove a device from the floor plan, right-click that device and then click **Remove**.

To add planned devices when creating a new floor plan, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Sites**.
The dashboard context for the selected site is displayed.
2. Under **Manage > Overview**, click **Floor Plan**. The **Floor Plan** dashboard is displayed.
3. Click **Edit**. In case of multiple floors, select the floor from the drop-down list and click **Edit**.
4. Click **Add Planned Devices** and select a device type (model) from the list of available devices.
5. Click and drag the device to the desired location on the floor.
6. To replace a planned AP with an AP that is available in Aruba Central, click **Auto-Match Planned Devices** from the **Action** tab.



To auto-match devices, ensure that you edit the device name or MAC address of the planned AP to match the name or MAC address of the AP added to Aruba Central.

7. To remove a planned device from the floor plan, right-click on that device and then click **Remove**.

Deleting a Floor with in a Site

To delete a floor within a site in summary view, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Sites**.
The dashboard context for the selected site is displayed.
2. Under **Manage > Overview**, click **Floor Plan**. By default, the **Floor Plan** dashboard with all floors is displayed in the summary view.
3. Hover over the floor and click the  **delete** icon and confirm the delete action to delete the floor.

To delete a floor within a site in list view, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Sites**.
The dashboard context for the selected site is displayed.
2. Under **Manage > Overview**, click **Floor Plan**. By default, the **Floor Plan** dashboard with all floors is displayed in the summary view.
3. Click **List** view. The floor plan dashboard with a list of floors is displayed.
4. Hover over the floor and click the  **delete** icon and confirm the delete action to delete the floor.

Customizing the Floor Plans View

To customize your floor plan view, click the **View** tab on the right sliding panel. The **View** tab displays the list of devices.

- Click **APs** to view the details of the access point and the RF environment.
- Click **Clients** to view the client details.
- Click **Rogues** to view the rogue details.

The **Floor Plan** navigation menu on the right pane consists of the **Properties**, **View**, and **Edit** tabs. The following table describes the menu options available for a floor:

Table 212: *Floorplan Menu Options*

Tabs	Options
Properties	<p>The Properties tab has the following menu options:</p> <ul style="list-style-type: none"> ■ APs—Displays the total number of APs, the planned APs, and the number of APs that are offline. ■ Floor name—Displays the floor name. ■ Floor number—Displays the floor number. ■ Width—Displays the current width of the floor plan. To change these settings, click the Measure icon and measure a portion of the floor. ■ Height—Displays the current height of the floor plan. To change these settings, click the Measure icon and measure a portion of the floor. ■ Gridsize—Displays the grid. Decreasing the grid size enables the location to place clients in a small grid which increases accuracy. ■ Advanced—Allows you to set the values to indicate if the environment is related to an office space, cubicles, offices, or concrete.
View	<p>The View tab has the following menu options:</p> <ul style="list-style-type: none"> ■ Devices—Displays APs, clients, and rogue devices detected on the floor. ■ AP Overlays—Shows the heatmap for the current and adjacent floors. ■ Floorplan Features—Displays the following details: <ul style="list-style-type: none"> ● Grid Lines—Allows you to change the grid size and color. ● Labels—Shows or hides the labels tagged to the devices on the floor. ● Origin—To ensure that multi-floor heatmaps display properly, ensure that your floor plans are vertically aligned. Floor Plan use the origination point for this alignment. By default, the origin appears in the upper left corner of the floor plan. You can drag and drop the origin point to the correct position. ● Regions—Displays the regions defined within a floor plan. For example, you can define two small regions of high density clients within a larger floor plan with lower client density. ● Walls—Displays walls drawn on the floor.
Edits	<p>The Edit tab has the following menu options:</p> <ul style="list-style-type: none"> ■ Drawing—Allows you to draw a region or wall for the floor. ■ Devices—Allows you to add and delete the already deployed or planned devices. ■ Actions—Displays the following options: <ul style="list-style-type: none"> ● Select All—Selects all floors. ● Export Floor Plans—Exports the floor plan of a specific floor. ● Undo—Cancels the previous action. ● New Floorplan—Allows you to create a new floor plan. ● Auto-match Planned Devices—Automatically matches the devices that are planned for deployment and reloads the page. ● Go to floor above—Allows you to navigate to the floor above. ● Go to floor below—Allows you to navigate to the floor below. ● Refresh—Refreshes the page. ● Replace Background—Allows you to replace the current background.

User Interface Elements of the Floor Plan Dashboard

The **Floor Plan** dashboard provides various options to customize your view. The customizable parameters include:

Table 213: User Interface Elements

UI Element	Description
	Click the drop-down to select a specific floor from the site.
	Click any of the AP to view the details of the access point and the RF environment in the Access Point Details window.
	Click any of the clients to view the client details in the Client Details window.
	Click the + or - icon to zoom in or zoom out of a floor plan. Additionally, click the box icon to view the floor plan in full screen mode and click the inward box icon to exit the full screen mode.
	Click the home icon to reset the floor plan view.
	<p>Click the eye icon to view the floor plan settings. The View Settings window includes the following information:</p> <ul style="list-style-type: none"> ■ Access Points <ul style="list-style-type: none"> ● Deployed Access Points—Shows or hides the deployed access points in the floor plan. ● Planned Access Points—Shows or hides the planned access points in the floor plan. ● Rogue access points—Shows or hides the rogue access points in the floor plan. ■ Air Monitors <ul style="list-style-type: none"> ● Deployed Access Monitors—Shows or hides the deployed air monitors in the floor plan. ● Planned Access Monitors—Shows or hides the planned air monitors in the floor plan. ■ Clients <ul style="list-style-type: none"> ● Clients—Shows or hides the clients in the floor plan. ■ Heatmap <ul style="list-style-type: none"> ● Show Heatmap—Shows or hides the strength of RF coverage in each location. ● Monochrome Heatmap—Select the check box to select either the monochrome display or the colored display of heatmaps. ● 2.4 GHz and 5 GHz—Select the check box to show or hide the strength of RF coverage for 2.4 GHz and 5 GHz APs. ● Show Regions—Select the check box to view the segregation of regions in the selected floor. ● Show Walls—Shows or hides the segregation of walls in the selected floor. ● Show labels—Shows or hides the labels tagged to the devices on the floor. ● Meters and Feet—shows the dimensions in feet or meters.
	Allows you to search for APs, Clients, and Rogues.
	Click the edit icon to edit or modify the floor plan properties.

Alerts & Events

The **Alerts & Events** pane displays all types of alerts and events generated for events pertaining to device provisioning, configuration, and user management.

Alerts & Events Dashboard

The **Alerts and Events** dashboard displays a list of alerts and events generated for events pertaining to device provisioning, configuration, and user management. You can view the alerts and events in **List** view and **Summary** view. Configuration view is used to configure alerts and it is available only at the **Global** context. The components of the **List** view is different for **Alerts** and **Events** tab whereas the **Summary** view displays similar components.

This section includes the following topics:

- [Viewing Alerts in List view](#)
- [Viewing Alerts & Events in Summary view](#)
- [Viewing Events List View](#)

Viewing Alerts in List view

You can view the details of the alerts and acknowledge alerts. Alerts are acknowledged automatically when the event count drops below the lowest severity threshold configured for the alert. Users with admin access can acknowledge alerts irrespective of the severity configuration. As manually acknowledging an alert does not reset the count data, the alert service continues to aggregate events. When the number of new events meets the configured threshold, an alert is triggered again.

To view the list of alerts and events and acknowledge alerts, complete the following procedure:

1. In the **Network Operations** app, select one of the following options:
 - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
 - To select a device in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices**, and then click **Access Points, Switches, or Controllers**.
A list of devices is displayed in the **List** view.
 - c. Click a device listed under **Device Name**.
The dashboard context for the device is displayed.
2. Under **Analyze**, click **Alerts & Events**.
By default, the **Alerts & Events** page displays the alert and events in the **List** view.
The **Alerts & Events** page offers a list view, summary view, and a configuration view.



Configuration view is only available at the **Global** context.

By default, the **Alerts** tab is selected and the **Open Alerts** table is displayed. The table displays all the generated alerts. The **Alerts** bar categorizes the alerts as **Critical, Major, Minor, and Warning**.

- Optionally, click **Acknowledge All** to acknowledge all the alerts at once.

Important Points:

Once an alert is acknowledged, the alert is moved to the **Acknowledged** tab.

All **Acknowledged Alerts** can be viewed when the **Show Acknowledged Alerts** button is ON.

If the user does not acknowledge an alert, the alert is suppressed for 5 minutes. The alert notification is then sent to the user every 5 minutes in case the issue still persists.

If the user acknowledges an alert, the alert is suppressed until the issue is resolved. After resolving the issue, if it re-occurs the alert is sent again.

- Optionally, enable the **Show Acknowledged Alerts** button to display the list of acknowledged alerts.

Table 214: *Acknowledged Alerts pane*

Data Pane Content	Description
Acknowledged On	Displays the timestamp of the acknowledged alert. Use the sort option to sort the events by date and time. Use the filter option to select a specific time range to display the alerts.
Acknowledged By	Displays the entry by whom the alert is acknowledged.
Occurred On	Displays the timestamp of the alert. Use the sort option to sort the events by date and time. Use the filter option to select a specific time range to display the alerts.
Elapsed Time	Displays the timestamp difference between when the alert actually occurred and, when the alert was acknowledged.
Category	Displays the category of the alert. Use the filter option to filter the alert by category.
Label	Displays the label name of the alert.
Site	Displays the site name of the alert.
Group	Displays the group name of the alert.
Severity	Displays the severity level of the alert. The severity can be Critical, Major, Minor, or Warning .
Description	Displays a description of the alert. Use the search option in filter bar to filter the alert based on description.

Advanced Alert Filtering

Aruba Central allows you to filter the alerts based on the alert categories. To filter alerts based on alert categories, complete the following steps:

- In the **Alerts** page, click **Click here for advanced filtering** to filter the alerts based on alert categories.

2. Select the alert category and click **Filter**. You can select multiple categories from the advanced filtering option.
3. The **Open Alerts** table displays the list of alerts generated in each alert category. The filter summary bar displays the total number of alerts in the selected categories.
4. Optionally, to clear advanced filtering option, from the alerts summary bar, click **Clear All**. The advanced filtering gets cleared.

The following table describes the information displayed in each column of the **Alerts** table:

Table 215: Alerts pane

Data Pane Content	Description
Occurred On	Displays the timestamp of the alert. Use the sort option to sort the events by date and time. Use the filter option to select a specific time range to display the alerts.
Category	Displays the category of the alert. Use the filter option to filter the alert by category.
Label	Displays the label name of the alert.
Site	Displays the site name of the alert.
Group	Displays the group name of the alert.
Severity	Displays the severity level of the alert. The severity can be Critical , Major , Minor , or Warning .
Description	Displays a description of the alert. Use the search option in filter bar to filter the alert based on description.

To customize the **Alerts & Events** table, click the ellipses  icon to select the required columns, or click **Reset to default** to set the table to the default columns.

Viewing Events List View

To view a list of events generated, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
 - To select a device in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices**, and then click **Access Points**, **Switches**, or **Controllers**.
A list of devices is displayed in the **List** view.
 - c. Click a device listed under **Device Name**.
The dashboard context for the device is displayed.

2. Under **Analyze**, click **Alerts & Events**.

By default, the **Alerts & Events** page displays the alert and events in the **List** view.

The **Alerts & Events** page offers a list view, summary view, and a configuration view.



Configuration view is only available at the **Global** context.

3. In the **Alerts & Events** summary bar, click **Events**. By default, the **List** view is selected and a consolidated list of events is displayed in the events table.

Advanced Event Filtering

Aruba Central allows you to filter the events based on the event types. To filter events based on event types, complete the following steps:

1. In the **Events** page, click **Click here for advanced filtering** to filter the events based on event types.
2. Select the event type and click **Filter**. You can select multiple event types from the advanced filtering option.
3. The events table displays the list of events generated in each event type. The filter summary bar displays the total number of events in the selected category and the type(s) of events.
4. Optionally, to clear advanced filtering option, from the events summary bar, click **Clear All**. The advanced filtering gets cleared.

The following table describes the information displayed in each column of the **Events** table:

Table 216: *Events pane*

Data Pane Content	Description
Occurred On	Displays the timestamp of the event. Use the sort option to sort the events by date and time. Use the filter option to select a specific time range to display the events.
Device Type	Displays the type of the device, Access Point, Controller, Switch. Use the filter option to filter events by device types.
Device Hostname	Displays the host name of the device where the event is generated.
Device MAC	Displays the MAC address of the device.
Client MAC	Displays the MAC address of the device to which the client is connected.
BSSID	Displays the BSSID of the device.
Event Type	Displays the type of the event.
Label	Displays the label name of the event.
Site	Displays the site name of the event.

Data Pane Content	Description
Group	Displays the group name of the event.
Description	Displays the description of the event. Use the column filter to perform a free search and filter an event based on the description. You can type a search phrase including client MAC, reason code, or BSSID and filter the events.



The event columns allows free text search at all column levels to enhance filtration.

Click the icon to see additional details for events related to controllers, switches, IAPs, and CAPs.

To customize the **Alerts & Events** table, click the ellipses icon to select the required columns, or click **Reset to default** to set the table to the default columns.

Aruba Central allows you to download the global list of events to your local browser. Click to download the events list in a CSV format.

Viewing Alerts & Events in Summary view

To view a summary of alerts and events, complete the following procedure:

- In the **Network Operations** app, select one of the following options:
 - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
 - To select a device in the filter:
 - Set the filter to **Global**.
 - Under **Manage**, click **Devices**, and then click **Access Points, Switches, or Controllers**.
A list of devices is displayed in the **List** view.
 - Click a device listed under **Device Name**.
The dashboard context for the device is displayed.
- Under **Analyze**, click **Alerts & Events**.
By default, the **Alerts & Events** page displays the alert and events in the **List** view.
The **Alerts & Events** page offers a list view and summary view, and a configuration view.



Configuration view is only available at the **Global** context.

- To view the graphs displaying alerts and events, click the **Summary** icon. By default, **ALL** tab is selected. Select each tab **Access Points, Switches, or Controllers** to view the graphs pertaining to each device type.



The **Alerts & Events** graphs are displayed for the time range selected. Select the time range from the Time Range Filter (🕒) to filter alerts and events.

The graphs in the **Summary** view displays the alerts and events in the following categories:

- **Alerts By Type**—Displays the alert categories under which the maximum alerts are generated. Hover your mouse over the bar graphs to see the total count of alerts generated under each category.
- **Alerts By Severity**—Displays the alert severity categorized under **Critical, Major, Minor, and Warning**. Hover your mouse to see the total count of alerts generated under each severity level.
- **Events By Type**—Displays the event categories under which the maximum events are generated. Hover your mouse over the bar graphs to see the total count of events generated under each category.

Configuring Alerts

To configure alerts, complete the following steps:

1. In the **Network Operations** app, use the filter to select **Global**.
The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Alerts & Events**.
The **Alerts & Events** page is displayed in the **List** view.
3. In the **Alerts & Events** page, click the **Config** icon.
The **Alert Severities & Notifications** is displayed.
4. Use the tabs to navigate between the alert categories.
5. Optionally, for **Access Point, Switch, Controller, and Central System** alerts, you can click the **Enable All** or **Disable All** button respectively to enable all the disabled alerts on a single click and vice versa. For more information on Enabled Alerts, see [Viewing Enabled Alerts](#).
6. Select an alert and click + to enable the alert with default settings. To configure alert parameters, click on the alert tile and do the following:
 - a. **Severity**—Set the severity. The available options are Critical, Major, Minor, and Warning. By default, the following alerts are enabled and the severity is **Major**:
 - Virtual Controller Disconnected
 - Rogue AP Detected
 - New User Account Added
 - Switch Detected
 - Switch Disconnected



For a few alerts, you can configure threshold value for one or more alert severities. Enter a value in the **exceeds** text box to set a threshold value for the alerts. The alert is triggered when one of the threshold values exceed the duration.

- b. **Duration**—Enter the duration in minutes.
- c. **Device Filter Options**—(Optional) You can restrict the scope of an alert by setting one or more of the following parameters:
 - **Group**—Select a group to limit the alert to a specific group.
 - **Label**—Select a label to limit the alert to a specific label.
 - **Device**—Select a device to limit the alert to a specific device.
 - **Site**—Select a site to limit the alert to a specific site.

d. Other Filter Options

- **Band**—For few **Access Point** alerts, you can select the band, 2.4 GHz or 5 GHz to limit the alert to a specific band.
- **Interface**—For few switch port alerts, you can mention an interface value to limit the alert criteria to a specific port.
- **SSID**—For few **Connectivity** alerts, you can select a SSID to limit the alert to a specific SSID.

e. Notification Options

- **Email**—Select the **Email** check box and enter an email address to receive notifications when an alert is generated. You can enter multiple email addresses, separate each value with a comma. The **Default Recipient** check box is selected by default. If you want to disable specific email addresses from the default list to avoid sending alert notification, click the number displayed in parenthesis and click  against each email address. To add or delete default recipient, see [Adding Default Recipients](#). Uncheck the **Default Recipient** check box in order to disable alert notifications to all the default email addresses.



The number displayed in the parenthesis denotes the total number of email addresses that have been already configured as default recipients to receive notifications when an alert is generated.

- **Streaming**—Select the **Streaming** check box to receive the streaming notifications when an alert is generated.
 - **Webhook**—Select the **Webhook** check box and select the Webhook from the drop-down list. For more information on Webhooks, see *Aruba Central Help Center*.
 - **Syslog**—Select the **Syslog** checkbox to receive the syslog notifications when an alert is generated.
 - **SNMP Trap**—Select the **SNMP Trap** checkbox to receive SNMP notifications when an alert is generated.
- f. Click **Save**.
- g. **Add Rule**—(Optional) For a few alerts, the **Add Rule** option appears. For such alerts, you can add additional rule(s). The rule summaries appear at the top of the page.



You can use the **Search box**, to search for alerts using keywords.

User Alerts

Aruba Central allows you to configure and enable the following user management alerts:

- **New User Account Added**—Generates an alert when a new user account is added. This alert is enabled by default and the alert severity is **Major**.
- **User Account Deleted**—Generates an alert when a user account is deleted.
- **User Account Edited**—Generates an alert when a user account is edited.

Access Point Alerts

Aruba Central allows you to configure and enable the following access point (AP) alerts:



To enable or disable all the access point alerts on a single click, you can use the **Enable All** or **Disable All** button respectively.

- **New Virtual Controller Detected**—Generates an alert when a new virtual controller is detected.
- **Virtual Controller Disconnected**—Generates an alert when a virtual controller is disconnected. This alert is enabled by default and the alert severity is **Major**. In the **Duration** field, enter the duration after which the alert must be generated. The default value is 10 minutes.
- **New AP Detected**—Generates an alert when a new AP is detected.
- **AP Disconnected**—Generates an alert when an AP is disconnected. In the **Duration** field, enter the duration after which the alert must be generated. The default value is 15 minutes.
- **Rogue AP Detected**—Generates an alert when a rogue AP is detected. This alert is enabled by default and the alert severity is **Major**.
- **Infrastructure Attack Detected**—Generates an alert when an infrastructure attack is detected.
- **Client Attack Detected**—Generates an alert when a client attack is detected.
- **Uplink Changed**—Generates an alert when an uplink has changed.
- **Modem Unplugged**—Generates an alert when the modem is unplugged.
- **Modem Plugged**—Generates an alert when the modem is plugged.
- **AP CPU Utilization**—Generates an alert when the AP CPU utilization exceeds the threshold value. In the **Duration** field, enter the duration after which the alert must be generated. You can add additional rule(s) for this alert.
- **AP Memory Utilization**—Generates an alert when the AP memory utilization exceeds the threshold value. In the **Duration** field, enter the duration after which the alert must be generated. You can add additional rule(s) for this alert.
- **Insufficient Power Supplied**—Generates an alert when the AP is supplied with lesser power than the required power.
- **AP With Missing Radios**—Generates an alert when the AP radio is faulty.
- **Radio Channel Utilization**—Generates an alert when the AP radio channel utilization exceeds the threshold value. In the **Duration** field, enter the duration after which the alert must be generated. From the **Band** drop-down, select the spectrum band: **2.4 GHz** or **5 GHz**. You can add additional rule(s) for this alert.
- **Radio Noise Floor**—Generates an alert when the Noise Floor (dBm) exceeds the threshold value. In the **Duration** field, enter the duration after which the alert must be generated. From the **Band** drop-down, select the spectrum band: **2.4 GHz** or **5 GHz**. You can add additional rule(s) for this alert.
- **Connected Clients per VC**—Generates an alert when the number of connected clients to the VC exceeds the threshold value. In the **Duration** field, enter the duration after which the alert must be generated. You can add additional rule(s) for this alert.
- **Connected Clients per AP**—Generates an alert when the number of connected clients to the AP exceeds the threshold value. User can enter the threshold value after which the alerts must be generated. The recommended value is 15 minutes and above. You can add additional rule(s) for this alert.
- **Radio Frames Retry Percent**—Generates an alert when the AP radio frames retry percent exceeds the threshold value. In the **Duration** field, enter the duration after which the alert must be generated. From the **Band** drop-down, select the spectrum band: **2.4 GHz** or **5 GHz**. You can add additional rule(s) for this alert.
- **IAP Firmware Upgrade Failed**—Generates an alert when there is any IAP upgrade failure such as, no firmware image is available or there is no response from the device.
- **Radio Non Wifi Utilization**—Generates an alert when the AP radio non-Wi-Fi utilization exceeds the threshold value. In the **Duration** field, enter the duration after which the alert must be generated. From

the **Band** drop-down, select the spectrum band: **2.4 GHz** or **5 GHz**. You can add additional rule(s) for this alert.

- **AP Tunnel Down**—Generates an alert when a single L3 tunnel configured on the AP goes down.
- **All AP Tunnels Down**—Generates an alert when all the L3 tunnels configured on the AP go down.

Switch Alerts

Aruba Central allows network administrators and users with admin permissions to configure alerts. For more information, see [Configuring Alerts](#).

Following are the switch alerts that you can configure:



To enable or disable all the switch alerts on a single click, you can use the **Enable All** or **Disable All** button respectively.

- **New Switch Connected**—Generates an alert when a new switch is connected.
- **Switch Disconnected**—Generates an alert when a switch is disconnected. This alert is enabled by default and the alert severity is **Major**. In the **Duration** field, enter the duration after which the alert must be generated. The default value is 10 minutes.
- **Switch Mismatch Config**—Generates an alert when there is a mismatch in switch configuration.
- **Switch Hardware Failure**—Generates an alert when the switch hardware fails. The following are the typical hardware failures for Aruba switches:
 - Fan failure
 - Power supply failure
 - Redundant power supply failure
 - High temperature
 - Management module failures—Management module failed self-test or lost communication with management module
 - Slot failure—Lost communications detected, slot self-test failure or unsupported module, or chassis hot swap failure
 - Fabric power failure
 - Internal power supply: Fan failure
 - Internal power supply failure
 - Internal power supply main PoE power failure
 - Internal power supply: Main inlet exceeds/within total fault count
 - Bad driver—Too many undersized/giant packets
 - Bad transceiver—Excessive jabbering
 - Bad cable—Excessive CRC/alignment errors
 - Too long cable—Excessive late collisions
 - Over bandwidth—High collision or drop rate
 - Broadcast storm—Excessive broadcasts
 - Duplex mismatch HDx—Duplex mismatch. Reconfigure to Full Duplex
 - Duplex mismatch FDx—Duplex mismatch. Reconfigure port to Auto
 - Link flap—Rapid detection of link faults and recoveries
 - eMMC—Endurance Storage utilization Failure (AOS-CX)

- **Switch NAE Status**—Generates an alert when the **NAE Status** for the AOS-CX switches exceed the **Normal** value, based on the severity configured. This alert is disabled by default and the alert severity is **Major**. If you want to generate alerts for the **NAE Status** of value **Disabled**, then set the alert severity to **Warning**.
- **Switch CPU Utilization**—Generates an alert when the switch CPU utilization exceeds the threshold value. In the **Duration** field, enter the duration after which the alert must be generated. You can add additional rule(s) for this alert.
- **Switch Memory Utilization**—Generates an alert when the switch memory utilization exceeds the threshold value. In the **Duration** field, enter the duration after which the alert must be generated. You can add additional rule(s) for this alert.
- **Switch Port Tx Rate**—In the **Transform Function** drop-down, select either **absolute** or **percentage**. Select **absolute** to generate an alert if the data transmission rate of the port (in terms of Mbps) exceeds the threshold value. Select **percentage** to generate an alert if the data transmission rate of the port (in terms of utilization as a percentage of total bandwidth available) exceeds the threshold value. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **Switch Port Rx Rate**—In the **Transform Function** drop-down, select either **absolute** or **percentage**. Select **absolute** to generate an alert if the data reception rate of the port (in terms of Mbps) exceeds the threshold value. Select **percentage** to generate an alert if the data reception rate of the port (in terms of utilization as a percentage of total bandwidth available) exceeds the threshold value. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **Switch Port Input Errors**—Generates an alert when the percentage of input errors on the port exceeds the threshold value. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **Switch Port Output Errors**—Generates an alert when the percentage of output errors on the port exceeds the threshold value. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **Switch Port Duplex Mode**—Generates an alert when the port is operating in half-duplex mode. In the **Interface** field, enter the interface name.
- **Switch PoE Utilization**—Generates an alert when the PoE utilization for a port exceeds the critical and major threshold value. This alert is enabled by default and the alert severity is **Critical**. You can add additional rule(s) for this alert.
- **Switch STP Root Change**—Generates an alert when a switch configured as the Spanning Tree Protocol (STP) root is replaced by another switch in the LAN. This alert is enabled by default and the alert severity is **Major**.
- **Stack Member Added/Removed**—Generates an alert when a stack member is added or removed. This alert is enabled by default and the alert severity is **Major**.
- **Switch Stack Commander Change**—Generates an alert when there is a change in Stack commander. This alert is enabled by default and the alert severity is **Major**.
- **Switch Uplink Port Usage**—Generates an alert when the total uplink port usage of a switch at a site exceeds the configured value in gigabytes (GB) within a specified duration. The severity for this alert is **Warning**. In the **exceeds (in GB)** field, enter the uplink port usage value in GB. In the **Duration** field, enter the duration after which the alert occurs. The alert must be generated if the condition persists even after this duration.
- **Switch Reboot (AOS-S)**—Generates an alert when a switch reboots or crashes. This alert is enabled by default and the alert severity is **Critical**. This alert is applicable only for AOS-Switches with firmware version 16.10.0015 and later.

Controller Alerts

Aruba Central allows you to configure and enable the following Controller alerts:



To enable or disable all the controller alerts on a single click, you can use the **Enable All** or **Disable All** button respectively.

- **New Controller Connected**—Generates an alert when new controller is connected to NMS.
- **Controller Disconnected**—Generates an alert when authorized, monitored controller has failed to respond to the NMS.
- **Controller CPU Utilization**—Generates an alert when the controller CPU utilization exceeds the threshold value. You can add additional rule(s) for this alert.
- **Controller Memory Utilization**—Generates an alert when the controller memory utilization exceeds the threshold value. You can add additional rule(s) for this alert.
- **Controller Cluster AP Capacity**—Generates an alert when the Controller Cluster AP capacity exceeds the threshold limit. This alert is applicable to Controller Cluster deployment.
- **Controller Cluster Client Capacity**—Generates an alert when the Controller Cluster Client capacity exceeds the threshold limit. This alert is applicable to Controller Cluster deployment.
- **Controller Cluster Tx Rate**—Generates an alert when the Controller Cluster Tx rate exceeds the threshold limit. This alert is applicable to Controller Cluster deployment.
- **Controller Cluster Rx Rate**—Generates an alert when the Controller Cluster Rx rate exceeds the threshold limit. This alert is applicable to Controller Cluster deployment.
- **Connected Clients to Controller**—Generates an alert when the total client count on the controller exceeds the threshold limit. This alert is applicable for all the controllers in different deployments.
- **Controller Tx Rate**—Generates an alert when the controller level Tx value exceeds the threshold limit. This alert is applicable for all the controllers in different deployments.
- **Controller Rx Rate**—Generates an alert when the controller level Rx value exceeds the threshold limit. This alert is applicable for all the controllers in different deployments.
- **Controller Port Input Errors**—Generates an alert when the controller port input errors rate exceeds the threshold.
- **Controller Port Output Errors**—Generates an alert when the controller port output errors rate exceeds the threshold.
- **Controller Port Tx Rate**—Generates an alert when the controller port Tx rate exceeds the threshold.
- **Controller Port Rx Rate**—Generates an alert when the controller port Rx rate exceeds the threshold.

Connectivity Alerts

Aruba Central allows network administrators and users with admin permissions to configure alerts. For more information, see [Configuring Alerts](#).

Following are the connectivity alerts that you can configure:

- **DNS Delay Detected**—Generates an alert when clients experience significant delays in response from the DNS server. Set the severity values to generate an alert if the percentage of delay from the DNS server exceeds the threshold value. The **Duration** field displays the duration after which the alert is generated. The default value is 30 minutes. You can add additional rule(s) for this alert.
- **DNS Failure Detected**—Generates an alert when wireless APs experience a high number of connection failures with the DNS server. Set the severity values to generate an alert if the DNS failure percentage

exceeds the threshold value. The **Duration** field displays the duration after which the alert is generated. The default value is 30 minutes. You can add additional rule(s) for this alert.

- **DHCP Delay Detected**—Generates an alert when there is excessive DHCP delay from client to AP in the network. Set the severity values to generate an alert if the percentage of the DHCP delay exceeds the threshold value. The **Duration** field displays the duration after which the alert is generated. The default value is 30 minutes. You can add additional rule(s) for this alert.
- **DHCP Failure Detected**—Generates an alert when there is high number of DHCP failure observed from client to AP in the network. Set the severity values to generate an alert if the DHCP failure percentage exceeds the threshold value. The **Duration** field displays the duration after which the alert is generated. The default value is 30 minutes. You can add additional rule(s) for this alert.
- **Authentication Delay Detected**—Generates an alert when there is excessive delay in the client authentication process with the AP in the network. Authentication failures include the following:
 - Wi-Fi security key-exchange failures
 - 802.1x authentication failures
 - MAC authentication failures
 - Captive failures

Set the severity values to generate an alert if the percentage of the authentication delay exceeds the threshold value. The **Duration** field displays the duration after which the alert is generated. The default value is 30 minutes. You can add additional rule(s) for this alert.

- **Authentication Failure Detected**—Generates an alert when there are high number of client authentication failures in the network. Authentication failures include the following:
 - Wi-Fi security key-exchange failures
 - 802.1x authentication failures
 - MAC authentication failures
 - Captive failures

Set the severity values to generate an alert if the authentication failure percentage exceeds the threshold value. The **Duration** field displays the duration after which the alert is generated. The default value is 30 minutes. You can add additional rule(s) for this alert.

- **Association Delay Detected**—Generates an alert when client association delay is detected in the network. Set the severity values to generate an alert if the percentage of the association delay exceeds the threshold value. The **Duration** field displays the duration after which the alert is generated. The default value is 30 minutes. You can add additional rule(s) for this alert.
- **Association Failure Detected**—Generates an alert when client association failure is detected in the network. Set the severity values to generate an alert if the association failure percentage exceeds the threshold value. The **Duration** field displays the duration after which the alert is generated. The default value is 30 minutes. You can add additional rule(s) for this alert.

Audit Alerts

Aruba Central allows administrators to enable alerts for configuration changes at group level. The **Config Change Detected** alert is under **Audit** tab. Configuration change alerts are intended for administrators handling large distributed network. Alerts are triggered under the following scenarios:

- Create New Template
- Update Existing Template

- Variable Upload
 - Device Level: Sends an alert with additional parameters such as serial number and MAC address of the device.
 - Group Level: Sends an alert with respective group name.
 - Configuration restore
- Configuration change at Device Level
- Configuration change at Group Level

The alert content includes the following information:

- Group Name
- Device Type
- User ID
- Config Change
- Device Serial number and MAC Address

The following table describes the behavior of the alert and alert content depending on the user action:

Table 217: *Config Alert Behavior*

User Action	Group Name	Device Type	User ID	Config Change	Device Serial/ MAC
Created a template	Template group name	IAP/ Switch/ Gateway	User ID	No Content	NO
Updated existing template	Template group name	IAP/ Switch/ Gateway	User ID	Changed content is displayed	NO
Uploaded variable at device level	Group name to which the device belongs	IAP/ Switch/ Gateway	User ID	No Content	YES
Uploaded variable at group level	Template group name	IAP/ Switch/ Gateway	User ID	No Content	NO
Made configuration at the device level	Group name to which the device belongs	IAP/ Switch/ Gateway	User ID	Changed content is displayed	YES
Made configuration change at the group level	UI group name	IAP/ Switch/ Gateway	User ID	Changed content is displayed	NO

Central System Alerts

Aruba Central allows you to configure and enable the following Central System alerts:



To enable or disable all the central system alerts on a single click, you can use the **Enable All** or **Disable All** button respectively.

- **System CPU Utilization**—Generates an alert when the system CPU utilization exceeds the threshold value at a specific period of time.
- **Memory Utilization**—Generates an alert when the system memory utilization exceeds the threshold value at a specific period of time.
- **Disk I/O Utilization**—Generates an alert when the system disk I/O utilization exceeds the threshold value at a specific period of time.
- **Disk Usage**—Generates an alert when the system disk usage exceeds the threshold value at a specific period of time.
- **COP Service Status**—Generates an alert when the status of the service is red for a certain duration.
- **Infra CPU Usage**—Generates an alert for when a pod's CPU usage is above threshold for a specific period of time.
- **Infra Memory Usage**—Generates an alert when a pod's memory usage is above threshold for a specific period of time.
- **Infra Disk Usage**—Generates an alert when a node's disk usage is above threshold for a specific period of time. This alert is enable by default.
- **Infra Load Average**—Generates an alert when a node's load average is above threshold for a specific period of time.
- **Node Not Ready**—Generates an alert when a node is not up or is in **Not Ready** status for a specific period of time. This alert is enable by default.
- **COP Upgrade Schedule**—Generates an alert when there is a new COP version available for upgrade. The grace period for the upgrade is set to 30 days. If the upgrade is not performed, then the COP user interface is locked for the customers. By default, the alert severity is set to **Critical** and the alert interval is set to 3 days, which indicates that every 3 days a notification is sent to the customer to complete the upgrade.
- **COP Upgrade Check Failed**—If the COP system is not connected to the internet, and upgrade check fails, then the system generates an alert to inform the customer to connect to the internet in 45 days. If not connected then the COP user interface is locked for the customers. By default, the alert severity is set to **Critical** and the alert interval is set to 3 days, which indicates that every 3 days a notification is sent to the customer to connect to the internet.

Site Alerts

Aruba Central allows you to configure and enable this alert for aggregated device disconnects. Aggregate device disconnect is intended to reduce the number of alerts that are generated for customers that prefer to have a single notification or a handful of notifications for mass outages where several devices may go down simultaneously in a given site.

For example, if site alerts are configured with **Severity** as Major, **Duration** being 10 minutes, and **Site** as site1, a single alert saying "Aggregated Device Disconnects" is raised on the user interface for every set of device belonging to "site1" that goes down within 10 minutes of the first DOWN event limited to 100 devices per alert. Any device that is not a part of "site1" is treated as not being aggregated.

The alert content includes the following information for each device:

- Hostname
- Device Serial Number
- MAC Address
- IP Address



Unlike other alerts types, site alerts will not be auto closed.

Adding Default Recipients

To set default recipients for alert notification, complete the following procedure:

1. In the **Network Operations** app, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Alerts & Events**.
The **Alerts & Events** page is displayed in the **List** view.
3. In the **Alerts & Events** page, click the **Config** icon.
The **Alert Severities & Notifications** is displayed.
4. In the **Alert Severities & Notifications** page, click **Default Recipients**.
The **Default Recipients** dialog box is displayed.
5. Click the **+** icon to add the email address that you want add as a default recipient to receive notifications when an alert is generated.
You can add multiple email addresses as required.
6. Click **Save**.



-
- You can also delete the existing email addresses that is already added as default recipients.
 - While configuring email addresses in the site dashboard, select the **Override** or **Append** button to either override or append the email addresses configured as default recipient in the global dashboard.
-

Suppressing Alert Notifications in the Site Dashboard

Suppressing alerts for a particular site prevents all devices within the site from generating alert notifications. You can enable alert suppression only at the **Site** level.

To suppress alerts, complete the following procedure:

1. In the **Network Operations** app, use the filter to select a **Site**.
The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Alerts & Events**.
The **Alerts & Events** page is displayed in the **List** view.
3. In the **Alerts & Events** page, click the **Config** icon.
The **Alert Notifications** screen is displayed.
4. Enable the **Suppress Alerts** toggle button.
5. To configure emails to receive notifications when an alert is generated, select one of the following options:
 - **Override**—When this option is selected, the effective email list that receives alert notification are the email addresses configured at the site level.
 - **Append**—When this option is selected, the effective email list that receives alert notification includes the configured default recipients list, emails configured at individual alert level, and emails configured at the site level.

When none of these options are configured the effective email list that receives alert notifications include default recipients list and emails configured at individual alert level. For more information on configuring alert notifications and default recipients, see

6. Click the **+** icon to add the email address to receive notifications when an alert is generated. You can add multiple email addresses as required.
7. From the time range drop-down list, select one of the following:
 - **All time**—This allows you to suppress alerts permanently for the selected site.
 - **Custom date & time**—This allows you to customize the time range for which you want to suppress alerts for the selected site. Select the time range from the drop-down list and then, select the period for which you to suppress the alerts.
8. Click **Save**.

Configuring Site-specific Email Notifications

Aruba Central (on-premises) enables you to configure site-specific email addresses for notifying alerts. When alerts are generated for a specific site, the email notification is automatically sent to the email addresses configured for that site. The email addresses configured in the site dashboard overrides the email addresses configured in the global dashboard. For more information on configuring alerts in the global dashboard, see [Configuring Alerts](#).

To add an email address, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Sites**. The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Alerts & Events**. The Alerts & Events page is displayed in the **List** view.
3. Click the **Config** icon. The Alert Notifications page is displayed.
4. In the **Email Configuration Override** window, click **+** to add an email address.
5. In the text-box, enter a valid email address.
6. Click **Save**.



-
- You can add up to a maximum of 10 email addresses for alert notifications in the site dashboard.
 - When you configure email addresses in the site dashboard, it overrides the email addresses configured in the global dashboard.
-

Deleting an Email Address in the Site Dashboard

To delete an email address, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Sites**. The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Alerts & Events**. The Alerts & Events page is displayed in the **List** view.
3. Click the **Config** icon. The Alert Notifications page is displayed.

4. In the **Email Configuration Override** window, click the delete icon beside the email address, that you want to delete.
5. Click **Save**.

Viewing Enabled Alerts

To view alerts that you have enabled, complete the following procedure:

1. In the **Network Operations** app, use the filter to select **Global**.
The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Alerts & Events**.
The **Alerts & Events** page is displayed in the **List** view.
3. In the **Alerts & Events** page, click the **Config** icon.
The **Alert Severities & Notifications** is displayed.
4. In the **Alert Severities & Notifications** page, click **Enabled**.
Use the tabs to navigate between the alert categories. The alerts enabled for each category are displayed in the respective tabs.

Reports

The Aruba Central (on-premises) dashboard enables you to create various types of reports. To create a report, you must have Read/Write or Admin access.

The Reports feature is available for Foundation license of APs, switches, and gateways.

Viewing the Reports Page

To view the **Reports** page, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under groups, labels, or sites.
For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Reports**.
The Reports page is displayed in the **Summary** view.

The **Reports** page has the following sections:

- **Browse**—Allows you to browse through the generated reports.
- **Manage**—Allows you to manage the scheduled reports.
- **Create**—Allows you to create and schedule a report.

This section includes the following topics:

- [Report Categories](#)
- [Report Configuration Options](#)
- [Previewing a Report](#)
- [Creating a Report](#)
- [Editing a Report](#)
- [Viewing the Generated Report](#)

- [Viewing the Scheduled Report](#)
- [Downloading a Report](#)
- [Deleting a Report](#)

Report Categories

The following list provides information about the types of report under each category of the report. For information about how to configure the Context, Transport Type, Report Order, Top N Count, Classify On, Report Subtype, Report Period, Recurrence, and Report Information for a report, see [Report Configuration Options](#).

■ Clients

- **Client Inventory**—The Client Inventory report provides information about the total number of clients and the type of connected networks. This information aids the administrators in planning for scalability and evaluate the deviations from the baseline. The report displays the client details summarized by all aggregation fields and includes the following details:
 - Client count by SSID
 - Client count by role
 - Client count by connection mode
 - Client count by connection type
 - Client count by OS
 - Client count by vendors
- **Client Session**—The Client Session report monitors the sessions of all the users in the network and provides insights related to usage analysis and connectivity patterns. The report also projects the WLAN user experience to assist the user in measuring the efficiency of the deployed networks. The report displays the details of client sessions for the SSIDs provisioned on Instant APs and includes the following details:
 - Clients
 - Sessions
 - Traffic
 - Top 100 sites by poor WLAN health (2.4GHz / 5.0GHz / combined)
 - Session Data by OS / Connection Mode / SSID / Role / MAC Vendor
 - Clients by OS / Connection Mode / SSID / Role / MAC Vendor
 - Time Spent by OS / Connection Mode / SSID / Role / MAC Vendor
 - Data Usage by OS / Connection Mode / SSID / Role / MAC Vendor
 - Client Device OS / Connection Mode / SSID / Role / MAC Vendor
 - Top 10 clients by usage that you can filter by SSIDs or Connection Types
- **Client Usage**—The Client Usage report displays the client usage and client connectivity details to assist the administrator in planning the expansion of the network and the application requirements. The report displays the client usage and count details and includes the following details:
 - Client Usage
 - Top 10 Clients by Usage that you can filter by SSIDs or Connection Types
 - Client Count by Wireless / Wired
 - Top 10 Applications by Usage
 - Top 10 Web Categories by Usage

- Top 10 App Categories
- Web Reputation
- **Guest**—Displays the guests and guest session details for all the SSIDs for a specific time period. The Guest report provides visibility for all the users associated to the cloud guest network that assists the user in conducting campaigns and also provides analytics of the guest users in the network.



Guest report does not support location based filtering for any selected device group, site, or label to ensure end user privacy protection.

- **Summary**—Displays the details about the wireless and wired clients, and the usage details of the wireless and wired clients over a time period of one year. The Summary reports assists the user in measuring the Key Performance Indicator (KPI) trends over a time period of one year that aids the user in planning for scalability.

In the **Summary** report, you can choose to generate a report from **Trends** such as **Unique clients per day**, **Clients per SSID**, **Unique client sessions per day**, **Average client sessions per day**, **Average clients per day**, and **Usage over time**. The **Average clients per day** is the number of concurrent users at a given time (updated every five minutes). **Unique clients per day** is the total number of clients that were seen for that day. For example, consider a scenario where four clients were connected in a day, and after every hour, one client disconnected and another was connected. Then, the count for **Average clients per day** was four and **Unique clients per day** was 27 (3+24=27).

You can further chose to generate a report form **Top N Widgets** such as **Top clients by usage**, **Top OS by usage**, **Top APs by usage**, **Bottom APs by usage**, **Top sites by WLAN usage**, and **Bottom sites by WLAN usage**. The **Top sites by WLAN usage** and **Bottom sites by WLAN usage** options are only available under **Top N widgets** section, when you select **All** in the **Groups** context level. You can choose **Top 5**, **Top 10**, **Top 25**, or **Top 50** from the **Show Results** drop-down list to view the data for top 5, top 10, top 25, or top 50 widgets. The report displays wireless and wired clients, and wireless and wired usage for one year and includes the following details:

- Usage
- Total Data Transfer, Total Data Downloaded, and Total Data Uploaded
 - Unique clients per day
 - Average clients per day
 - Clients per SSID
 - Unique client sessions per day
 - Average client sessions per day
 - Usage over time
- Top N Widgets—Top 5, Top 10, Top 25, or Top 50
 - Top OS by usage
 - Top APs by usage
 - Bottom APs by usage
 - Top sites by WLAN usage
 - Bottom sites by WLAN usage



Summary report is supported from Aruba Central 2.5.2 onwards and the data is available only after an upgrade to version 2.5.2 or later. Data prior to the 2.5.2 upgrade is not available in the report.

■ Infrastructure

- **Capacity Planning**—The Capacity Planning report provides information about the subscription utilization and most used devices in the network that assists the administrator to add more devices in a specific location to enhance the scalability and to increase the uplink capacity of the switching infrastructure. The report displays the throughput and client density information for devices provisioned in Aruba Central and includes the following details:
 - Subscription Utilization
 - Total Subscription, Used subscriptions, and Available subscriptions
 - Top 25 APs by usage
 - Top 25 switches by usage
 - Top 25 APs by peak clients
 - Top 25 APs by average clients
- **Configuration & Audit**—Displays the configuration and audit logs for all the device management, configurations, and user management events triggered in Aruba Central. The Configuration & Audit report aids the user in tracking the configuration changes in the network that assists in tracking the deviations from the IT policies. The context available for this report is only **Groups** and **Show overrides** option under **Audit Report**. The report displays the configuration and audit logs for all the device management, configurations, and user management events triggered in Aruba Central and includes the following details:
 - Configuration Audit Status
 - Aruba Switches Configuration Audit Status
 - Virtual Controllers Configuration Audit Status
- **Infra Inventory**—Displays the inventory and subscription information for the devices that are online or offline during a specific time period. The Infra Inventory report aids the user in maintaining a record of the infrastructure devices and validate the firmware versions compliance. The report displays the inventory and subscription information for the devices that are online during a specific duration and includes the following details:
 - Subscription Utilization
 - Total Subscription, Used subscriptions, and Available subscriptions
 - Subscription Keys
 - Number of APs
 - Number of Switches
 - Number of Gateways
 - Firmware Version Summary (AP)
 - Firmware Version Summary (Switch)
 - Firmware Version Summary (Gateway)
 - Devices by Site
 - Model and Firmware version (AP)
 - Model and Firmware version (Switch)
 - Model and Firmware version (Gateway)
 - AP interfaces summary
- **Network**—Displays the summary details of the network that aids the user in measuring the availability of every device in the network and projects compliance to the defined Network SLAs. The report displays the following parameters:



The - (hyphen) symbol in the **Uptime** column in **APs** table indicate that the IAP is in offline status.

- Top-Bottom Sites
 - Top 20 Sites By Availability
 - Bottom 20 Sites By Availability
 - Top 20 Sites By WLAN Usage
 - Bottom 20 Sites By WLAN Usage
- Number of APs
 - Name, Model, Virtual Controller, IP Address, Uptime, and Availability
 - AP model
- Number of Clients that you can filter based on SSIDs or Connection Types
 - Top Ten Clients by Usage
 - Device Types (Current)
- Data Usage
 - Top Ten APs By Usage
 - Total Usage By SSID
 - Wireless Clients by SSID
 - Wired Clients
 - Peak and Average Wireless Data Usage
 - Peak and Average Wired Data Usage
- Number of Switches
 - Switch Model
 - Top Ten Switches by Usage
 - Top Ten Ports by Usage
 - Switch Wired Peak and Average Uplink Stats
- Number of Gateways
 - Gateway Model
- **New Infra Inventory**— The New Infra Inventory report provides detail of the infrastructure devices added in a time period that assists the administrator in validating the network deployment progress against the deployment schedule. The report displays the inventory and subscription information to the devices that are newly added in Aruba Central and includes the following details:
 - Subscription Utilization
 - Total Subscription, Used subscriptions, and Available subscriptions
 - Subscription Keys
 - APs Added by Model
 - APs Added by Group
 - Switches Added by Model
 - Switches Added by Group
 - Gateways Added by Model
 - Gateways Added by Group
 - Total APs

- Total Switches
- Total Gateways
- **Resource Utilization**—Displays the details of the infrastructure devices that exceeded the configured thresholds on a daily, weekly, and monthly basis in the report. The Resource Utilization report provides information about the devices with high CPU and memory utilization that assists the administrator in evaluating the deviations against the device utilization baselines. The report displays the details of infrastructure devices that exceeded the configured thresholds on a daily, weekly, and monthly basis and includes the following details:
 - Resource Utilization Threshold
 - CPU/Memory Compliance
 - Sites with Non-Compliant Devices
 - Non-Compliance by Device Type
 - Non-Compliant Access Points
 - Non-Compliant Switches
 - Non-Compliant Gateways
- **RF Health**—The RF Health report provides details of the radios of an access point that has poor health indicators. This information assists the administrator in evaluating the deviation from the network baselines. The report displays the following RF usage statistics for the AP radios:
 - Problem Radios (5 GHz / 2.4 GHz)
 - Most Noise (5 GHz / 2.4 GHz)
 - Most Errors (5 GHz / 2.4 GHz)
 - Most Utilized by Channel Usage (5 GHz / 2.4 GHz)
 - Least Utilized by Channel Usage (5 GHz / 2.4 GHz)
 - Most Channel Changes (5 GHz / 2.4 GHz)
 - Most Transmit Power Changes (5 GHz / 2.4 GHz)
 - Radio with Least Goodput (5 GHz / 2.4 GHz)



For APs that support 5 GHz dual band in synchronization with Aruba Instant 8.3.0.0, the **Device** column in the **RF Health Report** shows the radio number of the operating radio along with the model number of the device.

- **Switch Capacity Planning**—The Switch Capacity Planning report provides an user with insights on the used and unused ports usage along with power consumed by clients that helps the user plan for scalability. The report displays the following details about the switch ports usage:
 - Total Used / Unused Switch Ports
 - Switch Port Summary
 - Switch POE Usage Summary



The data for this report is generated only after you upgrade to Aruba Central version 2.5.2. You can view or generate the report for 1, 7, 30, and 90 days after upgrading to Aruba Central version 2.5.2.

- **WAN Availability**—The report displays the WAN overlay and underlay availability information. The report displays WAN overlay and underlay availability information.

- The Underlay report with either Best Performing or Worst Performing option contains the following details:
- Branch Gateway
 - Site
 - Serial Number
 - Host name
 - MAC
- Uplink
 - VLAN
- Tunnel
 - Tunnel Name
- %Uptime
- Uptime
- Downtime
 - The Overlay report with either Best Performing or Worst Performing option contains the following details:
- Branch Gateway
 - Site
 - Serial Number
 - Host name
 - MAC
- Uplink
 - VLAN
- Tunnel
 - Tunnel Name
- %Uptime
- Uptime
- Downtime
 - **WAN Inventory**—Displays a list of Branch Gateways onboarded. The report is segregated by ArubaOS software version. The report displays the following information for each ArubaOS version:
 - Software Version
 - Site Name
 - Serial Number
 - Host name
 - MAC
 - IP Address
 - Model
 - Status
 - Street Address
 - **WAN Compliance**—Displays the worst performing or best performing links according to the SLA compliance violations and contains the following details:

- Policy Name
- Branch Gateway
- Site
- Serial Number
- Host Name
- MAC
- Uplink
 - Name
 - Type
- Value
 - Compliance
 - **WAN Transport Health**—Displays the top N links with probed values for overlay or underlay best or worst performance. The report contains the following details:
 - Loss
 - Latency
 - Jitter
 - Probe Destination IP
- Branch Gateway
 - Site
 - Serial Number
 - Host name
 - MAC
- Uplink
 - Name
 - Type
- Value
 - Loss (%) or Latency (ms) or jitter (ms)
 - **WAN Utilization**—Displays WAN bandwidth utilization information for underlay, overlay, or overall network with most or least order. The report contains the following details:
 - Branch Gateway
- Site
- Serial Number
- Host name
- MAC
 - Uplink
- Name
- Type
- VLAN
 - Usage

- Average Bandwidth (Mbps)
- SLA Bandwidth (Mbps)
- %Utilization
 - **WAN Web Content Classification**—The WAN Web Content Classification report provides information regarding the URLs, IP reputations, and geo-locations that aids an user in implementing policy enforcements. The report contains the following details:
 - Site
 - Serial #
 - Hostname
 - MAC
 - Top 5 Web Reputation
 - Web Category
 - Destination
 - Total Usage
- **Security Compliance**
 - **PCI Compliance**—Displays the PCI Compliance result with the number of violations and the PCI DSSv3.2 for an Instant AP. The PCI compliance report automatically executes some of the test cases of the PCI DSS test requirements and projects compliance results that reduces the manual efforts in validating the test cases. The report displays the following details:
 - Netmask
 - Compliance result as Fail or Pass with the number of violations
 - PCI DSSv3.2
 - Description
 - Result
 - **RAPIDS**—Displays the details of all the rogue devices in the network that aids the administrator about the possible threat and provides essential information needed to locate and manage the threat. The report contains the following details:
 - Name
 - Classification
 - Encryption
 - Last Detecting Device
 - First seen
 - Last seen
 - SSID
 - Radio
 - Radio MAC
 - Total Detecting Devices
 - **Security Compliance**—Displays the details of the rogue APs and wireless intrusions detected in the network that assists the administrator in validating the compliance to the security guidelines. The report includes the following details:
 - Rogue APs
 - MAC Address
 - Detecting AP

- Date/Time Detected
- SSID
- MAC Vendor
- Channel
- RSSI
- Wireless Intrusions
- Total Wireless Intrusions
- **Applications**
 - **AppRF**—Displays the application usage report for a specific device group in the network. The AppRF report provides information about the application usage patterns and the web usage patterns in the network that assists the administrators in evaluating the deviations from the data usage patterns. The report displays the following widgets:
 - Top 10 applications accessed by the clients
 - Top 10 web categories accessed by the clients
 - Top 10 applications for device types
 - Others
 - Application
 - Total Bytes

Important Points to Note

- When you select **Custom range** under **Report Period**, the **Every day**, **Every week**, and **Every month** options are not available under **Recurrence**.
- For the **Client Session** report, the **Show Detailed Report** option is available only for a selected site. Selecting this option restricts the **Report Period** to **Last Day** and **Custom Range** only. Selecting custom range enables you to select a one day time range from the particular day till the last seven days only.
- In the **Infra Inventory** report, select the **Offline** option in the **Device Inventory** section to generate the report with details of the devices that are offline. The PDF displays the distribution of inactive devices by the device type and CSV displays the list with additional information.
- In the **Configuration and Audit** report with local overrides details, the count for device override is available only for the **Groups** context. To include local overrides column in the **Configuration and Audit** report, select the **Show Override** option in the **Audit Report** section.
- When a new switch connects to Aruba Central, the **Last Used at** and **Unused Since (Days)** columns value is displayed as **NA** for all the ports that are down in the .csv file, that is created for the Switch Ports in the **Switch Capacity Planning** report. When a port continues to be in a down state, the **Last Used at** and **Unused Since (Days)** columns value will be displayed as **NA** for the time period of the generated report.

Report Configuration Options

Aruba Central allows you to create various types of reports based on your network requirements. For information about each type of report, [Report Categories](#).

The types of report categories supported by Aruba Central are:

- **Clients**
- **Infrastructure**

- **Security Compliance**
- **Applications**

Sections in Reports

Context

Allows you to select the context for which you want to create the report. Select one of the available options from the following:

- **Groups**—Allows you to generate the report for the devices attached to a group.
 - **Filter By**—Select either **Roles** or **SSIDs** to filter the devices within the selected group(s) based on their roles or SSIDs.
 - **Roles**—Select a device from the list of roles for which you want to generate the report.
 - **SSIDs**—Select a device from the list of SSIDs for which you want to generate the report.
 - **Trends**—Select a trend or multiple trends from the list for which you want to generate the report. Select **All** to generate the report for all the available trends in the list. Allows you to generate the report to view the data for one year for trends such as **Unique clients per day**, **Clients per SSID**, **Unique client sessions per day**, **Average client sessions per day**, **Average clients per day**, and **Usage over time**.
 - **Top N Widgets**—Select a widget or multiple widgets from the list for which you want to generate the report. Select **All** to generate the report for all the available widgets in the list. Allows you to generate the report to view the data for one year for widgets such as **Top clients by usage**, **Top OS by usage**, **Top APs by usage**, **Bottom APs by usage**, **Top sites by WLAN usage**, and **Bottom sites by WLAN usage**.
 - **Audit Report**—Select **Show Overrides** to include the override data of the devices within the group in the **Configuration & Audit** report.
 - **Device Inventory**—Select **Offline** to include the details of the offline devices within the group in the **Infra Inventory** report.
 - **Threshold**—Select the **Same as AP threshold** check-box to set the same threshold as the AP. Allows you to set the percentage of the CPU and the memory thresholds for APs, switches, and gateways within the group.
 - **Criteria**—Select **Used/Unused Ports** and/or **PoE** to include the data regarding the used ports, unused ports, and/or PoE usage in the **Switch Capacity Planning** report. When you select **Used/Unused Ports**, the **Switch Port Summary** report is generated. When you select **PoE**, the **Switch PoE Usage Summary** report is generated. The individual port details are available only in the .csv export of the **Switch Port Summary** report.
 - **Subnet/SSID List**—Select **Subnet/SSID List** to generate the report based on the CDE SSIDs or CDE subnets.
 - **CDE SSIDs**—Select an SSID from the list for which you want to generate the report.
 - **CDE Subnets**—Select a subnet from the list for which you want to generate the report.
- **Label**—Allows you to generate the report for the devices attached to a label.
 - **Label**—Select a label or multiple labels from the list for which you want to generate the report. Select **All** to generate the report for all the available labels in the list. The search bar allows you to filter a label from the list.

- **Site**—Allows you to generate the report for the devices attached to a site.
 - **Site**—Select a site or multiple sites from the list for which you want to generate the report. Select **All** to generate the report for all the available sites in the list. The search bar allows you to filter a site from the list.
 - **Detailed Report**—Select **Show Detailed Report** to include the client session details for each client within the site in the **Client Session** report.

Transport Type

Select one of the available options from the following:

- **Overlay**—Select **Overlay** you to include the WAN overlay availability information in the report.
- **Underlay**—Select **Underlay** to include the WAN underlay availability information in the report.
- **Internet**—Select **Internet** to include details of WebCC over the internet in the report.
- **VPN**—Select **VPN** to include details of WebCC over the VPN tunnel in the report.

Report Order

Select either **Best Performing** or **Worst Performing** to include the details of the best or worst performing WAN interfaces in the report.

Top N Count

Enter the range in the **Top N** for the number of results you want the include in the report. The Top N range should be between 1 to 250.

Classify On

Select either **web category** or **web reputation** to include data about the total usage of each device based on the web reputation or web category in the report.

Report Subtype

Select either **summary report** or **blocked urls report** to include the summary or blocked urls details in the report. A blocked URLs report will contain blocked URL Information along with the number of attempted session count.

Optional Widgets

Select the required options to include in the CSV format of the RF Health report:

- **RF Details (CSV)**—Select **RF Details (CSV)** to include the radio details in the CSV report.
- **IAP Uplink Usage (CSV)**—Select **IAP Uplink Usage (CSV)** to include the usage details of an IAP uplink in the CSV report.

Report Period

Specify the time period for which you want to create the report. Select one of the available options from the following:

- **Last day**—Select **Last day** to generate the report for the last day.
- **Last 7 days**—Select **Last 7 days** to generate the report for the last 7 days.
- **Last 30 days**—Select **Last 30 days** to generate the report for the last 30 days.
- **Last year**—Select **Last year** to generate the Summary report for the last year.

- **Custom range**—Select **Custom range** to generate the report for a time period within the last 90 days. When you select **Custom range**, the **Date Range** option is displayed. In the **Date Range** window, select a time period within the last 90 days for which you want to create the report.



The **Custom range** for the Summary report is available for the last one year, except the current date (today). All other reports are available for 90 days.

Recurrence

Select **Recurrence** to schedule the report. Select one of the available options from the following:

- **One time (Now)**—Select **One time (Now)** to schedule the report generation once for the current time.
- **One time (Later)**—Select **One time (Later)** to schedule the report generation once for a later time. When you select **One time (Later)**, the **Run Day** and **Run Time** options are displayed. In the **Run Day** window, select the date for which you want to schedule the report. In the **Run Time** window, select the time for which you want to schedule the report.
- **Every day**—Select **Every day** to schedule the report generation for every day. When you select **Every day**, the **Run Time** option is displayed. In the **Run Time** window, select the time for which you want to schedule the report.
- **Every week**—Select **Every week** to schedule the report generation for every week. When you select **Every week**, the **Run Day** and **Run Time** options are displayed. In the **Run Day** window, select the day for which you want to schedule the report. In the **Run Time** window, select the time for which you want to schedule the report.
- **Every month**—Select **Every month** to schedule the report generation for every month. When you select **Every week**, the **Run Day** and **Run Time** options are displayed. In the **Run Day** window, select the date from the **Day** drop-down list for which you want to schedule the report. In the **Run Time** window, select the time for which you want to schedule the report.

Report Information

Allows you to add a title, an email address, and specify the format of report to receive the email. Enter the following information:

- **Report title**—Enter the title of the report.
- **Email to**—Enter an email address to receive the report over an email.
- **Email Format**—Select **PDF** and/or **CSV** to specify the format of the report to receive the email.

Previewing a Report

Aruba Central allows you to preview a type of report prior to generating the report. The preview of the report displays dummy values.

To preview the report, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Reports**.
The Reports page is displayed in the **Summary** view.

3. Click **Create**.
The Reports page is displayed in the **List** view.
4. Hover over a report and then click **Preview** to preview the report.

The preview report provides the following details:

- **Report Name**—Name of the report.
- **Report Type**—Type of the report.
- **Date Run**—Time when the report was last run.
- **Group/Device**—The group or device for which the report was run.



In the preview of the report, the **PDF**, **CSV**, and **Email to** icons are dummy icons.

For more information about the reports under each category, see [Report Categories](#).

Creating a Report

Aruba Central (on-premises) allows you to generate a report for devices associated with a group, multi-group, label, or a site.



Although your page view is set to a specific group, site, or label, you can create reports for a different group, site, or a label. However, if your page view is set to an Instant Access Point (IAP) cluster or switch, you can schedule a report only for that IAP cluster or switch.

To create a report, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Reports**.
The Reports page is displayed in the **Summary** view.
3. Click **Create**.
The Reports page is displayed.
4. Select the type of report you want to create and then click **Next**.
5. Based on the type of report you select, a few options are displayed. Select one of the available options to set the context of the report. For example, for the **Client Inventory** report, select one of the available options under **Context**, which is either **Groups, Labels, or Sites**. Select **Groups** to generate reports for the devices attached to a group. Select **Labels** to generate reports for the devices attached to a label. Select **Sites** to generate reports for the devices attached to a site. Based on your selection of the context, further options are displayed to help create a report with more details. For more information, see [Report Categories](#).
6. Click **Next**.
The **Report Period** option is displayed.
7. Under **Report Period**, select one of the available options to create a report for the last day, last 7 days, last 30 days, last year, or for a custom range.



The **Custom range** for the Summary report is available for the last one year, except the current date (today). All other reports are available for 90 days.

8. Click **Next**.

The **Recurrence** option is displayed.

9. Under **Recurrence**, select one of the available options to schedule a report for the current time, later time, every day, every week, or every month.
10. Under **Report Information**, enter the title of the report and an email address.
11. Select **PDF** and/or **CSV** to specify the format of the report to receive the email.
12. Click **Generate**.

The report gets generated and is displayed under the **Scheduled Reports** table. The report gets emailed as an attachment to the email address provided.

Editing a Report

Aruba Central allows you to edit a report for devices associated with a group, multi-group, label, or a site.

To edit a report, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.

The dashboard context for the selected filter is displayed.

2. Under **Analyze**, click **Reports**.

The Reports page is displayed in the **Summary** view.

3. Click **Manage**.

The **Scheduled Reports** table is displayed in the **Config** view.

4. In the **Scheduled Reports** table, select a report and then click the edit icon.

The report that you want to edit is auto-selected in the **Reports** page.

5. Click **Next**.

6. Based on the type of report you select, a few options are displayed. Select one of the available options to set the context of the report. For example, for the **Client Inventory** report, select one of the available options under **Context**, which is either **Groups, Labels, or Sites**.

- **Groups**—Select **Groups** to generate reports for the devices attached to a group.

- **Labels**—Select **Labels** to generate reports for the devices attached to a label.

- **Sites**—Select **Sites** to generate reports for the devices attached to a site.

Based on the selected context, further options are displayed to create a report with more details. For more information, see [Report Configuration Options](#).

7. Click **Next**.

The **Report Period** option is displayed.

8. Under **Report Period**, select one of the available options to edit a report for the last day, last 7 days, last 30 days, last year, or for a custom range.



The **Custom range** for the Summary report is available for the last one year, except the current date (today). All other reports are available for 90 days.

9. Click **Next**.
The **Recurrence** option is displayed.
10. Under **Recurrence**, select one of the available options to re-schedule a report for the current time, for a later time, every day, every week, or every month.
11. Under **Report Information**, edit the title of the report and an email address.
12. Select **PDF** and/or **CSV** to specify the format of the report to receive the email.
13. Click **Generate**.
The report gets generated and is displayed under the **Scheduled Reports** table. The report gets emailed as an attachment to the email address provided.

Viewing the Generated Report

To view a generated report, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Reports**.
The Reports page is displayed in the **Summary** view.
3. Click **Browse**.
The **Generated Reports** table is displayed in the **List** view.
4. In the **Generated Reports** table, click a report name listed under **Title**.
The report details are displayed.

The **Generated Reports** table provides the following information:

- **Title**—Name of the report. Click  to filter the report based on the name of the report.
- **Date Run**—Timestamp indicating when the report was generated.
- **Group/Device**—The group or device for which the report was generated.
- **Label/Site**—The label or site for which the report was generated.
- **Type**—Type of report. Click  to filter the report based on the type of the report. Click  to select a type of report from the drop-down list.
- **Created By**—Email address of the user who created the report.



The reports are listed in the **Generated Reports** table only for one year from the date when the reports were generated. After one year, the reports are removed from the table.

Viewing the Scheduled Report

To view a scheduled report, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Reports**.
The Reports page is displayed in the **Summary** view.

3. Click **Manage**.
The Scheduled Reports table is displayed in the **Config** view.
4. In the **Scheduled Reports** table, click a report name listed under **Title**.
The report details are displayed.

The **Scheduled Reports** table provides the following information:

- **Title**—Name of the report. Click  to filter the report based on the name of the report.
- **Next Run**—Time when the report will run in the future.
- **Group/Device**—The group or device for which the report was run.
- **Label/Site**—The label or site for which the report was run.
- **Recurrence**—Time period of the scheduled report.
- **Type**—Type of report. Click  to filter the report based on the type of the report. Click  to select a type of report from the drop-down list.
- **Created By**—Email address of the user who created the report.
- **Status**—Status of the report. Click  to filter the report based on the status of the report. Click  to select a status of report from the drop-down list.

Downloading a Report

To download a report, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Reports**.
The Reports page is displayed in the **Summary** view.
3. Click **Browse**.
The Generated Reports table is displayed in the **List** view.
4. In the **Generated Reports** table, hover over the report you want to download.
5. Click the **PDF** or the **CSV** icon to download the report to the local system.
6. Optionally, click the **Email to** icon to generate an email attachment of the report.

Deleting a Report

To delete a report, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Reports**.
The **Reports** page is displayed in the **Summary** view.
3. Click **Browse**.
The **Generated Reports** table is displayed in the **List** view.
4. In the **Generated Reports** table, hover over the report that you want to delete.

5. Click the **Delete** icon.
The **Delete Report** pop-up window is displayed.
6. Click **Yes** to delete the report.
The selected report is deleted.

Deleting Multiple Reports

To bulk delete multiple reports, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Reports**.
The **Reports** Reports page is displayed in the **Summary** view.
3. Click **Browse**.
The **Generated Reports** table is displayed in the **List** view.
4. To bulk delete, select multiple reports by clicking the rows. Alternatively, press and hold the **Ctrl** key and select the reports.
The number of selected reports is displayed in a pop-up window.
5. In the pop-up window, click the  icon.
The **Delete Report** pop-up window is displayed.
6. Click **Yes** to bulk delete the selected reports.
The selected reports are deleted.

Viewing Audit Trail

The **Audit Trail** page shows the total number logs generated for all device management, configuration, and user management events triggered in Aruba Central. Audit Trail logs provide users both user-initiated and system-initiated actions.

To view the **Audit Trail** logs perform the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Analyze**, click **Audit Trail**. The **Audit Trail** table is displayed with the following details:
 - **Occurred On**—Timestamp of the audit log. Use the sort option to sort the audit logs by date and time. Use the filter option to select a specific time range to display the audit logs.
 - **IP Address**—IP address of the client device.
 - **Username**—Username of the admin user who applied the changes.
 - **Target**—The group or device to which the changes were applied.
 - **Category**—Type of modification and the affected device management category. It shows audit trail categories for system and user actions.
 - **Description**—A short description of the changes such as subscription assignment, firmware upgrade, and configuration updates. Click  to view the complete details of the event. For example, if an event was not successful, clicking the ellipsis displays the reason for the failure.



To customize the **Audit Trail** table, click the eclipses  icon to select the required columns, or click **Reset to default** to set the table to the default columns.

RAPIDS

Aruba Central (on-premises) supports the rogue detection and classification feature that enables administrators to detect intrusion events and classify rogue devices. Rogue devices refer to the unauthorized devices in your WLAN network. With RAPIDS, you can create a detailed definition of what constitutes a rogue device, and act on an rogue or interfering devices that can be later considered for investigation, restrictive action, or both. Once the interfering devices are discovered, Aruba Central (on-premises) sends alerts to your network administrators about the possible threat and provides essential information needed to locate and manage the threat.



RAPIDS is not supported on single-node deployments.

Aruba Central (on-premises) supports the following features:

- Automatic detection of unauthorized wireless devices.
- Wireless detection, using authorized wireless APs to report other devices within range to calculate and display rogue location on a VisualRF map.
- Ability to make a decision based on the AP classifications and send the information back to the AP.
- Obtaining the MAC address table from a switch to identify the switch port to which the rogue device is connected.

Viewing the RAPIDS Page

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**.
For all devices, set the filter to **Global**.
2. Under **Manage**, click **Security > RAPIDS**.
By default, the **IDS** page with **WIDS Events** table is displayed.
3. Click **Rogues** tab to view the rogues details page.

Monitoring IDS WIDS Events

The **Manage > Security > RAPIDS > IDS** tab provides a summary of the total number of wireless attacks detected for a given duration.

The **WIDS Events** table displays the following information category:

- **Infrastructure attacks**—Displays the number of infrastructure attacks detected in the network.
- **Client attacks**—Displays the number of client attacks detected in the network.

Viewing the IDS Page

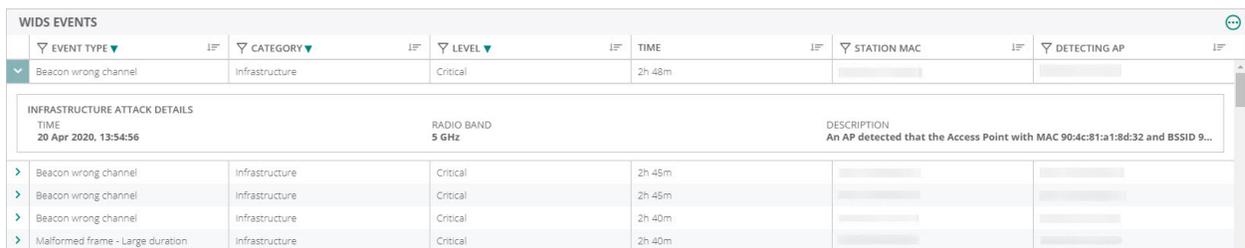
1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**.
For all devices, set the filter to **Global**.
2. Under **Manage**, click **Security > RAPIDS**.
By default, the **IDS** page with **WIDS Events** table is displayed.

Table 218: WIDS Events

Field	Description
Event Type	The type of the intrusion or attack detected. Click the drop-down arrow at the column heading to filter the event types based on your requirement.
Category	Category of the intrusion or attack, infrastructure, or client attack. Click the drop-down arrow at the column heading to filter the category that you want to display.
Level	The level of the intrusion or attack detected. Click the drop-down arrow at the column heading to filter the attack level.
Time	Time of the intrusion or attack.
Station MAC	MAC address of the station under attack or BSSID of the AP under attack.
Detecting AP	The MAC address of the device that detected the intrusion or attack.
Radio Band	Radio band on which the intrusion was detected. There are two radio band signals available, 2.4 GHZ and 5 GHZ. Click the drop-down arrow at the column heading to filter the radio band where the intrusion was detected.
Description	Details of the attack or the intrusion.

Note the following important points:

- Clicking  icon enables you to customize the **WIDS Events** table or set it to the default view.
- To view the details of each event that is generated, click the arrow against each row in the table.



WIDS EVENTS	EVENT TYPE	CATEGORY	LEVEL	TIME	STATION MAC	DETECTING AP
▼	Beacon wrong channel	Infrastructure	Critical	2h 48m		
INFRASTRUCTURE ATTACK DETAILS TIME: 20 Apr 2020, 13:54:56 RADIO BAND: 5 GHz DESCRIPTION: An AP detected that the Access Point with MAC 90:4c:81:a1:8d:32 and BSSID 9...						
>	Beacon wrong channel	Infrastructure	Critical	2h 45m		
>	Beacon wrong channel	Infrastructure	Critical	2h 45m		
>	Beacon wrong channel	Infrastructure	Critical	2h 40m		
>	Malformed frame - Large duration	Infrastructure	Critical	2h 40m		

- Intrusions are displayed for the time selected in **Time Range Filter**. The **WIDS Events** displayed data for a maximum time period of 1 week only.

Monitoring Rogues

The **Rogues** tab provides a summary of the rogue APs, suspected rogue APs, interfering APs, and neighboring APs, and the total number of wireless attacks detected for a given duration.

Viewing the Rogues Page

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**.
For all devices, set the filter to **Global**.
2. Under **Manage**, click **Security**.
By default, the **RAPIDS > IDS** tab is displayed.
3. Click **Rogues** tab to view the page.

The APs in Aruba Central (on-premises) are classified as one of the following:

Table 219: AP Classification in Aruba Central (on-premises)

Classification	Description
Rogue AP	An unauthorized AP plugged into the wired side of the network.
Suspect Rogue AP	An unauthorized access point with a signal strength greater or equal to -75 dBm that might have connected to the wired network.
Interfering AP	An AP detected in the RF environment with a signal strength lesser than -75 dBm but not connected to the wired network. These access points may potentially cause RF interference, but cannot be considered as a direct security threat as these devices are not connected to the wired network. For example, an interfering AP can be an access point that belongs to a neighboring office's WLAN but is not part of your WLAN network.
Neighbor AP	A neighboring AP, for which the BSSIDs are known. Once classified, a neighboring AP does not change its state.

The **Security > RAPIDS > Rogues** page displays the following information tabs:

- **Total**—Shows the total number of rogues classified as **Rogue**, **Suspected Rogue**, or **Interfering**, that are detected in the network.
- **Rogues**—Shows the total number of devices classified as rogue APs.
- **Suspected Rogues**—Shows the total number of devices classified as suspected rogues APs.
- **Interfering**—Shows the total number of devices classified as interfering APs.
- **Neighbors**—Shows the total number of devices classified as neighbor APs.

Click the respective tabs to display specific rogue information pertaining to each classification. By default, the Total information tab is selected and the Detected Access Points table displays all the detected rogue APs.

Table 220: Rogues

Fields	Description
BSSID	The BSSIDs broadcast by the rogue device.
Name	Name of the rogue device detected in the network.
Classification	Classification of the rogue device (monitored device) as Suspect Rogue, or Interferer. Click the drop-down arrow at the column heading to filter the rogue classification that you want to display.

Fields	Description
SSID	The SSID broadcast by the rogue device.
Last Seen	The time relative to the current moment, for example, 6 minutes or an hour, at which the rogue device was last detected in the network.
Last Seen By	The AP name of the last device that reported the monitored AP.
First Seen	The time relative to the current moment (for example, 6 minutes or an hour) at which the rogue device was first detected in the network.
Signal	The signal strength of the AP that detected the rogue device.
Encryption	The type of encryption used by the device that detected the rogue device; for example, WPA, Open, WEP, Unknown. Generally, this field alone does not provide enough information to determine if a device is a rogue device, but it is a useful attribute. If a rogue is not running any encryption method, that implies you have a wider security hole than with an AP that is using encryption.
Containment Status	Details of the containment status. Click the drop-down arrow at the column heading to filter the status that you want to display.
MAC Vendor	The vendor name associated to the MAC OUI of the rogue device.

Note the following important points:

- VisualRF uses the heard signal information to calculate the physical location of the device.
- Click  to customize the **Detected Access Points** table columns or set it to the default view.
- To view details of each rogue device, click the arrow against each row in the table.

DETECTED ACCESS POINTS																																																																																										
Name	Classification	SSID	Last Seen	Last Seen by	Signal																																																																																					
Aruba, a Hew-0F9C48	Suspect Rogue	TMM-cp-bandi-internal	29 Jan 2021, 13:14:42	f4:2e:7f:cb:76:18	-41																																																																																					
<table border="1"> <thead> <tr> <th colspan="2">OVERVIEW</th> <th colspan="5">LOCATION</th> </tr> <tr> <td>SSID</td> <td>TMM-cp-bandi-internal</td> <td>ACCESS POINT NAME</td> <td>SNR (DB)</td> <td>BAND</td> <td>BSSID</td> <td>RF CHANNEL</td> </tr> </thead> <tbody> <tr> <td>BSSID</td> <td>00:24:6C:0F:9C:40</td> <td>00:4e:35:c2:97:34</td> <td>-14</td> <td>2.4 GHz</td> <td>00:4E:35:A9:73:40</td> <td>1</td> </tr> <tr> <td>FIRST SEEN</td> <td>05 Jan 2021, 13:34:38</td> <td>00:4e:35:c2:82:1e</td> <td>-37</td> <td>2.4 GHz</td> <td>00:4E:35:A8:21:E0</td> <td>1</td> </tr> <tr> <td>FIRST SEEN BY</td> <td>00:4e:35:c2:89:9c</td> <td>00:4e:35:c2:7c:9e</td> <td>-37</td> <td>2.4 GHz</td> <td>00:4E:35:A7:C9:E0</td> <td>1</td> </tr> <tr> <td>LAST SEEN</td> <td>29 Jan 2021, 13:14:42</td> <td>00:4e:35:c2:7c:9a</td> <td>-50</td> <td>2.4 GHz</td> <td>00:4E:35:A7:C9:A0</td> <td>1</td> </tr> <tr> <td>LAST SEEN BY</td> <td>f4:2e:7f:cb:76:18</td> <td>00:4e:35:c2:84:88</td> <td>-49</td> <td>2.4 GHz</td> <td>00:4E:35:A8:48:80</td> <td>6</td> </tr> <tr> <td>SWITCH PORT</td> <td>--</td> <td>00:4e:35:c2:80:ae</td> <td>-35</td> <td>2.4 GHz</td> <td>00:4E:35:A8:0A:E0</td> <td>6</td> </tr> <tr> <td></td> <td></td> <td>00:4e:35:c2:7e:78</td> <td>-6</td> <td>2.4 GHz</td> <td>00:4E:35:A7:E7:80</td> <td>1</td> </tr> <tr> <td></td> <td></td> <td>00:4e:35:c2:89:9c</td> <td>-41</td> <td>5 GHz</td> <td>00:4E:35:A8:99:D0</td> <td>149</td> </tr> <tr> <td></td> <td></td> <td>00:4e:35:c2:9e:06</td> <td>-13</td> <td>2.4 GHz</td> <td>00:4E:35:A9:E0:60</td> <td>1</td> </tr> <tr> <td></td> <td></td> <td>f4:2e:7f:cb:62:b2</td> <td>-33</td> <td>2.4 GHz</td> <td>F4:2E:7F:86:2B:20</td> <td>6</td> </tr> </tbody> </table>							OVERVIEW		LOCATION					SSID	TMM-cp-bandi-internal	ACCESS POINT NAME	SNR (DB)	BAND	BSSID	RF CHANNEL	BSSID	00:24:6C:0F:9C:40	00:4e:35:c2:97:34	-14	2.4 GHz	00:4E:35:A9:73:40	1	FIRST SEEN	05 Jan 2021, 13:34:38	00:4e:35:c2:82:1e	-37	2.4 GHz	00:4E:35:A8:21:E0	1	FIRST SEEN BY	00:4e:35:c2:89:9c	00:4e:35:c2:7c:9e	-37	2.4 GHz	00:4E:35:A7:C9:E0	1	LAST SEEN	29 Jan 2021, 13:14:42	00:4e:35:c2:7c:9a	-50	2.4 GHz	00:4E:35:A7:C9:A0	1	LAST SEEN BY	f4:2e:7f:cb:76:18	00:4e:35:c2:84:88	-49	2.4 GHz	00:4E:35:A8:48:80	6	SWITCH PORT	--	00:4e:35:c2:80:ae	-35	2.4 GHz	00:4E:35:A8:0A:E0	6			00:4e:35:c2:7e:78	-6	2.4 GHz	00:4E:35:A7:E7:80	1			00:4e:35:c2:89:9c	-41	5 GHz	00:4E:35:A8:99:D0	149			00:4e:35:c2:9e:06	-13	2.4 GHz	00:4E:35:A9:E0:60	1			f4:2e:7f:cb:62:b2	-33	2.4 GHz	F4:2E:7F:86:2B:20	6
OVERVIEW		LOCATION																																																																																								
SSID	TMM-cp-bandi-internal	ACCESS POINT NAME	SNR (DB)	BAND	BSSID	RF CHANNEL																																																																																				
BSSID	00:24:6C:0F:9C:40	00:4e:35:c2:97:34	-14	2.4 GHz	00:4E:35:A9:73:40	1																																																																																				
FIRST SEEN	05 Jan 2021, 13:34:38	00:4e:35:c2:82:1e	-37	2.4 GHz	00:4E:35:A8:21:E0	1																																																																																				
FIRST SEEN BY	00:4e:35:c2:89:9c	00:4e:35:c2:7c:9e	-37	2.4 GHz	00:4E:35:A7:C9:E0	1																																																																																				
LAST SEEN	29 Jan 2021, 13:14:42	00:4e:35:c2:7c:9a	-50	2.4 GHz	00:4E:35:A7:C9:A0	1																																																																																				
LAST SEEN BY	f4:2e:7f:cb:76:18	00:4e:35:c2:84:88	-49	2.4 GHz	00:4E:35:A8:48:80	6																																																																																				
SWITCH PORT	--	00:4e:35:c2:80:ae	-35	2.4 GHz	00:4E:35:A8:0A:E0	6																																																																																				
		00:4e:35:c2:7e:78	-6	2.4 GHz	00:4E:35:A7:E7:80	1																																																																																				
		00:4e:35:c2:89:9c	-41	5 GHz	00:4E:35:A8:99:D0	149																																																																																				
		00:4e:35:c2:9e:06	-13	2.4 GHz	00:4E:35:A9:E0:60	1																																																																																				
		f4:2e:7f:cb:62:b2	-33	2.4 GHz	F4:2E:7F:86:2B:20	6																																																																																				
Aruba, a Hew-0F9E48	Interfering	aruba-ap	29 Jan 2021, 14:14:43	f4:2e:7f:cb:62:b2	-65																																																																																					
Aruba, a Hew-80:65:30	Suspect Rogue	TMM-cp-bandi-internal	29 Jan 2021, 13:24:31	00:4e:35:c2:7e:9e	-47																																																																																					

- Rogue devices are displayed for the time selected in **Time Range Filter**. The **Detected Access Points** displays data for a maximum time period of 1 week only.

Configuring IDS Parameters

The type and severity of Intrusion Detections raised by an AP is configurable and affects the data that is seen in **Security**.

Generating Alerts for Security Events

Aruba Central (on-premises) supports configuring alerts for rogue AP detections and IDS events. To generate alerts, complete the following steps:

1. In the **Network Operations** app, use the filter to select **Global**.
2. Under **Analyze**, click **Alerts & Events**. The **Alerts & Events** page is displayed.
3. In the **Alerts & Events** page, click the **Config** icon.
The **Alert Severities & Notifications** page is displayed.
4. Select **Access Point** to display the AP dashboard. Aruba Central (on-premises) supports three alert types for identifying interfering devices:
 - Rogue AP Detected
 - Infrastructure Attacks Detected
 - Client Attack Detected
5. Select an alert and click **+** to enable the alert with default settings. To configure alert parameters, click on the alert tile (anywhere within the rectangular box) and do the following:
 - a. **Severity**—Set the severity. The available options are Critical, Major, Minor, and Warning.
 - b. **Device Filter Options**—(Optional) You can restrict the scope of an alert by setting one or more of the following parameters:



For a few alerts, you can configure threshold value for one or more alert severities. To set the threshold value, select the alert and in the exceeds text box, enter the value. The alert is triggered when one of the threshold values exceed the duration.

- **Label**—Select a label to limit the alert to a specific label.
 - **Sites**—Select a site to limit the alert to a specific site.
- c. **Notification Options**
 - **Email**—Select the **Email** check box and enter an email address to receive notifications when an alert is generated. You can enter multiple email addresses, separate each value with a comma.
 - **Streaming**—Select the **Streaming** check box to receive the streaming notifications when an alert is generated.
 - **Webhook**—Select the **Webhook** check box and select the Webhook from the drop-down list. For more information, see Aruba Central Help Center.
 - **Syslog**—Select the **Syslog** checkbox to receive the syslog notifications when an alert is generated.
 - d. Click **Save**.
 - e. **Add Rule**—(Optional) For a few alerts, the **Add Rule** option appears. For such alerts, you can add additional rule(s). The rule summaries appear at the top of the page.

Generating Reports for Security Events

Aruba Central (on-premises) supports generating reports for rogue AP detections and IDS events. To generate reports, complete the following steps:

1. In the **Network Operations** app, use the filter to select **Global**.
2. Under **Analyze**, click **Reports**.
3. In the **Reports** page, click **Create**. Aruba Central (on-premises) supports **RAPIDS** to display the report of all wireless intrusions.

Monitoring Sites in the Topology Tab

In Aruba Central (on-premises), the **Topology** tab is displayed only when you select a site from the filter. The Topology tab provides a graphical representation of the site including the network layout, details of the

devices deployed, and the health of the WAN uplinks and tunnels.

For APs and Gateways, the topology feature is available for both Foundation and Advanced licenses; and for switches, the feature is available for Foundation licenses.



In Aruba Central (on-premises), the Topology tab does not support Campus controllers and Campus APs.

The Topology feature is available for Foundation and Advanced licenses for APs, switches, and gateways.

This section includes the following topics:

- [Before You Begin](#)
- [Viewing the Topology Map](#)
 - [Features on Topology User Interface](#)
 - [Device or Link Details](#)
 - [Details Pane](#)
 - [Unreachable Devices](#)
 - [VLAN Overlay Details](#)

Before You Begin

The following types of devices are displayed as part of the **Topology** tab:

- Access Point (AP)
- AOS-S and AOS-CX switch
- AOS-S and AOS-CX switch stack

In the topology map, Aruba Central (on-premises) supports third-party routers, switches, and APs from the vendors listed below:

- Cisco
- Procurve
- Juniper
- HPE Comware
- Meraki
- Cumulus
- Huawei
- Mikrotik
- Extreme
- HPE OfficeConnect Switch
- Arista
- 3Com
- Ruckus
- Mojo
- Mist
- Motorola
- Netgear
- Dell
- Comware

- Hirschmann Railswitch
- Ubiquiti

Pre-requisites

This section discusses the pre-requisites associated with the devices so that they are displayed correctly in the **Topology** tab:

- The topology map filters devices based on sites. To view the topology map, ensure that you have assigned the devices to sites.
- The minimum required ArubaOS version for access points (APs) in the topology map is ArubaOS version 8.1.0.0-1.0.1.1.
- To view AOS-CX switches in the topology map, you must create a template configuration for the switch with the password in plaintext.

-
- According to the current topology, there should be a one-to-one mapping between a site and a device. Topology does not currently support unmanaged devices belonging to multiple sites. All Aruba Central (on-premises) managed devices that are connected to a common unmanaged device must terminate on the same site.
 - In Aruba Central (on-premises), the maximum number of devices supported per site in the topology tab is 500.
 - To identify a valid third-party device in the topology, the neighbor device must have a valid third-party vendor name in either hostname or system description for the devices on the site. Also, the enabled capability for the unmanaged neighbor device must include one of the following:
 - **Access Point**
 - **Router**
 - **Bridge**
 - **Repeater**
 - **Other**
 - **Unknown but not Station or Telephone**



Viewing the Topology Map

To view the topology map, complete the following steps:

1. In the **Network Operations** app, set the filter to a site for which you want to view the topology map.
The dashboard context for the site is displayed.
2. Under **Manage**, click **Overview > Topology**.
The topology map for the selected site is displayed.
3. In the topology map, hover over a device or a link to view the details. For more information, see [Device or Link Details](#).
4. In the device or the link details, click the **Show Details** link to view the **Details** pane. For more information, see [Details Pane](#).

Features on Topology User Interface

The following figure shows the different features available on the **Topology** tab:

Figure 100 Features on Topology Tab

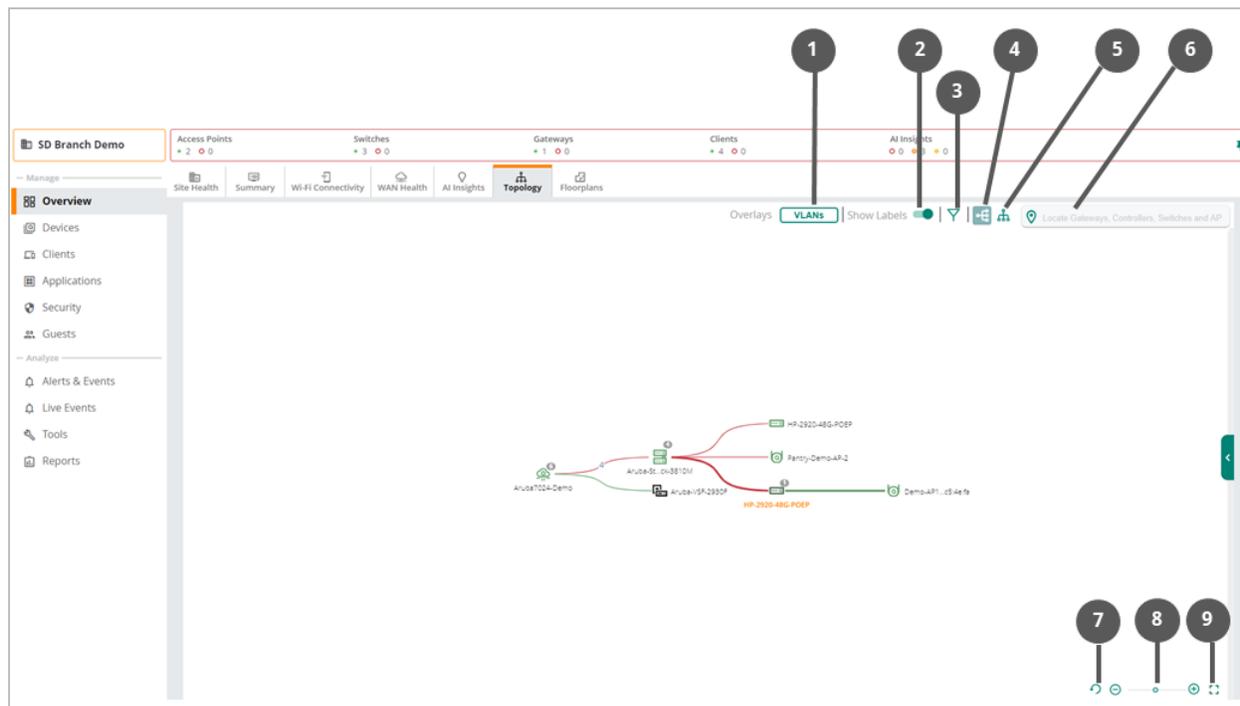


Table 221: Icon Details

Callout Number	Description
1	Click the  icon to show or hide the VLANs pane.
2	Click the Show Device Names  toggle switch to show or hide the device name.
3	Click the  filter icon to filter the type of devices to be shown on the map. The following options are available: <ul style="list-style-type: none"> ■ Access Points—Allows you to show or hide the APs from the topology map. ■ Security Cloud—Allows you to show or hide the Zscaler and Palo Alto Prisma Access™ Cloud Service from the topology map. ■ Switch—Allows you to show or hide the switches from the topology map. ■ VPNC—Allows you to show or hide the VPNCs and the virtual gateways from the topology map. ■ Unmanaged—Allows you to show or hide the unmanaged devices from the topology map. ■ Show Devices Without Link—Allows you to show or hide the devices without link from the topology map.
4	Click the  icon to view the topology map in a left to right orientation. The default orientation of the topology map is left to right orientation.

Callout Number	Description
5	Click the  icon to view the topology map in a top-down orientation.
6	The search bar allows you to locate a device in the topology map. The search bar field supports exact and partial text searches.
7	Click the  icon to reset the topology map to the default view.
8	Click the  ,  icons to change the zoom level of the topology map. Alternatively, you can drag the slider to set the zoom level of the topology map.
9	Click the  icon to view the topology map in full-screen view. In the full-screen view, the device or link details feature is disabled in the topology map.



When the number of downstream devices connected to a device is less than or equal to 10, the devices are visible in the topology map. When the number of downstream devices connected to a device is more than 10, click the device icon to view the devices in the topology map. A bubble icon on the device represents the number of connected downstream devices.

Table 222: Icon Types

Icon	Type
	AP
	Switch
	Switch Stack
	Unmanaged Device

Icon Status

- —Indicates that the device health is poor when the CPU usage is greater than 90% and the memory usage is greater than 90%.
- —Indicates that the device health is good when the CPU usage is lower than or equal to 75% and the memory usage is lower than or equal to 75%.
- —Indicates that the device health is fair when the CPU usage is greater than 75% and the memory usage is greater than 75%.
- —Indicates that the device is online.
- —Indicates that the device is offline.

Device or Link Details

When you hover over a device or link, a pop-up displays the following details:

Figure 101 Device or Link Details

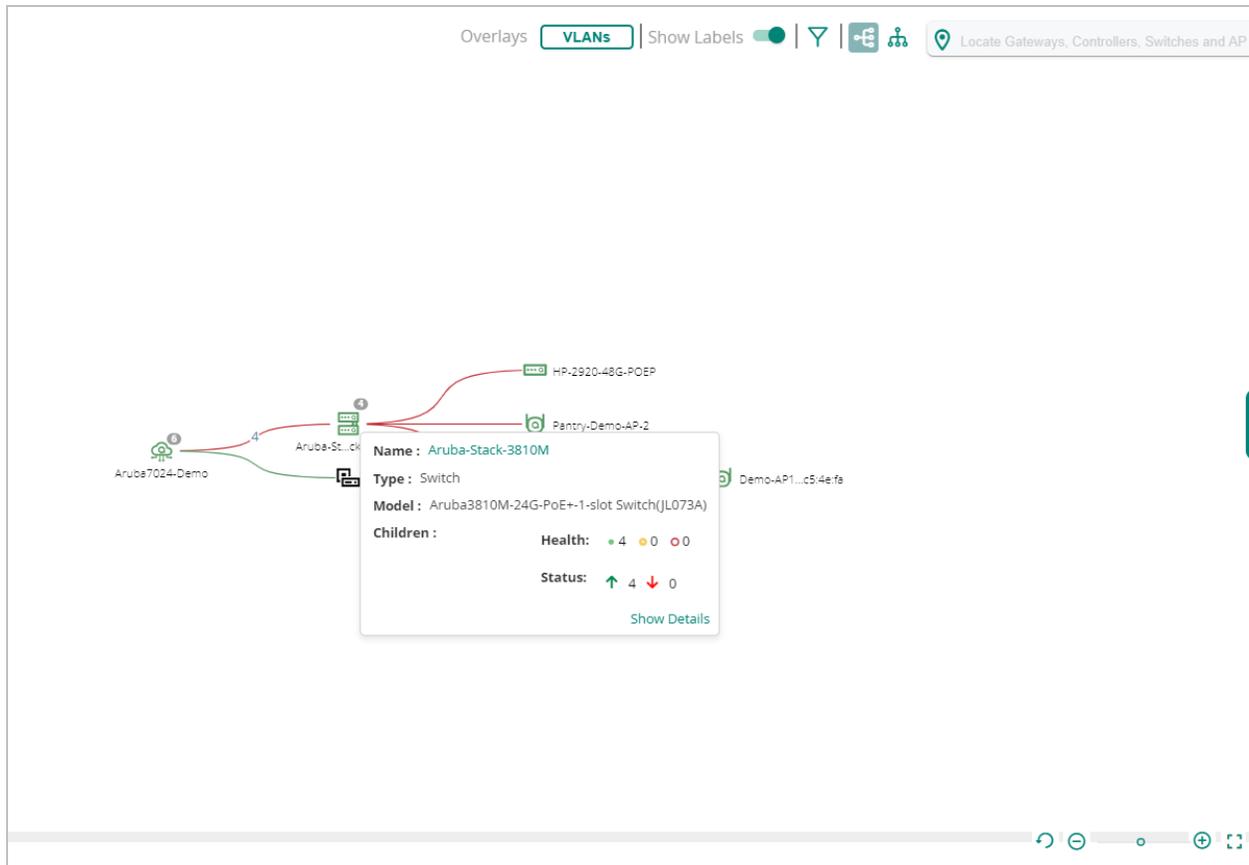


Table 223: Device or Link Details

Type	Description
Access Point	<p>Displays the following details:</p> <ul style="list-style-type: none"> ■ Name—Hostname of the access point. ■ Type—Type of the device. ■ Model—Hardware model of the access point. ■ Health Reason—The health status of the access point. This parameter is only available when the access point is offline. ■ Show Details—Click the link to view the Details pane.
Unmanaged	<p>Displays the following details:</p> <ul style="list-style-type: none"> ■ Name—Name of the unmanaged device. ■ IP Address—IP address of the unmanaged device. ■ Show Details—Click the link to view the Details pane. <p>NOTE: The value of the IP Address parameter is empty if LLDP does not provide the neighbor information.</p>
Switch	<p>Displays the following details:</p> <ul style="list-style-type: none"> ■ Name—Hostname of the switch. ■ Type—Type of the device. ■ Model—Hardware model of the switch.

Type	Description
	<ul style="list-style-type: none"> ■ Children—Number of devices connected to the switch categorized, based on the health and status of the devices. The Children field displays the following details: <ul style="list-style-type: none"> ○ Health—Count of devices connected to the switch based on the health of the device. For more information, see Icon Status. ○ Status—Count of devices connected to the switch based on the current status of the devices. The arrow in green indicates that the device is online. The arrow in red indicates that the device is offline. ■ VLANs—List of VLANs configured on the switch. This field is displayed only when the VLANs option is selected under Overlays. For more information, see VLAN Overlay Details. ■ Show Details—Click the link to view the Details pane.
Switch Stack	<p>Displays the following details:</p> <ul style="list-style-type: none"> ■ Name—Hostname of the switch stack. ■ Type—Type of the device. ■ Model—Hardware model of the switch. ■ Children—Number of devices connected to the switch categorized based on the health and status of the devices. The Children field displays the following details: <ul style="list-style-type: none"> ○ Health—Count of devices connected to the switch based on the health of the device. For more information, see Icon Status. ○ Status—Count of devices connected to the switch based on the current status of the devices. The arrow in green indicates that the device is online. The arrow in red indicates that the device is offline. ■ VLANs—List of VLANs configured on the switch. This field is displayed only when the VLANs option is selected under Overlays. For more information, see VLAN Overlay Details. ■ Show Details—Click the link to view the Details pane.
AOS-CX VSX Switch	<p>Displays the following details:</p> <ul style="list-style-type: none"> ■ Name—Name of the AOS-CX switch that is configured with VSX. The name is displayed in the VSX_<Device Name> format. For example, VSX_8320-switch-primary. ■ Type—Type of the device. ■ Model—Hardware model of the AOS-CX switch. ■ VSX Role—Role of the AOS-CX switch in the VSX configuration. Supported values are Primary and Secondary. ■ Children—Number of devices connected to the switch categorized based on the health and status of the devices. The Children field displays the following details: <ul style="list-style-type: none"> ○ Health—Count of devices connected to the switch based on the health of the device. For more information, see Icon Status. ○ Status—Count of devices connected to the switch based on the current status of the devices. The arrow in green indicates that the device is online. The arrow in red indicates that the device is offline. ■ VLANs—List of VLANs configured on the switch. This field is displayed only when the VLANs option is selected under Overlays. For more information, see VLAN Overlay Details. ■ Show Details—Click the link to view the Details pane.
Edge	<p>Displays the following information about the edge link:</p>

Type	Description
	<ul style="list-style-type: none"> ■ <Interface of the device>—Interface number of the device. ■ <Name of the device>—Displays the name of the device. ■ Health Reason—Displays the health status of the down edge link. This parameter is only available when the edge link is down. ■ Alternative links—Number of the alternative links. <p>The edge in green color indicates that the edge is up. The edge in red color indicates that the edge is down. Click the edge link to view the Details pane.</p>
Unmanaged edge	<p>Displays the following information about the link:</p> <ul style="list-style-type: none"> ■ <Name of the connected device>—Name of the device connected with the edge link. ■ <Port Identifier>—Port number of the device. ■ Health Reason—Displays the health status of the down edge link. This parameter is only available when the edge link is down. ■ Alternative links—Number of the alternative links. <p>The unmanaged edge in green color indicates that the unmanaged edge is up. The unmanaged edge in red color indicates that the unmanaged edge is down. Click the unmanaged edge link to view the Details pane.</p>
ISL edge in AOS-CX VSX topology map	<p>Displays the following information about the link:</p> <ul style="list-style-type: none"> ■ ISL—Number of inter-switch link (ISL) present between the AOS-CX switches configured with VSX. ■ Other Links—Number of other links present between the AOS-CX switches configured with VSX.

Details Pane

In the topology map, the **Details** pane provides a summary of the devices, uplinks, and tunnel details.

A green bullet icon indicates that the device health is good when the CPU usage is lower than or equal to 75% and the memory usage is lower than or equal to 75%. A yellow bullet icon indicates that the device health is fair when the CPU usage is greater than 75% and the memory usage is greater than 75%. A red bullet icon indicates that the device health is poor when the CPU usage is greater than 90% and the memory usage is greater than 90%. The arrow in green indicates that the device is online. The arrow in red indicates that the device is offline.

In the topology map, select a device and then click the **Show Details** link in the pop-up window to view the **Details** pane. To view the **Details** pane for a tunnel, uplink, or edge, click the link.

The **Details** task pane displays the following information:

Figure 102 Details Pane

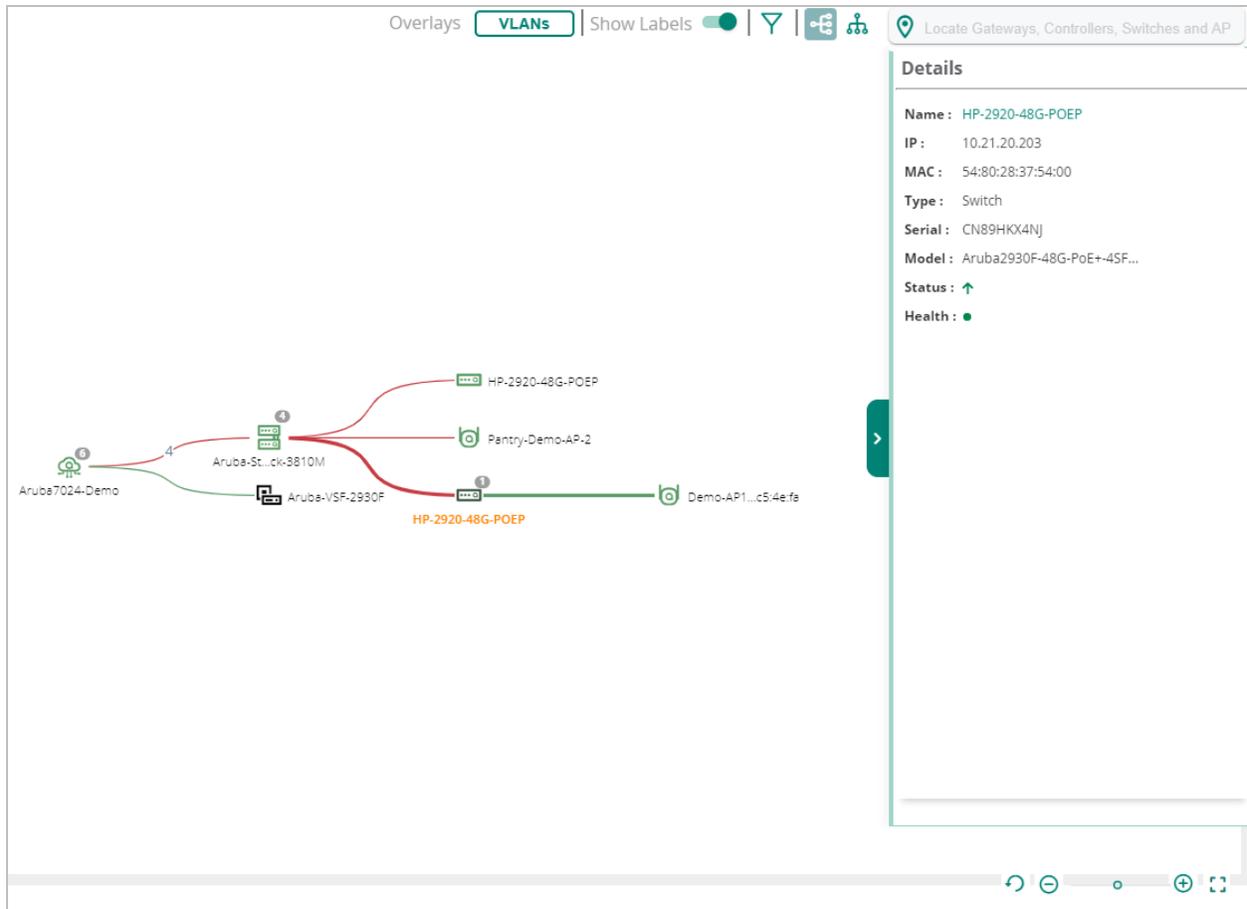


Table 224: Contents of the Details Pane

Type	Description
Access Point	<p>Displays the following details:</p> <ul style="list-style-type: none"> ■ Name—Hostname of the access point. Click the access point name to view the Access Point Details page. ■ IP—IP address of the access point. ■ MAC—MAC address of the access point. ■ Type—Type of the device. ■ Serial—Serial number of the access point. ■ Model—Hardware model of the access point. ■ Status—Operational status of the access point. ■ Health—Operational health of the access point.
Unmanaged	<p>Displays the following details:</p> <ul style="list-style-type: none"> ■ Name—Name of the unmanaged device. ■ Description—Description of the unmanaged device. ■ IP—IP address of the unmanaged device. ■ Capabilities—Displays the capabilities of the unmanaged device. ■ Supported—Lists the supported capabilities of the unmanaged device. ■ Enabled—Lists the enabled capabilities of the unmanaged device.

Type	Description
	<p>NOTE: The value of the parameters are empty if LLDP does not provide the neighbor information.</p>
Switch	<p>Displays the following details:</p> <ul style="list-style-type: none"> ■ Name—Hostname of the switch. Click the switch name to view the Switch Details page. ■ IP—IP address of the switch. ■ MAC—MAC address of the switch. ■ Type—Type of the device. ■ Serial—Serial number of the switch. ■ Model—Hardware model of the switch. ■ Status—Operational status of the switch. ■ Health—Operational health of the switch.
Switch Stack	<p>Displays the following details:</p> <ul style="list-style-type: none"> ■ Name—Hostname of the switch. Click the switch name to view the Switch Details page. ■ IP—IP address of the switch. ■ MAC—MAC address of the switch. ■ Type—Type of the device. ■ Serial—Serial number of the switch. ■ Stack Role—Role of the switch in the stack. ■ Model—Hardware model of the switch. ■ Status—Operational status of the switch stack. ■ Health—Operational health of the switch stack. ■ Stack Members—Provides the Name, Role, and State details of the stack member. Click the stack member name to view the Switch Details page.
AOS-CX VSX	<p>Displays the following details:</p> <ul style="list-style-type: none"> ■ Name—Hostname of the AOS-CX switch with VSX configured. Click the switch name to view the Switch Details page. ■ IP—IP address of the switch. ■ MAC—MAC address of the switch. ■ Type—Type of the device. ■ Serial—Serial number of the switch. ■ Model—Hardware model of the switch. ■ Status—Operational status of the switch. ■ Health—Operational health of the switch. <p>VSX section displays the following details:</p> <ul style="list-style-type: none"> ■ ISL State—State of the ISL connection with the peer AOS-CX switch. Following are the supported values: <ul style="list-style-type: none"> ○ WAITING_FOR_PEER—Waiting for connectivity to the peer. ○ PEER_ESTABLISHED—Steady state. VSX LAGs are up when the device is in this state. ○ SPLIT_SYSTEM_PRIMARY—Lost ISL connectivity to the peer and the device is operating as primary. ○ SPLIT_SYSTEM_SECONDARY—Lost ISL connectivity to the peer and the device is operating as secondary. ○ SYNC_PRIMARY—ISL connectivity to the peer restored and the device is syncing states to the peer.

Type	Description
	<ul style="list-style-type: none"> ○ SYNC_SECONDARY—ISL connectivity to the peer restored and the device is learning states from the peer. VSX LAGs are down when the device is in this state. ○ SYNC_SECONDARY_LINKUP_DELAY—Device has learned its states from the peer and monitoring for hardware is to be programmed. VSX LAGs are down when the device is in this state. ■ ISL Port—ISL port number of the selected AOS-CX switch. If the ISL is a LAG, then this field displays the LAG name. ■ ISL Mgmt State—Management state of the ISL. Following are the supported values: <ul style="list-style-type: none"> ○ OPERATIONAL—ISL management is operational. ○ INTER_SWITCH_LINK_MGMT_INIT—ISL management is in initialization state. ○ CONFLICTING_OR_MISSING_DEVICE_ROLES—Either the role is missing on one of the VSX peers or the same role is configured on both VSX peers. ○ SW_IMAGE_VERSION_MISMATCH_ERROR—Software version on the primary device does not match with the software version on the secondary device. ○ INTER_SWITCH_LINK_DOWN—ISL is down. ○ INTERNAL_ERROR—ISL management has internal errors. ■ Config Sync Enabled—Configuration synchronization between the VSX switches are enabled or disabled. ■ Config Sync Status—Status of the configuration synchronization between the VSX switches. Following are the supported values: <ul style="list-style-type: none"> ○ IN-SYNC—Configuration synchronization is operational and the VSX switches are in sync. ○ DISABLED—Configuration synchronization is disabled. ○ SW_IMAGE_VERSION_MISMATCH_ERROR—Software image version on the primary device does not match with the software image version on the secondary device. ○ CONFLICTING_OR_MISSING_DEVICE_ROLES—Either the role is missing on one of the VSX peers or the same role is configured on both VSX peers. ○ PEER_DB_CONNECTION_ERROR—Error in connecting to peer database. It involves errors due to ISL or ISL management. ○ CONFIGURATION_SYNC_CONFLICT—Configuration synchronization is operational, but has conflicts synchronizing the configuration. Conflicts can occur if the configuration on the primary device is marked for sync, but the same configuration on the secondary device is not marked for sync. ○ CONFIGURATION_SYNC_MISSING_REFERENCE—Configuration synchronization is operational, but has missing references in synchronizing the configuration. ■ Role—Role of the AOS-CX switch in the VSX configuration. Supported values are Primary and Secondary. ■ Peer IP—IPv4 address of the peer switch. ■ Peer Serial—Serial number of the peer switch. ■ Peer MAC—MAC address of the peer switch. ■ Peer Name—Hostname of the peer switch. ■ Last Seen—Date on which the peer switch was last synced.
Edge	<p>Displays the following information about the link:</p> <ul style="list-style-type: none"> ■ Interface numbers—Interface numbers of the device. ■ Interface—Interface number of the individual device. ■ Serial—Serial number of the individual device. ■ Device Name—The name of the individual device. ■ Port Number—The port number of the individual device.

Type	Description
Unmanaged edge	<p>Displays the following information about all the links:</p> <ul style="list-style-type: none"> ■ Interface numbers—Interface numbers of the device. ■ Health Reason—Displays the health status of the edge link. This parameter is only available when the edge link is down. ■ Interface—Interface number of the device. ■ Serial—Serial number of the device. ■ Device Name—Name of the device. ■ Port Number—Port number of the device. ■ Interface—Interface number of the unmanaged device. ■ MAC—MAC address of the unmanaged device. ■ Device Name—Name of the unmanaged device. ■ Port Identifier—Displays the port ID, port name, or MAC address of the unmanaged device.
ISL edge in AOS-CX VSX topology map	<p>Displays the following information about the ISL edge:</p> <ul style="list-style-type: none"> ■ Inter-Switch Link Status—Status of the ISL connection with the peer. ■ <LAG-name> - ISL section displays details about all the interfaces that are part of the LAG. The section also displays the details of the devices connected to these interfaces. It displays the following details: <ul style="list-style-type: none"> ○ Serial—Serial number of the individual device. ○ Device Name—Name of the individual device. ○ Port Number—Port number of the individual device. ■ Other—This section displays details about the other links present between the VSX configured AOS-CX switches. It displays the following details: <ul style="list-style-type: none"> ○ Serial—Serial number of the individual device. ○ Device Name—Name of the individual device. ○ Port Number—Port number of the individual device.

Unreachable Devices

The **Unreachable Devices** pane provides information about the orphan and the offline unmanaged devices. An unmanaged device is considered to be orphan when all its neighboring Aruba devices get deleted and are only displayed in the **Unreachable Devices** list. An unmanaged device is considered to be offline when all its neighboring Aruba devices are offline and are displayed both in the **Topology** map and in the **Unreachable Devices** list.

When an unmanaged device is either offline or disconnected, they are only displayed in the **Unreachable Devices** list. The devices listed in the **Unreachable Devices** pane are deleted after 15 days.

To view the **Unreachable Devices** pane, click the **Unreachable Devices** button. The **Unreachable Devices** pane displays the following details:

- **Name**—Name of the unmanaged device.
- **Type**—Type of the unreachable device.
- **MAC**—MAC address of the unmanaged device.
- **Last Seen**—The last active time and date of the unmanaged device.

VLAN Overlay Details

The topology map displays information about the VLANs configured on switches running AOS-Switch and AOS-CX software. To view the VLAN information:

1. Select the **VLANs** option under **Overlays**. The **VLANs** pane is displayed and the network elements in the topology map, such as device icons and edge links, are grayed out.
The **VLANs** pane displays the first 50 VLANs (unique VLAN ID and name pairs) in the ascending order of VLAN IDs. To search for other VLANs, click the search icon.
2. Select a VLAN from the **VLANs** pane. You can also enter a VLAN name or ID in the search box.
3. The topology map displays the following information:
 - The switches that have the selected VLANs configured are highlighted in a color depending on the status of the switch, green for online and red for offline.
 - The edge link connecting two switches is highlighted in blue, if the following conditions are met:
 - The VLAN IDs are present in both the switches and in the ports associated with the edge link between the switches.
 - The VLAN type (tagged or untagged) configured is the same in both the switches.
4. Hover over the switch to view the list of all VLANs (comma separated) configured on the switch. The VLAN IDs are also listed as a range if consecutive VLAN IDs are configured. For example, 100-178, 190, 210.
5. Hover over the edge link connecting the two switches. The pop-up displays the following information:
 - Host name of the switch
 - Serial number of the switch
 - VLAN ID
 - Type of VLAN: **tagged**, **untagged**, or **missing**

Upgrading Device Firmware

The **Firmware** page provides an overview of the latest firmware version supported on the device, details of the device, and the option to upgrade the device.

Viewing Firmware Details

To view the firmware details for devices provisioned in Aruba Central (on-premises):

1. In the **Network Operations** app, select one of the following options:
 - To select a group in the filter, set the filter to one of the options under **Group**. For all devices, set the filter to **Global**. The dashboard context for the selected filter is displayed.
 - To select a device in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices**, and then click **Access Points**, **Switches**, or **Controllers**. A list of devices is displayed.
 - c. Click a device listed under **Device Name**. The dashboard context for the device is displayed.
2. Under **Maintain**, click **Firmware**. The **Firmware** dashboard displays the following information:
The following image displays the **Firmware** dashboard at the global level:

Name	Site	Firmware Version	Recommended Version	Upgrade Status	Compliance Status
4448c11c2e9c4	Unassigned	8.5.0.5_73491	-	Firmware up to date	Not Set
b45d550c621e8	vf_sim1608301	8.6.0.5_75707	-	Firmware up to date	Not Set
B5H00001	DENVER	8.5.2.0_59123	-	Firmware up to date	Not Set
B5H00003	DENVER	8.5.2.0_59123	-	Firmware up to date	Not Set
IAP-344-904c31c2042ec	2.5.3-Site-HYD	8.6.0.5_75979	-	Firmware up to date	Not Set
IAP-70	2.5.3-Site-WY	8.6.0.6_77124	-	Firmware up to date	Not Set
instant-0FAB64	Dummy	6.5.4.16_73934	-	No Update from the device. Plea...	Set
instant-C66187	Dummy	6.4.4.8-4.2.4.16_73658	-	Firmware up to date	Set
Instant-CB469C	Dummy	6.5.4.17_75343	-	Firmware up to date	Set
JG3R00001 (5)	vf_iap_sim1614...	8.5.2.0_59123	-	Firmware up to date	Not Set
JG3R00006 (5)	vf_iap_sim1614...	8.5.2.0_59123	-	Firmware up to date	Not Set
JG3R00011 (5)	vf_iap_sim1614...	8.5.2.0_59123	-	Firmware up to date	Not Set
JG3R00016 (5)	vf_iap_sim1614...	8.5.2.0_59123	-	Firmware up to date	Not Set

Firmware Maintenance Window

The following are the data pane items and description:

1. **Access Points**—Displays the following information:
 - **Name**—Name of the AP. The and icons allow you to sort the names in ascending or descending order. Clicking on the device name opens a window with connected APs and allows you to select and view the device Summary page. For more information, see [Wireless Client Details](#).
 - **Group**—Displays the group information only on global context. The and icons allow you to sort the groups in ascending or descending order.
 - **Site**—Displays the site information only on global context. The and icons allow you to sort the sites in ascending or descending order.
 - **Firmware Version**—The current firmware version running on the device. The and icons allow you to sort the firmware versions in ascending or descending order.
 - **Recommended Version**—The version to which the device is recommended for the upgrade.
 - **Upgrade Status**—Filters the device list based on any of the following firmware upgrade status:
 - **New firmware available**
 - **Scheduled**
 - **In progress**

- **Failed**
- **Firmware up to date**
- **Compliance Status**—Status of the firmware compliance setting. Based on the setting, the column displays one of the following values:
 - **Set**
 - **Not Set**
 - **Compliance scheduled on**

Hover over any device to view the version number and compliance configured level for set compliance and displays the date, time (UTC), firmware version number, and compliance configured level for a scheduled compliance.



Clicking on the device name from the **Name** columns, opens a window with connected APs and allows you to select and view the device **Summary** page. For more information, see [Wireless Client Details](#). Click any site name from the **Site** column to view the site associated APs with their firmware details page.

1. **Switches**—Displays the following details about Aruba switches managed through Aruba Central:
 - **Name**—Host name of the switch. The  and  icons allow you to sort the names in ascending or descending order.
 - **Family**—Displays the following types of switches:
 - AOS-S
 - CX

This information is only available for Aruba switch and Aruba CX switches.
 - **Site**—Displays the site information only on global context. The  and  icons allow you to sort the sites in ascending or descending order.
 - **Group**—Displays the group information only on global context. The  and  icons allow you to sort the groups in ascending or descending order.
 - **MAC Address**—MAC address of the switch. The  and  icons allow you to sort the address in ascending or descending order.
 - **Model**—Hardware model of the switch. The  and  icons allow you to sort the models in ascending or descending order.
 - **Firmware Version**—The current firmware version running on the switch. The  and  icons allow you to sort the firmware versions in ascending or descending order.
 - **Recommended Version**—The version to which the device is recommended for the upgrade.
 - **Upgrade Status**—Filters the device list based on any of the following firmware upgrade status:
 - **New firmware available**
 - **Scheduled**
 - **In progress**
 - **Failed**
 - **Firmware up to date**
 - **Compliance Status**—Status of the firmware compliance setting. Based on the setting, the column displays one of the following values:

- **Set**
- **Not Set**
- **Compliance scheduled on**

Hover over any device to view the version number and compliance configured level for set compliance and displays the date, time (UTC), firmware version number, and compliance configured level for a scheduled compliance.



-
- The **Switches** tab displays details of both AOS-Switch and AOS-CX switches.
-

2. **Controllers**—Displays the following details about the controllers managed through Aruba Central in **Standalone** mode and in **Cluster** mode:

a. **Standalone** mode:

- **Name**—Host name of the controllers. The and icons allow you to sort the names in ascending or descending order.
- **Site**—Displays the site information only on global context. The and icons allow you to sort the sites in ascending or descending order.
- **Group**—Displays the group information only on global context. The and icons allow you to sort the groups in ascending or descending order.
- **MAC Address**—MAC address of the controllers. The and icons allow you to sort the address in ascending or descending order.
- **Model**—Hardware model of the controllers. The and icons allow you to sort the models in ascending or descending order.
- **Firmware Version**—The current firmware version running on the controllers. The and icons allow you to sort the firmware versions in ascending or descending order.
- **Recommended Version**—The version to which the device is recommended for the upgrade.
- **Upgrade Status**—Filters the device list based on any of the following firmware upgrade status:
 - **New firmware available**
 - **Scheduled**
 - **In progress**
 - **Failed**
 - **Firmware up to date**
- **Compliance Status**—Status of the firmware compliance setting. Based on the setting, the column displays one of the following values:
 - **Set**
 - **Not Set**
 - **Compliance scheduled on**

Hover over any device to view the version number and compliance configured level for set compliance and displays the date, time (UTC), firmware version number, and compliance configured level for a scheduled compliance.

b. **Cluster** mode:

- **Name**—Host name of the controllers. The and icons allow you to sort the names in ascending or descending order.

- **Group**—Displays the group information only on global context. The  and  icons allow you to sort the groups in ascending or descending order.
- **Firmware Version**—The current firmware version running on the controllers. The  and  icons allow you to sort the firmware versions in ascending or descending order.
- **Upgrade Status**—Filters the device list based on any of the following firmware upgrade status:
 - **New firmware available**
 - **Scheduled**
 - **In progress**
 - **Failed**
 - **Firmware up to date**
- **Compliance Status**—Status of the firmware compliance setting. Based on the setting, the column displays one of the following values:
 - **Set**
 - **Not Set**
 - **Compliance scheduled on**

Hover over any device to view the version number and compliance configured level for set compliance and displays the date, time (UTC), firmware version number, and compliance configured level for a scheduled compliance.

3. **Set Compliance**—Allows you to set firmware compliance for devices within a group. Click **Set Compliance** and turn on the toggle switch to enable and view the list of supported firmware versions for each device in a group in the **Manage Firmware Compliance** page.
 - a. **Set Compliance for Access Points**—To ensure firmware version compliance, complete the following parameters in the **Manage Firmware Compliance** page:
 - **Groups**—Select a specific group or multiple groups for which the compliance must be set. Select **All Groups** if you want to set compliance for all the groups.
 - **Firmware Version**—Select the firmware version number from the drop-down list to which the compliance is required to be set.
 - **When**—Select one of the following radio buttons to specify if the compliance must be carried out immediately or at a later date and time.
 - **Now**—Select this if you want the compliance to be carried out immediately.
 - **Later Date**—Select this if you want the compliance to be carried out in a specific time zone at the later date and time.
 - Click **Save** button to save the firmware compliance with the above settings. To clear the compliance, turn off the toggle switch.
 - b. **Set Compliance for Switches**—To ensure firmware version compliance, complete the following parameters in the **Manage Firmware Compliance** page:
 - **Groups**—Select the group for which the compliance must be set. Select the specific group to set compliance at group level.
 - **AOS-S Firmware Version**—Select the AOS-S firmware version number from the drop-down list to which the compliance is required to be set.
 - **CX Firmware Version**—Select the Aruba CX switch version number from the drop-down list to which the compliance is required to be set.
 - **When**—Select one of the following radio buttons to specify if the compliance must be carried out immediately or at a later date and time:

- **Now**—Select this if you want the compliance to be carried out immediately.
- **Later Date**—Select this if you want the compliance to be carried out in a specific time zone at the later date and time.
- **Install on**—Use the drop-down to select a primary partition or a secondary partition to install on.
- **Automatically reboot to complete the upgrade**—Select this check box to reboot Aruba Central automatically after the build is downloaded on the device. On reboot, the new build is installed on the device.
- Click **Save** button to save the firmware compliance with the above settings. To clear the compliance, turn off the toggle switch.



Aruba Central lists all available Aruba CX switches software versions. Select the software version that is applicable to the Aruba CX switch to which compliance is required to be set. For example, version 10.04.0020 is not applicable to Aruba CX 6200 and 6400 switch series.

- c. **Set Compliance for Controllers in Standalone Mode**—To ensure firmware version compliance, complete the following parameters in the **Manage Firmware Compliance** page:
 - **Groups**—Select a specific group or multiple groups for which the compliance must be set. Select **All Groups** if you want to set compliance for all the groups.
 - **Firmware Version**—Select the firmware version number from the drop-down list to which the compliance is required to be set.
 - **When**—Select one of the following radio buttons to specify if the compliance must be carried out immediately or at a later date and time:
 - **Now**—Select this if you want the compliance to be carried out immediately.
 - **Later Date**—Select this if you want the compliance to be carried out in a specific time zone at the later date and time.
 - **Install on**—Use the drop-down to select a primary partition or a secondary partition to install on.
 - **Automatically reboot to complete the upgrade**—Select this check box to reboot Aruba Central automatically after the build is downloaded on the device. On reboot, the new build is installed on the device.
 - Click **Save** button to save the firmware compliance with the above settings. To clear the compliance, turn off the toggle switch.
- d. **Set Compliance for Controllers in Cluster Mode**—To ensure firmware version compliance, complete the following parameters in the **Manage Firmware Compliance** page:
 - **Groups**—Select a specific group or multiple groups for which the compliance must be set. Select **All Groups** if you want to set compliance for all the groups.
 - **Firmware Version**—Select the firmware version number from the drop-down list to which the compliance is required to be set.
 - **Auto Reboot**—Select this check box to reboot Aruba Central automatically after the build is downloaded on the device. On reboot, the new build is installed on the device.
 - **When**—Select one of the following radio buttons to specify if the compliance must be carried out immediately or at a later date and time:
 - **Now**—Select this if you want the compliance to be carried out immediately.
 - **Later Date**—Select this if you want the compliance to be carried out in a specific time zone at the later date and time.
 - **Install on**—Use the drop-down to select a primary partition or a secondary partition to install

on.

- **Automatically reboot to complete the upgrade**—Select this check box to reboot Aruba Central automatically after the build is downloaded on the device. On reboot, the new build is installed on the device.
 - Click **Save** button to save the firmware compliance with the above settings. To clear the compliance, turn off the toggle switch.
4. **Upgrade All**—Allows you to simultaneously upgrade firmware for all devices. Click **Upgrade All** to view a list of supported firmware versions for each device.
- a. **To Upgrade all Access Points**—Click **Upgrade All** and complete the following parameters in the **Upgrade Access Points Firmware** page:
 - **Sites**—Select a specific site or multiple sites for which the upgrade must be set. You can also search for the site in the search filter.
 - **Firmware Version**—Select the firmware version number from the drop-down list to which the compliance is required to be set. Select **None** for none of the firmware versions.
 - **When**—Select one of the following radio buttons to specify if the upgrade must be carried out immediately or at a later date and time:
 - **Now**—Select this if you want the compliance to be carried out immediately.
 - **Later Date**—Select this if you want the compliance to be carried out in a specific time zone at the later date and time.
 - **Upgrade**—Click this button to start the upgrade with the above settings.
 - **Schedule**—Click this button to schedule the upgrade with the above settings.
 - **Cancel**—Click this button to cancel the upgrade.



While upgrading a large number of APs, cancel operation may not work as intended, and continues to upgrade.

- b. **To Upgrade all Switches**—Click **Upgrade All** and complete the following parameters in the **Upgrade Switch Firmware** page:
 - **Sites**—Select a specific site or multiple sites for which the upgrade must be set. You can also search for the site in the search filter.
 - **AOS-S Firmware Version**—Select the AOS-S firmware version number from the drop-down list to which the compliance is required to be set.
 - **CX Firmware Version**—Select the CX switch firmware version number from the drop-down list to which the compliance is required to be set.
 - **Auto Reboot**—Select this check box to reboot Aruba Central automatically after the build is downloaded on the device. On reboot, the new build is installed on the device.
 - **When**—Select one of the following radio buttons to specify if the upgrade must be carried out immediately or at a later date and time:
 - **Now**—Select this if you want the compliance to be carried out immediately.
 - **Later Date**—Select this if you want the compliance to be carried out in a specific time zone at the later date and time.
 - **Upgrade**—Click this button to start the upgrade with the above settings.
 - **Schedule**—Click this button to schedule the upgrade with the above settings.
 - **Cancel**—Click this button to cancel the upgrade.
- c. **To Upgrade all Controllers in Standalone Mode**—click **Upgrade All** and complete the following parameters in the **Upgrade Controller Firmware** page:

- **Sites**—Select a specific site or multiple sites for which the upgrade must be set. You can also search for the site in the search filter.
 - **Firmware Version**—Select the firmware version number from the drop-down list to which the compliance is required to be set.
 - **Auto Reboot**—Select this check box to reboot Aruba Central automatically after the build is downloaded on the device. On reboot, the new build is installed on the device.
 - **When**—Select one of the following radio buttons to specify if the upgrade must be carried out immediately or at a later date and time.
 - **Now**—Select this if you want the compliance to be carried out immediately.
 - **Later Date**—Select this if you want the compliance to be carried out in a specific time zone at the later date and time.
 - **Upgrade**—Click this button to start the upgrade with the above settings.
 - **Schedule**—Click this button to schedule the upgrade with the above settings.
 - **Cancel**—Click this button to cancel the upgrade.
- d. **To Upgrade all Controllers in Cluster Mode**—click **Upgrade All** and complete the following parameters in the **Upgrade Controller Firmware** page:
- **Firmware Version**—Select the firmware version number from the drop-down list to which the compliance is required to be set.
 - **Auto Reboot**—Select this check box to reboot Aruba Central automatically after the build is downloaded on the device. On reboot, the new build is installed on the device.
 - **When**—Select one of the following radio buttons to specify if the upgrade must be carried out immediately or at a later date and time.
 - **Now**—Select this if you want the compliance to be carried out immediately.
 - **Later Date**—Select this if you want the compliance to be carried out in a specific time zone at the later date and time.
 - **Upgrade**—Click this button to start the upgrade with the above settings.
 - **Schedule**—Click this button to schedule the upgrade with the above settings.
 - **Cancel**—Click this button to cancel the upgrade.
5. **Upload**—Allows you to upload the software image for multiple devices.
 6. **Search Filter**—Allows you to define a filter criterion for searching devices based on the following properties:
 - Common to all devices—Name, Firmware Version, Recommended Version and Upgrade Status of the device.
 - Specific to switches and controllers—MAC address and Model.
 7. **Column Filter**—Clicking the filter icon enables you to customize the table columns or set it to the default view.
 8. **Continue**—Allows you to continue with firmware upgrade.
 9. **Cancel Upgrade**—Cancels a scheduled upgrade.
 10. **Cancel All**—Cancels a scheduled upgrade for all devices.

Uploading a Software Image

To upload a software image for the device:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Firmware > Upload**.
3. Select the device from the **Device list** drop-down for which you want to upload the software image.

4. Click **Choose File** option to browse to your local directory and select the software image.
5. Click **Upload**. The updated file details is displayed in the **Uploaded Files** table.

This section also includes the following topics:

- [Upgrading a Single Device or Multiple Devices](#)
- [Upgrading Devices using Upgrade All Option](#)
- [Setting Firmware Compliance For Access Points](#)
- [Setting Firmware Compliance For Switches](#)
- [Setting Firmware Compliance For Controllers](#)

Upgrading a Single Device or Multiple Devices

Aruba Central (on-premises) allows you to upgrade a single device or multiple devices in the following ways:

1. In the **Network Operations** app, select one of the following options:
 - a. To select a group, site or global in the filter:
 - Set the filter to one of the options under **Group** or **Sites**. For all devices, set the filter to **Global**. The dashboard context for the selected filter is displayed.
 - Under **Maintain**, click **Firmware**.
 - Select one or more devices from the device list and click the **Upgrade** icon at the bottom of the page or hover over one of the selected device and click the **Upgrade** icon. The **Upgrade <Device> Firmware** pop-up window opens.
 - b. To select a device in the filter:
 - Set the filter to **Global**.
 - Under **Manage**, click **Devices**, and then click **Access Points**, **Switches**, or **Controllers**. A list of devices is displayed.
 - Click a device listed under **Device Name**. The dashboard context for the device is displayed.
 - Under **Maintain**, click **Firmware** and click **Upgrade** in the **Firmware Details** window. The **Upgrade <Device> Firmware** pop-up window opens.
2. In the **Upgrade <Device> Firmware** pop-up window, select the appropriate firmware version. You can either select a recommended version or manually choose a specific firmware version.



-
- To obtain custom build details, contact Aruba Central Technical Support.
 - The recommended firmware versions can be different for different devices and depends on the device model and software architecture.
-

3. Select one of the following radio buttons to specify if the compliance must be carried out immediately or at a later date and time:
 - **Now**—Allows you to set the compliance to be carried out immediately.
 - **Later Date**—Allows you to set the compliance to be carried out at the later date and time. Select a specific time zone from the **Select Zone** drop-down options to schedule the upgrade at a specific zone time.
4. From the **Install On** drop-down, select any one of the following partition options:
 - **Primary partition**—Select this if you want to install the firmware version in the primary partition.
 - **Secondary partition**— Select this if you want to install the firmware version in the secondary partition.

5. Select the check box if you want Aruba Central to automatically reboot after device upgrade.



The **Auto Reboot** option is available for AOS-Switch, AOS-CX switches, and Controllers.

6. Click **Upgrade**. The device downloads the image from the server, saves it to flash, and reboots. Depending on the progress and success of the upgrade, one of the following messages is displayed:
 - **Upgrading**—While image upgrade is in progress.
 - **Upgrade failed**—When the upgrade fails.
7. If the upgrade fails, retry upgrading your device.



After upgrading a switch, click **Reboot**.

Upgrading Devices using Upgrade All Option

To upgrade multiple devices using the **Upgrade All** option, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Group** or **Sites**. For all devices, set the filter to **Global**. The dashboard context for the selected filter is displayed.
2. Under **Maintain**, click **Firmware**.
The firmware dashboard for Access Points is displayed by default.
3. Click **Upgrade All**. The **Upgrade <Device> Firmware** pop-up window opens.
4. In the **Upgrade <Device> Firmware** pop-up window, select the specific site or multiple sites from the **Sites** drop-down list. This option is available only at the global context.
5. Select the appropriate firmware version (for Access points and Controllers) and AOS-S firmware version and CX firmware version (for AOS-CX and AOS-Switches) from their respective drop-down list. You can either select a recommended version or manually choose a specific firmware version.



-
- To obtain custom build details, contact Aruba Central Technical Support.
 - The recommended firmware versions can be different for different devices and depends on the device model and software architecture.
-

6. Select one of the following radio buttons to specify if the compliance must be carried out immediately or at a later date and time:
 - **Now**—Allows you to set the compliance to be carried out immediately.
 - **Later Date**—Allows you to set the compliance to be carried out at the later date and time. Select a specific time zone from the **Select Zone** drop-down options to schedule the upgrade at a specific zone time.
7. From the **Install On** drop-down, select any one of the following partition options:
 - **Primary partition**—Select this if you want to install the firmware version in the primary partition.
 - **Secondary partition**—Select this if you want to install the firmware version in the secondary partition.
8. Select the check box if you want Aruba Central to automatically reboot after device upgrade.



The **Auto Reboot** option is available for AOS-Switch, AOS-CX switches, and Controllers.

9. Specify if the upgrade must be carried out immediately or at a later date and time.

10. Click **Upgrade**. The device downloads the image from the server, saves it to flash, and reboots. Depending on the progress and success of the upgrade, one of the following messages is displayed:
 - **Upgrading**—While image upgrade is in progress.
 - **Upgrade failed**—When the upgrade fails.
11. If the upgrade fails, retry upgrading your device.



After upgrading a switch, click **Reboot**.

Setting Firmware Compliance For Access Points

Aruba Central allows you to run a firmware compliance check and force firmware upgrade for all APs in a group. To force a specific firmware version for all APs in a group, complete the following steps:

1. In the **Global** dashboard, under **Maintain**, click **Firmware**.
The **Access Points** tab is selected by default.
2. Verify the firmware upgrade status for all APs.
3. Click **Set Compliance** at the top right and turn on the toggle switch to enable the **Manage Firmware Compliance** window.
4. In the **Groups** drop-down list, select a single group, multiple, or All Groups.
5. Select a firmware version from the **Firmware Version** drop-down list.
6. Select one of the following radio buttons to specify if the compliance must be carried out immediately or at a later date and time:
 - **Now**—Allows you to set the compliance to be carried out immediately.
 - **Later Date**—Allows you to set the compliance to be carried out at the later date and time. Select a specific time zone from the **Select Zone** drop-down options to schedule the upgrade at a specific zone time.
7. Click **Save**.
Aruba Central initiates a firmware upgrade operation only for the devices that support the selected firmware version. If any of selected devices do not support the firmware version selected for the upgrade, a list of unsupported devices is displayed.

Setting Firmware Compliance For Switches

To force a specific firmware version for all Aruba switches in a group, complete the following steps:

1. In the **Global** dashboard, under **Maintain**, click **Firmware > Switches** tab.
2. Verify the firmware upgrade status for all switches.
3. Click **Set Compliance** at the top right and turn on the toggle switch to enable the **Manage Firmware Compliance** window.
4. In the **Groups** drop-down list, select a single group, multiple, or All Groups.
5. Select a AOS-S firmware version from the **AOS-S Firmware Version** drop-down list.
6. Select a CX firmware version from the **CX Firmware Version** drop-down list.
7. Select one of the following radio buttons to specify if the compliance must be carried out immediately or at a later date and time:
 - **Now**—Allows you to set the compliance to be carried out immediately.

- **Later Date**—Allows you to set the compliance to be carried out at the later date and time. Select a specific time zone from the **Select Zone** drop-down options to schedule the upgrade at a specific zone time.
- 8. From the **Install On** drop-down, select any one of the following partition options:
 - **Primary partition**—Select this if you want to install the firmware version in the primary partition.
 - **Secondary partition**— Select this if you want to install the firmware version in the secondary partition.
- 9. Select the check box if you want Aruba Central to automatically reboot.
- 10. Click **Save**. Aruba Central initiates a firmware upgrade operation only for the devices that support the selected firmware version. If any of selected devices do not support the firmware version selected for the upgrade, a list of unsupported devices is displayed.

Setting Firmware Compliance For Controllers

To force a specific firmware version for all controllers in standalone mode, complete the following steps:

1. In the **Global** dashboard, under **Maintain**, click **Firmware > Controllers** tab.
All the controllers with standalone mode is displayed.
2. Verify the firmware upgrade status for all controllers.
3. Click **Set Compliance** at the top right and turn on the toggle switch to enable the **Manage Firmware Compliance** window.
4. In the **Groups** drop-down list, select a single group, multiple, or All Groups.
5. Select a firmware version from the **Firmware Version** drop-down list.
6. Select one of the following radio buttons to specify if the compliance must be carried out immediately or at a later date and time:
 - **Now**—Allows you to set the compliance to be carried out immediately.
 - **Later Date**—Allows you to set the compliance to be carried out at the later date and time. Select a specific time zone from the **Select Zone** drop-down options to schedule the upgrade at a specific zone time.
7. From the **Install On** drop-down, select any one of the following partition options:
 - **Primary partition**—Select this if you want to install the firmware version in the primary partition.
 - **Secondary partition**— Select this if you want to install the firmware version in the secondary partition.
8. Select the check box if you want Aruba Central to automatically reboot.
9. Click **Save**. Aruba Central initiates a firmware upgrade operation only for the devices that support the selected firmware version. If any of selected devices do not support the firmware version selected for the upgrade, a list of unsupported devices is displayed.

To force a specific firmware version for all controllers in cluster mode, complete the following steps:

1. In the **Global** dashboard, under **Maintain**, click **Firmware > Controllers** tab.
All the controllers with cluster mode is displayed.
2. Verify the firmware upgrade status for all controllers.
3. Click **Set Compliance** at the top right and turn on the toggle switch to enable the **Manage Firmware Compliance** window.
4. In the **Groups** drop-down list, select a single group, multiple, or All Groups.
5. Select a firmware version from the **Firmware Version** drop-down list.

6. Select one of the following radio buttons to specify if the compliance must be carried out immediately or at a later date and time:
 - **Now**—Allows you to set the compliance to be carried out immediately.
 - **Later Date**—Allows you to set the compliance to be carried out at the later date and time. Select a specific time zone from the **Select Zone** drop-down options to schedule the upgrade at a specific zone time.
7. From the **Install On** drop-down, select any one of the following partition options:
 - **Primary partition**—Select this if you want to install the firmware version in the primary partition.
 - **Secondary partition**— Select this if you want to install the firmware version in the secondary partition.
8. Select the check box if you want Aruba Central to automatically reboot.
9. Click **Save**. Aruba Central initiates a firmware upgrade operation only for the devices that support the selected firmware version. If any of selected devices do not support the firmware version selected for the upgrade, a list of unsupported devices is displayed.

System management tab allows you to perform administrative tasks such as setting up the system, enabling SMTP settings, notifications, migration, and even backup and restore.



All system operations will be disabled till the current or the ongoing system operation is complete.

Viewing System Management in the Account Homes Page

To view the system management tab:

1. In the **Account Home** page, under **Global Settings**, click **System Management**.
2. The System Management page is displayed.
3. In the system management page, the following tabs are displayed:
 - [Performance](#)
 - [Version](#)
 - [Network](#)
 - [External Services](#)
 - [Backup and Restore](#)
 - [Migration](#)

Viewing System Performance

To view the Aruba Central (on-premises) system performance:

1. Go to the **Account Home** page.
2. Under **Global Settings**, click **System Management**.
3. The **Performance** tab displays the following components:
 - **Central System**—The **Central System** section displays the overall status of all the appliances, Central Processing Units, memory units, and data storage units as **Good** or **Poor**. For more information, see [Viewing Central System Status](#).
 - **Appliance Resources**—The **Appliance Resources** table displays details such as the percentage of CPU and memory utilization, status of the appliances in the cluster, percentage of disk space usage, and so on. For more information, see [Viewing Appliance Resources](#).
 - **Service Monitoring**—The **Service Monitoring** table displays details such as the status of various deployments, the number of restarts undergone by the services, and the age of the services, and so on. For more information, see [Monitoring Services](#).
 - **Logs**—The **Logs** table displays the various log files that are related to the appliances and services. The table also displays the time and date at which the log files were created. For more information, see [Viewing Appliance Resources](#).

- **System Operations**—The **System Operations** table displays details of various system operations running across the cluster. For more information, see [Viewing System Operations Details](#).

Viewing Central System Status

The **Central System** section displays the following details:

- **Appliance Status**—The **Appliance Status** indicates whether the overall status of the appliances in the cluster is **Good** or **Poor**.
- **CPU Status**—The **CPU Status** indicates whether the overall status of the processing units usage is **Good**, **Fair**, or **Poor**.
- **Memory Status**—The **Memory Status** indicates whether the overall status of the memory units usage is **Good**, **Fair**, or **Poor**.
- **Disk Status**—The **Disk Status** indicates whether the overall status of the disk usage is **Good**, **Fair**, or **Poor**.



NOTE

The Central System displays **Poor** in **Appliance Status**, **CPU Status**, **Memory Status**, and **Disk Status** even if one of the appliances' status is **Down** or the status in **CPU Status**, **Memory Status**, and **Disk Status** is **Poor**, respectively.

Viewing Appliance Resources

The **Appliance Resources** section displays a table with the following columns:

- **Appliance**—The **Appliance** column displays the FQDN of the appliance in the cluster.
- **Status**—The **Status** column displays the status of the appliance as **Up** or **Down**.
- **CPU**—The **CPU** column displays the percentage of CPU utilization of the appliance in the cluster.
- **Memory**—The **Memory** column displays the percentage of memory usage of the appliance in the cluster.
- **Storage**—The **Storage** column displays the percentage of storage utilization of the appliance in the cluster.
- **Disk(Read)**—The **Disk(Read)** column displays the percentage of disk utilization for the read operation.
- **Disk(Write)**—The **Disk(Write)** column displays the percentage of disk utilization for the write operation.
- **Network Usage Up**—The data transmitted from the appliance measured in bytes.
- **Network Usage Down**—The data received by the appliance measured in bytes.
- **Uptime**—The **Uptime** column displays the total duration for which the appliance was operational.

Clicking the  at the top right corner of the table pops up the **Add Appliance Resource** page. Enter the number of appliances to be added to the cluster along with corresponding FQDNs of the appliances and click **Add**.



NOTE

The  option is available for clusters that contain 3 or 5 appliances only. The  option is unavailable in a setup that contains a single or 7 devices.



You can click the  icon and select or de-select the columns required to be displayed in the table.



You can restart the appliance and generate logs by clicking the  and  icons, respectively.



To replace a device, click the  icon corresponding to the device. The **Replace Appliance Resource** page pops up. Enter the FQDN of the new appliance and click **Replace**.

Monitoring Services

The **Appliance Resources** section displays a table with the following columns:

- **Deployment**—The **Deployment** column displays the various deployment services running in the cluster.
- **Appliance**—The **Appliance** column displays the FQDN of the appliance in which the service is running.
- **Namespace**—The **Namespace** column displays the namespace of the services.
- **Status**—The **Status** column displays the status of the service as **Up**, **Down**, or **Partially Up**.
- **Restarts**—The **Restarts** column displays the number of restarts that the services have undergone.
- **Age**—The **Age** column displays the time duration for which the services were operational.



Click the  icon at the top right corner of the **Service Monitoring** table to generate log files related to all the listed services.

- You can restart the service, and generate logs related to a specific service in the **Service Monitoring** table by clicking the  and  icons, respectively.
- Viewing Log Files
- The **Logs** section displays a table with the following columns:
- **File**—The **File** column displays the name of the log file that is generated.
- **Type**—The **Type** column displays whether the file is readable for a single pod log or non-readable format snapshot for global level logs.
- **Created**—The **Created** column displays the time and date at which the log files were created.



You can click the  icon and select or de-select the columns required to be displayed in the table.



To download a specific log file, hover the mouse over the row in the **Logs** table and click the  icon.



To delete a specific log file, hover the mouse over the row in the **Logs** table and click the  icon.

Viewing System Operations Details

The **System Operations** section displays a table with the following columns:

- **Operation Type**—The **Operation Type** column displays the type of operation system running in the cluster.
- **Status**—The **Status** column displays the current status of the system operations as **Success, Failed, In Progress, or Timeout**.
- **More Details**—The **More Details** column displays additional details about the system operation status.
- **Start Time**—The **Start Time** column displays the time at which the system operation had begun.
- **End Time**—The **End Time** column displays the time at which the system operation had ended.

Upgrade Watcher

Aruba Central (on-premises) strongly recommends that you upgrade your On-premise version to the next available major version for a smooth and hassle free operation of your account. Upgrade watcher checks for any major versions release and notifies you for its availability on your next Central account login. The upgrade workflow differs based on the regular-Online and occasional-online user accounts.



The Upgrade operation can only be done by the user with admin rights.

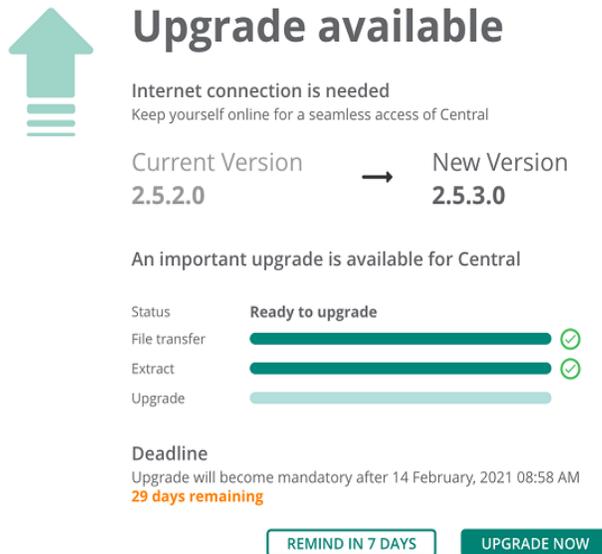
Upgrade Watcher Workflow for Regular-Online User

This section describes the upgrade workflow and the requirements for the regular-online Central user accounts. Based on the version availability, upon logging to your Central account, one of the following pages is displayed:

1. **Upgrade Available**—This window is displayed when you log in to your Central account within the deadline of the version upgrade (30 days from the date of version release). The upgrade available window provides the following information:
 - **Internet Connection is needed**—Informs the connectivity requirement for the process.
 - **Current version**—Current running version.
 - **New versions**—Next major available version.
 - **Status**—Provides the status and progress bar for file transfer, extract, and upgrade.
 - **Deadline**—Displays the number of days remaining for upgrade. The number of days varies depending on the version available date and the day of login. For example, if the version was available on 10th of December and the user logs in on 12th of December, the remaining days gets changed to 27 days within which the account needs to be upgraded.
 - **Upgrade Now**—Allows you to initiate the upgrade process.
 - **Go to Versions**—This tab is displayed if any one of the extraction stage is interrupted, in progress or failed. Clicking on the **Go to version** navigates to **System Management > Version** tab with version upgrade in process.
 - **Remind in x days**—Allows you to snooze the notification for some days. Notification can be snoozed for 7 days (30-20 remaining days), 5 days (20-10 remaining days), 3 days (10-5 remaining days), 2 days (5-3 remaining days), and 1 (for the rest remaining days). On snoozing the notification, you can use the account with all the normal functionality and the next notification comes after the set dates.

To upgrade the version once notified, click **Upgrade Now** to initiate the upgrade process. You can also navigate to **System Management > Version** tab to initiate the upgrade. For more information on how to navigate to version tab, see [Version](#).

The following example image displays the **Upgrade available** window:



2. **Upgrade Required**—This window is displayed when you log in to your Central account after the deadline is missed. This window indicates that you have missed the upgrade deadline and an immediate upgrade is required. All the account GUI functionality is blocked till the Aruba Central (on-premises) is upgraded to the latest version. To upgrade, click **Upgrade Now** to initiate the upgrade. The upgrade required window provides the following information:
- **Internet Connection is needed**—Informs the connectivity requirement for the process.
 - **Current version**—Current running version.
 - **New versions**—Next major available version.
 - **Status**—Provides the status and progress bar for file transfer, extract, and upgrade.
 - **Deadline**—Displays the number of overdue days post deadline.
 - **Upgrade Now**—Allows you to initiate the upgrade process.
 - **Retry**—This tab is displayed only when any one of the upgrade stage fails. Click **Retry** to retry the upgrade process. If the Upgrade fails after multiple retries, contact Aruba Central support representative.

Once the upgrade is successful, the account comes to its normal functionality.

The following example image displays the **Upgrade required** window with retry option:



Upgrade required

Internet connection is needed
Keep yourself online for a seamless access of Central

Current Version → New Version
2.5.2.0 → 2.5.3.0

An important upgrade is available for Central

Status	Upgrade failed
File transfer	<div style="width: 100%;"><div style="width: 100%;"></div></div> ✓
Extract	<div style="width: 100%;"><div style="width: 100%;"></div></div> ✓
Upgrade	<div style="width: 100%;"><div style="width: 80%; background-color: #f08080;"></div></div> ✗ Failed during pre-snapshot stage

Deadline
Upgrade overdue on 01 January, 2021 06:51 AM
7 days overdue

RETRY

Upgrade Watcher Workflow for Occasional-Online User

This section describes the upgrade workflow and the requirements for the occasional-online Central user accounts. This scenario is based on the users that logs into Central after 39 days or a maximum of 45 days from the date of connectivity loss. All the account GUI functionality is allowed and the user has to upgrade to the major available version within the prescribed period. Based on the account login period, one of the following pages is displayed:

1. **Upgrade Check Failed**—This window is displayed when the user logs into Central within the above mentioned periods. The upgrade check failed window provides the following information:
 - **Internet Connection is needed**—Informs the connectivity requirement for the process.
 - **Last Upgrade Check**—Displays the date of last upgrade check.
 - **Deadline**—Displays the remaining days for mandatory upgrade check.
 - **Check for Upgrade**—Once connected, it check for the status and redirects you to the Upgrade available/ Upgrade required page.
 - **Remind in x days**—Allows you to snooze the notification. Snoozing can be done for 5 days (on 39th day) and 1 day for the remaining.

The following example image displays the **Upgrade check failed** window:



Upgrade check failed

Internet connection is needed
Keep yourself online for a seamless access of Central

Last upgrade check
21 October, 2020

Deadline
Upgrade check will become mandatory after 05 December, 2020 12:08 PM
5 days remaining

REMIND IN 5 DAYS

CHECK FOR UPGRADE

- Upgrade Check Required**—This window is displayed when the user logs into Central account after 45 days from the day of connectivity loss. In this scenario, the user account is blocked and an immediate upgrade check is required. The upgrade check required window displays the following information:
 - **Internet Connection is needed**—Informs the connectivity requirement for the process.
 - **Last Upgrade Check**—Displays the date of last upgrade check.
 - **Deadline**—Displays the remaining days for mandatory upgrade check.
 - **Check for Upgrade**—Once connected, it check for the status and redirects you to the Upgrade available/ Upgrade required page.

The following example image displays the **Upgrade check required** window:



Upgrade check required

Internet connection is needed
Keep yourself online for a seamless access of Central

Last upgrade check
14 October, 2020

Deadline
Upgrade check overdue on 28 November, 2020 12:08 PM
1 day overdue

CHECK FOR UPGRADE

Version

The **Version** tab displays the installed version, available version for upgrade, upgrade status, and you can generate logs related to events that occurred during an upgrade.

Viewing Installed and Available Version Information

To view the Aruba Central (on-premises) versions:

1. Go to the **Account Home** page.
2. Under **Global Settings**, click **System Management > Version** tab.
3. The **Installed Version** displays the currently installed version in the Aruba Central (on-premises) server.
4. The **Available Version** displays the version that is currently available and the user can upgrade to this version.

Upgrading Aruba Central (on-premises)

To upgrade Aruba Central (on-premises) to the latest version:

1. Go to the **Account Home** page.
2. Under **Global Settings**, click **System Management > Version** tab.
3. In the Upgrade section, click **Upgrade Now** to upgrade to the latest version of Aruba Central (on-premises).
4. This section also details and provides the status of the upgrade like overall Status, File Transfer, Extract, and Upgrade.

Generating Logs

Aruba Central (on-premises) allows you to view and download logs related to the events that occurred during the upgrade process. To generate the logs for the events, click the **Generate Logs** menu option in the **Logs** pane. Once generated, the logs can be viewed from the logs table.

The **Logs** table displays the following information and also allows you to download or delete logs:

- **File**— Displays the generated file name.
- **Created**— Displays the date and time of the log creation.
- **Status**— Displays the status of the generated logs.
- **Action**— Allows you to do the following actions:
 - **Download**— Select the file and click the  icon to download the generated file.
 - **Delete**— Select the file that you want to delete and click the delete icon. In the **Confirm Action** pop-up window, click **Yes**.

Network

The **Network** tab displays the summary of the network settings configured for a cluster and allows you to test the proxy server and configure the support connection.

Viewing Network Settings Information

To view the Aruba Central (on-premises) network:

1. Go to the **Account Home** page.
2. Under **Global Settings**, click **System Management > Network** tab.

3. The Network pane displays the following information:
 - **FQDN**
 - **VIP**
 - **Subnet Mask**
 - **Gateway**
 - **Primary DNS**
 - **Secondary DNS**
 - **NTP IP or FQDN**
 - **NTP time Zone**



The information displayed in Network pane is read-only and based on the data that you configure while setting up the network. For more information, see Aruba Central (on-premises) Installation and Setup Guide.

Viewing Proxy settings

To view the Aruba Central (on-premises) network:

1. Go to the **Account Home** page.
2. Under **Global Settings**, click **System Management > Network** tab.
3. Click **Network** tab. In the **Proxy** pane, enter the following information:
 - **Port**— Enter the proxy server port.
 - **Proxy Server**— Enter the proxy server host name or IP address.
 - **Username**— Enter the username.
 - **Password**— Enter the password.
 - **Confirm Password**— Re-enter the password to confirm.
4. Click **Save** or **Test Proxy** to validate the proxy settings.



To validate the Proxy server, ensure that you provide a valid server details. You can also setup the Proxy Server in the **Proxy Server Setup Option** while configuring the cluster. For more information, see Aruba Central (on-premises) Installation and Setup Guide.

Viewing Support Connection

To view the Aruba Central (on-premises) network:

1. Go to the **Account Home** page.
2. Under **Global Settings**, click **System Management > Network** tab.
3. The **Support Connection** pane with **Status** is displayed.

You can start the connection from the UI by clicking the **Start** button in the **Support Connection** pane. After a connection is established between the tunnels, you can stop by clicking the **Stop** button in the same pane. On successful operation, the status shown as **active**.

You can also start, stop, restart, upload support connection file, or check the status of the Support Connection using the CLI command. For more information, see Support Command section in Aruba Central (on-premises) User Guide.

External Services

This tab helps you configure the SMTP server settings, syslog servers, and SNMP traps destination.

To view the External Services:

1. Go to the **Account Home** page.
2. Under **Global Settings**, click **System Management**.
3. Click the **External Services** tab.

The tab displays the following components:

SMTP—The **SMTP** section displays a table of SMTP servers, the ports used by the servers, and the server status. You can configure only one SMTP server in COP. For more information, see [SMTP](#).

SNMP Traps Destination—The **SNMP Traps Destination** table displays details such as the trap destination IP addresses of the SNMP server where the trap is sent, and the SNMP server versions. For more information, see [SNMP Traps Destination](#).

SysLog—The **SysLog** table displays a list of syslog servers with the corresponding IP addresses and the associated ports. For more information, see [SysLog Server Details](#).

SMTP

To ensure correct delivery of emails to the user accounts configured in your setup, you must configure the server settings in Aruba Central (on-premises). Starting from Aruba Central (on-premises) 2.5.3.0, unencrypted email server communication is supported. A new option, **No encryption** is supported for SMTP. When you configure SMTP, you can choose **TLS**, **SSL**, or **No encryption**.

The SMTP table displays the following details:

- **Server**—The **Server** column displays the SMTP server names.
- **Port**—The **Port** column displays the configured SMTP port for the server. The default Aruba SMTP Port is **587**.
- **Status**—The **Status** indicates the status of the SMTP server. The status is indicated as **Failure** or **Success**.

To edit the SMTP server, perform the following steps:

1. In the **SMTP** pane, hover over the SMTP server name and click the  icon.
2. The **Edit SMTP Server** section is displayed. Enter the following details:
 - **Host name or IP address**—Host name or Address of the SMTP server.
 - **Port**—Port number of the SMTP server.
 - **User Name**—Email address of the user.
 - **Password**—Password. Retype the password to confirm.
 - **Use TLS**—Enables TLS for secure communication.
 - Add a recipients email address in the **Test Email** section.
3. Click **Save**.

SNMP Traps Destination

An SNMP trap is a notification that is sent to an SNMP server when certain events occur, such as faults or security events. The trap destination IP address is the IP address of the SNMP server where the trap will be sent. The SNMP Traps Destination section displays a table with the following columns:

- **Server**—The **Server** column displays the SNMP trap server name or IP of the traps server.
- **Version**—The **Version** column displays the version of the SNMP. The version supported is v2 version.

Clicking the  icon displays the **Add SNMP Trap** page. To add a new SNMP trap, enter the SNMP server name, host name, port details, and click **Save**.

Clicking the  icon to download MIB files. You can download and use the MIB files in your SNMP manager to monitor memory status, hardware status, etc. within the device.

SysLog Server Details

To enable Aruba Central (on-premises) to send system events to a logging server, ensure that you configure the Syslog server details on Aruba Central (on-premises). The **SysLog** table displays the following columns:

- **Server**—This column displays the name of the syslog servers.
- **IP Address**—This column displays the IP address of the specific syslog server.
- **Port**—This column displays the port number associated with the specific syslog server.

Clicking the  icon at the top right corner of the table displays the **Add Syslog Server** page. To add a new syslog server, enter the syslog server name, server IP address, server port and click **Save**.

Backing up and Restoring Aruba Central System Data

Aruba Central (on-premises) supports backing up of system information, group configuration data, alerts, events, audit trail, sites, labels, and historical reports. You can backup Aruba Central data either manually or set a schedule for an automatic backing up of the data.

Important Points to Note

- Before backing data, you must have a file server configured and ready to save the backup file.
- Backups consumes large amounts of space (up to 5 terabyte). Make sure you have sufficient space for a successful backup operation.
- The restore operation deletes any configuration applied before the restore. It also deletes and replaces device variables with the backed up that is being restored.
- For restore operation, make sure you provide the file path that you used for backup and select the appropriate backup file version.
- During backup and restore operation, the IO system alert should be considered normal due to the intense read and write carried out on the file system.

Manually Backup Data

To manually backup data:

1. In the **Account Home** page, under **Global Settings**, click **System Management**.
2. Click **Backup and Restore** tab. The Backup and Restore page is displayed.
3. In the **Backup** pane, click the **Backup Now** menu option. The **Immediate Backup** window opens.
4. In the **Immediate Backup** window, configure the following parameters:
 - a. **Host name or IP address**— Specify the host name or IP address of the server.
 - b. **Protocol Type**— Specify **SFTP** or **SCP**. By default, **SFTP** is selected.
 - c. **File Path**— Specify the file path or folder name in the server to which you want to save the data.
 - d. **Username**— Specify the server SFTP or SCP username.
 - e. **Password**— Provide the server SFTP or SCP password.
5. Click **Backup Now** to start backing up the data to the server. In case of successful backup, the **Status** in the backup pane shows **Completed**. You can also view the status of the supported data types by clicking the **Backed up Systems** arrow. The status sign against each data type turns green representing a successful backup and red representing a failed backup.
6. The following are the supported data types:
 - a. **PostgreSQL**
 - b. **Cassandra**
 - c. **Elasticsearch**
 - d. **Elasticsearch Aggregation**
 - e. **Minio**

Figure 103 *Backup Now*

IMMEDIATE BACKUP

Host name or IP address

User name

Protocol Type
SFTP 

SFTP

SCP

Password 

File Path

Creating a Backup Schedule

To set a schedule for regular backing up of Aruba Central data:

1. In the **Account Home** page, under **Global Settings**, click **System Management**.
2. Click **Backup and Restore** tab. The Backup and Restore page is displayed.
3. In the **Backup** pane, click the **Backup Later** menu option. The **Scheduled Backup** window opens.
4. In the **Scheduled Backup** window, configure the following parameters:
 - a. Specify a backup Frequency from the following options:
 - **Back up daily**— Select this option to have a backup daily. Specify the starting time at which the backup must be run.

- **Back up weekly**— Select this option to have a backup weekly. Specify the backup day and starting time at which the backup must be run.
 - **Disable backup schedule**— Select this to disable the backup schedule.
- b. **Host name or IP address**— Specify the host name or IP address of the server.
 - c. **Protocol Type**— Specify **SFTP** or **SCP**. By default, **SFTP** is selected.
 - d. **File Path**— Specify the file path or folder name in the server to which you want to save the data.
 - e. **Username**— Specify the server SFTP or SCP username.
 - f. **Password**— Provide the server SFTP or SCP password.
5. Click **Save**.

Figure 104 *Backup Later*

SCHEDULED BACKUP

Back up daily
 Back up weekly
 Disable backup schedule

Backup day
 Select Starting at 12 : 43

Host name or IP address User name

Protocol Type
 SFTP Password

SFTP
 SCP

File Path

Restoring Data

To restore the backed up data:

1. In the **Account Home** page, under **Global Settings**, click **System Management**.
2. Click **Backup and Restore** tab. The Backup and Restore page is displayed.
3. In the **Restore** pane, click the **Restore Now** menu option. The **Restore** window opens.
4. In the **Restore** window, configure the following parameters:
 - a. **Host name or IP address**— Specify the host name or IP address of the server used to save the backup data.
 - b. **Protocol Type**— Specify **SFTP** or **SCP**. By default, **SFTP** is selected.
 - c. **File Path**— Specify the file path or folder name in the server from which you want to restore the saved data.
 - d. **Username**— Specify the server SFTP or SCP username.
 - e. **Password**— Provide the server SFTP or SCP password.
5. Click **Restore System**.

Figure 105 *Restore*

RESTORE

Host name or IP address _____ User name _____

Protocol Type
SFTP 

SFTP
SCP

File Path _____ Password _____ 

Generating Logs

During the the restore process, most of the services will be offline for the restore and get back online when the restore is complete. You can view the progress of the restore operation by logging into Aruba Central CLI through a serial console and use the show command to navigate to Backup-Restore status. For more information, see [Accessing the Aruba Central CLI](#) and [Show Commands](#) in the Aruba Central (on-premises) user guide



NOTE

The **Logs** table displays the following information and also allows you to download or delete logs:

- **File**— Displays the generated file name.
- **Created**— Displays the date and time of the log creation.
- **Status**— Displays the status of the generated logs.
- **Action**— Allows you to do the following actions:
 - **Download**— Select the file and click the  icon to download the generated file.
 - **Delete**— Select the file that you want to delete and click the delete icon. In the **Confirm Action** pop-up window, click **Yes**.

Migrating the AirWave Server

Important Information for Migration

The following are the requirements and guidelines for the migration process:

- The AirWave system must be running a minimum AirWave version of 8.2.8.2 for the online migration to proceed and a minimum version of 8.2.11.0 to proceed with offline migration. If the AirWave system is running an earlier version, refer to the AirWave documentation to upgrade the version to minimum supported versions.
- Only those APs, controllers, and switches that are supported in Aruba Central (on-premises) are migrated. For information on supported hardware, see [Supported Platforms](#) section.
- As part of migration, Visual RF and the device inventory for CAPs, IAPs, controllers, and Aruba/HPE switches are migrated.
- For controllers, the device credentials for SNMP and HTTPS profiles are mapped.

- Migration of multiple AirWave systems to a single Aruba Central (on-premises) server is supported. That is, you can migrate multiple AirWave systems to Aruba Central (on-premises) by adding the IP addresses or **AMP Hostnames** of each AirWave system individually.
- All the historical data including data related to reports, monitoring, and stats are not migrated from Airwave to Aruba Central (on-premises) during the migration process.
- Templates are not migrated from Airwave to Aruba Central (on-premises) during the migration process. You must manually create a new template in Aruba Central (on-premises) based on the requirement.
- All data related to VisualRF is migrated from Airwave to Aruba Central (on-premises) during the migration process.

Accessing the Migration Page

To access the migration page, perform the following procedure:

1. Log in to your Aruba Central (on-premises) account as an administrator.
2. Click the **Account Home** page icon.
The Account Home page is displayed.
3. Click **Global Settings > System Management**.
4. Click the **Migration** tab.

The migration page is displayed.



During the migration process, a new AMP back up is created in AirWave and transferred to the Aruba Central (on-premises). The scheduled nightly backup is independent of the backup operation performed as a part of the migration process.

Following table lists the **Migration** tab details:

Table 225: Migration Parameters

Name	Description
Airwave Address	FQDN or IP address of the AMP.
Migration Status	Indicates if the migration is ongoing, failed, or successful. For more information, see Migration Status and Migration Descriptions .
Description	Displays the ongoing step in the migration process. For example, the Description column provides information
Summary	You can hover over the Provides a summary of the migration activity occurring during migration. Following are some of the messages displayed: <ul style="list-style-type: none">■ Number of devices existing on Aruba Central (on-premises)■ Number of devices on AirWave 8.x■ Number of devices to migrate■ Number of devices successfully migrated■ Number of devices failed to migrate
Action	Allows you to restart the migration process by clicking the restart  icon. You can also delete an AMP from the migration table by clicking the delete  icon.

5. Click the **Migration** tab at the top right corner of the table to add a new migration task. For more information, see [Performing the Migration](#).

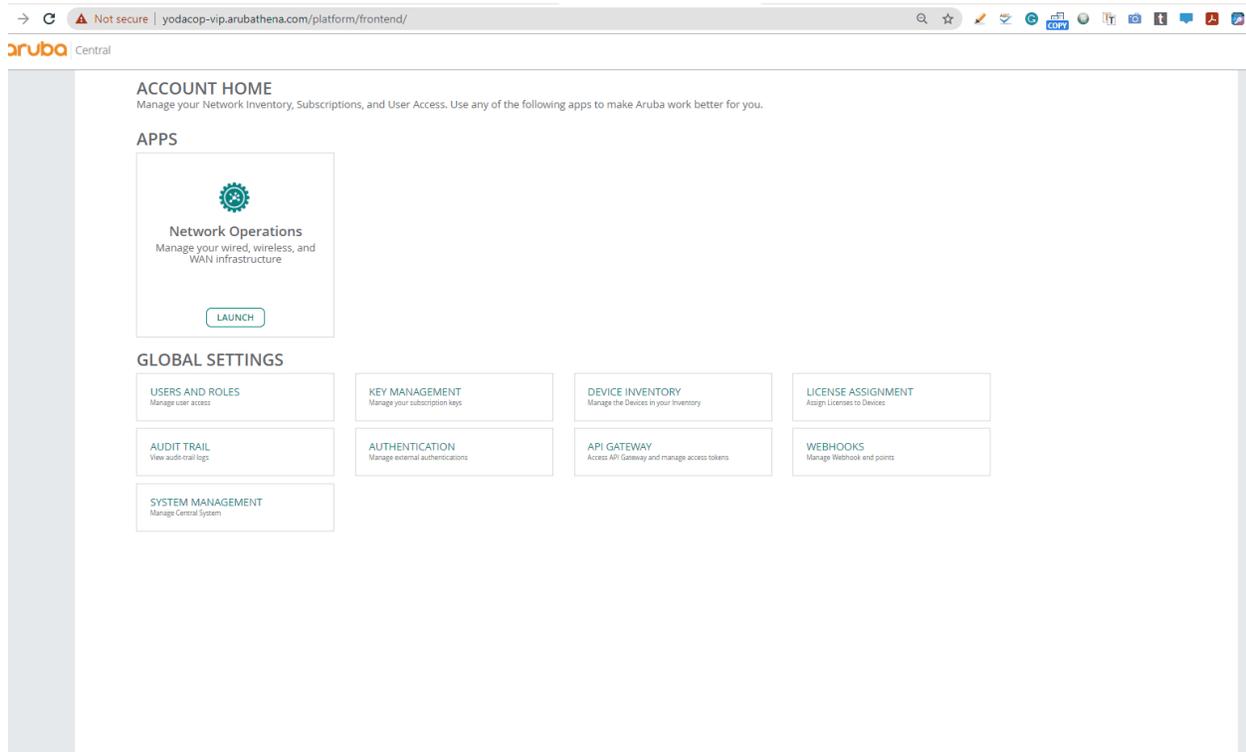
Performing the Migration

First you need to add the AirWave server that is running the older software version to Aruba Central. After the migration process completes, the Device Inventory page becomes available.

Aruba Central (on-premises) supports both offline and online migration.

Online Migration

When you begin the migration, the Aruba Central server establishes a connection with the AirWave server using the information you provide on the Migration page.



To perform an online migration, perform the following steps with an Internet connection:

1. Log in to your Aruba Central (on-premises) account as an administrator.
2. Click the **Account Home** page icon.
The Account Home page is displayed.
3. Click **Global Settings > System Management**.
4. Click the **Migration** tab to display the Migration page.
5. Click  in the AirWave Migration table to display the **Add Migration** page.
6. In the **Add Migration** page, select the **Online Migration** option.
7. Enter the following details:
 - **Host Name or IP Address**—Enter the IP address of the AirWave Management Platform (AMP).
 - During the migration process, a new AMP back up is created in AirWave and transferred to the Aruba Central (on-premises). The scheduled nightly backup is independent of the backup operation performed as a part of the migration process.
 - **Password**—Enter the password associated with the administrative account.
 - **Confirm Password**—Re-enter the password.
8. Click **Save** to begin the migration process.
9. You can add multiple IP addresses to migrate from multiple AirWave servers to one Aruba Central (on-premises) server. In this case, each AMP will be migrated sequentially one after another.



You can not delete an AMP when the migration is in-progress.

10. In the **Airwave Migration** table of the **Migration** page, the online migration entry has the  ,





icons allowing you to edit, restart, and delete the migration respectively.

Figure 106 Add Migration Using Host Name

The screenshot shows a web form titled "ADD MIGRATION". At the top, there are two radio buttons: "Online Migration" (selected) and "Offline Migration". Below this, there are four input fields: "Hostname or IP Address" containing "cluster.arubathena.com", "AMP User name" containing "admin", "Password" (masked with dots), and "Confirm password" (masked with dots). At the bottom right, there are two buttons: "CANCEL" and "SAVE".

Figure 107 Add Migration Using IP Address

The screenshot shows a web form titled "ADD MIGRATION". At the top, there are two radio buttons: "Online Migration" (selected) and "Offline Migration". Below this, there are four input fields: "Hostname or IP Address" containing "10.22.153.226", "AMP User name" containing "admin", "Password" (masked with dots), and "Confirm password" (masked with dots). At the bottom right, there are two buttons: "CANCEL" and "SAVE".



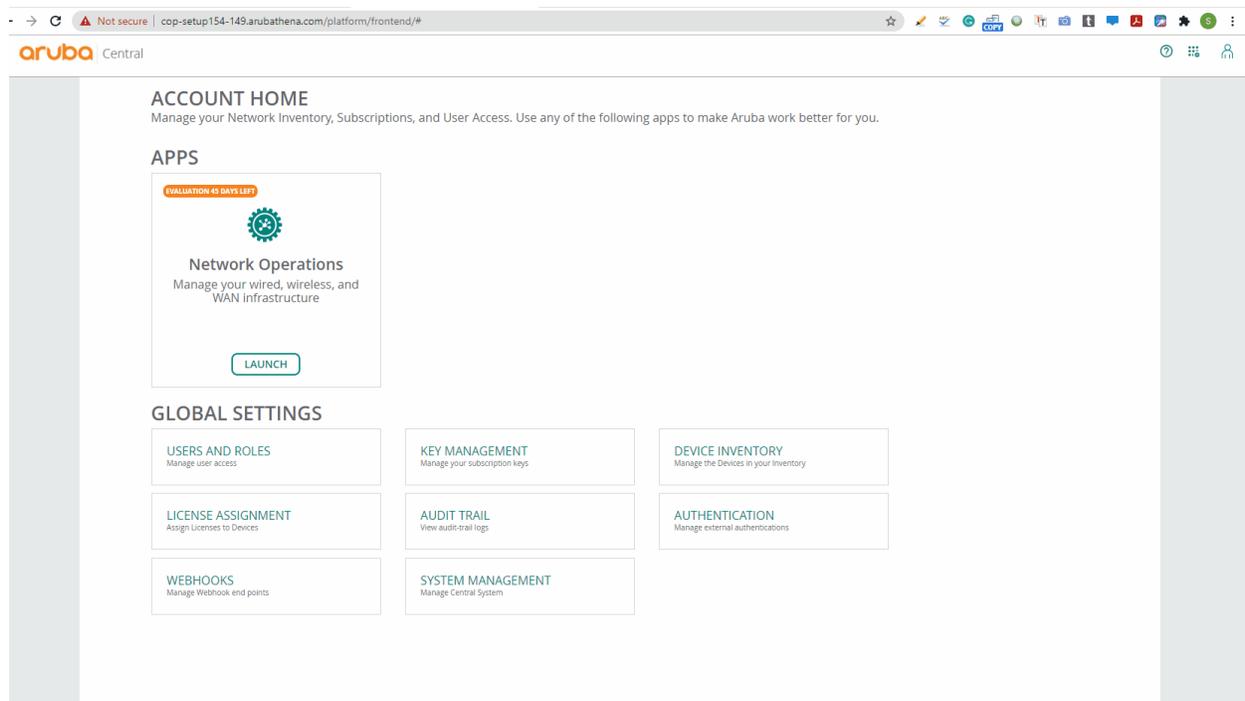
All system operations are disabled until the active system operation is complete. The migration, backup and restore, high availability processes, and the upgrade operations are the system operations in Aruba Central (on-premises).

Offline Migration

In addition to the online migration, Aruba Central (on-premises) allows you to perform offline migration of the Device Inventory data and Visual RF data from AirWave to Aruba Central (on-premises) by uploading the backup file that was earlier downloaded from AirWave.

This process is called Offline Migration. Offline Migration is also called as the Inplace Migration. The user need not have the AirWave server up and running for an offline migration.

Offline migration is required when the user wants to deploy Aruba Central (on-premises) on the same AirWave server. The advantage of offline migration is that the user can bring in all the devices to Aruba Central (on-premises) from AirWave with a single operation.



In offline migration, the Aruba Central (on-premises) is installed on the servers where the AMP is operational.



The minimum supported version for the migration is AirWave 8.2.11.0.

Follow these steps to migrate your data using offline migration:

1. Log in to your Aruba Central (on-premises) account as an administrator.
2. Click the **Account Home** page icon.
The Account Home page is displayed.
3. Click **Global Settings > System Management**.

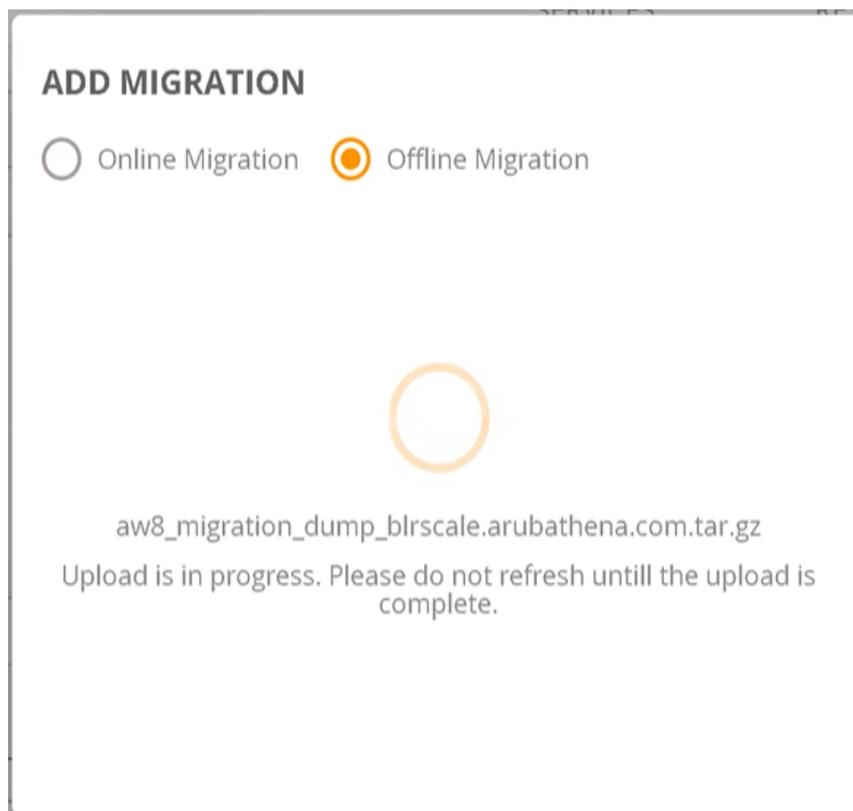
4. Click the **Migration** tab to display the Migration page.
5. Click  in the AirWave Migration table.
The Add Migration page is displayed.
6. Select the **Offline Migration** option.
7. Browse to the location to choose the migration file that was downloaded from AirWave.
8. Click **Save**.

ADD MIGRATION

Online Migration Offline Migration

Choose migration file downloaded from AirWave

BROWSE



In the **Airwave Migration** table of the **Migration** page, only



icon is available corresponding to the offline migration entry.



When the upload is in progress, you must not refresh the page.

Validating the Migration Process

After you click **Save** on the migration window, the migration process starts. If multiple AMPs are added, each AMP will be migrated sequentially one after another.

The following figure shows the main components of the Migration page.

Figure 108 Screen Capture of Offline Migration

GO TO ACCOUNT HOME

PERFORMANCE VERSION NETWORK EXTERNAL SERVICES BACKUP AND RESTORE **MIGRATION**

All system operations will be disabled till the active system operation is complete.

Airwave Migration (1)			
Migration	Migration Status	Description	Summary
ump_blrscle.arubathena.com.tar.gz	COP migration is in progress	Restoring AMP backup in COP	-

LOGS
NOTE:Generating logs can take time. GENERATE LOGS

FILE	CREATED	STATUS	ACTIONS
Migration file uploaded successfully			

Figure 109 Screen Capture of a successful Migration.

PERFORMANCE VERSION NETWORK EXTERNAL SERVICES BACKUP AND RESTORE **MIGRATION**

Airwave Migration (1)			
Migration	Migration Status	Description	Summary
aw8_migration_dump_blrscle.arubathena.com.tar.gz	Migration Success	Migration of AMP completed successfully	Devices existing on COP:IP(1), Switch(1), CAP(2) Aruba de...

Logs
NOTE:Generating logs can take time. GENERATE LOGS

File	Created	Status	Actions
migration-plain-1m-1605771003	Nov 19, 2020, 13:00	DOWNLOAD READY	Download Icon
migration-plain-1m-1605783700	Nov 19, 2020, 16:31	DOWNLOAD READY	Download Icon
migration-plain-1m-1605783661	Nov 19, 2020, 16:31	DOWNLOAD READY	Download Icon
migration-plain-1m-1605770757	Nov 19, 2020, 12:55	DOWNLOAD READY	Download Icon



The default time out period for the backup process during the migration is **120 minutes**.

During the migration process, a fresh AMP back up is created in Airwave 8.x and transferred to the Aruba Central (on-premises). The scheduled nightly backup is not performed as a part of the migration process.

Logs

The **Logs** table displays all the logs related to the migrations that are either complete or failed.

You can create or generate the log files in one of the following ways:

- In the **Account Home > Global Settings > System Management > Migration > Logs** table, click **Generate Logs** to create the log files.
- In the **Account Home > Global Settings > System Management > Performance > Service**



Monitoring table, select the deployment service and click the icon.

The log files that are generated contains the cumulative data of all the AMP migrations.

You can view the device migration POD logs from the Aruba Central (on-premises) backend or from the UI.

The VisualRF migration POD logs are available in one of the COP cluster node and can be viewed in the `/var/log/visualrf` path.



Figure 110 Log File

LOGS						GENERATE LOGS
NOTE: Generating logs can take time.						
FILE	IP	CREATED	IP	STATUS	IP	ACTIONS
migration-plain-1m-1591867996		Jun 11, 2020, 15:03		DOWNLOAD READY		
migration-plain-1m-1591868005		Jun 11, 2020, 15:03		DOWNLOAD READY		
migration-plain-1m-1593511280		Jun 30, 2020, 15:31		DOWNLOAD READY		
migration-plain-1m-1591772020		Jun 10, 2020, 12:23		DOWNLOAD READY		
migration-plain-1m-1593511213		Jun 30, 2020, 15:30		DOWNLOAD READY		

The **Logs** table displays the following columns:

Table 226: Logs Table

Name	Description
File	The name of the log file that is generated.
Created	The date and time when the log file is created.
Status	Indicates the status of the logs that are generated. The status indicated is Download Ready, In Progress, Successful, or Failed.
Action	Enables you to perform the following actions: <ul style="list-style-type: none"> ■ Downloading the generated log files by clicking the download icon. The files are then saved to the local drive as a TAR file. ■ Deleting the log file by clicking the delete icon.

Migration Status

Following is a list of migration status displayed in the Airwave Migration table:

- Waiting to start migration
- Migration Stopped
- Migration Started
- AW8.X generating migration dump
- AW8.X migration dump is ready
- COP migration is in progress
- Migration Success
- Migration Failed

Migration Descriptions

Following is a list of migration status descriptions that are displayed during the migration process under the description heading of the migration table:

- Migration of AMP not started
- Starting migration of AMP to COP
- Connecting to AMP
- Could not establish connection to AMP
- Could not prepare backup on AMP
- Waiting for AMP backup to be prepared
- AMP backup not prepared after 2 hrs, please check AMP logs
- AMP backup is ready for download from AMP
- AMP backup is being downloaded to COP
- AMP backup download failed
- AMP backup downloaded successfully
- Restoring AMP backup in COP
- AMP version not supported for migration
- Migrating devices to COP Migrating profiles to COP
- Checking for VRF data to migrate VRF migration in progress
- Migration of VRF data failed VRF
- Migration did not complete after 2 hrs, please check the VRF logs
- Migration of AMP completed successfully, VRF data not found
- Migration was terminated abruptly, please retry migration
- Migration of AMP completed successfully
- Exception occurred during migration, please check the logs
- Another system operation is active, retry after sometime

In the **Network Operations** app, use the filter to select a group or a device and then, select **Tools** menu option under **Analyze**. The **Tools** menu allows network administrators and users with troubleshooting permission to perform troubleshooting or diagnostics tests on devices and networks managed by Aruba Central. Users with admin role and custom roles that allow edit access to the troubleshooting module can troubleshoot network and device issues. For more information on user roles, see [Configuring User Roles](#)



-
- The **Tools** menu option is not visible to users who do not have troubleshooting permission.
 - Aruba Central does not support performing diagnostic checks on offline devices.
-

The **Tools** page is divided into the following tabs:

- **Network Check**—Allows you to run diagnostic checks on networks and troubleshoot client connectivity issues. You must have admin privileges or read-write privileges to perform network checks.
- **Device Check**—Allows you to run diagnostic checks and troubleshoot switches. You must have admin privileges or read-write privileges to perform device checks.
- **Commands**—Allows you to perform network health check on devices at an advanced level using command categories. Read-only users can also perform advance checks.

Troubleshooting Network Issues

Network check aims to identify, diagnose, and debug issues detected in an Aruba Central-managed network. The **Network Check** tab on the **Tools** page captures the troubleshooting utilities that are used to test a network entity and collect results based on your selection.

To perform a diagnostic check on the Aruba Central-managed network, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**. The dashboard context for the selected filter is displayed.
 - To select a device in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices**, and then click **Access Points, Switches, or Controllers**.
 - c. A list of devices is displayed in the **List** view.
 - d. Click a device listed under **Device Name**.
The dashboard context for the device is displayed.

2. Under **Analyze > Tools**, click the **Network Check** tab.

The **Network Check** page is displayed.

3. Select a device. You can run diagnostic checks on the following types of devices managed by Aruba Central:
 - [Troubleshooting AP Connectivity Issues](#)
 - [Troubleshooting Switch Connectivity Issues](#)
 - [Troubleshooting Controller Connectivity Issues](#)

The following table lists the tests available for each type of device.

Table 227: Tests and Devices

Test	Campus Access Point	Instant Access Point	Switch	Controller
Ping Test	Not Available	Available	Available	Available
Traceroute	Not Available	Available	Available	Available
HTTP Test	Not Available	Available	Not Available	Not Available
HTTPS Test	Not Available	Available	Not Available	Not Available
TCP Test	Not Available	Available	Not Available	Not Available
Speed Test (iPerf)	Available	Available	Not Available	Available
Ping Sweep Test	Not Available	Not Available	Not Available	Not Available



Devices which are already running commands shall not execute newly added commands.

This section includes the following topics:

- [Troubleshooting AP Connectivity Issues](#)
- [Troubleshooting Switch Connectivity Issues](#)
- [Troubleshooting Controller Connectivity Issues](#)

Troubleshooting AP Connectivity Issues

The following tests are available to diagnose issues pertaining to WLAN network connections:

Ping Test

Sends ICMP echo packets to the hostname or IP addresses of the selected devices to check for latency issues.

To perform a ping test on APs, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.

- To select a device in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices > Access Points**.
A list of access points is displayed in the **List** view.
 - c. Click an access point listed under **Device Name** for which you want to perform diagnostic test.
The dashboard context for the access point is displayed.
- 2. Under **Analyze > Tools**, click **Network Check**.
- 3. From the **Device Type** drop-down list, select **Access Point**.
- 4. From the **Sources** drop-down list, select source(s). You can select multiple APs.
- 5. From the **Test** drop-down list, select **Ping Test**.
- 6. From the **Destination Type** drop-down list, select one of the following:
 - **Hostname/IP Address**—Enter the hostname or IP address.
 - **Client**—Select a client.
- 7. Select the SSID from the **SSID** drop-down list, if the selected device is running on version 10.3 or above.



-
- The **SSID** drop-down list is not available if the selected device firmware version is less than 10.3.
 - The **SSID** drop-down list is disabled if you select multiple devices in the **Source** drop-down list.
 - If you select client from the **Destination Type** drop-down list, the SSID is automatically selected based on the client.
-

8. To use additional parameters, click **Show Additional Test Settings** and enter values in the following fields:



Show Additional Test Settings is not displayed when a **Test** type is not selected.

- a. In the **Packet Size** field, enter the packet size in order to capture and store the data packet to analyze network issues at a later stage. The range is from 10 to 65507 bytes.
- b. In the **Count** field, enter the count. The value should be between 1 to 2147483647.
- c. Select **Port** from the **Source Interface** drop-down list and select the port number.



-
- If SSID is selected the packet size range changes to 10 to 2000 and the count range changes to 1 to 100.
 - The **Source Interface** drop-down list is not displayed when SSID is selected.
-

9. Click **Run**.

The output is displayed in the **Device Output** section.

Traceroute

Tracks the packets routed from a network host.

To perform a traceroute test on APs, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Group, Label, or Site**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
 - To select a device in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices > Access Points**.
A list of access points is displayed in the **List** view.
 - c. Click an access point listed under **Device Name** for which you want to perform diagnostic test.
The dashboard context for the access point is displayed.
2. Under **Analyze > Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **Traceroute**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
6. Enter the hostname or IP address.
7. Click **Run**.
The output is displayed in the **Device Output** section.

HTTP Test

Sends packets to the HTTP URL and tries to establish a connection and exchange data. If the HTTP website returns a response, it indicates that the web server is up and reachable. If the HTTP website does not return a response, it indicates that the server is down and did not return a response.

To perform an HTTP test on APs, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Group, Label, or Site**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
 - To select a device in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices > Access Points**.
A list of access points is displayed in the **List** view.
 - c. Click an access point listed under **Device Name** for which you want to perform diagnostic test.
The dashboard context for the access point is displayed.
2. Under **Analyze > Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **HTTP Test**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
6. Enter the HTTP URL for which you want to perform the HTTP test, in the **URL** field, For example, `http://hostname` or `http://ipaddress`.
7. To use additional parameters, click **Show Additional Test Settings**, and in the **Timeout** field, enter the timeout value in seconds.
The value should be from 1 to 10 seconds. The default timeout value is 1 second.



Show Additional Test Settings is not displayed when a **Test** type is not selected.

8. Click **Run**.

The test output is displayed in the **Device Output** section.

Important Points to Note

- HTTP test is supported only for APs residing on AOS version 8.3.0.0 or above.
- The test supports only IPv4 address or domain name in the **URL** field.

HTTPS Test

Sends packets to the HTTPS URL and tries to establish a connection and exchange data. If the HTTPS website returns a response, it indicates that the web server is up and reachable. If the HTTPS website does not return a response, it indicates that the server is down and did not return a response.

To perform an HTTPS URL test on APs, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Group, Label, or Site**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
 - To select a device in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices > Access Points**.
A list of access points is displayed in the **List** view.
 - c. Click an access point listed under **Device Name** for which you want to perform diagnostic test.
The dashboard context for the access point is displayed.
2. Under **Analyze > Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **HTTPS Test**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
6. Enter the HTTPS URL for which you want to perform the HTTPS test, in the **URL** field, For example, `https://URL` or `https://IPv4`.
7. To use additional parameters, click **Show Additional Test Settings** and in the **Timeout** field, enter the timeout value in seconds. The value should be from 1 to 10 seconds. The default timeout value is 1 second.



Show Additional Test Settings is not displayed when a **Test** type is not selected.

8. Click **Run**.

The test output is displayed in the **Device Output** section.

Important Points to Note

- HTTPS test is supported only for APs residing on AOS version 8.4.0.0 or above.
- The test supports only IPv4 address or domain name in the **URL** field.

TCP Test

Sends packets to the host, for example, FTP server, and tries to establish a connection and exchange data. If the FTP server returns a response, the issue could be isolated to the client device.

To perform a TCP test on APs, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Group, Label, or Site**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
 - To select a device in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices > Access Points**.
A list of access points is displayed in the **List** view.
 - c. Click an access point listed under **Device Name** for which you want to perform diagnostic test.
The dashboard context for the access point is displayed.
2. Under **Analyze > Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **TCP Test**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
6. Enter a valid IPv4 address in the **Host** field. Hostname is not supported.
7. Enter the port number., in the **Port** field. The port number should be between 1 to 65535.
8. To use additional parameters, click **Show Additional Test Settings**, and in the **Timeout** field, enter the timeout value in seconds. The value should be from 1 to 10 seconds. The default timeout value is 5 seconds.



Show Additional Test Settings is not displayed when a **Test** type is not selected.

9. Click **Run**.
The output is displayed in the **Device Output** section.

Important Point to Note

- TCP test is supported only for APs residing on AOS version 8.3.0.0 or above.

Speed Test (iPerf)

Performs a speed test to measure network speed and bandwidth. To perform a speed test, you must provide the iPerf server address, protocol type, and speed test options such as bandwidth.

To execute a speed test on APs, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Group, Label, or Site**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.

- To select a device in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices > Access Points**.
A list of access points is displayed in the **List** view.
 - c. Click an access point listed under **Device Name** for which you want to perform diagnostic test.
The dashboard context for the access point is displayed.

2. Under **Analyze > Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **Speed Test (iPerf)**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.



While performing troubleshooting on APs, a maximum of 20 APs are listed in the drop-down list. If there are more than 20 APs, use the **Search** option to search for an AP on which you would like to perform diagnostic checks.

If you navigate from the device details page, the **Tools** page appears, where the device context is already set and the **Source** field is automatically populated based on your selection.

6. In the **Host** field, enter a valid hostname.
7. From the **Protocol** drop-down list, select the protocol. The available options are **TCP** or **UDP**.
8. To use additional parameters, click **Show Additional Test Settings**, and in the **Options** field, enter an option. For example, bandwidth.



Show Additional Test Settings is not displayed when a **Test** type is not selected.

9. Click **Run**.
The test output is displayed in the **Device Output** section.



For Campus AP only **Speed Test** is available to diagnose the connectivity issues.

For information about viewing and downloading the output, see [Viewing the Device Output](#).

Troubleshooting CAP Connectivity Issues

To diagnose issues pertaining to network connections for Campus Access Points, you can use **Speed Test**.

Speed Test

Performs a speed test to measure network speed and bandwidth. To perform a speed test, you must provide the iPerf server address, protocol type, and speed test options such as bandwidth.

To execute a speed test on CAPs, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Group, Label, or Site**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.

- To select a device in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices > Access Points**.
A list of access points is displayed in the **List** view.
 - c. Click an access point listed under **Device Name** for which you want to perform diagnostic test.

The dashboard context for the access point is displayed.

2. Under **Analyze > Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **Speed Test**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.

While performing troubleshooting on APs, a maximum of 20 APs are listed in the drop-down list. If there are more than 20 APs, use the **Search** option to search for an AP on which you would like to perform diagnostic checks.



NOTE

If you navigate from the device details page, the **Tools** page appears, where the device context is already set and the **Source** field is automatically populated based on your selection.

6. In the **Host** field, enter a valid hostname.
7. From the **Protocol** drop-down list, select the protocol. The available options are **TCP** or **UDP**.
8. To use additional parameters, click **Show Additional Test Settings**, and in the **Options** field, enter an option. For example, bandwidth.



NOTE

Show Additional Test Settings is not displayed when a **Test** type is not selected.

9. Click **Run**.

The test output is displayed in the **Device Output** section.



NOTE

For Campus AP only **Speed Test** is available to diagnose the connectivity issues.

For information about viewing and downloading the output, see [Viewing the Device Output](#).

Troubleshooting Switch Connectivity Issues

The following tests are available to diagnose issues related to wired network connections:

Ping Test

Sends ICMP echo packets to the IP address of the selected switch to check for latency issues.

To perform a ping test on switches, complete the following procedure:

1. In the **Network Operations** app, select one of the following options:
 - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.

- To select a switch in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name** for which you want to perform diagnostic test.
The dashboard context for the switch is displayed.
- 2. Under **Analyze > Tools**, click **Network Check**.
- 3. From the **Device Type** drop-down, select **Switch**.
- 4. From the **Test** drop-down, select **Ping Test**.
- 5. From the **Sources** drop-down, select source(s). You can select multiple switches.



You can select Aruba Switch or Mobility Access Switch from the **Sources** drop-down.

- 6. From the **Destination Type** drop-down, select one of the following:
 - **Hostname/IP Address**—Enter the hostname or IP address in the **Hostname/IP Address** field.
 - **Client**—Select a client from the **Client** drop-down.
- 7. To use additional parameters, click **Show Additional Test Settings** and enter values in the following fields:



Show Additional Test Settings is not displayed when a **Test** type is not selected.

- In the **Repetitions** field, enter the repetition value. The value should be between 1 to 500.
- In the **Data Size** field, enter the data size. The value should be between 0 to 65399.



Mobility Access Switches do not support repetition and data size.

- 8. Select the **Use Management Interface** option if you want to use VRF Management interface. To use VRF Default interface, clear this option, which is the default.



Use Management Interface option is available only for AOS-CX switches.

- 9. Click **Run**.
The test output is displayed in the **Device Output** section.

For information about viewing and downloading the output, see [Viewing the Device Output](#).



If you navigate from the device details page, the **Tools** page appears, where the device context is already set and the **Source** field is automatically populated based on your selection.

Troubleshooting Controller Connectivity Issues

The following tests are available to diagnose issues pertaining to controller network connections:

Ping Test

Sends ICMP echo packets to the IP addresses of the selected devices to check for latency issues.

To perform a ping test on Controllers, complete the following procedure:

1. In the **Network Operations** app, select one of the following options:
 - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
 - To select a device in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices > Controllers**.
A list of controllers is displayed in the **List** view.
 - c. Click a controller listed under **Device Name** for which you want to perform diagnostic test.
The dashboard context for the controller is displayed.
2. Under **Analyze > Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Controller**.
4. From the **Test** drop-down list, select **Ping Test**.
5. From the **Sources** drop-down list, select source(s). You can select multiple Controllers.
6. From the **Destination Type** drop-down list, select one of the following:
 - **Hostname/IP Address**—Enter the hostname or IP address.
 - **Client**—Select a client.
 - **VPNC**—Select the VPN Concentrator.
7. To use additional parameters, click **Show Additional Test Settings** and enter values in the following fields:



Show Additional Test Settings is not displayed when a **Test** type is not selected.

- a. In the **Packet Size** field, enter the packet size to capture and store the data packet to analyze network issues at a later stage. The range is from 10 to 2000 bytes.
 - b. In the **Count** field, enter the count. The value should be between 1 to 1000.
 - c. In the **Time to Live** field, enter the time range. The value should be between 1 to 225 seconds.
 - d. In the **DSCP** field, enter the packet header value. The value should be between 0 to 63.
 - e. From the **Source Interface** drop-down list, select one of the following:
 - **Loopback**—Select loopback to verify if ping functionality is working when the source address is set as logical address. It is a logical interface.
 - **Management Interface**—Select management interface to verify if ping functionality is working when the source address is set as management interface. It is a physical interface which is dedicated to configuration and management operation in the network.
 - **VLAN Interface**—Select VLAN interface to verify if ping functionality is working when the source address is set as VLAN interface. It is a virtual LAN used to avoid broadcast domain in a switch or controller.
 - f. Optionally, you can select the **Don't Fragment** toggle button. This option is used when the packet size is more than the Maximum Transmission Unit (MTU) size of the interface.
8. Click **Run**.
The output is displayed in the **Device Output** section.

Traceroute

Tracks the packets routed from a network host.

To perform a traceroute test on Controllers, complete the following procedure:

1. In the **Network Operations** app, select one of the following options:
 - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Group, Label, or Site**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
 - To select a device in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices > Controllers**.
A list of s is displayed in the **List** view.
 - c. Click a controller listed under **Device Name** for which you want to perform diagnostic test.
The dashboard context for the controller is displayed.
2. Under **Analyze > Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Controller**.
4. From the **Test** drop-down list, select **Traceroute**.
5. From the **Sources** drop-down list, select source(s). You can select multiple Controllers.
6. Enter the hostname or IP address.
7. To use additional parameters, click **Show Additional Test Settings**, and from the **Source Interface** drop-down list, select **VLAN Interface**.
8. From the **VLAN Interface** drop-down list, select the required VLAN ID displayed along with the IP address.
9. Click **Run**.
The output is displayed in the **Device Output** section.



If you navigate from the device details page, the **Tools** page appears, where the device context is already set and the **Source** field is automatically populated based on your selection.

Speed Test (iPerf)

Performs a speed test to measure network speed and bandwidth. To perform a speed test, you must provide the iPerf server address, protocol type, and speed test options such as bandwidth.

To execute a speed test on Controllers, complete the following procedure:

1. In the **Network Operations** app, select one of the following options:
 - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Group, Label, or Site**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
 - To select a device in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices > Controllers**.
A list of access points is displayed in the **List** view.
 - c. Click an access point listed under **Device Name** for which you want to perform diagnostic test.
The dashboard context for the access point is displayed.
2. Under **Analyze > Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Controller**.

4. From the **Test** drop-down list, select **Speed Test (iPerf)**.
5. From the **Sources** drop-down list, select source(s). You can select multiple Controllers.
6. In the **Host** field, enter a valid hostname or IP address.
7. To use additional parameters, click **Show Additional Test Settings** and enter values in the following fields:



Show Additional Test Settings is not displayed when a **Test** type is not selected.

- a. **Port**—Select the port.
 - b. **VLAN Interface**—Select the VLAN ID from the drop-down list.
8. Click **Run**.

The test output is displayed in the **Device Output** section.

For more information about viewing and downloading the output, see [Viewing the Device Output](#).

Viewing the Device Output

After you execute troubleshooting commands on the devices, Aruba Central displays the output in the **Device Output** section of the **Tools** page.

The output pane displays a list of devices on which the troubleshooting commands were executed, the test type, initial timestamp, source, and target. It also shows the status of the tests as, in progress, complete, and the buffer time. If there are multiple devices, select the device for which you want to view the output.



Output history of device with buffer space issues shall be automatically cleared.

You can perform the following tasks from the **Device Output** section:

- Click **Clear** to clear the output. You can clear the output for a single device or for all devices. The **Clear** option is disabled for read-only users.
- Click the search icon to search for text in the output.
- Click the email icon and click **Send** to send the output as an email. You can also add email recipients in the **CC** field.
- Click the download icon to export the command output as a zip file.
- Click the maximize icon to maximize the device output pane.

For more information on the output displayed for the CLI commands, see the following documents:

- *Aruba Instant CLI Reference Guide* for Instant AP CLI command output
- *HPE ArubaOS-Switch Management and Configuration Guide* for Aruba Switch CLI command output
- *ArubaOS CLI Reference Guide* for SD-WAN Gateway CLI command output

Troubleshooting Device Issues

Device check aims to identify, diagnose, and debug issues on your device. The **Device Check** tab in the **Tools** page can be used to perform troubleshooting check for Aruba Switches only. When a troubleshooting operation is initiated, Aruba Central establishes a session with the Switch selected for the troubleshooting operation and displays the output in the **Device Output** section.

To perform a device check on a switch, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
 - To select a device in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. A list of devices is displayed in the **List** view.
 - d. Click a switch listed under **Device Name** for which you want to perform diagnostic test.
The dashboard context for the switch is displayed.
2. Under **Analyze**, click **Tools**. The **Tools** page opens.
3. Click the **Device Check** tab.



-
- By default, the **Device Type** is set to **Switch** if a switch is configured in the data path, else a warning is displayed.
 - Multiple device selection is not allowed at this level.
 - Devices which are already running commands shall not execute newly added commands.
-

4. From the **Switch** drop-down list, select the switch.
5. Select one of the following tests to perform diagnostic checks on the selected switch:
 - **Cable Test**—Enables testing of the electrical connections in the switch cable. It checks whether the cabling is conformed to the cabling plans and is of expected quantity. It is useful for production and maintenance.



-
- Cable Test is supported in a AOS-Switch only from version 16.05.000 or above.
 - Cable Test is not supported in AOS-CX switch.
-
- **Interface Bounce**—Restarts the port interface and forces a client to re-initiate a DHCP request. This option is available only for Aruba Switches.
 - **PoE Bounce**—Restarts the PoE port and the device that is either connected to the PoE port or powered by it. This option is available only for Aruba Switches.



-
- If you select **Cable Test**, **PoE Bounce**, or **Interface Bounce**, you must enter the port number or the port number range as mentioned in the example text.
 - If you navigate to the **Tools** page from the **Clients** page, under **Device Check** the client context is already set and the port number is auto filled based on the client selected.
-

- **Chassis Locate**—Activates the Switch locator LED. The locator LED indicates the physical location where an Aruba Switch is currently installed.

6. Click **Run**.

The output is displayed in the **Device Output** section.

Important Points to Note

- Interface Bounce, PoE Bounce, and Chassis Locate tests are supported only from the following versions in switches:
- AOS-Switch: See [Supported AOS-Switch Platforms](#).
- AOS-CX: See [Supported AOS-CX Switch Platforms](#).

Viewing the Device Output

After you execute troubleshooting commands on the devices, Aruba Central displays the output in the **Device Output** section of the **Tools** page.

The output pane displays a list of devices on which the troubleshooting commands were executed, the test type, initial timestamp, source, and argument. It also shows the status of the tests as, in progress, complete, and the buffer time.



Output history of device with buffer space issues shall be automatically cleared.

You can perform the following tasks from the **Device Output** section:

- Click **Clear** to clear the output. You can clear the output for a single device or for all devices. The **Clear** option is disabled for read-only users.
- Click the search icon to search for text in the output.
- Click the email icon and click **Send** to send the output as an email. You can also add email recipients in the **CC** field.
- Click the export to export the command output as a zip file.
- Click the maximize icon to maximize the device output pane.

Unlike the other tests, for Cable Test, the output is displayed in a tabular format, and you cannot download, email, or export the output.

For more information on the output displayed for the CLI commands, see the following documents:

- *Aruba Instant CLI Reference Guide* for Instant AP CLI command output
- *HPE ArubaOS-Switch Management and Configuration Guide* for Aruba Switch CLI command output

Advanced Device Troubleshooting

Advanced device check aims to identify, diagnose, and debug issues on your device at an advanced level using commands. The **Commands** tab on the **Tools** page lists commands specific to a particular device to test the device entity and collect results based on your selection. When a troubleshooting operation is initiated, Aruba Central establishes a session with the devices selected for the troubleshooting operation and displays the output in the **Device Output** section.



For detailed information about the commands, see [The CLI Bank](#). Use the search feature to locate the required CLI. A command name can be same between the products, so ensure to choose your command based on the native product or feature. For example, [ArubaOS](#) or [Aruba Instant](#).

To perform advanced troubleshooting on devices, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
 - To select a device in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices**, and then click **Access Points, Switches, or Controllers**.
A list of devices is displayed in the **List** view.
 - c. Click a device listed under **Device Name**.
The dashboard context for the device is displayed.
2. Under **Analyze > Tools**, click the **Commands** tab.
The **Commands** page is displayed.
3. Select a device. Network administrators can perform advanced troubleshooting on the following types of devices managed by Aruba Central:
 - [Troubleshooting Access Points](#)
 - [Troubleshooting Switches](#)
 - [Troubleshooting Controllers](#)



Devices which are already running shall not execute newly added commands.

Troubleshooting Access Points

To troubleshoot APs at an advanced level, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.

- To select a device in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices > Access Points**.
A list of access points is displayed in the **List** view.
 - c. Click an access point listed under **Device Name** for which you want to perform diagnostic test.

The dashboard context for the access point is displayed.

2. Under **Analyze > Tools**, click **Commands**.
3. In the **Commands** tab, select the device type as **Access Point**.
4. From the **Available Devices** drop-down list, select the AP. You can select multiple APs.
5. Select any command category and the **Commands** pane displays the associated commands.
6. Click **Add>** to add the selected commands to the **Selected Commands** pane.
7. If you have selected a command marked with either '*' or '+', enter the filtration parameters as displayed in the **Additional Filters** dialog box. For more information on filtering commands, see [Filtering Commands](#).
8. (Optional) Select command(s) and click **<Remove** to remove selected command(s) or click **<Remove All** to clear the **Selected Commands** pane.
9. (Optional) To set a frequency for automatically executing the troubleshooting commands, complete the following steps:
 - a. Click the **Repeat** checkbox.
 - b. Specify an interval for executing the troubleshooting commands. You can also specify how frequently the commands must be executed during a given interval.
 - c. Click **Reset** to modify the values in all the fields, and **Cancel All** for canceling all the repeats. Click the stop icon to stop a particular repeat.
10. Click **Run**.

The output is displayed in the **Device Output** section.

For information about viewing and downloading the output, see [Viewing the Device Output](#).



-
- To perform advanced troubleshooting on APs, the minimum software version required on Instant APs is 6.4.3.1-4.2.0.3.
 - If you navigate from the device details page, the **Tools** page appears, where the device context is already set and the **Source** field is automatically populated based on your selection.
-

Troubleshooting Switches

To troubleshoot switches at an advanced level, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.

- To select a switch in the filter, complete the following steps:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch under **Device Name** for which you want to run a diagnostic test.
The dashboard context for the switch is displayed.
- 2. Under **Analyze > Tools**, click **Commands**.
The **Commands** page is displayed.
- 3. From the **Device Type** drop-down, select **Switch**.
- 4. From the **Available Devices** drop-down, select the switch. You can select multiple switches.
- 5. Select any command category in the **Categories** pane and the **Commands** pane displays the associated commands.



Aruba CX switches support only the `show tech` and `show running-config` commands.

6. Click **Add >** to add the selected commands to the **Selected Commands** pane.
7. If you have selected a command marked with either '*' or '+', enter the filtration parameters as displayed in the **Additional Filters** dialog box. For more information on filtering commands, see [Filtering Commands](#).
8. (Optional) Select command(s) and click **< Remove** to remove selected command(s) or click **< Remove All** to clear the **Selected Commands** pane.
9. (Optional) To set a frequency for automatically executing the troubleshooting commands, complete the following steps:
 - a. Click the **Repeat** checkbox.
 - b. Specify an interval for executing the troubleshooting commands. You can also specify how frequently the commands must be executed during a given interval.
 - c. Click **Reset** to modify the values in all the fields, and **Cancel All** for canceling all the repeats. Click the stop icon to stop a particular repeat.
10. Click **Run**.
The output is displayed in the **Device Output** section.

For information about viewing and downloading the output, see [Viewing the Device Output](#).

Troubleshooting Controllers

To troubleshoot Controllers at an advanced level, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
 - To select a device in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices > Controllers**.
A list of controllers is displayed in the **List** view.

- c. Click a controller listed under **Device Name** for which you want to perform diagnostic test.
The dashboard context for the controller is displayed.
2. Under **Analyze > Tools**, click **Commands**.
3. In the **Commands** tab, select the device type as **Controller**.
4. From the **Available Devices** drop-down list, select the controller. You can select multiple controllers.
5. Select any command category and the **Commands** pane displays the associated commands.
6. Click **Add>** to add the selected commands to the **Selected Commands** pane.
7. If you have selected a command marked with either '*' or '+', enter the filtration parameters as displayed in the **Additional Filters** dialog box. For more information on filtering commands, see [Filtering Commands](#).
8. (Optional) Select command(s) and click **<Remove** to remove selected command(s) or click **<Remove All** to clear the **Selected Commands** pane.
9. (Optional) To set a frequency for automatically executing the troubleshooting commands:
 - a. Click the **Repeat** checkbox.
 - b. Specify an interval for executing the troubleshooting commands. You can also specify how frequently the commands must be executed during a given interval.
 - c. Click **Reset** to modify the values in all the fields, and **Cancel All** for canceling all the repeats. Click the stop icon to stop a particular repeat.
10. Click **Run**.
The output is displayed in the **Device Output** section.

For information about viewing and downloading the output, see [Viewing the Device Output](#).

Viewing the Device Output

After you execute troubleshooting commands on the devices, Aruba Central displays the output in the **Device Output** section of the **Tools** page.

If there are multiple devices, select the device for which you want to view the output. It shows the status of the tests as, in progress, complete, and the buffer time.



Output history of device with buffer space issues shall be automatically cleared.

You can perform the following tasks from the **Device Output** section:

- Click **Clear** to clear the output. You can clear the output for a single device or for all devices. The **Clear** option is disabled for read-only users.
- Click the search icon to search for text in the output.
- Click the email icon and click **Send** to send the output as an email. You can also add email recipients in the **CC** field.
- Click the download icon to export the command output as a zip file.
- Click the maximize icon to maximize the device output pane.

For more information on the output displayed for the CLI commands, see the following documents:

- *Aruba Instant CLI Reference Guide* for Instant AP CLI command output
- *HPE ArubaOS-Switch Management and Configuration Guide* for Aruba Switch CLI command output
- *ArubaOS CLI Reference Guide* for SD-WAN Gateway CLI command output

Filtering Commands

In order to streamline the debug process and avoid huge data generation while troubleshooting, few commands enable Client MAC address, IP Address, and Port filtration.

To filter commands, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
 - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
 - To select a device in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices**, and then click **Access Points, Switches, or Controllers**.
A list of devices is displayed in the **List** view.
 - c. Click a device listed under **Device Name**.
The dashboard context for the device is displayed.
2. Under **Analyze > Tools**, click **Commands**.
The **Commands** page is displayed.
3. Select the device type, **Access Point, Switch, or Controller** as required from the drop-down list.
4. Select any command category and the **Commands** pane displays the associated commands.



If you navigate from the device details page, the **Tools** page appears, where the device context is already set and the **Source** field is automatically populated based on your selection.

Mandatory filters—Commands marked with '*'

To filter commands based on mandatory filters, complete the following steps:

1. Select a command marked with '*' and click **Add**.
The **Additional Filters** dialog box appears.
2. Enter the parameters such as, Client MAC address, IP address, port number, port list, or policy name as required.
The parameters are generated based on the commands selected.
3. Click **Apply**.



In case of mandatory filter commands, if you do not enter the filtering parameters in the additional filters dialog box, the command does not get added to the selected command pane and you cannot perform the troubleshooting.

4. (Optional) Click **Edit All** to reset the filtration parameters for all the commands added in the selected command pane.

Optional filters— Commands marked with '+'

To filter commands based on optional filters, complete the following steps:

1. Select a command marked with '+' and click **Add**.
The **Additional Filters** dialog box appears.
2. (Optional) Enter the parameters such as, Client MAC address, IP address, port number, port list, or policy name as required.
The parameters are generated based on the commands selected.
3. Click **Apply**.



In case of optional filter commands, if you do not enter the filtering parameters in the additional filters dialog box, the command still gets added to the selected command pane and you can perform your troubleshooting.

4. (Optional) Click **Edit All** to reset the filtration parameters for all the commands added in the selected command pane.

Troubleshooting System Issues

To monitor the performance of the Aruba Central appliance, use the Grafana dashboard. This provides useful metrics on CPU, Memory and IO usage of the Aruba Central node. It also provides cluster wide information in case of an Aruba Central cluster.

To access Grafana dashboard from a web browser, go to <https://<hostname or IP address>/grafana>

Use the following default credentials to access the Grafana dashboard:

- Username—**grafana**
- Password—**grafana#21**

In order to debug Aruba Central logs, use the Kibana dashboard.

To access Kibana dashboard from a web browser, go to <https://<hostname or IP address>/airwavelogging>

Use the following default credentials to access the Kibana dashboard:

- Username—**grafana**
- Password—**grafana#21**

Enter the following index pattern to access the Aruba Central logs:

```
<IP Address>-coplogs-<category>-<year>.<month>.<data>.<hour>
```

Collecting Logs

To collect logs generated for the Aruba Central, complete the following steps:

1. Log in to Aruba Central.
2. The setup shows a list of 9 commands that can be used to perform different tasks.
3. In order to collect Aruba Central logs, run the following commands:

```
Support  
Collect All Logs
```

The script generates a *tar.gz* file that you can share with the Aruba support team for debugging issues.

The following archive (*tar.gz* file) contains all the log information required for troubleshooting issues:

```
/home/core/log_collection/aw10-setup91.arubathena.com_log_collection_2019-08-07_05-29-15_UTC.tar.gz
```

Creating Log Snapshot

You can now collect log snapshots of specific categories. To create log snapshots for the Aruba Central, complete the following steps:

1. Log in to Aruba Central.
2. The setup shows a list of 10 commands that can be used to perform different tasks.
3. To create Aruba Central log snapshot, run the following commands:

```
Support
Log Snapshot Operations
Generate Snapshots for a Category
```

The script captures logs for the following pods:

- kube
- nginx
- alert
- infra
- syslog
- system

Downloading Log Snapshot

After creating the snapshot, it is saved as a file and to download the snapshot file, complete the following steps:

1. Log in to Aruba Central.
2. The setup shows a list of 10 commands that can be used to perform different tasks.
3. To download Aruba Central log snapshots, run the following commands:

```
Support
Log Snapshot Operations
Download Logs/Snapshots
```

The list of available snapshots and their status is displayed.

1. Enter the snapshot name to download. For example, *upgrade-snap-<time range>-<create time>*.
2. Enter the remote host and path name.

Creating Pod Logs

To create pod logs, complete the following steps:

1. Log in to Aruba Central.
2. The setup shows a list of 10 commands that can be used to perform different tasks.
3. To generate Aruba Central pod logs, run the following commands:

```
Support
Log Snapshot Operations
Generate Pod Logs
```

4. Enter a pod name to generate logs.

Deleting Log Snapshot

To delete a log snapshot, complete the following steps:

1. Log in to Aruba Central.
2. The setup shows a list of 10 commands that can be used to perform different tasks.
3. In order to delete Aruba Central log snapshots run the following commands:

```
Support
Log Snapshot Operations
Delete Logs/Snapshots
```

4. Select the snapshot name that you want to delete.

Downloading Upgrade Logs

Aruba Central (on-premises) allows you to view and download logs related to the events that occurred during the upgrade process.

1. Go to the **Account Home** page.
2. Under **Global Settings**, click **System Management > Version** tab.
3. Click **Generate Logs** in the Logs pane.

Once generated, the logs can be viewed from the logs table. The **Logs** table displays the following information and also allows you to download or delete logs:

- **File**— Displays the generated file name.
- **Created**— Displays the date and time of the log creation.
- **Status**— Displays the status of the generated logs.
- **Action**— Allows you to do the following actions:
 - **Download**— Select the file and click the  icon to download the generated file.
 - **Delete**— Select the file that you want to delete and click the delete icon. In the **Confirm Action** pop-up window, click **Yes**.

The growing use of Wi-Fi and the proliferation of mobile, tablet, portable, and smart devices and clients cause control and visibility challenges for communication and collaboration applications such as Lync or Skype for Business. To overcome these challenges, Aruba offers the Unified Communications service to manage your enterprise communication ecosystem.

The Unified Communications service provides a seamless user experience for voice and video calls and application sharing when using Lync or Skype for Business applications. The service actively monitors and provides visibility into Lync or Skype for Business traffic and allows you to prioritize sessions. The Unified Communications service leverages the functions of the service engine and provides rich visual metrics for analytical purposes.



NOTE

UCC is not supported on Instant APs.

The Unified Communications service supports the following functions based on the type of device:

- Session prioritization—Based on the type of device provisioned in your network, the Unified Communication service receives call control information from APs, switches, and controllers. The Unified Communications service uses this data to detect and classify the traffic type and dynamically prioritize voice and video call traffic over data traffic. Based on the type of device, the following information sources are used for session prioritization.
 - The Lync or Skype for Business SDN API—The SDN API provides an interface for the Aruba devices to access diagnostic information for a comprehensive and a real-time view of applications, users, devices, the Wi-Fi, and the LAN network infrastructure. The Unified Communications service uses this data to prioritize voice and video traffic. The SDN API can be installed on a Lync or Skype for Business server.
 - Heuristics—A built-in method that detects the Lync or Skype for Business traffic and works with all on-premises and Skype for Business online deployments. The heuristics data detection and classification method is used to identify clients in the call, classify, and prioritize media packets. Switches do not support heuristics-based prioritization. The session prioritization for switches is based on the data from the Skype server through OpenFlow.
- Session visibility—The application also provides call session visibility correlated across the Skype server and mobility network to simplify operations for the network administrator. The administrators can monitor wireless and wired network connectivity health on a per-session basis and analyze the quality of experience.

Licensing

Multi-tier licensing is applicable to Unified Communications applications. A foundation license provides heuristics-based prioritization of the media traffic without visibility. An advanced license provides session prioritization with visibility.

See the following sections for information about configuring and monitoring UCC:

- [Configuring UCC](#)
- [Monitoring UCC in List View](#)
- [Monitoring UCC in Summary View](#)

Configuring UCC

The following topics are discussed in this section:

- [Enabling Unified Communications](#)
 - [Enabling Retain Client QoS](#)
 - [Editing a Protocol](#)
- [Configuring Devices for Session Prioritization](#)
 - [OpenFlow Configuration](#)
- [SDN API-Based Classification](#)
 - [Configuring SDN Manager for SDN API](#)
 - [HTTPS Connectivity with SDN Manager](#)
- [Heuristics Classification](#)
 - [Configuring ACLs on Controllers for Media Classification](#)
 - [Configuring UCC](#)
 - [Creating a Management Server Profile on Controller](#)
 - [Configuring Devices for Session Visibility](#)

Enabling Unified Communications

To access the Unified Communications application, obtain a valid subscription. To obtain a subscription for the **Unified Communications** application, contact the Aruba Central Sales team.



UCC is available for 8.x version or later IAPs and APs that run on foundation license.

To enable Unified Communications, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage**, click **Applications > UCC**.
3. Click the **Config** icon.
The **Settings** page is displayed.
4. Move the **Activate UCC** slider to the right.
The Unified Communications is enabled.

Enabling Retain Client QoS

When retain client QoS is enabled, all configured ALGs are disabled, all traffic is treated as Real-Time Transport Protocol (RTP) traffic, default prioritization defined by the client is honored, and call visibility is provided.

To enable retain client QoS, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage**, click **Applications > UCC**.
3. Click the **Config** icon.
The **Settings** page is displayed.
4. Move the **Retain Client QoS** slider to the right.

Editing a Protocol

To edit a protocol, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage**, click **Applications > UCC**.
3. Click the **Config** icon.
The **Settings** page is displayed with the **Protocols** table.
4. In the **Protocols** table, hover over the required protocol and click the  icon in the **Action** column.
Unified Communications supports SIP, Skype for Business, and Wi-Fi Calling protocols.
5. Edit the parameters listed in [Protocol Parameters](#).

Table 228: *Protocol Parameters*

Parameter	Description
Voice	Configure voice priority tag.
Video	Configure video priority tag.
DNS Pattern	Configure the carrier for Wi-Fi calling.

6. Click **Save Settings**.

Adding Carriers to Wi-Fi Calling Protocol

To add carriers to the Wi-Fi Calling protocol, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage**, click **Applications > UCC**.
3. Click the **Config** icon.
4. Hover over the **Wi-Fi Calling** protocol and click the  icon in the **Action** column.
The **Edit Wi-Fi Calling** page is displayed.
5. Click **Show Advanced Setting**.
The **DNS Pattern** table displays the default carriers list.
6. Click **+** to add a new carrier.
The **DNS Pattern** window is displayed.
7. Specify **Carrier Name** and **DNS Pattern**.
8. Click **Save**.
The new carrier name is displayed in the **DNS Pattern** table.

Configuring Devices for Session Prioritization

Based on the ArubaOS software version, controllers support session prioritization using both SDN API and heuristics as the source for information. If both methods are enabled, the SDN API-based Skype for Business classification takes precedence.

OpenFlow Configuration

For both SDN API and heuristics-based classification and prioritization, OpenFlow configuration is required.

- In the SDN API-based Skype for Business classification method, the Unified Communications application receives the media identification data from the SDN Manager and call quality report from the devices through OpenFlow.
- In heuristics-based media classification method, the Unified Communications application receives media identification and the call quality reports from the devices through OpenFlow.

Enabling OpenFlow on Controller

To enable the OpenFlow on controller, issue the following commands in the CLI:

```
(host)# configure terminal
(host) (config)# openflow-profile
(host) (openflow-profile)# controller-ip <controller-ip> 30633
(host) (openflow-profile)# bind-vlan 1
(host) (openflow-profile)# bind-vlan add <range of vlan-ids>
(host) (openflow-profile)# openflow-enable
(host) (openflow-profile)# write memory
(host) (openflow-profile)# exit
```

To enable OpenFlow in the user-role and virtual AP of a controller, issue the following commands in the CLI:

```
(host) (config) # user-role <user-role>
(host) (config-submode) # openflow-enable
(host) (config-submode) # exit
(host) (config) #wlan virtual-ap <virtual-ap>
(host) (Virtual AP profile "<virtual-ap>") #openflow-enable
(host) (Virtual AP profile "<virtual-ap>") #write memory
```

Enable OpenFlow on Switch

To enable OpenFlow on switch:

1. To configure OpenFlow on switch, issue the following commands in the CLI:

```
(host)# configure terminal
(host) (config)# openflow
(host) (openflow)# controller-id <number> ip <ip-addr-of-OFC> port <OFC-TCP-
port> controller-interface vlan <vlan-id-used-to-connect-to-OFC>
(host) (openflow)# write memory
(host) (openflow)# exit
```

2. To configure OpenFlow instance on switch, issue the following commands in the CLI:

```
(host)# configure terminal
(host)(config)# openflow
(host)(openflow)# instance <instance-name>
(host)(openflow)# member vlan <vlan-id-of-the-member>
(host)(openflow)# controller-id <same as the number given for controller-id
in the OFC details>
(host)(openflow)# version 1.3
(host)(openflow)# pipeline-model standard-match
(host)(openflow)# exit
```

3. To enable OpenFlow and OpenFlow instance on switch, issue the following commands in the CLI:

```
(host)(config)# configure terminal
(host)(config)# openflow instance <instance-name> enable
(host)(config)# openflow enable
(host)(config)# exit
```



Aruba switches support only the SDN API source for session prioritization.

Enabling OpenFlow on AP

If the Unified Communications subscription is enabled on the APs, OpenFlow is automatically enabled on the APs. Therefore, no explicit configuration from the user is required for enabling OpenFlow.

SDN API-Based Classification

For the Lync/Skype for Business SDN API to dynamically prioritize traffic at the edge of a network using OpenFlow, the OpenFlow controller and its instances must be configured on controllers and switches. For information on configuring OpenFlow instances, see [OpenFlow Configuration](#).

Configuring SDN Manager for SDN API

To enable Skype SDN Manager to send XML messages to the Unified Communications application, complete the following configuration:

1. Log in to the Skype SDN Manager.
2. Ensure that you have the *SDNManager.exe* program installed.
3. Open the command prompt and go to the folder in which the *SDNManager.exe* program is installed.
4. Execute the following command:

```
SDNManager.exe p s <some-string> submituri=[https://<Cluster-
IP>/skypeSDN/<customer-id>
```



Use the **GET /v1/SkypeCentralURL** API to get the Lync/Skype for Business URL for the Aruba Central cluster that you are using.

HTTPS Connectivity with SDN Manager

The customer premises with the Lync/Skype for Business SDN infrastructure must access Aruba Central through an HTTPS connection only. Aruba Central acts as a server while Lync/Skype for Business SDN Manager acts as a client.

For the client and server mutual authentication and TLS handshake, the client must have a root CA certificate provided by GeoTrust to validate the certificate presented by Aruba Central.

Heuristics Classification

In the heuristics method, APs perform deep packet inspection on the Skype for Business traffic to determine Skype for Business voice and video traffic. For the heuristics classification method, no changes or additional components are required on the Skype for Business server.

The heuristics classification method includes the following steps:

- ACL definition on the controller to listen on port TCP 5061 and 5063. The classify-media option in the ACL is enabled and is mapped to a user role.
- When the Skype for Business calls are established, classify-media in the ACL is triggered and Skype for Business clients are marked as media-capable clients.
- Any subsequent UDP data flow with source/destination port numbers above 1023 from or to media-capable users go through the Skype for Business media DPI.
- If an RTP session is based on DPI, the payload type in the RTP header is used to determine if it is a voice or video session.

Configuring ACLs on Controllers for Media Classification

If the controllers are running ArubaOS 6.5.x release version, configure the following commands to classify media:

```
host) (config) # ip access-list session <acl-name> any any tcp 5061 permit  
classify-media
```

or

```
host) (config) # user-role authenticated access-list session skype-acl
```

or

```
host) (config) # firewall allow-stun
```

For more information on configurations steps related to heuristics classification method, see the *ArubaOS User Guide*.

Creating a Management Server Profile on Controller

If the controllers are running ArubaOS 6.5.x.x or 8.x.x.x, configure the controllers to send call session data through AMON periodically. After Aruba Central receives these AMON messages, it displays the aggregated and per-client statistics on the **Unified Communications > Activity** page. This helps the administrator to assess the overall health and troubleshoot issues if any.

To configure the management server profile on controller:

1. Access the controller CLI.
2. Configure the following commands:

```
(host) (config) # mgmt-server profile <name>
(host) (Mgmt Config profile "<name>") # uccmonitoring-enable
(host) (Mgmt Config profile "<name>") # stats-enable
(host) (Mgmt Config profile "<name>") # sessions-enable
(host) (Mgmt Config profile "<name>") # monitored-info-enable
(host) (Mgmt Config profile "<name>") # monitored-info-del-enable
(host) (Mgmt Config profile "<name>") # monitored-info-snapshot-enable
(host) (Mgmt Config profile "<name>") # mgmt-server primary-server <Central-
SE-cluster-virtual IP> profile <profile-name>
(host) (Mgmt Config profile "<name>") # write memory
(host) (openflow) # exit
```

Configuring Devices for Session Visibility

If the controllers are running ArubaOS 6.5.x.x or 8.x.x.x, configure the controllers to send call session data through Application Monitoring (AMON) periodically. After Aruba Central receives these AMON messages, it displays the aggregated and per-client statistics in the UI. This helps the administrator to assess the overall health and troubleshoot issues if any.

To enable controllers to send AMON feeds about Unified Communications statistics to Aruba Central, ensure that the Aruba Central management server profile is configured on the controller.

To configure the management server profile, complete the following steps:

1. Access the controller CLI.
2. Configure the following commands:

```
(host) (config) # mgmt-server profile <name>
(host) (Mgmt Config profile "<name>") # uccmonitoring-enable
(host) (Mgmt Config profile "<name>") # write memory
(host) (openflow) # exit
```

For more information about configuration required for the Unified Communications application on the controller, see the *ArubaOS User Guide*.

Monitoring UCC in List View

The **Application > UCC** page displays graph and table view to assess the quality of calls in the network. You can view data for the **Global** level.



-
- For the Application Layer Gateway (ALG) like Skype SDN, the end-to-end Mean Opinion Score (MOS) is used. A good call has a MOS of more than 3.5, a fair call has a MOS in the range of 2.0 to 3.5, a poor call has a MOS of less than 2.0, and an unknown call does not have a MOS.
 - Wi-Fi Calling calls are not assigned an UCC RTPA score (RTP analysis) and are categorized as unknown.
-

List view

The **List** view in the **Applications > UCC** page provides a lists to assess the quality of calls in the network.

Time Filter

The  time filter allows you to set a time range to display the corresponding data on the graph. You can set the filter to any of the following time ranges:

- **3 Hours**—The graph displays the details for the past three hours.
- **1 Day**—The graph displays the details for the current day.
- **1 Week**—The graph displays the details for the current week.
- **1 Month**—The graph displays the details for the current month.

Calls List

The **Calls** list displays the following details:

Table 229: *Calls*

Parameter	Description
CDR	Displays the Call Detail Record (CDR). The value displayed in the column indicates the number of calls for the corresponding client. The  icon indicates wireless and  icon indicates wired connection type. Click the value displayed in the column to view detailed information. For more information, see Call Details .
Start Time	Displays the date and time when the call was started.
Client Name	Displays the name of the client.
Call Quality	Displays the quality of the call. You can filter the data by: <ul style="list-style-type: none">■ Good■ Fair■ Poor■ Unknown
Client Health	Displays the client health score.
SSID	Displays the SSID.
Protocol Type	Displays the type of protocol. You can filter the data by: <ul style="list-style-type: none">■ Facetime■ RTP■ SIP■ Skype for Business■ Wi-Fi Calling■ H.323■ Jabber■ Microsoft Teams■ SCCP■ WebRTC

Table 229: Calls

Parameter	Description
Session Type	Displays the type of session. You can filter the data by: <ul style="list-style-type: none"> ■ Audio ■ Desktop Sharing ■ Video
OS	Displays the operating system running on the client.
User Role	Displays the user role that initiated the call.
Call Duration	Displays the duration of the call.
Client IP Address	Displays the IP address of the client.
Peer IP Address	Displays the peer IP address of the client.
AP Host Name	Displays the host name of the AP.
AP type	Displays the type of AP.
BSSID	Displays the BSSID of the client.
DSCP	Displays the DSCP of the client.
Quality Score	Displays the quality score of the call.
Source Port	Displays the source port number.
Destination Port	Displays the destination port number.
WMM Priority	Displays the priority value for Wifi Multimedia (WMM).
Codec	Displays the Codec name.
From	Displays the device originating the call.
To	Displays the device receiving the call.

Call Details

The following image shows the Call Details window that is displayed when you click the value in the **CDR** column.

Figure 111 Call Details

CALL DETAILS X

<p>CALLER DETAILS</p> <p>FROM 99.99.99.253</p> <p>IP ADDRESS 99.99.99.253</p> <p>MAC ADDRESS e4:b3:18:08:36:35</p> <p>CLIENT e4:b3:18:08:36:35</p> <p>TO 10.15.101.162</p> <p>DESTINATION IP 10.15.101.162</p>	<p>CALL INFORMATION</p> <table border="0" style="width: 100%;"> <tr> <td>START TIME</td> <td>CDR</td> <td>DURATION</td> </tr> <tr> <td>2021 Jul 29, 04:20:44 PM</td> <td>7</td> <td>18 mins 43 secs</td> </tr> </table> <p>UCC CALL ID AP Name STATE</p> <p>-- Niket-C2c-AP315-6_70:3a:0e:c0:7e:ee TERMINATED</p> <p>CLIENT HEALTH TERMINATION REASON IN CALL ROAM</p> <p>86 % --</p> <p>APPLICATION QOS CORRECTION</p> <p>Skype For Business --</p>	START TIME	CDR	DURATION	2021 Jul 29, 04:20:44 PM	7	18 mins 43 secs	<p>CALL QUALITY</p> <p>QUALITY</p> <p>● Fair</p> <p>QUALITY SCORE</p> <p>68.40955</p>
START TIME	CDR	DURATION						
2021 Jul 29, 04:20:44 PM	7	18 mins 43 secs						

Monitoring UCC in Summary View

The **Application > UCC** page displays graph and table view to assess the quality of calls in the network. You can view data for the **Global** level.



- For the Application Layer Gateway (ALG) like Skype SDN, the end-to-end Mean Opinion Score (MOS) is used. A good call has a MOS of more than 3.5, a fair call has a MOS in the range of 2.0 to 3.5, a poor call has a MOS of less than 2.0, and an unknown call does not have a MOS.
- Wi-Fi Calling calls are not assigned an UCC RTPA score (RTP analysis) and are categorized as unknown.

Summary view

The **Summary** view in the **Applications > UCC** page provides the following information:

Time Filter

The  time filter allows you to set a time range to display the corresponding data on the graph. You can set the filter to any of the following time ranges:

- **3 Hours**—The graph displays the details for the past three hours.
- **1 Day**—The graph displays the details for the current day.
- **1 Week**—The graph displays the details for the current week.
- **1 Month**—The graph displays the details for the current month.

Summary Bar

The banner in the header pane shows the following details:

- **Calls**—Displays the total number of calls that have ended.
- **Good**—Displays the total number of good calls that have ended. A good call has an UCC RTPA score of more than 70.
- **Fair**—Displays the total number of fair calls that have ended. A fair call has an UCC RTPA score in the range of 30 to 70.
- **Poor**—Displays the total number of poor calls that have ended. A poor call has an UCC RTPA score of less than 30.
- **Unknown**—Displays the total number of calls whose status is unknown. A call is classified as unknown if the ALG does not support RTPA or the UCC score is not available.

Click any option to view the corresponding graph. For example, if you click **Good**. The graph displays only the calls that are categorized as good for the selected time range.

Calls

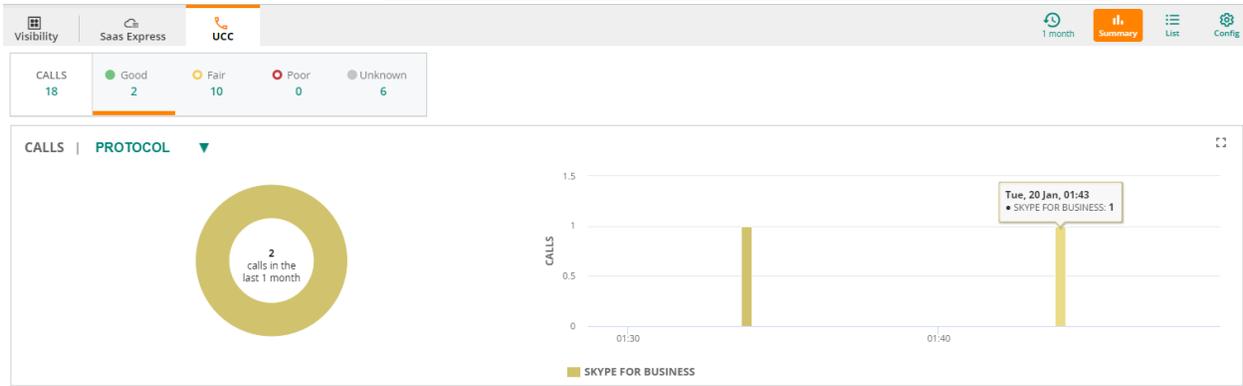
The Calls section displays a donut graph and bar graph of all, good, fair, poor, or unknown calls. You can filter the graph by **Health**, **SSID**, **Protocol**, **Operating System**, **Session Type**, or **Quality**. By default, the graph is displayed for **Protocol**. You can hover over any segment on the graph to view additional

information. Click the  enlarge icon to view the graph in a zoom in.



Only the bar graph is displayed when you select **Health**.

Figure 112 Summary View



Aruba Central (on-premises) supports a robust set of REST APIs to enable users to build custom applications and integrate the APIs with their applications. The Aruba Central API framework uses OAuth protocol to authenticate and authorize third-party applications, and allows them to obtain secure and limited access to an Aruba Central service.

API Gateway

The **API Gateway** feature in Aruba Central supports the REST API for all Aruba Central services. This feature allows Aruba Central users to write custom applications, embed, or integrate the APIs with their own applications. The REST APIs support HTTP GET and POST operations by providing a specific URL for each query. The output for these operations is returned in the JSON format.

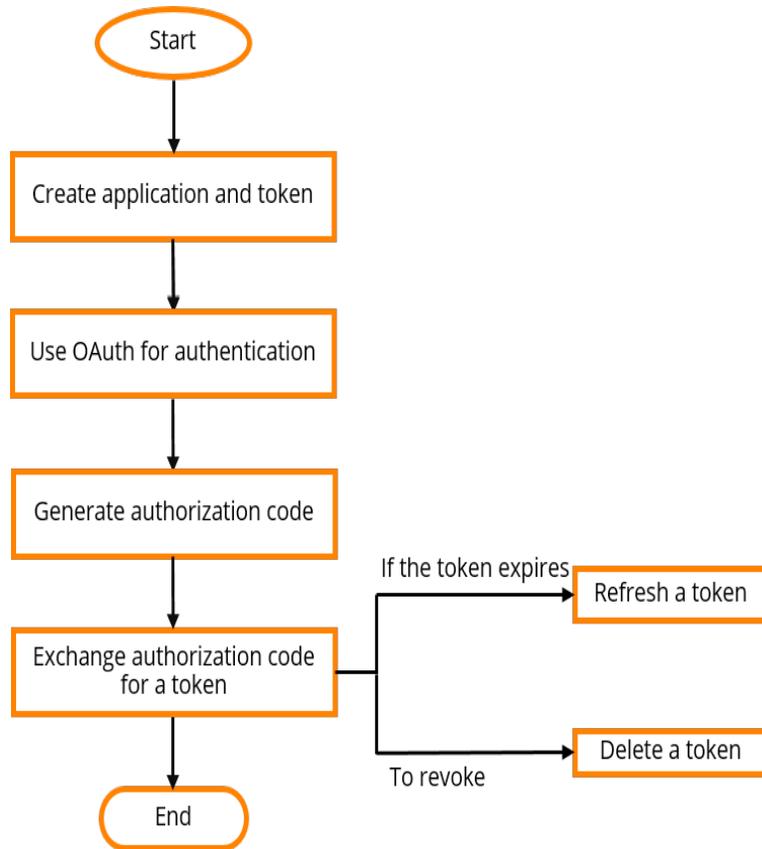
For secure access to the APIs, the Aruba Central API Framework plug-in supports OAuth protocol for authentication and authorization. The access tokens provide a temporary and secure access to the APIs. The access tokens have a limited lifetime for security reasons and the applications should use the refresh API to obtain new tokens periodically (every 2 hours).



To access the API Gateway interface, you must ensure that the FQDN in the API Gateway URL resolves to the same IP address as the Aruba Central server.

To avoid any error in the server certification, make sure that you include the API gateway FQDN as a Subject Alternate Name (SAN) in the certificate. For more information, refer to Aruba Central (on-premises) User Guide.

The following figure illustrates the API gateway workflow for the users:



Accessing API Gateway

To access the API Gateway:

1. In the **Account Home** page, under **Global Settings**, click **API Gateway**.

The **API Gateway** page is displayed. You can get new tokens and refresh old tokens. To obtain a new token application, you must set authentication parameters for a user session.

Figure 113 Account Home Page with API Gateway Option Page

ACCOUNT HOME

Manage your Network Inventory, Subscriptions, and User Access. Use any of the following apps to make Aruba work better for you.

APPS

EVALUATION 3571 DAYS LEFT



Network Operations

Manage your wired, wireless, and WAN infrastructure

LAUNCH

GLOBAL SETTINGS

USERS AND ROLES Manage user access	KEY MANAGEMENT Manage your subscription keys	DEVICE INVENTORY Manage the Devices in your Inventory
SUBSCRIPTION ASSIGNMENT Assign and modify device and service subscriptions	AUDIT TRAIL View audit-trail logs	AUTHENTICATION Manage external authentications
API GATEWAY Access API Gateway and manage access tokens	WEBHOOKS Manage Webhook end points	SYSTEM MANAGEMENT Manage Central System

Important Points to Note

- The admin user profile has **System Apps & Tokens** tab which displays all the apps and tokens generated locally in the admin user profile. This tab also displays all the apps created in the non-admin user profiles. Clicking these apps lists out all the associated tokens created for the non-admin user profile.
- Administrator role is specific to an app and hence the administrator account related RBAC library APIs and decorators must contain the application name as one of the parameters in the access verification query.

Viewing Swagger Interface

To view the APIs managed through Aruba Central, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **API Gateway**.
The **API Gateway** page with the list of published APIs is displayed.



The API Gateway is `apigw-<clusterFQDN>` by default. Make sure that this URL is added in DNS record for VIP of the Central On-Premise cluster. For example, if the Central On-Premise cluster FQDN is `yodacop-vip.arubathena.com`, then the API Gateway URL will be `apigw-yodacop-vip.arubathena.com`.

2. To view the Swagger interface, click the link in the **Documentation** column next to the specific published API name. The documentation is displayed in a new window. Below is an example figure of the API Gateway window.

Figure 114 API Gateway Page



List of Supported APIs

Aruba Central supports the following APIs for the managed devices.

Table 230: APIs and Description

API	Description
Monitoring	Gets network, client, and event details. It also allows you to manage labels and switches.
Configuration	Allows you to configure and retrieve the following: <ul style="list-style-type: none"> ■ Groups ■ Templates ■ Devices
AppRF	Gets Top N AppRF statistics.
User Management	Allows you to manage users and also allows you to configure various types of users with a specific level of access control.
Audit Event Logs	Gets a list of audit events and the details of an audit event.
Device Inventory	Gets device details and device statistics.
Licensing	Allows you to manage and retrieve subscription keys.
Device Management	Allows you to manage devices.
Firmware	Allows you to manage firmware.
Troubleshooting	Gets a list of troubleshooting commands for a specific type of device.
Notification	Gets notification alerts generated for events pertaining to device provisioning, configuration, and user management.
Unified Communications	Retrieves data for all sessions for a specific period of time. It also retrieves the total number of clients who made calls in the given time range and gets the Lync/Skype for Business URL for the Aruba Central cluster that you are using.

Table 230: APIs and Description

API	Description
Refresh API Token	Allows you to refresh the API token.
Reporting	Gets the list of configured reports for the given customer ID.
WAN Health	Allows you to the following: <ul style="list-style-type: none">■ Get list of configured WAN health policies.■ Create a new WAN health policy.■ Delete an existing WAN health policy.■ Get the details of any specific WAN health policy.■ Update an existing WAN health policy.■ Get policy schedule details.■ Create a schedule for a WAN health policy.■ Get statistics for WAN health cookie generated for a site.■ Get WAN health test results.■ Get WAN health test results for a specific site.
Network Health	Allows you to get data for all the labels and sites.
VisualRF	Allows you retrieve information on floor plans, location of APs, clients and rogue devices.

For a complete list of APIs and the corresponding documentation, see [https://apigw-*<fqdn of the Aruba Central Instance>*/swagger/apps/nms/](https://apigw-<i><fqdn of the Aruba Central Instance></i>/swagger/apps/nms/).

Creating Application and Token

To create an application, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **API Gateway**.
The **API Gateway** page is displayed.
2. Click the **My Apps & Tokens** tab.



The admin user will be able to create new apps for all the non-admin user by clicking + **Add Apps & Tokens** in the **System Apps & Tokens** tab.

3. Click + **Add Apps & Tokens**.

Figure 115 API Gateway Dashboard

The screenshot shows the API Gateway Dashboard. At the top, there is a navigation bar with a home icon and the text 'GO TO ACCOUNT HOME'. Below this is the 'API GATEWAY' title and three tabs: 'APIs', 'My Apps & Tokens' (which is selected), and 'Usage'. A dropdown menu labeled 'SELECT APP' is currently set to 'All Apps'. On the right side, there is a red-bordered button with a plus sign and the text '+ Add Apps & Tokens'. Below the navigation bar, there are two main sections. The first section is titled 'My Apps & Tokens' and contains a table with columns: NAME, CLIENT ID, CLIENT SECRET, REDIRECT URI, APPLICATION, and CREATED AT. The table is currently empty and displays a 'No data to display right now' message with a circular icon. The second section is titled 'Token List' and contains a table with columns: TOKEN ID, USER NAME, APPLICATION, GENERATED AT, REVOKE TOKEN, and DOWNLOAD TOKEN. This table is also empty and displays a 'No data to display right now' message with a circular icon.

4. In the **New Token** pop-up window, do the following:
 - a. Enter the application name. In non-admin user profile, the **Application Name** field contains the logged-in user name and is non-editable.
 - b. In the **Redirect URI** field, enter the redirect URL.
 - c. From the Application drop-down list, select the application.
 - d. Click **Generate**. A new application is created and added to the **My Apps & Tokens** table. The **My Apps & Tokens** table displays the following details:
 - **Name**—Name of the application. In non-admin user profile, the **Application Name** field contains the logged-in user name and is non-editable. Any new tokens generated in non-admin user profile is associated with the same application name.
 - **Client ID**—Unique ID for each application.
 - **Client Secret**—Unique secret ID for each application.
 - **Redirect URI**—Redirect URL.
 - **Application**—Name of the application. For example, Network Operations.
 - **Tokens**—Token created for the application. The option is available to admin user profile only.
 - **Created At**—Date on which the application was created.
5. To delete the added application, click delete  icon on the row corresponding to an application and click **Yes** to delete that application.



Only admin users will be able to generate tokens with multiple application names. In non-admin user profile, the **Application Name** field contains the user name and is non-editable. Any new tokens generated in non-admin user profile is associated with the same application name. However, all the multiple application names and the associated tokens in non-admin user profiles from the earlier versions is retained in the **Token List** table.

Using OAuth 2.0 for Authentication

For secure access to the APIs, the Aruba Central API Framework plug-in supports OAuth protocol for authentication and authorization. OAuth 2.0 is a simple and secure authorization framework. It allows applications to acquire an access token for Aruba Central through a variety of work flows supported within the OAuth 2.0 specification.

All OAuth 2.0 requests must use the SSL endpoint available at <https://apigw-<fqdn> of the Aruba Central instance>/swagger/central>.

Access and Refresh Tokens

The access token is a string that identifies a user, app, or web page and is used by the app to access an API. The access tokens provide a temporary and secure access to the APIs.

The access tokens have a limited lifetime. If the application uses web server or user-agent OAuth authentication flows, a refresh token is provided during authorization that can be used to get a new access token.

If you are writing a long running applications (web app) or native mobile application you should refresh the token periodically. For more information, see [Refreshing a token](#).

This section includes the following topics:

- [Obtaining Access Token](#)
- [Accessing APIs](#)
- [Viewing and Revoking Tokens](#)
- [Adding a New Token](#)

Obtaining Access Token

Users can generate the OAuth token using one of the following methods:

- [Obtaining Token Using Offline Token Mechanism](#)
- [Obtaining Token Using OAuth Grant Mechanism](#)

Accessing APIs

To access the API, use the following URL:

<https://apigw-<FQDN> of the Aruba Central instance>/>.

This endpoint is accessible over SSL and the HTTP (non-SSL) connections are redirected to the SSL port.

Table 231: *Accessing the API*

URL	Description
<a href="https://apigw-<FQDN> of the Aruba Central instance>/">https://apigw-<FQDN> of the Aruba Central instance>/ .	The API gateway URL. All APIs can be accessed from this URL by providing a correct access token.

The parameters for the API are as follows:

Table 232: Parameters for the API

Parameter	Value	Description
request_path	URL Path	URL path of an API, for example, to access monitoring APIs, use the path <i>/monitoring/v1/aps</i> .

Table 233: Header for the API

Header	Value	Description
Authorization	Bearer ouzMaXEbBbB6XqGtsWomK7MvaTuhrrqDQ1	Pass the access token in the header.

Example

Request Method: GET

<https://apigw-<fqdn> of the Aruba Central instance>/monitoring/v1/aps>

Request Header:

Authorization: Bearer ouzMaXEbBbB6XqGtsWomK7MvaTuhrrqDQ1

Response:

```
{
  "aps": [
    {
      "firmware_version": "6.4.4.4-4.2.3.1_54637",
      "group_name": "00TestVRK",
      "ip_address": "10.29.18.195",
      "labels": [
        "Filter_242",
        "Ziaomof",
        "roster",
        "242455",
        "Diegso"
      ],
      "macaddr": "6c:f3:7f:c3:5d:92",
      "model": "AP-134",
      "name": "6c:f3:7f:c3:5d:92",
      "radios": [
        {
          "band": 0,
          "index": 1,
          "macaddr": "6c:f3:7f:b5:d9:20",
          "status": "Down"
        },
        {
          "band": 1,
          "index": 0,
          "macaddr": "6c:f3:7f:b5:d9:30",
          "status": "Down"
        }
      ],
      "serial": "AX0140586",
      "status": "Down",
      "swarm_id": "e3bf1ba201a6f85f4b5eaedeed5e502d85a9aef58d8e1d8a0",
      "swarm_master": true
    }
  ],
}
```

```
"count": 1
}
```

Viewing and Revoking Tokens

To view or revoke tokens, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **API Gateway**.
The **API Gateway** page is displayed.
2. Click **My Apps & Tokens**. The **Token List** table displays the following:
 - **Token ID**—Token ID of the application.
 - **User Name**—Name of the user to whom this token is associated to. An application can be associated to multiple users.
 - **Application**—Name of the application to which this token is associated to. For example, Network Operations.
 - **Generated At**—Date on which the token was generated.
 - **Revoke Token**—Click **Revoke Token** and click **Yes** to revoke the token associated to a particular user. For example, if two users are associated to an application and if you want to remove access to a particular user, revoke the token associated to that user.
 - **Download Token**—Click **Download Token** to download the token.



NOTE

The admin user profile has **System Apps & Tokens** tab which displays all the apps and tokens generated in all non-admin user profiles in addition to the apps and tokens created in the admin user profile. To view all the tokens of admin and non-admin user, go to **Account Home > Global Settings > API Gateway > System Apps & Tokens**.

Adding a New Token

To add a new token, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **API Gateway**.
The **API Gateway** page is displayed.
2. Click **My Apps & Tokens**.



NOTE

The admin user can create new tokens for all non-admin users by clicking + **Add Apps & Tokens** in the **System Apps & Tokens** tab.

3. Click + **Add Apps & Tokens** to add a new token.
4. Enter the application name in the **Application Name** box and click **Generate**.



NOTE

If you have registered a custom URI when creating a new app under **System Apps and Tokens**, the **Redirect URI** option is disabled for you in the **My Apps and Tokens** tab > **Add Apps and Tokens** > **New Token** . In such cases, the **Redirect URI** option in **Add Apps and Tokens** > **New Token** under **My Apps and Tokens** populates your already registered URI.

Obtaining Token Using Offline Token Mechanism

To obtain tokens using the offline token method, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **API Gateway**.
The **API Gateway** page is displayed.
2. Click **My Apps & Tokens**.



The admin user profile can view the **System Apps & Tokens** tab which displays all the apps and tokens generated in all the non-admin user profiles in addition to the apps and tokens created in the admin user profile.

3. Click **+ Add Apps & Tokens**. The **New Token** pane is displayed.
4. Enter the application name and redirect URI in the **Application Name** and **Redirect URI** fields respectively.
5. Choose the application from the **Application** drop-down list and click **Generate** to generate a new token.
6. The **Token List** table displays the following:
 - **Token ID**—Token ID of the application.
 - **User Name**—Name of the user to whom this token is associated to. An application can be associated to multiple users.
 - **Application**—Name of the application to which this token is associated to. For example, Network Operations.
 - **Generated At**—Date on which the token was generated.
 - **Revoke Token**—Click **Revoke Token** and click **Yes** to revoke the token associated to a particular user. For example, if two users are associated to an application and if you want to remove access to a particular user, revoke the token associated to that user.
 - **Download Token**—Click **Download Token** to download the token.

Obtaining Token Using OAuth Grant Mechanism

The following section describes the steps for obtaining the access token and refresh token using the authorization code grant mechanism:



API calls are limited to 1 API per second. This rate-limit is applicable only to the APIs in the first 3 steps mentioned below.

Step 1: Authenticate a User and Create a User Session

The following API authenticates a user and returns a user session value that can be used to create future requests for a client with the specified username and password. It is assumed that you already have a client ID for your application. For more information on how to create an application and obtain tokens, see [Creating Application and Token](#).

If user authentication is successful, the request will return HTTP code 200 and the response header will include the following attributes.

Table 234: Authentication and User session Response Codes

Header Key	Values	Description
<code>https://apigw-<FQDN of the Aruba Central instance>/oauth2/authorize/central/api/login?client_id=<client_id></code>	<code>csrftoken=xxxx;</code> <code>session=xxxx</code>	The server returns a CSRF token and identifies the user session, which must be used for all subsequent HTTP requests.

Example

Request Method: POST

URL: `https://apigw-<FQDN of the Aruba Central instance>/oauth2/authorize/central/api/login?client_id=<client_id>`

Host: `apigw.central.arubanetworks.com`

Request Header:

Accept: `application/json`

Content -Type: `application/json`

POST Request Body(JSON):

```
{
  "username": "xxxxxx",
  "password": "xxxxxx"
}
```

Error Response:

```
400: Bad Request
```

Response Body (JSON):

```
{
  "extra": {},
  "message": "<error string>"
}
```

```
401: Auth failure
```

Response Body (JSON):

```
{
  "message": "Auth failure",
  "status": false
}
```

```
429: API rate limit exceeded
```

Response Body (JSON):

```
{
  "message": "API rate limit exceeded"
}
```

Success Response:

```
200: OK
```

Response Body (JSON):

```
{
  "status": true
}
```

Response Header:

```
Set-Cookie: csrftoken=xxxx;session=xxxx;
```



The **csrf token** value received in the successful response message must be used as a parameter for all subsequent POST/PUT requests. The **session** value must also be used for all subsequent requests to maintain the user session context.

Step 2: [Optional] Generating Client Credentials

To generate client credentials, use the following URI and the request method:

Example

Request Method: POST

URI—https://apigw-<FQDN of the Aruba Central instance>/central/api/client_credentials?client_id=<client_id>

POST Request Body(JSON):

```
{
  "customer_id": "<tenant_id>"
}
```

Request Header: (Values from login API request)

```
Set-Cookie: csrftoken=xxxx;session=xxxx;
```

Response Body(JSON):

```
{
  "client_id": "<new-client-id>,"
}
```

```
"client_secret": <new-client-secret>"
}
```

```
429: API rate limit exceeded
```

Response Body (JSON):

```
{
  "message": "API rate limit exceeded"
}
```

Step 3: Generate Authorization Code

After the user is authenticated and you have a valid session for that user, use this API to get authorization code. The authorization code is valid only for 5 minutes and must be exchanged for a token within that time.

Table 235: URL for to Generate an Authorization Code

URL	Description
<a href="https://apigw-<FQDN of the Aruba Central instance>/oauth2/authorize/central/api">https://apigw-<FQDN of the Aruba Central instance>/oauth2/authorize/central/api	The endpoint is a POST call to get an authorization code.

Query parameters for this API are as follows:

Table 236: Query Parameters for the Auth Code API

Parameter	Values	Description
client_id	client_id is a unique hexadecimal string	The client_id is a unique identifier that identifies the caller. Application developers obtain a client ID and a client secret when they register with the API gateway admin.
response_type	code	Use code as the response type to get the authorization code that can be exchanged for token
scope	all or read	Requested API permissions may be either all (for both read and write access) or read for read-only access.

Example

Request Method: POST

URL: https://apigw-<FQDN of the Aruba Central instance>/oauth2/authorize/central/api/?client_id=<client_id>&response_type=code&scope=all HTTP/1.1

Host: apigw.central.arubanetworks.com

Request Header:

Accept: application/json Cookie: "session=xxxx" X-CSRF-Token: xxxx

Content -Type: application/json

POST Request Body(JSON):

```
{
  "customer_id": "xxxxx"
}
```

Error Response:

```
400: Bad Request
```

Response Body (JSON):

```
{
  "extra": {},
  "message": "<error string>"
}
```

```
401: Auth failure
```

Response Body (JSON):

```
{
  "message": "Auth failure",
  "status": false
}
```

```
429: API rate limit exceeded
```

Response Body (JSON):

```
{
  "message": "API rate limit exceeded"
}
```

Success Response:

```
200: OK
```

Response Body (JSON):

```
{
  " auth_code ": "xxxx"
}
```



Pass the **csrf-token** value you obtained in step one in the request header, otherwise the request will be rejected. Note the **auth_code** value in the response, as you will use this code to obtain an OAuth token.

Response Header:

```
Set-Cookie: csrftoken=xxxx;session=xxxx;
```

Step 4: Exchange Auth Code for a Token

Once you have an authorization code, you just use that code to request an access from the server. The exchanges should be done within 300 seconds of obtaining the auth code from the previous step, or the API will return an error.

Table 237: URL for to Generate an Auth Token

URL	Description
<a href="https://apigw-<FQDN of the Aruba Central instance>/oauth2/token">https://apigw-<FQDN of the Aruba Central instance>/oauth2/token	The endpoint is a POST call to get an access token using the authorization code obtained from the server.

Query parameters for this API are as follows:

Table 238: Query Parameters for the Auth Code API

Parameter	Values	Description
client_id	client_id is a unique hexadecimal string	The client_id is a unique identifier that identifies the caller. Application developers obtain a client ID and a client secret when they register with the API gateway admin.
client_secret	client_secret is a unique hexadecimal string	The client_secret is a unique identifier provided to each developer at the time of registration. Application developers can obtain a client ID and client secret when they register with the API gateway admin.
grant_type	authorization_code	Use code to get the authorization code that can be exchanged for the token.
code	auth_code received from step 1	The authorization code received from the authorization server.
redirect_uri	string	The redirect URI must be the same as the one given at the time of registration. This is an optional parameter.

The response to this API query is a JSON dictionary with following values:

Table 239: Auth Token Values

Parameter	Values	Description
token_type	bearer	Identifies the token type. Central supports only the bearer token type (See https://tools.ietf.org/html/rfc6750)

Parameter	Values	Description
refresh_token	string	Refresh tokens are credentials used to renew or refresh the access_token when it expires without repeating the complete authentication flow. A refresh token is a string representing the authorization granted to the client by the resource owner.
expires_in	seconds	The lifetime, in seconds, of the access token.
access_token	string	Access tokens are credentials used to access protected resources. An access token is a string representing an authorization issued to the client.

Example

Request Method: POST

URL: https://apigw-<FQDN of the Aruba Central instance>/oauth2/token?client_id=<Ccentral-API-app-clientid>&client_secret=xxxx&grant_type=authorization_code&code=xxxx \

Content -Type: application/json

Response:

```
{
  "refresh_token": "xxxx",
  "token_type": "bearer",
  "access_token": "xxxx",
  "expires_in": 7200
}
```

Step 5: Refreshing a Token

You can use the refresh token obtained in the previous step to update the access token without repeating the entire authentication process. A refresh token is only required once your access token is expired. You can only refresh a token for a new access token every 15 minutes. For example, when you refresh a new token, you can use the provided access token for 2 hours. If you want a new access token, you have to again refresh the token after 15 minutes from its last refresh.

Table 240: URL to Refresh a Token

URL	Description
<a href="https://apigw-<FQDN of the Aruba Central instance>/oauth2/token">https://apigw-<FQDN of the Aruba Central instance>/oauth2/token	The endpoint is a POST call to refresh the access token using the refresh token obtained from the server

Query parameters for this API are as follows:

Table 241: Query Parameters for Refresh Tokens

Parameter	Value	Description
client_id	client_id is a unique hexadecimal string	The client_id is a unique identifier that identifies the caller. Application developers obtain a client ID and a client secret when they register with the API gateway admin.

Parameter	Value	Description
client_secret	client_secret is a unique hexadecimal string	The client_secret is a unique identifier provided to each developer at the time of registration. Application developers obtain a client ID and a client secret when they register with the API gateway admin.
grant_type	refresh_token	Specify refresh_token as the grant type to request that an authorization code be exchanged for a token
refresh_token	string	A string representing the authorization granted to the client by the resource owner.

The response to this API query is a JSON dictionary with following values:

Parameter	Value	Description
token_type	bearer	Identifies the token type. Only the bearer token type is supported. For more information, see https://tools.ietf.org/html/rfc6750 .
refresh_token	string	Refresh tokens are credentials used to renew or refresh the access token when it expires without going through the complete authorization flow. A refresh token is a string representing the authorization granted to the client by the resource owner.
expires_in	seconds	The expiration duration of the access tokens in seconds.
access_token	string	Access tokens are credentials used to access the protected resources. An access token is a string representing an authorization issued to the client.

Example

Method: POST

https://apigw-<FQDN of the Aruba Central instance>/oauth2/token?client_id=<Central-API-app-clientid>&client_secret=xxxx&grant_type=authorization_code&code=xxxx \

Response

```
{
  "refresh_token": "xxxx",
  "token_type": "bearer",
  "access_token": "xxxx",
  "expires_in": 7200
}
```

Step 6: Deleting a Token

To delete the access token, access the following URL:

Table 242: URL to Delete a Token

URL	Description
<a href="https://apigw-<FQDN of the Aruba Central instance>/oauth2/token">https://apigw-<FQDN of the Aruba Central instance>/oauth2/token	This endpoint is accessible over SSL. The HTTP (non-SSL) connections are redirected to SSL port. Customer ID is a string.

Example

Method : DELETE

URL: <https://apigw-<FQDN of the Aruba Central instance>/oauth2/api/tokens>

JSON Body:

```
{
  "access_token": "<access_token_to_be_deleted>",
  "customer_id": "<customer_id_to_whom_token_belongs_to>"
}
```

Headers:

Content-Type: application/json

X-CSRF-Token: <CSRF_token_obtained_from_login_API>

Cookie: "session=<session_obtained_from_login_API>"

Viewing Usage Statistics

The **API Gateway** page includes the **Usage** tab that displays the API usage. The **Usage** tab is available only for administrators and the usage data is stored only for the previous 30 days. The following details are displayed:

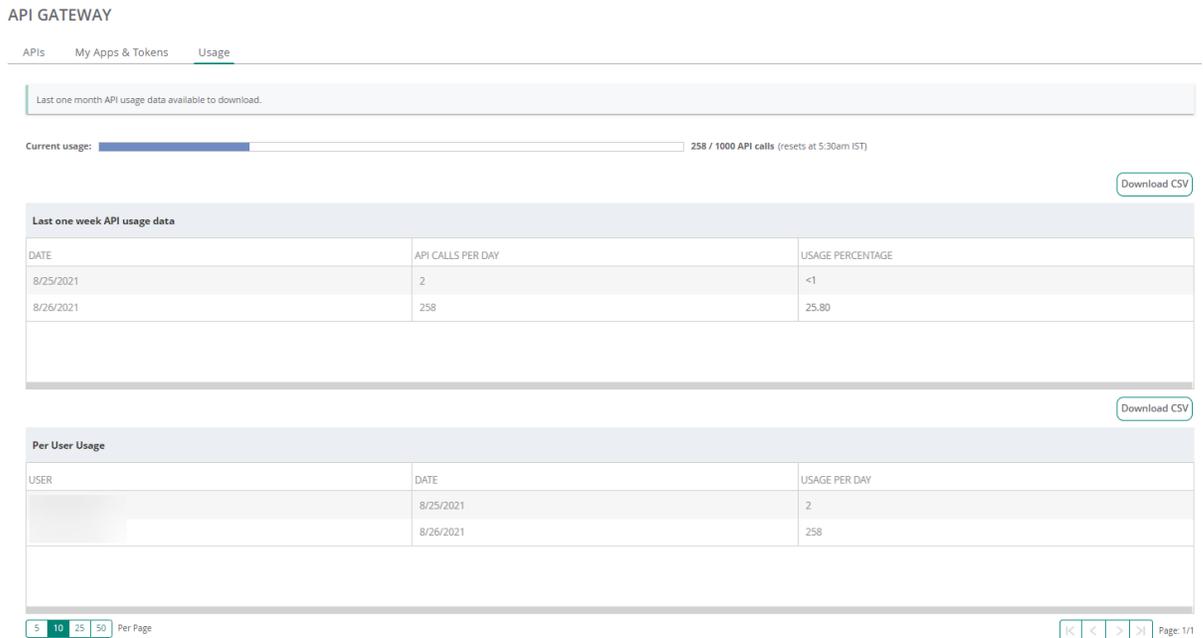
- Current Usage
- Last one week API usage data
- Per user usage.
- Download CSV

To view the usage statistics for users of API Gateway, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **API Gateway**.
The **API Gateway** page is displayed.

- Click **Usage**. The following details are displayed:

Figure 116 API Gateway Usage Page



- Current usage**—Current usage of API calls assigned for a day along with the reset time in local time zone .
 - Last one week API usage data:**
 - Date**—The date of usage.
 - API Calls Per Day**—API calls per day.
 - Usage Percentage**—Usage percentage for a specific date.
 - Per User Usage:**
 - User**—The name of the user.
 - Date**—The date on which the application was accessed.
 - Usage Per Day**—The total usage by the user per day. This is derived based on the total number of API calls made on a per day basis. This is an aggregate across all customers.
- To download the API gateway usage statistics, Click **Download CSV** for the respective usage type to download the stat file in CSV format.



The **Usage** tab is only available for administrators and the usage data is stored only for the previous 30 days.

Changes to Aruba Central APIs

This section lists the new APIs, deprecated APIs, alternative APIs, and APIs removed from Aruba Central:

- [New APIs](#)
- [Modified API](#)

New APIs

The following table lists the new APIs:

Table 243: New APIs

New API	Description
Monitoring > Clients APIs	
<ul style="list-style-type: none"> ■ [GET] /monitoring/v2/clients 	<p>This API is introduced to get a list of unified clients and it is backward compatible with the version 1 APIs (GET /monitoring/v1/clients/wired and GET /monitoring/v1/clients/wireless). This API version is introduced with the following parameter inclusions:</p> <ul style="list-style-type: none"> ■ last_client_mac—Use this parameter to fetch the next set of clients beyond set limit. This is used to fetch the clients details beyond 10000 clients. ■ timerange— Use this to filter the unified client information based on the time range. By default, 3 hours is selected. ■ client_type—Use this to select the client type as WIRELESS or WIRED. By default, client type is selected as WIRELESS. ■ client_status—Use this to select either CONNECTED for a list of connected clients or FAILED_TO_CONNECT for a list failed clients. By default, the client status is selected as CONNECTED.
<ul style="list-style-type: none"> ■ [GET] /monitoring/v2/clients/{macaddr} 	<p>This API is introduced to get the client details (wired and wireless).</p>
Authentication & Policy > Client Policy APIs	
<ul style="list-style-type: none"> ■ [GET] /client_policy 	<p>This API is introduced to fetch a policy that allows network access for registered clients, based on their MAC address and client profile tag.</p>
<ul style="list-style-type: none"> ■ [DELETE] /client_policy 	<p>This API is introduced to delete an existing policy to remove network access for all registered clients.</p>
<ul style="list-style-type: none"> ■ [PUT] /client_policy 	<p>This API is introduced to configure or update a policy that allows network access for registered clients, based on their MAC address and client profile tag.</p>
Authentication & Policy > Client Registration APIs	
<ul style="list-style-type: none"> ■ [GET] /client_registration 	<p>This API is introduced to fetch the list of registered clients that are allowed to access the network.</p>
<ul style="list-style-type: none"> ■ [DELETE] /client_registration/{mac_address} 	<p>This API is introduced to delete the registered client and to remove network access.</p>
<ul style="list-style-type: none"> ■ [POST] /client_registration 	<p>This API is introduced to add a registered client to allow network access.</p>
<ul style="list-style-type: none"> ■ [PATCH] /client_registration/{mac_address} 	<p>This API is introduced to update Client Name for the registered clients.</p>
Authentication & Policy > User policy APIs	

Table 243: New APIs

New API	Description
<ul style="list-style-type: none"> ▪ [GET] /user_policy 	This API is introduced to fetch a policy that allows wireless network access for users, based on their user groups.
<ul style="list-style-type: none"> ▪ [DELETE] /user_policy 	This API is introduced to delete existing policy to remove wireless network access for all users.
<ul style="list-style-type: none"> ▪ [PUT] /user_policy 	This API is introduced to configure a policy to allow wireless network access for users, based on their user groups.
Configuration > WLAN Configuration APIs	
<ul style="list-style-type: none"> ▪ [GET] /configuration/full_hotspot/{group_name_or_guid} 	This API is introduced to get the WLAN list of an UI group.
<ul style="list-style-type: none"> ▪ [GET] /configuration/full_hotspot/{group_name_or_guid}/{mode_name} 	This API is introduced to get the hotspot list of an UI group or swarm with mode name.
<ul style="list-style-type: none"> ▪ [GET] /configuration/full_hotspot/{group_name_or_guid}/template 	This API is introduced to get the WLAN default configuration.
<ul style="list-style-type: none"> ▪ [GET] /configuration/full_hotspot/{group_name_or_guid}/{hotspot_name}/{mode_name} 	This API is introduced to initiate backup of running config for the switch with the given serial and store output against a name starting with the given prefix.
<ul style="list-style-type: none"> ▪ [POST] /configuration/full_hotspot/{group_name_or_guid}/{hotspot_name}/{mode_name} 	This API is introduced to create a new hotspot.
<ul style="list-style-type: none"> ▪ [DELETE] /configuration/full_hotspot/{group_name_or_guid}/{hotspot_name}/{mode_name} 	This API is introduced to delete an existing hotspot.
<ul style="list-style-type: none"> ▪ [PUT] /configuration/full_hotspot/{group_name_or_guid}/{hotspot_name}/{mode_name} 	This API is introduced to update an existing hotspot.
Troubleshooting APIs	
<ul style="list-style-type: none"> ▪ [GET] /troubleshooting/v1/running-config-backup/serial/{serial} 	This API is introduced to get list of backups associated with the device serial.
<ul style="list-style-type: none"> ▪ [GET] /troubleshooting/v1/running-config-backup/serial/{serial}/prefix/{prefix} 	This API is introduced to filter/list the backups associated with the device serial and starting with the prefix.
<ul style="list-style-type: none"> ▪ [GET] /troubleshooting/v1/running-config-backup/name/{name} 	This API is introduced to fetch the backup stored against the given name.

Table 243: New APIs

New API	Description
<ul style="list-style-type: none"> ■ [POST] /troubleshooting/v1/running-config-backup/serial/{serial}/prefix/{prefix} 	<p>This API is introduced to initiate backup of running config for the switch with the given serial and store output against a name starting with the given prefix.</p>
<ul style="list-style-type: none"> ■ [POST] /troubleshooting/v1/running-config-backup/group_name/{group_name}/prefix/{prefix} 	<p>This API is introduced to initiate backup of running config for switches in the group and store output against names starting with the given prefix.</p>
<p>AI OPs > Wi-Fi Connectivity at Global APIs</p> <p>NOTE: For all AI Ops APIs, AI Insights will get triggered only when there are failure events in the user network, so all Insights might not be present all the time. Therefore, providing an empty API response for a selected time period.</p>	
<ul style="list-style-type: none"> ■ [GET] /aiops/v1/connectivity/global/stage/{stage}/export ■ [GET] /aiops/v1/connectivity/site/{site_id}/stage/{stage}/export ■ [GET] /aiops/v1/connectivity/group/{group}/stage/{stage}/export 	<p>This APIs are introduced to get the overall Connectivity Information for a given time duration. Use stage parameter to get the information for that stage.</p>
<p>AI OPs > AI Insights List APIs</p>	
<ul style="list-style-type: none"> ■ [GET] /aiops/v2/insights/global/list ■ [GET] /aiops/v2/insights/site/{site_id}/list ■ [GET] /aiops/v2/insights/ap/{ap_serial}/list ■ [GET] /aiops/v2/insights/client/{sta_mac}/list ■ [GET] /aiops/v2/insights/gateway/{gw_serial}/list ■ [GET] /aiops/v2/insights/switch/{sw_serial}/list 	<p>This APIs are introduced to get the list of insights for a given time duration</p>
<p>AI OPs > AI Insight Details APIs</p>	
<ul style="list-style-type: none"> ■ [GET] /aiops/v2/insights/global/id/{insight_id}/export ■ [GET] /aiops/v2/insights/site/{site_id}/id/{insight_id}/export ■ [GET] /aiops/v2/insights/ap/{ap_ 	<p>This APIs are introduced to get details of single insight for a given time duration.</p>

Table 243: *New APIs*

New API	Description
<ul style="list-style-type: none"> serial}/id/{insight_id}/export ▪ [GET] /aiops/v2/insights/client/{sta_mac}/id/{insight_id}/export ▪ [GET] /aiops/v2/insights/gateway/{gw_serial}/id/{insight_id}/export ▪ [GET] /aiops/v2/insights/switch/{sw_serial}/id/{insight_id}/export 	
<p>Service IPMS > Aruba ipms APIs</p> <p>NOTE: In the API parameter, make sure that the node_type and node_id fields are set to Global.</p>	
<ul style="list-style-type: none"> ▪ [GET] /ipms-config/v1/node_list/{node_type}/{node_id}/config/address_pool/{pool_name}/ip_range/ 	This API is introduced to retrieve an ip range.
<ul style="list-style-type: none"> ▪ [DELETE] /ipms-config/v1/node_list/{node_type}/{node_id}/config/ 	This API is introduced to delete a config.
<ul style="list-style-type: none"> ▪ [GET] /ipms-config/v1/node_list/{node_type}/{node_id}/config/ 	This API is introduced to retrieve a config.
<ul style="list-style-type: none"> ▪ [GET] /ipms-config/v1/node_list/{node_type}/{node_id}/config/address_pool/ 	This API is introduced to retrieve an address pool.
<ul style="list-style-type: none"> ▪ [DELETE] /ipms-config/v1/node_list/{node_type}/{node_id}/config/address_pool/{pool_name}/ 	This API is introduced to delete an address pool.
<ul style="list-style-type: none"> ▪ [GET] /ipms-config/v1/node_list/{node_type}/{node_id}/config/address_pool/{pool_name}/ 	This API is introduced to retrieve an address pool by identifier pool name.
<ul style="list-style-type: none"> ▪ [POST] /ipms-config/v1/node_list/{node_type}/{node_id}/config/address_pool/{pool_name}/ 	This API is introduced to create an address pool by identifier pool name.
<ul style="list-style-type: none"> ▪ [PUT] /ipms-config/v1/node_list/{node_type}/{node_id}/config/address_pool/{pool_name}/ 	This API is introduced to create or update the address pool by identifier pool name.

Table 243: *New APIs*

New API	Description
<ul style="list-style-type: none"> ▪ [DELETE] /ipms-config/v1/node_list/{node_type}/{node_id}/config/address_pool/{pool_name}/ip_range/{range_id}/ 	This API is introduced to delete the IP range by identifier range id.
<ul style="list-style-type: none"> ▪ [GET] /ipms-config/v1/node_list/{node_type}/{node_id}/config/address_pool/{pool_name}/ip_range/{range_id}/ 	This API is introduced to retrieve the IP range by identifier range id.
<ul style="list-style-type: none"> ▪ [POST] /ipms-config/v1/node_list/{node_type}/{node_id}/config/address_pool/{pool_name}/ip_range/{range_id}/ 	This API is introduced to create IP range by identifier range id.
<ul style="list-style-type: none"> ▪ [PUT] /ipms-config/v1/node_list/{node_type}/{node_id}/config/address_pool/{pool_name}/ip_range/{range_id}/ 	This API is introduced to create or update the IP range by identifier range id.
<ul style="list-style-type: none"> ▪ [GET] /ipms-config/v1/node_list/{node_type}/{node_id}/ 	This API is introduced to have global level config for IPMS service.

Modified API

The following table lists the modified APIs:

Table 244: *Modified APIs*

Modified API	Description
Monitoring > Client API	
<ul style="list-style-type: none"> ▪ [GET] /monitoring/v1/clients/wireless ▪ [GET] /monitoring/v1/clients/wired 	<ul style="list-style-type: none"> ▪ site parameter is introduced to filter the APIs by site name. ▪ To retrieve clients beyond 10,000, use the last_client_mac parameter to fetch the next set of clients.
Topology	
<ul style="list-style-type: none"> ▪ [GET] /{site_id} 	<p>Following fields are added/modified in the response:</p> <ul style="list-style-type: none"> ▪ vlangs—Lists the vlans configured on the device. ▪ taggedVlans and untaggedVlan—Lists the tagged and untagged vlan associated to the ports of the edge. This is applicable only for switches. ▪ In alignment with the redesign of HPE engineering terminology, the term Master in the API response changed to Conductor.

Table 244: *Modified APIs*

Modified API	Description
<ul style="list-style-type: none">▪ [GET] /devices/{device_serial}	<ul style="list-style-type: none">▪ In alignment with the redesign of HPE engineering terminology, the term Master in the API response changed to Conductor.

Webhook

An application can provide real-time information or notifications to other applications using the Webhook service. You can access the Webhook service through the **Account Home** or API Gateway. Using the Webhook service, you can list, add, or delete Webhooks; get Webhook token; refresh Webhook token; update Webhook settings; do Webhook settings for a specific item; and test for Webhook notification.

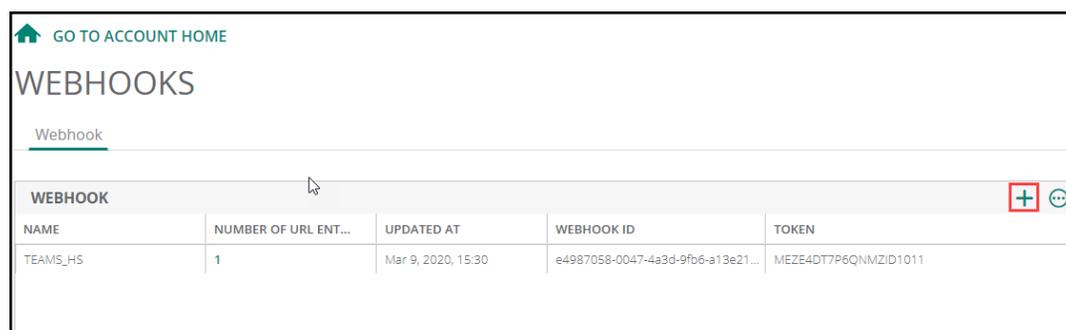
Aruba Central allows you to integrate Webhook with other third-party applications such as ServiceNOW, Zapier, IFTTT, and so on.

Configuring and Modifying Webhook Through the User Interface

To access the Webhooks service from the UI:

1. In the **Account Home** page, under **Global Settings**, click **Webhooks**.
The **Webhooks** page is displayed.
2. In the **Webhook** tab, click + sign. The **Add Webhook** pop-up box opens.

Figure 117 Webhooks Page



WEBHOOK				
NAME	NUMBER OF URL ENT...	UPDATED AT	WEBHOOK ID	TOKEN
TEAMS_HS	1	Mar 9, 2020, 15:30	e4987058-0047-4a3d-9fb6-a13e21...	MEZE4DT7P6QNMZID1011

Figure 118 *Add Webhooks Page*

ADD WEBHOOK

Name
Example

Retry Policy

None

Important (up to 5 retries over 6 minutes)

Critical (up to 5 retries over 27 hours)

URL
No data to display

CANCEL **ADD**

3. To create webhooks, enter the following details:
 - a. **Name**—Enter a name for the Webhook
 - b. **Retry Policy**— Select any one of the following options:
 - **None**—Select this to have no retry.
 - **Important**—Select this to have up to 5 retries over 6 minutes.
 - **Critical**—Select this to have up to 5 retries over 27 hours.
 - c. **URLs**—Enter the URL. Click + to enter another URL. You can add up to three URLs.
4. Click **Save**. The Webhooks is created and listed in the **Webhook** table.

Viewing Webhooks

To view the Webhooks, complete the following steps:

The **Webhook** table displays the following information and also allows you to edit or delete Webhooks:

1. In the **Account Home** page, under **Global Settings**, click **Webhooks**.
2. The **Webhooks** page with Webhook table is displayed.

The **Webhook** table allows you to edit or delete Webhooks and also displays the following information:

 - **Name**—Name of the Webhooks.
 - **Number of URL Entries**—Number of URLs in Webhooks. Click the number to view the list of URLs.
 - **Updated At**—Date and time at which Webhooks was updated.
 - **Webhook ID**—Webhooks ID.

- **Token**—Webhooks token. Webhooks token enables header authentication and the third-party receiving service must validate the token to ensure authenticity.
- **Edit**—Select the Webhook from the list and click the **Edit** icon to edit the Webhook. You can refresh the token and add URLs. Click **Save** to save the changes.
- **Delete**—Select the Webhook from the list and click the **Delete** icon and click **Yes** to delete the Webhook.
- **Test Webhooks**—Select the Webhook from the list and click the **Test Webhooks** icon to test the Webhook by posting sample webhook payload to the configured URL. The **Test Webhooks** table provides the **URL** and **Status** of the selected Webhook.
- **View Dispatch Logs**—Select the Webhook from the list and click the **View Dispatch Log** icon to view the **Dispatch Logs** for the selected Webhook. The **Dispatch Logs** table provides the **URL**, **Status**, and **Dispatched Time**. Click the arrow against each row to view the **Log Details** and **Attempts** in the drop-down for the respective URL.

Figure 119 *Dispatch Logs Details Page*

DISPATCH LOGS (3)		
URL	STATUS	DISPATCHED TIME
https://example.org/webh...	3	Jun 05, 2020, 16:51

ATTEMPTS (1)	
TIME	STATUS
Jun 05, 2020, 16:51	404

Refreshing Webhooks Token Through the UI

To refresh Webhooks token through the UI:

1. In the **Account Home** page, under **Global Settings**, click **Webhooks**.
The **Webhooks** page is displayed.
2. In the **Webhook** table, select the Webhook from the list and click **Edit** icon to edit.
3. In the pop-up window, click the **Refresh** icon next to the token. The token is refreshed.

Configuring and Modifying Webhook Through the API Gateway

To access and use the API Webhook service

1. Log in to **Account Home**.
2. Under **Global Settings**, click **API Gateway**.
3. In the **APIs** tab, click the **Swagger** link under the **Documentation** header. The [Swagger](#) website opens.
4. In the [Swagger](#) website, select **Webhook** from the **URL** drop-down list. All available Webhooks APIs are listed under **API Reference**.



For further help on API Webhook Service and creating a Webhook ID (WID), refer to <https://apigw-<fqdn of the Aruba Central Instance>/swagger/apps/nms/>.

The following HTTP methods are defined for Aruba Central API Webhook resource:

- **GET**
- **POST**
- **PUT**
- **DELETE**

You can perform CRUD operation on the Webhook URL configuration. The key configuration elements that are required to use API Webhook service are Webhook URL and a shared secret.

A shared secret token is generated for a Webhook URL when you register for Webhooks. A hash key is generated using SHA256 algorithm by using the payload and the shared secret token. The API required to refresh the shared secret token is provided for a specific Webhook configuration. You can choose the frequency at which you want to refresh the secret token.

Sample Webhook Format for a New Alert Generation

URL POST <webhook-url>

Custom Headers

Content-Type: application/json

X-Central-Service: Alerts

X-Central-Event: Radio-Channel-Utilization

X-Central-Delivery-ID: 72d3162e-cc78-11e3-81ab-4c9367dc0958

X-Central-Delivery-Timestamp: 2016-07-12T13:14:19-07:00

X-Central-Customer-ID: <#####>

Body

```
{
  "alert_type": "AP_RADIO_NOISE_FLOOR",
  "description": "Noise floor on AP iap-303-iphone456-offline operating on Channel
10 and serving 0 clients has been above -110 dBm
for about 10 minutes since 2019-07-24 07:06:00 UTC.",
  "timestamp": 1563952560,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-1253",
```

```
"state": "Open",
"nid": 1253,
"details": {
  "_rule_number": "0",
  "group": "3",
  "name": "iap-303-iphone456-offline",
  "_radio_num": "1",
  "client_count": "0",
  "labels": "3,118",
  "_band": "0",
  "duration": "10",
  "time": "2019-07-24 07:06:00 UTC",
  "threshold": "110",
  "ds_key": "201804170291.CNGHKGX004.radio.noisefloor",
  "serial": "CNGHKGX004",
  "channel": "10"
},
"operation": "create",
"device_id": "CNGHKGX004",
"id": "AWwiljjgVQ01ZtiGThDB",
"severity": "Critical"
}
```

Streaming APIs

Streaming APIs allow customers to subscribe to a select set of services instead of polling the NB API to get an aggregated state or statistics of the events. For example, with streaming APIs, the customers can get notifications about the following types of events:

- The UP and DOWN status of the devices
- Change in the location of APs

For a complete list of supported services, see the next section. With streaming API, the customers can write value-added applications based on the aggregated context.



API streaming is not supported on a single node clusters.

Supported Services

The streaming API supports the following services, for a definition of each of the services, see the next section.

- Location
- Security
- AppRF
- Audit
- Monitoring

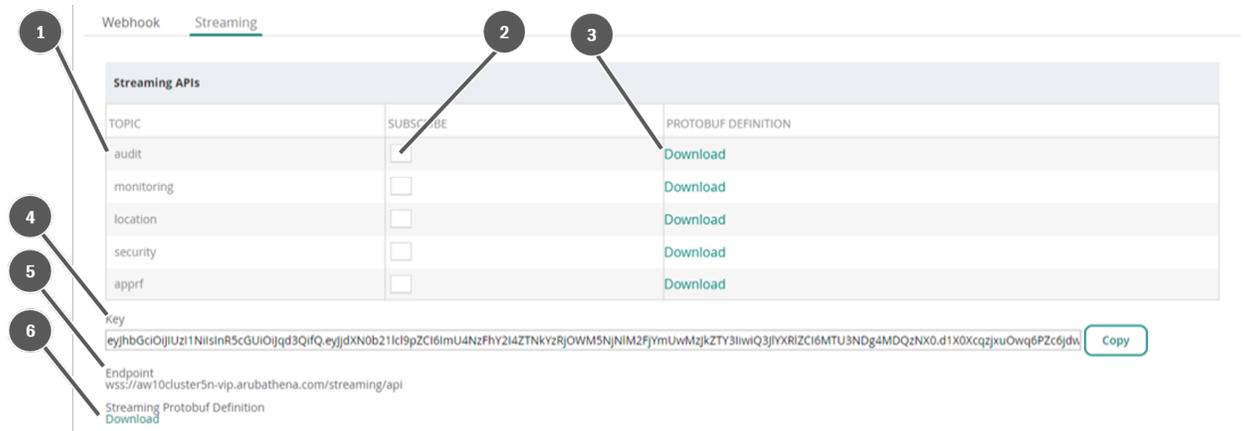
Viewing the Streaming API Page

Perform the following steps to view the **Streaming API** page:

1. Log in to **Account Home**.
2. Under **Global Settings**, click the **Webhooks** menu option.
3. Click the **Streaming** tab.

The following is an illustration of the **Streaming API** page:

Figure 120 View of the Streaming API Page



The parameters in the page are described in the following table. Refer to the callout numbers.

Table 245: Parameters of the Streaming API Page

Callout	API	Description
1	Topic	A list of available topics for streaming APIs. To receive streaming events from a topic, subscribe to the specific topic.
2	Subscribe	Enables Aruba Central to stream events for a specific topic when this box is enabled.
3	Protobuf Definition	Definition of the specific topic. All WebSocket response messages are encapsulated in a protocol buffer, the format of which you can download.
4	Key	Access token for establishing a WebSocket connection.
5	Endpoint	WebSocket endpoint address for the Aruba Central instance.
6	Streaming Protobuf Definition	The protocol buffer in which all the incoming streaming messages are encapsulated. This protobuf is further used to identify the topic of the message received and decode the topic-specific protobuf message.

Subscribing or Unsubscribing a Streaming API Topic

To receive streaming events from a topic, first subscribe to the topic in Aruba Central.



Only Aruba Central admin users can subscribe to, or unsubscribe from, a topic.

To subscribe to a streaming API topic:

1. Log in to **Account Home**.
2. Under **Global Settings**, click the **Webhooks** menu option.
3. Click the **Streaming** tab.
4. In the **Streaming APIs** tab, select the check box corresponding to the topic that you want to subscribe.

To unsubscribe a topic, clear the corresponding check box. The following topics are available for download:

- **Location**—The location messages publish the location of associated clients or rogues and these are published every 50 messages or 10 seconds apart.
- **Security**—When a new rogue is detected or a suspect is promoted to rogue, a rogue event is published to the streaming server.
- **AppRF**—AppRF stream is the flow of all the client sessions which is intra-internet bound happening in the network.
- **Audit**—The Audit messages are sent to notify events like device connectivity, configuration status, and firmware status.
- **Monitoring**—Monitoring publishes the messages about statistics and states of monitoring data.

Downloading Protobuf Definition for a Streaming API topic

To download the protobuf definition, complete the following steps:

1. Log in to **Account Home**.
2. Under **Global Settings**, click the **Webhooks** menu option.
3. Click the **Streaming** tab.
4. In the **Streaming APIs** table, click the **Download** button corresponding to the protobuf definition for the topic to which you have subscribed.

Decoding WebSocket Response Messages

All WebSocket response messages are encapsulated in a protocol buffer. When a message is received, use the subject (topic) to identify the message and invoke an appropriate message processor. To decode the message, refer to the protocol buffer specification of the respective topic.

The format is as follows:

```
message MsgProto {
  string subject = 2; // subject
  bytes data = 3; // payload
  int64 timestamp = 4; // received timestamp
  string customer_id = 5; // customer id to which this data belongs
  string msp_id = 6; // optional field indicating the msp_id
}
```

Enabling Data Streaming From a Topic

Use the WebSocket endpoint and access token to establish a WebSocket connection and start streaming data for the topics to which you have enabled subscription. Create a WebSocket connection to enable API streaming from Aruba Central.

Complete the following steps to receive streaming events from Aruba Central:

1. Create a WebSocket connection:
`wss://<central-host>/streaming/api`

2. Set the following additional headers:

Header	Description
UserName	Username of the admin. This is an optional header.
Authorization	Access token. For more information about how to generate the key, see Subscribing or Unsubscribing a Streaming API Topic .
Topic	Value of the topic to which you have subscribed. The value should be one of the following: <ul style="list-style-type: none">■ Location■ Security■ AppRF■ Audit■ Monitoring

3. Start the read loop to read the events. The payload is a protocol buffer message.

Retrieving a New Token

The access token comes with a validity of seven days after which a new token needs to be generated.

You can retrieve the token either directly from the UI or by using the API.

1. To retrieve the new access token from the Aruba CentralUI, complete the following steps:
 - a. In the **Account Home** page, under **Global Settings**, click **Webhooks > Streaming** tab. The **Streaming** page is displayed.
 - b. You can retrieve the valid token from the **Key** field. The token gets refreshed automatically after seven days of its generation.
2. To retrieve the new access token from the API, here are the details required:
 - **API**—`https://<central-host>/streaming/token/validate`
 - **Method**—GET
 - **Authorization**—Enter the current token

The API will return the same token if the old token is not expired or will return a new token in case the old token is expired.

This section lists the documents that provide information related to Aruba Central (on-premises) and the devices managed by Aruba Central (on-premises).

Aruba Central (on-premises) Release Notes

[Aruba Central \(on-premises\) 2.5.4.4 Release Notes](#)

[Aruba Central \(on-premises\) 2.5.4.3 Release Notes](#)

[Aruba Central \(on-premises\) 2.5.4.2 Release Notes](#)

Aruba Central (on-premises) 2.5.4.3 PDF Documents

[Aruba Central \(on-premises\) User Guide](#)

[Aruba Central \(on-premises\) Supported Devices Guide](#)

Aruba Central (on-premises) 2.5.4.0 PDF Documents

[Aruba Central \(on-premises\) User Guide](#)

[Aruba Central \(on-premises\) Release Notes](#)

[Aruba Central \(on-premises\) API Reference Guide](#)

[Aruba Central \(on-premises\) Installation and Setup Guide](#)

[Aruba Central \(on-premises\) Migration Guide](#)

[Aruba Central \(on-premises\) Supported Devices Guide](#)

Aruba Central (on-premises) APIs

For a complete list of APIs and the corresponding documentation, see *Swagger*. For more information about accessing the API documentation on Swagger, see *Aruba Central (on-premises) API Reference Guide*.

ArubaOS and Aruba Instant Documentation

For information on controllers and Instant APs, see the following documents at the [Aruba Support site](#):

- *ArubaOS User Guide*
- *ArubaOS CLI Reference Guide*
- *Aruba Instant User Guide*
- *Aruba Instant CLI Reference Guide*

Aruba Switch Documentation

For information on Aruba switches, see the following documents at the HPE support site:

- *HPE ArubaOS-Switch Management and Configuration Guide*
- *HPE ArubaOS-Switch Software Feature Support Matrix*

Accessing Documentation on Support Sites

To view documents hosted on the Aruba support site:

1. Go to [Aruba Support Portal](#).
2. Click the **Documentation** tab.
3. Navigate to the desired product category.

To view documents on the HPE support site:

1. Go to www.hpe.com/support/hpsc.
2. On the product support page, search for the desired product category. For example, Aruba 3810 Switches. The support information for the selected product category is displayed.
3. Click the **Manuals** tab.
4. Click **view all**. The list of documents published for the selected product category is displayed.
5. From the list, click the required document.