

AOS 10.x User Guide



a Hewlett Packard
Enterprise company

Copyright Information

© Copyright 2021 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 Document	1
Intended Audience	1
Related Documents	1
Conventions	1
Contacting Support	2
About AOS 10.x	3
Campus Architecture with Devices Running AOS 10.x	3
About Aruba Central and Network Operations App	5
AOS 10.x Terminology	5
Getting Started with the Deployment	12
AOS 10.x Subscriptions	12
Getting Started with AOS 10.x Workflow	13
Getting Started with AOS 10.x Flowchart	14
Creating an Aruba Central Account	14
Onboarding Devices	19
Assigning Subscriptions	23
Assigning Devices to Sites	27
Assigning Labels	28
Creating a Group	28
Assigning Gateways to a Group	29
Assigning APs to a Group	29
Connecting Aruba APs to Aruba Central	30
Connecting Aruba Gateways to Aruba Central	30
Viewing Configuration Status	31
Viewing the Configuration Audit Page	32
Applying Configuration Changes	32
Viewing Configuration Overrides and Errors	34
Bridge Mode Deployment	42
AP Configuration and Client Connection Workflow	43
Bridge Mode Deployment Workflow	43
Bridge Mode Deployment Flowchart	44
Configuring a WLAN SSID Profile in Bridge Mode	45
Configuring VLANs for a WLAN SSID Profile in Bridge Mode	46
Configuring Security for a WLAN SSID Profile in Bridge Mode	47
Configuring Access Rules and Roles for WLAN Clients in Bridge Mode	68
Viewing Network Summary for a WLAN SSID Profile in Bridge Mode	71
Gateway Cluster and Tunnel Orchestration	73
Types of Gateway Clusters	73
Features of Gateway Clusters	74
Gateway Cluster Architecture	76
Gateway Cluster Deployment	78
Gateway Cluster Configuration Modes	80
Cluster Group Mode	80
Cluster Configuration Mode	82
Configuring Automatic and Manual Clusters in the Same Group	83

Deleting a Gateway from a Cluster	84
Deleting Cluster Profile	84
Monitoring Gateway Clusters	85
Configuring Authentication Survivability on a Gateway Cluster	85
Tunnel Orchestration for WLAN Deployments	86
Configuring Aruba Gateways for Campus WLAN Deployment	92
Tunnel and Mixed Mode Deployment	93
Network Setup for Tunnel and Mixed Mode Deployment	94
Tunnel and Mixed Mode Deployment Workflow	95
MultiZone	97
Guidelines for MultiZone	98
Creating a WLAN Profile in Tunnel and Mixed Mode	99
Configuring VLAN Settings for WLAN SSID Profile in Tunnel and Mixed Mode	99
Important Points to Note	100
Configuring a Security for a WLAN SSID Profile in Tunnel and Mixed Mode	100
Configuring External Authentication Servers in the SSID Security Profile	101
Configuring Access Rule for a WLAN SSID Profile in Tunnel and Mixed Mode	103
Viewing Network Summary of Tunnel and Mixed Mode	106
User-Based Tunneling in Dynamic Segmentation	106
Configuring VLANs on Aruba Gateways	109
Configuring User Roles	110
Micro Branch Deployment	113
WLAN Tunnel Orchestration for Micro Branch Deployments	113
Micro Branch Deployment Workflow	114
Micro Branch Deployment Flowchart	114
Enabling Micro Branch on the AP Group	115
Configuring WLAN SSID Settings for Micro Branch Deployments	116
Configuring External Authentication Servers in an SSID Security Profile	132
Configuring Traffic Forwarding for Micro Branch APs	136
Verifying Micro Branch Configuration	137
Configuring APs	138
Viewing AP Configuration Options	138
Deploying a Wireless Network Using APs	139
Configuring a Captive Portal Splash Page	165
Configuring New External Captive Portal Profile	169
Containment Methods	194
Protection Against Wired Attacks	194
Configuring 802.1X Authentication for a Network Profile	195
Configuring MAC Authentication for a Network Profile	196
Enabling Multiple PSK for Wireless Networks	203
Creating an MPSK Local Profile	204
Editing an MPSK Local Profile	205
Deleting an MPSK Local Profile	205
Enabling MPSK Local for Wireless Networks	205
Configuring a Wired Server with the IP Address	209
Configuring a Wired Server with the MAC Address	209
Important Points to Note	213
Creating a User Role	218
Creating a Role Derivation Rule	220

Configuring VLAN Assignment Rule	220
Configuring VLAN Derivation Rules	221
Configuring Management Subnets	224
Configuring Restricted Access to Corporate Network	225
Creating a List of Error Page URLs	225
Configuring ACL Rules to Redirect Users to a Specific URL	225
Configuring Restricted Access to Corporate Network	228
Creating a CALEA Profile	247
Creating ACLs for CALEA Server Support	247
Configuring an AP for Network Integration	248
Switching Uplinks Based on VPN Status	274
Switching Uplinks Based on Internet Availability	274
Group Management for AOS 10.x	276
Important Points to Remember	276
Converting a Group to AOS 10.x	276
Converting to AOS 10.x in MSP Mode	276
AirMatch	279
RF Optimization	279
Monitoring Radios in Summary View	280
Monitoring Radios in List View	283
Dual 5 GHz Radio Mode	285
Support for Automatic Dual 5 GHz Radio Mode	286
Guest Access	288
Guest Access Dashboard	288
Creating Apps for Social Login	289
Configuring a Cloud Guest Splash Page Profile	291
Configuring Visitor Accounts	300
AirGroup	303
AirGroup Changes	303
AirGroup Licensing	304
AirGroup Features	304
AirGroup Services	304
AirGroup Limitations	305
Enabling AirGroup	305
Configuring AirGroup Services	305
Monitoring AirGroup	306
Troubleshooting AirGroup	308
IoT Operations	316
Configuring IoT Operations	316
Creating an IoT Connector	316
Configuring AP	318
Configuring Transport Profile	318
Monitoring IoT	320
Unified Communications	322
Licensing	322
Heuristics Classification	322
Protocols	323
Limitations	323

Subscribing to Unified Communications	323
Enabling Unified Communications	324
Monitoring Unified Communications	325
WebRTC Prioritization	328
Troubleshooting Unified Communications	328

The AI Insights Dashboard 333

Insights Context	335
Cards	341
Baselines	343
Access Points with Excessive Number of Channel Changes	344
Access Points with High Number of Reboots	346
Access Point with High CPU Utilization	347
Access Points Impacted by High 2.4 GHz Usage	348
Access Points Radios with Frequent Transmit Power Changes	351
Access Point Transmit Power can be Optimized	352
Access Points Impacted by High 5 GHz Usage	353
Access Points with High Memory Usage	356
Clients with High Roaming Latency	357
Clients with Low SNR Minutes	359
Clients with High Number of MAC authentication Failures	362
Clients with DHCP Server Connection Problems	364
Clients with High Number of Wi-Fi Association Failures	366
Clients with High Wi-Fi Security Key-Exchange Failures	367
Clients with High 802.1X Authentication Failures	369
Clients with Captive Portal Authentication Problems	371
Clients who Roamed Excessively	373
Coverage Holes Identified	375
Dual-band (2.4/5 GHz) Clients Primarily using 2.4 GHz	376
Delayed DNS Request or Response	378
DNS Servers Rejected High Number of Queries	380
Gateways with High CPU Utilization	382
Gateways with High Memory Usage	383
Failure to Establish Gateway Tunnels	385
DNS Queries Failed to Reach or Return from the Server	387
Telemetry Information not Received from APs or Radios	389
Outdoor Clients Impacting Wi-Fi Performance	390

Monitoring Gateway Clusters 393

Monitoring Gateways in List View	393
Monitoring Gateways in Summary View	394
Monitoring Gateway Clusters	395
Gateway Cluster > Overview > Summary	396
Gateways Cluster > Overview > Gateways	397
Gateway Cluster > Overview > Tunnels	398

Monitoring APs 400

Monitoring APs in Summary View	400
Monitoring APs in List View	401
Access Point > Overview > Summary	407
Viewing the Overview > Summary Tab	407
Actions	412
Go Live	412
Access Point > Overview > AI Insights	412
Access Point > Overview > Floor Plan	413
Access Point > Overview > Performance	414

Access Point > Overview > RF	415
Access Point > Security > VPN	416
Rebooting an AP	417
Tech Support for an AP	417
Opening a Remote Console	418
Enabling Live AP Monitoring	418
AP Live Events	419
Monitoring Clients	421
All Clients Monitoring in List View	421
All Clients Monitoring in Summary View	427
Dashboard for Wireless Clients	430
Dashboard for Wired Clients	440
Viewing Applications Monitored by AirSlice	445
Monitoring the Overall Network	448
Monitoring Network Health	448
Monitoring WAN Health	449
Monitoring Network Summary	451
About Floorplans	452
Manage > Applications > Visibility	458
Graph View in Websites Section	459
RAPIDS	460
Monitoring Sites in the Topology Tab	465
Analyzing AOS 10.x	479
Alerts & Events	479
Configuring Dynamic Logs	484
Device Licensing for Dynamic Logs	485
Viewing the Dynamic Logs Notifications	485
Filtering Events at an Advanced Level	485
Viewing Audit Trail	504
Using Troubleshooting Tools	504
Important Points to Note	508
Important Points to Note	508
Important Point to Note	509
Reports	528
Managing Software Upgrades	539
Provisioning Devices using Configuration Templates	554
Creating a Group with Template-Based Configuration Method	554
Forming Tunnels Manually	554
Editing a Template	556
Configuring APs Using Templates	556
Provisioning Gateways Using Configuration Templates	563
Configuring Gateways Using a Template	564
Supported Devices for AOS 10.x	574
Supported Aruba APs	574
Supported Aruba Gateways	574
Supported Switch Platforms	575
AOS 10.x Command-Line Interface	577
Navigating to the Commands page	577

Filtering Information	577
FAQs	617
Navigation	617
How do I view the details of an AP?	617
How do I configure an AP?	617
How do I view the details of a Gateway?	617
How do I configure a Gateway?	617
How do I access the global dashboard?	617
How do I view the overall network summary?	618
How do I view AI Insights?	618
How do I view network health?	618
How do I access the VisualRF dashboard?	618
How do I view client details?	618
How do I create a group?	619
How do I create a template group?	619
How do I view the Visibility dashboard?	619
Network Profile	620
What is an SSID?	620
What are the deployment modes supported?	620
What is a Bridge mode deployment ?	620
What is a Tunnel mode deployment?	620
What is a Mixed mode deployment?	620
How do I create an SSID profile?	620
How is user authentication performed ?	621
What is the basic requirement to set up Tunnel and Mixed mode?	621
How do I view the configurations of an already existing network profile?	621
What is a Gateway cluster?	621
What are the types of clusters supported for Gateways?	621
What are the Gateway cluster configuration methods supported in the AOS 10.x?	621
How do I monitor the Gateway clusters?	622
What is Dynamic Segmentation?	622
What is User-Based Tunneling ?	622
What is Tunnel Orchestrator for LAN Tunnels	622
How to enable automatic Gateway cluster configuration ?	622
What is a Micro Branch Deployment ?	622
How many APs can you deploy in a Micro Branch deployment?	623
What are the traffic forwarding modes currently supported for Micro Branch deployments?	623
How do I enable the Micro Branch setting on an AP group?	623
How do I verify the Micro Branch configuration on an AP?	623
Security	623
What is a Rogue AP?	623
What is Security?	624
How does Security determine classification?	624
How do I locate a rogue device to remove it from my network?	624
What is VisualRF?	624
What user role is needed to view the Rogue APs and interfering devices?	624
What are the available classification for Rogue APs?	624
How can we generate alerts and reports for Security?	624
Tools	624
What type of troubleshooting can be performed under Tools?	624
What user role is needed to perform troubleshooting?	625
Alerts and Events	625
What does the Alert & Events pane displays?	625
What are the alert severity levels displayed?	625
What does Acknowledged Alerts mean?	625

What does the WIDS Events table displays?	625
AirMatch	626
What is RF optimization?	626
How do I optimize the radio frequencies?	626
How do I monitor my Access Points using the Radio Monitoring Dashboard?	626
List the uses of Radio Resource Management.	626
Applications	627
How do I enable AirGroup?	627
How do I enable call prioritization?	627
Clients	627
How do I view wireless clients in my network?	627
How do I live monitor clients?	627
How do I disconnect a wireless client from an AP?	627
How can I troubleshoot a client in real time?	628

This user guide describes AOS 10.x and provides detailed instructions for setting up, configuring, and managing all supported deployments.

Intended Audience

This guide is intended for network administrators who administer and manage WLANs in a campus or branch network.

Related Documents

In addition to this document, see the following:

- Aruba Central *Help Center* at https://help.central.arubanetworks.com/latest/documentation/online_help/content/home.htm.
- *AOS 10.x Release Notes*
- *AOS 10.x User Guide*

Conventions

[Table 1](#) lists the typographical conventions 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.

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

Campus Architecture with Devices Running AOS 10.x	3
About Aruba Central and Network Operations App	5
AOS 10.x Terminology	5

A **campus network** refers to a proprietary local area network (LAN) or a set of interconnected LANs serving a corporation, government agency, university, or a similar organization. A typical campus network encompasses a set of buildings in close proximity with a large number of Wi-Fi-connected clients and applications deployed in public, private, and hybrid clouds. A **branch network** is generally an offshoot of the campus network with a small area of operation.

In campus and branch networks, the Wireless Local Area Networks (WLANs) are critical to address the challenges of widespread user mobility, client density, and security. Over the last few years, the architecture of WLANs has evolved significantly to keep pace with the changing needs of wireless users. However, with digital transformation and applications moving to cloud, WLANs must rapidly evolve to provide seamless user experience and operational simplicity to quickly deploy, manage, and monitor networks.

To address some of these business challenges, Aruba offers APs and gateways running AOS 10.x. You can now deploy and manage your WLANs from a single and unified cloud-based network management system called Aruba Central. Devices running AOS 10.x simplifies network administration in Aruba Central with automated workflows, end-to-end visibility, AI powered insights, and analytics to enhance and optimize wireless experience for users.



AOS 10.x is currently a limited availability product from Aruba. Installing the operating system on APs and gateways requires specific pre-configuration settings that are performed by the Aruba Technical Support team.

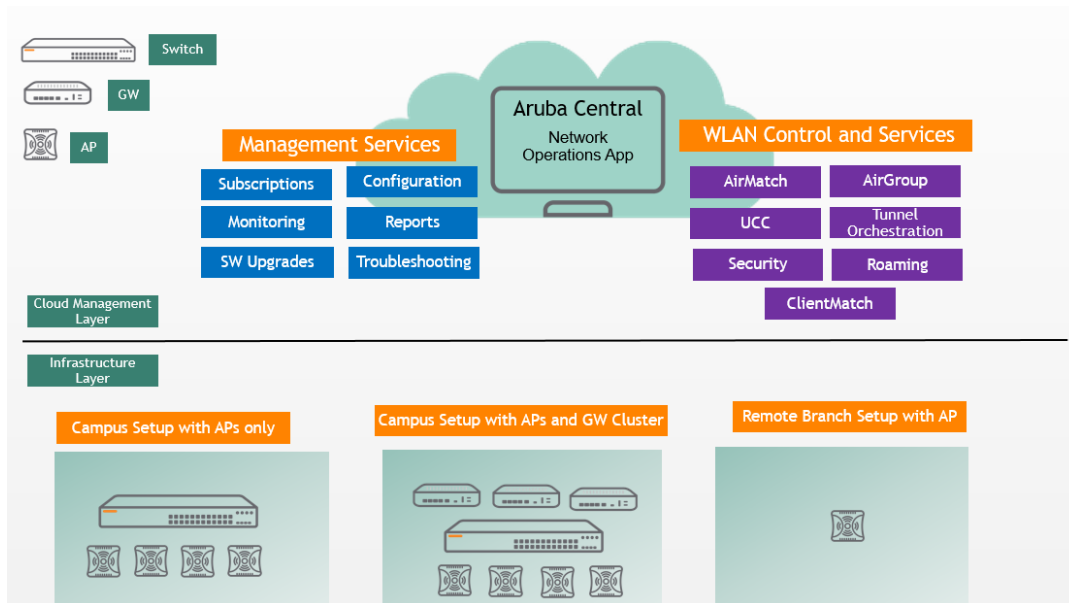
Campus Architecture with Devices Running AOS 10.x

The Aruba campus architecture consists of two layers:

- **Infrastructure layer**—The infrastructure layer consists of a WLAN setup which can be either a campus setup or a branch setup. The campus setup can consist only of access points (APs) or APs combined with gateway clusters. In case of a branch setup, the infrastructure layer includes an AP.
- **Cloud management layer**—The cloud management layer consists of Aruba Central which is a cloud management SAAS platform. The Network Operations app is one of the Aruba apps which is a part of Aruba Central and this app helps to create the SSID profiles for the different WLAN campus and branch setups.

The following figure is an architectural representation of the AOS 10.x with components displayed for both the cloud management and infrastructure layers. As shown in the figure, Aruba Central and the Network Operations app offers both management and WLAN control and services for the underlying infrastructure layer.

Figure 1 Aruba Campus Architecture and Components for Devices Running AOS 10.x



As shown in the figure, Aruba Central and the Network Operations app offers the following services for the underlying infrastructure layer:

- Management Services for managing WLAN devices—These services include the following options:
 - Onboarding
 - Configuration
 - Monitoring
 - Live Upgrades
 - Licensing
 - Troubleshooting
- WLAN Services for managing and monitoring the WLAN setup as a whole. These services include the following options:
 - **AirMatch RF Management and Optimization**—AirMatch analyzes periodic RF data across the entire network, or a subset of the network, to algorithmically derive configuration changes for every Aruba AP on the network. The APs receive regular updates based on changing environmental conditions, which benefits both IT and users. AirMatch is the enhanced version of the Adaptive Radio Management (ARM) technology. It has new automated channel optimization, transmit power adjustment and channel width tuning system that utilizes dynamic machine learning intelligence to automatically generate the optimal view of the entire WLAN network.
 - **UCC**—The Unified Communications application on Aruba devices provides a seamless user experience for voice calls, video calls, and application sharing when using communication and collaboration tools. The Unified Communications application actively monitors voice, video, and application sharing sessions, provides traffic visibility and allows you to prioritize the sessions. The Unified Communications application also leverages the functions of the Service Engine on the cloud platform and provides rich visual metrics for analytical purposes.
 - **ClientMatch**—ClientMatch continually monitors the RF neighborhood of the client to support the ongoing band steering and load balancing of channels, and enhanced reassignment for roaming mobile clients. The ClientMatch service helps to improve the experience of wireless clients. ClientMatch identifies wireless clients that are not getting the required level of service at the AP to which they are currently associated and intelligently steers them to an AP radio that can provide better service and thereby improves user

experience. ClientMatch periodically checks the health of current association of the clients and determines if a sticky steer or band steer should be considered.

- **AirGroup**—AirGroup capabilities are available as a feature in Aruba WLANs where Wi-Fi data is distributed among APs. AirGroup is a unique enterprise-class capability that leverages zero configuration networking to enable Bonjour® services like Apple® AirPrint and AirPlay from mobile devices in an efficient manner. Bonjour, the trade name for the zeroconf implementation introduced by Apple, is the most common example. Apple AirPlay and AirPrint services are based on the Bonjour protocol are essential services in campus Wi-Fi networks.
- **Cloud-Assisted Roaming Services**—The Cloud-Assisted Roaming Services feature supports 802.11r fast transition and Opportunistic Key Caching (OKC), to enable seamless roaming with minimal or no disruption to the application traffic such as voice and video.
- **Rogues and Intrusion Detection** —With Rogues and Intrusion Detection, you can quickly identify and act on a rogue or interfering device that can be later considered for investigation, restrictive action, or both. After rogue devices are discovered, Aruba Central sends alerts to your network administrators about the possible threat and provides essential information needed to locate and manage the threat.
- **Tunnel Orchestrator**— Gateways running AOS 10.x form clusters in both homogeneous and heterogeneous modes. The IPsec between the AP and the Gateway cluster is orchestrated by the WLAN Tunnel Orchestration service. Even if one Gateway joins the deployment, an automatic cluster is formed by this service.

About Aruba Central and Network Operations App

The management layer in the Aruba campus architecture with devices running AOS 10.x is called Aruba Central a SAAS . The Aruba Central platform can run on public, private, or hybrid clouds. AOS 10.x devices Aruba Central to provision, configure, monitor, and troubleshoot the WLAN setup.

Aruba Central enables the onboarding of devices to the infrastructure layer. Along with device and network management functions, the SAAS platform also provides value-added services such as customized guest access, client presence, service assurance analytics and a number of apps for more network services. The **Network Operations** app is one such app that is used to create the SSID workflows for AOS 10.x APs and to monitor the infrastructure layer.

AOS 10.x Terminology

Before getting started with configuring AOS 10.x, it is important to understand some important configuration concepts and terminology. The following topics are discussed in this section:

- **SSIDs**—Wireless networks are identified using a service set identifier (SSID). The SSIDs distinguish a wireless network from other networks configured within a WLAN boundary. Aruba uses the SSIDs of APs to orchestrate and configure a number of management policies.
For more information, see [WLAN SSIDs on APs](#).
- **Traffic Forwarding Modes**—Depending on the type of WLAN setup, the SSIDs are also used to specify the traffic forwarding modes. AOS 10.x supports automated workflows to set up these SSID profiles.
For more information, see [Traffic Forwarding Modes](#).
- **Supported Authentication Methods**—In creating the SSID profiles in the automated workflows, you must specify
 - an authentication method. AOS 10.x supports a number of authentication methods and each is recommended for a specific deployment type.
For more information, see [Authentication Methods](#).

- **Supported Encryption Methods**—In creating the SSID profiles in the automated workflows, you must specify an encryption method. AOS 10.x supports a number of encryption methods and each is recommended for a specific deployment type.
For more information, see [Encryption Methods](#).
- **Cloud-Assisted Roaming Services**—The Cloud-Assisted Roaming Services feature facilitates fast roaming of 802.11r and Opportunistic Key Caching (OKC) clients, to enable seamless roaming with minimal or no disruption to the application traffic such as voice and video.
For more information, see [Cloud-Assisted Roaming Services](#).
- **Access Rules and Firewall Policies**—The Access Control List (ACL) is a logic that handles stateless inspection of traffic. An ACL is used in many types of implementations including routing policies and user policies. A firewall is a device that performs stateful inspection of traffic (checks for encapsulation) passing through a part of the network and decides whether to allow or deny the traffic. You can configure both ACLs and firewall policies on APs and Gateways.
For more information, see [Access Rules and Firewall Policies](#).
- **User Roles and VLANs**—A client connecting to a WLAN SSID that is broadcast by an AP is assigned a user role or VLAN to define the client's network privileges, the frequency of re-authentication, and the applicable bandwidth contracts.
For more information, see [User Roles and VLANs](#).
- **Supported Device Configuration Methods in Aruba Central**—In order to configure the management layer, Aruba Central supports a number of configuration options that includes UI workflows, templates, and APIs.
For more information, see [Device Configuration Methods in Aruba Central](#).

WLAN SSIDs on APs

An SSID profile on access points (APs) allows administrators to define the following elements:

- Type of WLAN and its intended users; for example, employee, guest, or voice WLAN.
- IP address assignment criteria to clients; for example, the method of assigning IP address to the clients that connect to a WLAN.
- Forwarding modes for managing client traffic.
- Security profiles for authentication of clients and encryption of client traffic.
- Firewall policies and user roles for user access control.

Traffic Forwarding Modes

AOS 10.x APs support the following deployments based on the infrastructure layer components and how traffic is managed:

- **Bridge mode**—For LAN setups, the user traffic can either be bridged locally or tunneled to a Gateway cluster for redundancy and failover. Accordingly, if the traffic is bridged locally, the infrastructure layer requires only APs. To configure AOS 10.x APs for such a deployment, you must configure the SSID in **Bridge mode**. In the **Bridge mode**, APs function as bridges between the wireless interface and the wired network deployed at a site. For example, a wireless laptop can use a bridge-mode SSID to discover network printers within the same VLAN. In the bridge mode, clients can obtain IP addresses from the access point (AP) or an external DHCP server based on the SSID specification. For more information on configuring AOS 10.x APs in a LAN setup in **Bridge mode**, see [Bridge Mode Deployment](#).
- **Tunnel mode**—For LAN setups, where user traffic is tunneled to a gateway cluster, the infrastructure layer requires at least one Gateway in additions to the APs. A Gateway cluster is automatically formed for such AOS 10.x deployments and the cluster functions as a tunnel endpoint. To configure AOS 10.x APs for such a deployment, you must configure the SSID in **Tunnel mode**.

In the **Tunnel mode**, APs set up a secure mobility tunnel for clients that roam between the VLANs. The client traffic is encapsulated and routed to a tunnel endpoint. The tunnel-mode SSID allows a client device to maintain a consistent IP address and experience uninterrupted access when roaming across VLANs.

AOS 10.x employs the Decrypt-Tunnel-Mode or the D-tunnel decrypt mode in which the traffic between the AP and the Gateway is encrypted and then decrypted at the AP level. Hence, the AP performs encryption and decryption in addition to being a bridge between the clients and the Gateways.

For more information on configuring AOS 10.x APs in a LAN setup in Tunnel mode, see [Tunnel and Mixed Mode Deployment](#).

- **Mixed mode**—Apart from **Bridge mode** and **Tunnel mode**, in specific deployments some user VLANs are on an AP uplink, while the other user VLANs are on Gateway clusters.

Based on the user VLAN, the client traffic is either locally bridged or tunneled to the Gateway cluster mapped to the SSID. Similarly, clients are assigned an IP address from a DHCP server based on the VLAN from which a connection request is initiated. This type of deployment is called a **Mixed mode** deployment. In **Mixed mode**, APs can intelligently determine if client traffic must be bridged or tunneled based on the client VLAN.

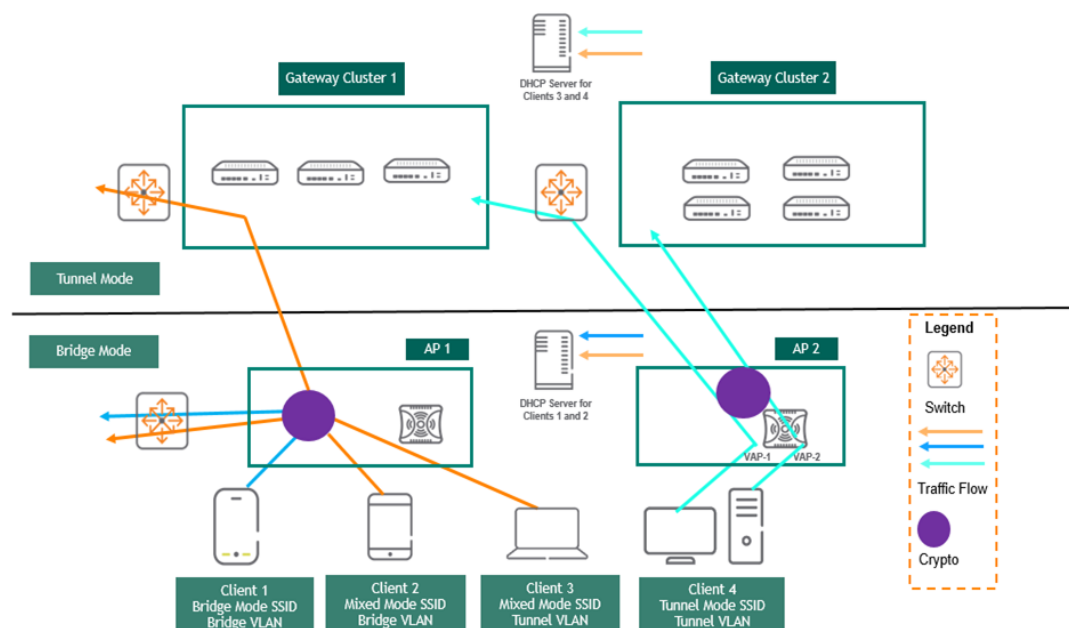
AOS 10.x employs the Decrypt-Tunnel-Mode or the D-tunnel decrypt mode in which the traffic between the AP and the Gateway is encrypted and then decrypted at the AP level. Hence, the AP performs encryption and decryption in addition to being a bridge between the clients and the Gateways.

For more information on configuring AOS 10.x APs in a WAN setup in mixed mode, see [Tunnel and Mixed Mode Deployment](#).

- **Micro Branch mode**—For WAN setups, traffic is bridged through IPsec tunnels to a Gateway cluster. At the remote location, the infrastructure layer requires a minimum of one AP. To configure such a deployment, you must configure AOS 10.x APs in **Micro Branch mode**. For more information, see [Micro Branch Deployment](#).

The following figure illustrates the SSIDs with **Bridge**, **Tunnel**, and **Mixed** traffic forwarding modes:

Figure 2 SSID Configuration



The above figure shows three SSIDs (in blue, orange, and green) with a client connected to each of these SSIDs. These SSIDs represent different SSID configuration and traffic forwarding modes:

- **Blue**—The blue line represents an SSID in the bridge forwarding mode. As illustrated in the above figure, the client traffic is bridged locally in this SSID and security policies including firewall, QoS, bandwidth contract are

applied to the client traffic by the AP. Each AP acts as an authenticator with the AP IP address configured as a Network Access Server (NAS) IP in the RADIUS authentication server profiles.

- **Orange**—The orange line represents an SSID with the mixed forwarding mode. This SSID requires a deployment topology with a Gateway cluster in addition to the APs. The above figure shows Client 2 connected to bridge mode SSID and client 3 connected to tunnel mode SSID to illustrate that both bridge mode and tunnel mode clients can co-exist in the same SSID. Based on the VLANs to which the client is assigned, the client traffic is bridged locally or forwarded to Gateway through a secure tunnel. The AP acts as an authenticator and also applies firewall policies on the tunneled traffic.

In the mixed forwarding mode, Captive Portal can be configured on the AP, while QoS, Firewall, Bandwidth Contract, and WAN policies can be applied on Gateway. In mixed mode, both bridged and tunneled users are authenticated through the AP. The Gateway IP address is configured as the NAS IP even for bridged users.

- **Green**—The green line represents an SSID with the tunnel forwarding mode. This SSID requires a deployment topology with a Gateway cluster in addition to the APs. As shown in the above figure, the client traffic is tunneled to the Gateway through different virtual APs. The Gateway receives 802.3 packets already decrypted by the AP. The AP acts as an authenticator while the Gateway acts as authentication proxy. The MultiZone feature segregates the tunnel traffic of VAP-1 and VAP-2 and forwards the traffic to different Gateways under Gateway Cluster 1 and Gateway Cluster 2.

Authentication Methods

When configuring a WLAN SSIDs on APs, you can configure a number of supported authentication types for WLAN clients. These authentication methods can be configured for all traffic modes and are described in the following section:

- **802.1X Authentication**—802.1X authentication method authenticates the identity of a user before providing network access to the user. APs support external RADIUS servers for 802.1X authentication. For authentication purpose, the wireless client can associate to a NAS or RADIUS client. NAS acts as a gateway to guard access to a protected resource. A client connecting to a SSID connects to the NAS first; therefore, based on the SSID specification, the APs or the Gateways can be configured as NAS clients to a RADIUS server to provide secure access to WLAN clients.
- **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. However, MAC authentication can be combined with other forms of authentication such as WEP authentication or 802.1X authentication for additional security.
- **MAC Authentication with 802.1X Authentication**—The administrators can enable MAC authentication for 802.1X authentication. If a wireless or wired client connects to the network, MAC authentication is performed first. After a successful 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.
- **Captive Portal Authentication**—Captive portal authentication is used for authenticating guest users. If the captive portal authentication profile is configured on an SSID and the guest users connect to this SSID for the Internet access, a web page with the usage policy and terms is presented to the guest users before providing access to the network. The SSID administrators can also enable authentication of guest users using an external server on cloud or outside the WLAN domain.
- **Walled Garden**—When captive portal authentication is configured on an SSID, the administrators can configure Walled garden access to allow clients to view websites in a specific domain without connecting to the Internet. For example, in a hotel environment, clients can view to a designated login page (for example, a hotel website) and all its contents before connecting to the Internet. When clients try to access other websites that are not allowlisted for walled garden access, they are redirected to the login page for authentication.

Aruba APs support 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.

Encryption Methods

Aruba APs support SSIDs with the following types of encryption:

- **WPA-Enterprise and WPA-Personal**—WLAN SSIDs support security profiles with WPA for enterprise or the personal network users. WPA supports TKIP (Temporal Key Integrity Protocol), which supports a unique encryption key for each wireless frame to provide a secure connection.
- **WPA2-Enterprise and WPA-Personal**—The WPA2-Enterprise encryption uses authentication standards such as 802.1X along with other WPA2 features such as AES. WPA2-Enterprise encryption provides a secure wireless network for enterprise use. For personal wireless network, the WPA-Personal encryption type can be used along with a pre-shared key.
- **WPA3-Enterprise and WPA3-Personal**—The WPA3 encryption provides robust protection with unique encryption per user session and thus allows the SSID administrators to provide a highly secured connection even on a public Wi-Fi hotspot. WPA3-Enterprise encryption can be used to provide secure wireless network for enterprise, whereas the WPA-Personal encryption with a pre-shared key can be configured for a personal network.
- **Dynamic WEP**—Dynamic WEP encryption method combines of 802.1X authentication standard and the Extensible Authentication Protocol (EAP). With Dynamic WEP security, WEP keys are changed dynamically.
- **MPSK-AES**—Multi-Pre-Shared Key (MPSK) supports multiple PSKs simultaneously on a single SSID. MPSK-AES is supported only when Aruba ClearPass Policy Manager is configured as an authentication server on the WLAN SSID.
- **MPSK-Local**—MPSK Local supports 24 pre-shared keys per SSID without an external policy engine like ClearPass Policy Manager.

Cloud-Assisted Roaming Services

The Cloud-Assisted Roaming Services feature supports 802.11r fast transition and Opportunistic Key Caching (OKC), to enable seamless roaming with minimal or no disruption to the application traffic such as voice and video. When a client roams from one access point (AP) to another, Cloud-Assisted Roaming Services ensures that the client's wireless connection is seamless without a need for re-authentication. This feature is dependent on AirMatch to obtain the AP RF neighborhood information. It maintains a table of client key records which is updated by APs, and is propagated to neighboring APs.

The Cloud-Assisted Roaming Services feature provides seamless roaming in the following two scenarios:

- In the OKC based roaming, the AP stores one Pairwise Master Key (PMK) per client, which is derived from last 802.1x authentication completed by the client in the network. The cached PMK is used when a client roams to a new AP. This allows faster roaming of clients between the APs in a cluster, without requiring a complete 802.1X authentication.
- In case of 802.11r clients, the Cloud-Assisted Roaming Services feature is used for secure distribution of PMK-R1 to neighboring APs in Bridge-mode APs, and D-Tunnel modes where the AP acts as authenticator.

The Cloud-Assisted Roaming Services feature is enabled automatically. However, you must connect 802.11r client to 802.11r enabled SSID and OKC client to OKC enabled SSID. You can enable 802.11r and OKC in the following opmodes in the WebUI:

- WPA2-AES (802.1x), WPA2-PSK-AES (PSK), and MPSK-AES (PPSK) for 802.11r
- WPA2-AES (802.1x) for OKC

For more information on enabling the 802.11r and OKC clients in the SSID profile, see [Configuring Security for a WLAN SSID Profile in Bridge Mode](#).

Access Rules and Firewall Policies

Aruba access points (APs) and Gateways support identity-based controls to enforce application-layer security, traffic prioritization and forwarding, and network performance policies for WLAN and WAN clients.

You can configure firewall policies on the AP or Gateway cluster to define user access to network, set a priority queue for Quality of Service (QoS), and assign bandwidth contracts.

A firewall policy identifies specific characteristics about a data packet and performs one of the following actions:

- Firewall action such as permitting or denying the packets.
- Administrative action such as logging the packets.
- The QoS action such as placing packets in a priority queue.

You can configure the following types of ACLs on APs and Gateways.

- **Standard ACL**—Permits or denies traffic based on the source IP address of the packet. Standard ACLs use a bit-wise mask to specify the portion of the source IP address to be matched.
- **Extended ACLs**—Permits or denies traffic based on source or destination IP address, source or destination port number, or IP protocol.
- **MAC ACLs**—Filters traffic on a specific source MAC address or range of MAC addresses.
- **Ethertype ACLs**—Filters traffic based on the Ether type field in the frame header. Ether type ACLs can be used to permit IPs while blocking other non-IP protocols, such as IPX or AppleTalk.
- **Session ACLs**—Restricts all services from specific hosts and subnets. Rules with this ACL are applied to all traffic on the AP or Gateway regardless of the ingress port or VLAN.
- **Route ACLs**—Forwards all packets to a device defined by an IPsec map, a next hop list, a tunnel or a tunnel group.

User Roles and VLANs

A client connecting to a WLAN SSID that is broadcast by an access point (AP) is assigned a user role to define the client's network privileges, the frequency of re-authentication, and the applicable bandwidth contracts.

A client device is assigned a user role by several methods:

- **Initial user role**—The initial user role or VLAN assigned for the unauthenticated clients.
- **User-derived role**—The user role can be derived from user attributes when a client connects to an AP. You can configure access rules for a user role and assign it to the clients when they match the criteria defined in the user role. For example, you can configure a rule to assign the role **VoIP-Phone** to any client that has a MAC address that starts with xx:yy:zz. The user-derived roles are applied before client authentication.
- **Default user role**—The default user role configured for an authentication method, such as 802.1X or VPN. You can configure a default role for the clients that successfully authenticate based on the specified authentication method in the SSID.
- **Server-derived role**—The user role can be derived from attributes returned by the authentication server. If the client authenticates to an authentication server, the user role for the client can be based on one or more attributes returned by the server during authentication. Server-derived roles are assigned after clients complete the authentication.
- **VSA-Derived Role**—Many NAS vendors, including Aruba, use vendor-specific attributes to provide features that are not supported in standard RADIUS attributes. The Aruba VSAs allow deriving user roles and VLAN for the clients that authenticate to the RADIUS server. A role derived from a VSA takes precedence over other types of user roles.

Device Configuration Methods in Aruba Central

Aruba Central offers the following options for configuring devices in your account:

- **Groups**—You can use the Groups feature to create a logical subset of devices. If you have devices that must share common configuration settings, ensure that you assign these devices to the same group. Any new device joining a group inherits the configuration that is already applied on the devices in a group.
- **Device-specific configuration**—If you have fewer devices that do not have the same configuration requirements, you can apply configuration changes at the device level. In some cases, although the devices are assigned to a group, you may want to have a slightly different configuration on one specific device in a group. In such cases, you can modify the device configuration and apply changes at the device level.
- **Configuration templates**—You can also leverage the configuration templates feature to quickly deploy. To use a template-based configuration method for APs, ensure that you enable the template-based configuration mode when creating AP groups.

AOS 10.x Subscriptions	12
Getting Started with AOS 10.x Workflow	13
Getting Started with AOS 10.x Flowchart	14
Creating an Aruba Central Account	14
Onboarding Devices	19
Assigning Subscriptions	23
Assigning Devices to Sites	27
Assigning Labels	28
Creating a Group	28
Assigning Gateways to a Group	29
Assigning APs to a Group	29
Connecting Aruba APs to Aruba Central	30
Connecting Aruba Gateways to Aruba Central	30
Viewing Configuration Status	31
Viewing the Configuration Audit Page	32
Applying Configuration Changes	32
Viewing Configuration Overrides and Errors	34

- [Provisioning Workflow](#)
- [Flowchart for Provisioning Aruba Unified Network Architecture](#)

Ensure that the APs and Gateways (where applicable) used are running ArubaOS version 10.x and were not a part of any Aruba Central configuration. In case a device is running the factory default image of ArubaOS version 6.x or ArubaOS version 8.x, ensure that the device is upgraded to ArubaOS version 10.x either manually or as part of the Aruba Central compliance.

Make sure you go through these following topics before you proceed with the provisioning workflow:

- [Decide on the deployment mode \(Bridge, Tunnel, Mixed, or Micro Branch\)](#)
- [Check the compatibility matrix for your Aruba APs and Gateways](#)
- [AOS 10.x Subscriptions](#)

AOS 10.x 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 Gateways already deployed in the network, you can skip the initial steps and navigate to the configuration procedures.



Aruba Central 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.

Getting Started with AOS 10.x Workflow

The provisioning workflow for AOS 10.x deployments includes the following steps:

1. Step 1: Create an Aruba Central Account

Whether you are planning to evaluate or purchase the solution, you must sign up for an account as the first step towards deploying the solution. You can access the sign up page from the www.arubanetworks.com website.

For more information on signing up for Aruba Central, selecting the appropriate URL for the zone that you are in, and then selecting the required apps, see [Creating an Aruba Central Account](#).

2. Step 2: Onboard Devices to Aruba Central

After you have access to Aruba Central, you must ensure that all your devices are added to the software. If you are an evaluating user, you must add the devices manually. If you are a paid user, the devices are added automatically. If in case the devices are not being added automatically, there are a number of processes to add the devices to Aruba Central.

For more information on adding devices to Aruba Central, see [Onboarding Devices](#).

3. Step 3: Assign Subscriptions

Aruba Central offers three types of subscriptions: devices, network services, and gateway subscriptions. Depending on the type of deployment, you have to select one or all of the subscriptions to manage your devices and add-on network services.

For more information on assigning subscriptions, see [Assigning Subscriptions](#).

4. Step 4: Create Groups

Aruba Central 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.

For more information on creating groups for your solution, see [Creating a Group](#).

5. Step 5: Assign Gateways to Groups

Gateways are used in the tunnel mode topology of deployments. In the tunnel mode topology, APs forward user traffic to a Gateway cluster through a secure tunnel. Gateways running ArubaOS 10.0.0.0 can form a cluster automatically when they are assigned to an UI group.

For more information on assigning Aruba Gateways to a group, see [Assigning Gateways to a Group](#).

6. Step 6: Assign APs to Groups

Whether you are planning to evaluate or purchase the solution, you must sign up for an account as the first step towards deploying the solution. You can access the sign up page from the www.arubanetworks.com website.

For more information on signing up for Aruba Central, selecting the appropriate URL for the zone that you are in, and then selecting the required apps, see [Assigning APs to a Group](#).

7. Step 7: Connect APs to the Aruba Central Account

The APs have the ability to automatically provision themselves and connect to Aruba Central after they are powered on. The APs support zero touch provisioning (ZTP) using which devices can download their provisioning parameters from the Activate server.

For more information on provisioning APs, see [Connecting Aruba APs to Aruba Central](#).

8. Step 8: Connect Gateways to the Aruba Central Account

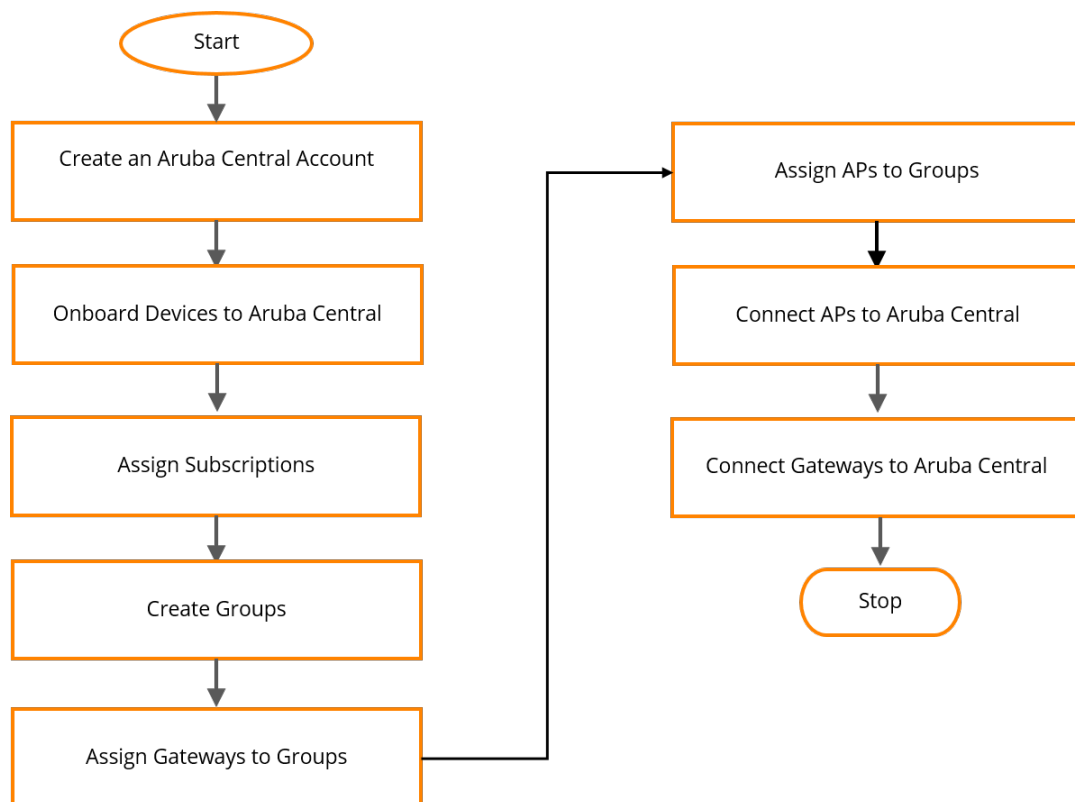
The Aruba Gateways have the ability to automatically provision themselves and connect to Aruba Central once they are powered on. The Gateways also support multiple active uplinks for ZTP (also referred to as automatic provisioning). The supported ZTP ports for different hardware platforms are listed in the following table. All these ZTP ports are assigned to VLAN 4094.

For more information on provisioning Gateways, see [Connecting Aruba Gateways to Aruba Central](#).

Getting Started with AOS 10.x Flowchart

The following figure illustrates the workflow for getting started with AOS 10.x:

Figure 3 AOS 10.x Getting Started Workflow



Creating an Aruba Central Account

To start using Aruba Central, you need to register and create an Aruba Central account. Both evaluating and paid subscribers require an account to start using Aruba Central.

Zones and Sign Up URLs

Aruba Central instances are available on multiple regional clusters. These regional clusters are referred to as zones. When you register for an Aruba Central account, Aruba creates an account for you in the zone that is mapped to the country you selected during registration.

If you access the Sign Up URL from the www.arubanetworks.com website, you are automatically redirected to the sign up URL. To create an Aruba Central account in the zone that is mapped to your country, use the following zone-specific sign up URLs.

Table 3: Sign Up URLs & Apps

Regional Cluster	Sign Up URL
US-1	https://portal.central.arubanetworks.com/signup
US-2	https://portal-prod2.central.arubanetworks.com/signup OR https://signup.central.arubanetworks.com/
China-1	https://portal.central.arubanetworks.com.cn/signup
EU-1	https://portal-eu.central.arubanetworks.com/signup
Canada-1	https://portal-ca.central.arubanetworks.com/signup
APAC-1	https://portal-apac.central.arubanetworks.com/signup
APAC-EAST1	https://portal-apaceast.central.arubanetworks.com/signup

Signing up for an Aruba Central Account

You can choose one of the following ways to start your Aruba Central account trail:

1. Go to <http://www.arubanetworks.com/products/sme/eval/>.
 - Click **Start Demo** and fill the form to start a product demo.
 - Click **Got an Aruba AP? Start your trial here**. The **Registration** page opens.
2. Enter your email address. Based on the email address you entered, the Registration page guides you to the subsequent steps:

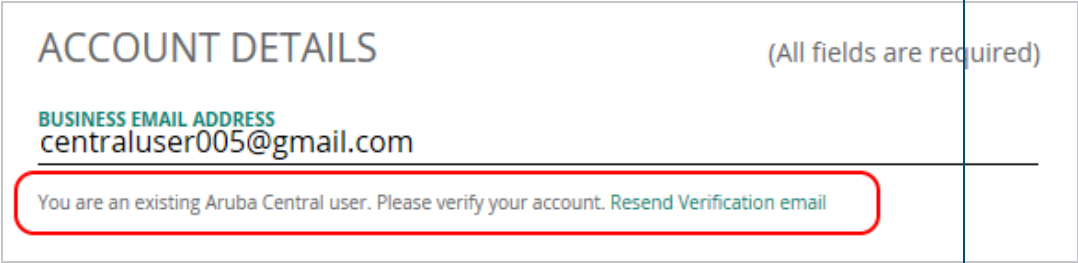
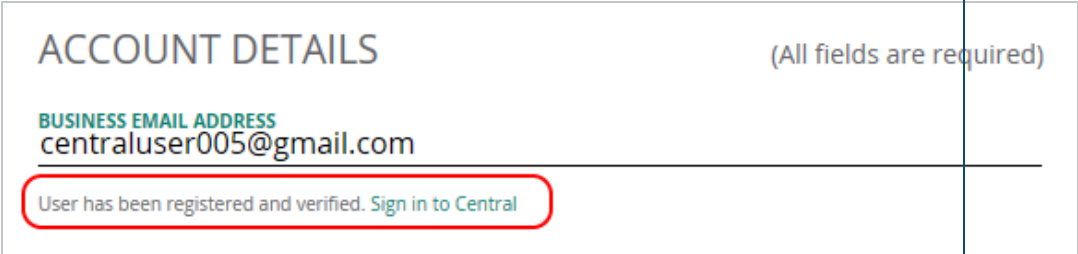

Table 4: Registration Workflow

If...	Then...
If you are a new user:	The Registration page prompts you to create a password. To continue with the registration, enter a password in the Password and Confirm Password fields.

Table 4: Registration Workflow

If...	Then...
	<div data-bbox="509 243 1581 611"> <p>ACCOUNT DETAILS (All fields are required)</p> <p>BUSINESS EMAIL ADDRESS user001@gmail.com</p> <hr/> <p>PASSWORD This field is required Use 8 or more characters with a mix of letters, numbers & symbols</p> <p>CONFIRM PASSWORD This field is required</p> </div>
<p>If you are an existing Aruba customer, but you do not have an Aruba Central account:</p>	<p>The Registration page displays the following message: Email already exists. Please enter the password below. To continue with registration, validate your account:</p> <ol style="list-style-type: none"> 1. Enter the password. 2. Click Validate Account. <p>NOTE: If you do not remember the password, click Forgot Password to reset the password.</p>
<p>If your email account is already registered with Aruba, but you do not have an Aruba Central account:</p>	<div data-bbox="509 909 1581 1304"> <p>ACCOUNT DETAILS (All fields are required)</p> <p>BUSINESS EMAIL ADDRESS kba0708+test249cl1@gmail.com</p> <hr/> <p>Email already exists. Please enter the password below.</p> <p>PASSWORD <input type="password"/></p> <p>Validate Account</p> <p>Forgot password?</p> </div>
<p>If you are invited to join as a user in an existing Aruba Central customer account:</p>	<p>The Registration page displays the following message: An invitation email has already been sent to your email ID. Resend. To continue with the registration:</p> <ol style="list-style-type: none"> 1. Go to your email box and check if you have received the email invitation. 2. If you have not received the email invitation, go to the Registration page and click Resend. A registration invitation will be sent your account. 3. Click the registration link. The user account is validated. 4. Complete the registration on the Sign Up page to sign in to Aruba Central.

Table 4: Registration Workflow

If...	Then...
<p>If you are a registered user of Aruba Central and have not verified your email yet:</p>	<p>The Registration page displays the following message: You are an existing Aruba Central user. Please verify your account. Resend Verification email. To continue:</p> <ol style="list-style-type: none"> 1. Go to your email box and check if you have received the email invitation. 2. If you have not received the email invitation, go to the Registration page and click Resend Verification email. A registration invitation will be sent your account. 3. Click the account activation link. 4. After the email verification is completed successfully, click Log in to access Aruba Central.  <p>The screenshot shows the 'ACCOUNT DETAILS' section with the business email address 'centraluser005@gmail.com'. A red box highlights the message: 'You are an existing Aruba Central user. Please verify your account. Resend Verification email'.</p>
<p>If you are already a registered user of Aruba Central and have verified your email:</p>	<p>The Registration page displays the following message: User has been registered and verified. Sign in to Central. Click Sign in to Central to skip the registration process and access the Aruba Central portal.</p>  <p>The screenshot shows the 'ACCOUNT DETAILS' section with the business email address 'centraluser005@gmail.com'. A red box highlights the message: 'User has been registered and verified. Sign in to Central'.</p>
<p>If your email address is in the arubanetworks.com or hpe.com domain:</p>	<p>The Single Sign-On option is enabled. You can use your respective Aruba or HP Enterprise credentials to log in to your Aruba Central account after the registration.</p>  <p>The screenshot shows the 'ACCOUNT DETAILS' section with the business email address 'user1@hpe.com'. A red box highlights the message: 'Single sign-on enabled'.</p>

3. To continue with registration, enter your first name, last name, company name, address, country, state, ZIP code, and phone details.

- Specify if you are an Aruba partner.
- Ensure that you select an appropriate zone. The **Registration** page displays a list of zones in which the Aruba Central servers are available for account creation. Based on the country you select, the Aruba Central server is automatically selected. If you want your account and Aruba Central data to reside on a server from another zone, you can select an Aruba Central server from the list of available servers.

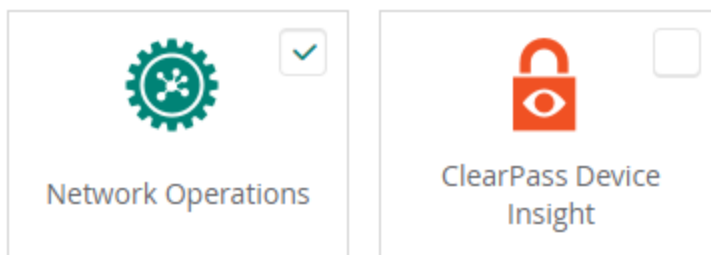
The screenshot shows a registration form with the following fields:

- ADDRESS:** Market Square, Outer Ring Road
- CITY:** Bangalore
- STATE:** Karnataka
- ZIP CODE:** 560103
- PHONE NUMBER:** +91 9240598432
- Are you an Aruba Partner?:** No (selected)
- SERVER DETAILS:** APAC-SOUTH1 (All fields are required)

A callout box points to the server details field with the text: "Based on the location you specify, the Aruba Central server is pre-selected."

- From the **Interested Apps** section, select **Network Operations**.

INTERESTED APPS



See [Table 3](#) for the app(s) available in the zone in which you are signing up.

- Select the **I agree to the Terms and Conditions** check box.
- Set a preferred mode of communication for receiving notifications about Aruba products and services.
- Optionally, to read about the the privacy statement, click the **HPE Privacy Statement** link. To opt out of marketing communication, you can either click the unsubscribe link available at the bottom of the email or click the link as shown in the following figure:

For more information on how HPE manages, uses and protects your information please refer to [HPE Privacy Statement](#). You can always withdraw or modify your consent to receive marketing communication from HPE. This can be done by using the opt-out and preference mechanism at the bottom of our email marketing communication or by following this [link](#).

10. Click **Sign Up**. Your new account is created in the zone you selected and an email invitation is sent to your email address for account activation.
11. Access your email account and click the **Activate Your Account** link. After you verify your email, you can log in to Aruba Central.

Onboarding Devices

- [Adding Devices \(Paid Subscription\)](#)
- [Manually Adding Devices](#)

Aruba Central supports the following options for adding devices.

- If you are an evaluating user, you must manually add the serial number and MAC address of the devices that you want to manage from Aruba Central. For more information, see [Adding Devices \(Evaluation Account\) on page 19](#).
- If you are a paid subscriber, Aruba Central retrieves devices associated with your purchase order from Activate. Set up a sync to import devices from the Activate database, see [Adding Devices \(Paid Subscription\) on page 19](#). For more information on Activate, see https://activate.arubanetworks.com/registration/static/help/Activate_Index.htm

Adding Devices (Evaluation Account)

Use one of the following methods to add devices to Aruba Central:

Using the Initial Setup Wizard

1. In the **Add Devices** tab of the Initial Setup wizard, click **Add Device**.
2. Enter the serial number of MAC address of your devices.
You can find the serial number and MAC address of Aruba devices on the front or back of the hardware.
3. Click **Done**.
4. Review the devices in your inventory.

Using the Device Inventory Page

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 and the MAC address of each device.
You can find the serial number and MAC address of Aruba devices on the front or back of the hardware.
4. Click **Done**.
5. Review the devices in your inventory.

Adding Devices (Paid Subscription)

If your devices are not added to your inventory, set up a device sync by adding one device from your purchase order.

To set up device sync, use one of the following methods:

In the Initial Setup Wizard

1. Ensure that you have added a subscription key and click **Next**.
2. In the **Add Devices** tab, enter the serial number and MAC address of one device from your purchase order.
Most Aruba devices have the serial number and MAC address on the front or back of the hardware.
3. Click **Add Device**. Aruba Central imports all other devices mapped to your purchase order.
4. Review the devices in your inventory.
5. Perform the following options:
 - **Add Devices Manually**—Manually add devices by entering the MAC address and serial number of each device.
 - **Add Via Mobile App**—Add devices from the Aruba Central mobile app. You can download the Aruba Central app from Apple App Store on iOS devices and Google Play Store on Android devices.
 - **Contact support**—Contact Aruba Technical Support.

From the Device Inventory Page

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.
The **Device Inventory** page is displayed.



Aruba Central

imports only devices associated with your Central account from Activate.

2. Do one of the following:
 - Click **Sync Devices**. Enter the serial number and MAC address and click **Add Device**.
 - Click **Add Devices** to manually add devices by entering the MAC address and serial number of each device.
 - To add devices using a CSV file, click **Import Via CSV** and select the CSV file to be imported. For a sample CSV file, click **Download sample CSV file**.



Manual addition of devices using a CSV file is restricted to 100 devices or to the number of available device management tokens. The UI displays an error message if more than 100 devices are imported using the Device Inventory page.

The status of the CSV upload can be viewed in the Account Home > Audit Trail page.

3. Review the devices in your inventory.
4. Perform the following options:
 - **Add Devices Manually**—Manually add devices by entering the MAC address and serial number of each device.
 - **Add Via Mobile App**—Add devices from the Aruba Central mobile app. You can download the Aruba Central app from Apple App Store on iOS devices and Google Play Store on Android devices.
 - **Contact support**—Contact Aruba Technical Support.

Manually Adding Devices

Aruba Central allows you to set up only manual sync of devices from Activate database using one of the following methods:

- [Adding Devices Using MAC address and Serial Number on page 21](#)
- [Adding Devices Using Activate Account on page 21](#)
- [Adding Devices Using Cloud Activation Key on page 22](#)

You can only set up only a manual sync for -managed folders such as the default, licensed, and non-licensed folders.

Adding Devices Using MAC address and Serial Number

You can find the serial number and MAC address of Aruba devices on the front or back of the hardware.

In the Initial Setup Wizard

If you are using the Initial Setup wizard:

1. In the **Add Devices** tab of the Initial Setup wizard.
2. Click **Add Device**.
3. Enter the serial number or MAC address of your device.
4. Click **Done**.
5. Review the list of devices.

From the Device Inventory Page

To add devices from the **Device Inventory** page:

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.
The **Device Inventory** page is displayed.
2. Do one of the following:
 - Click **Add Devices** to manually add devices by entering the MAC address and serial number of each device.
 - To add devices using a CSV file, click **Import Via CSV** and select the CSV file to be imported. For a sample CSV file, click **Download sample CSV file**.



Manual addition of devices using a CSV file is restricted to 100 devices or to the number of available device management tokens. The UI displays an error message if more than 100 devices are imported using the Device Inventory page.

The status of the CSV upload can be viewed in the Account Home > Audit Trail page.

3. Click **Done**.
4. Review the devices added to the inventory.



When you add the serial number and MAC address of one AP from a cluster or a switch stack member, imports all devices associated in the AP cluster and switch stack respectively.

Adding Devices Using Activate Account

To add devices from your Activate account:

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.
The **Device Inventory** page is displayed.
2. Click **Advanced** and select **Using Activate**.
3. Enter the username and password of your Activate account.
4. Click **Add**.
5. Review the devices added to the inventory.

Use this device addition method only when you want to migrate your inventory from Aruba or a standalone AP deployment to the management framework.



Use this option with caution as it imports all devices from your Activate account to the Aruba Central device inventory.

You can use this option only once. After the devices are added, Aruba Central does not allow you to modify or re-import the devices using your Aruba Activate credentials.

Adding Devices Using Cloud Activation Key



When you import devices using the Cloud Activation Key, all your devices from the same purchase order are added to your Aruba Central inventory.

Before adding devices using cloud activation key, ensure that you have noted the cloud activation key and MAC address of the devices to add.

Locating Cloud Activation Key and MAC Address

To know the cloud activation key:

- For APs:
 1. Log in to the WebUI or CLI.
 - If using the WebUI, go to the **Maintenance > About**.
 - If using the CLI, execute the **show about** command.
 1. Note the cloud activation key and MAC address.
 - For Aruba Switches:
 2. Log in to the switch CLI.
 3. Execute the **show system | in Base** and **show system | in Serial** commands.
 4. Note the cloud activation key and MAC address in the command output.
 - For Mobility Access Switches
 5. Log in to the Mobility Access Switch UI or CLI.
 - If using the UI, go to the **Maintenance > About**.
 - If using the CLI, execute the **show inventory | include HW** and **show version** commands.
 6. Note the cloud activation key and MAC address. The activation key is enabled only if the switch has access to the Internet.

Adding Devices Using Cloud Activation Key

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.
The **Device Inventory** page is displayed.
2. Click **Advanced** and select **With Cloud Activation Key**. The **Cloud Activation Key** pop-up window opens.
3. Enter the cloud activation key and MAC address of the device.
4. Click **Add**.



If a device belongs to another customer account or is used by another service, displays it as a blocked device. As does not support managing and monitoring blocked devices, you may have to release the blocked devices before proceeding with the next steps.

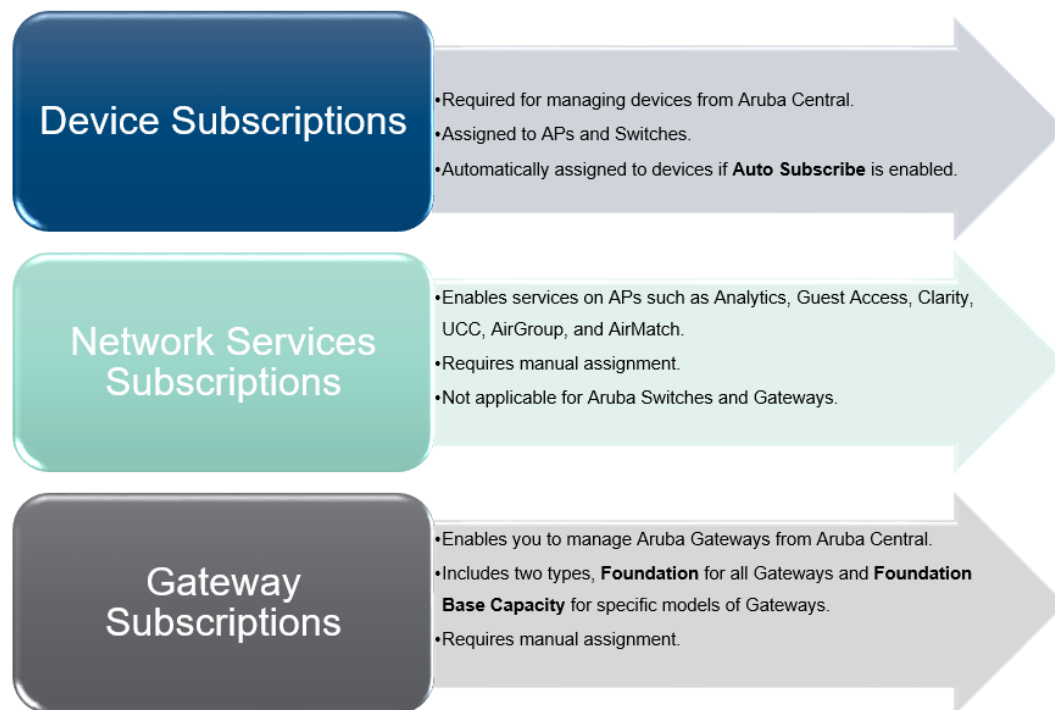
Assigning Subscriptions

- [Assigning Network Service Subscriptions](#)
- [Assigning Gateway Subscriptions](#)
- [Removing Subscriptions from Devices](#)
- [Acknowledging Subscription Expiry Notifications](#)
- [Renewing Subscriptions](#)

Aruba Central supports the following types of subscriptions:

- **Device subscription**—Allows you to manage and monitor your devices from Aruba Central. The device subscriptions can be assigned only to the devices managed by Aruba Central.
- **Network Service subscription**—Allows you to enable value added services on the APs managed from Aruba Central. For example, if you have APs, you can assign a service subscription for Guest Access.
- **Gateway subscription**—Allows you to manage and monitor SD-WAN Gateways from Aruba Central.

The following figure illustrates the supported subscription types and the assignment criteria:



Assigning Device Subscriptions

You can either enable automatic assignment of subscriptions or manually assign subscriptions for the devices added in Aruba Central.

Enabling Automatic Assignment of Subscriptions.

To enable automatic assignment of subscriptions, use one of the following methods:

In the Initial Setup Wizard

1. Verify that you have valid subscription key.
2. Ensure that you have successfully added your devices to the device inventory.
3. In the Assign Subscription tab, turn on the **Auto Subscribe** toggle switch.

From the Subscription Assignment Page

1. In the **Account Home** page, under **Global Settings**, click **Subscription Assignment**.
The **Subscription Management** page is displayed.
2. Under **Device Subscriptions**, toggle the **Auto Subscribe** slider to ON. All the devices in your inventory are selected for automatic assignment of subscriptions. You can edit the list by clearing the existing selection and re-selecting devices.



When a subscription assigned to a device expires or is cancelled, checks for the available subscription tokens in your account and assigns the longest available subscription token to the device. If your account does not have an adequate number of subscriptions, you may have to manually assign subscriptions to as many devices as possible. To view the subscription utilization details and the number of subscriptions available in your account, go to Global Settings > Key Management page.

To manually assign subscriptions, turn off the **Auto Subscribe** toggle.

Manually Assigning Subscriptions

To manually assign subscriptions to devices or override the current assignment:

1. In the **Account Home** page, under **Global Settings**, click **Subscription Assignment**.
The **Subscription Management** page is displayed.
2. Ensure that the **Auto Subscribe** toggle is turned off.
3. Select the devices to which you want to assign subscriptions.

Assigning Network Service Subscriptions

To assign a network service subscription, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Subscription Assignment**.
The **Subscription Management** page is displayed.
2. Under **Network Service Subscriptions**, select the AP from the table on the right.
3. Drag and drop the device to the subscription selected in the table on the left.

Assigning Gateway Subscriptions

For Aruba Gateways to function as Aruba Gateways, you must onboard them to the Aruba Central's device inventory and ensure that a valid subscription is assigned to each Gateway. A valid subscription allows the Gateway to be managed by Aruba Central.

Aruba Central supports the following types of subscriptions for Gateways:

- **Foundation**—This subscription can be assigned to all Gateways irrespective of the hardware model.
- **Foundation-Base capacity** —This subscription can be assigned to Aruba 7005, Aruba 7008, and Aruba 9004 Series Gateways. Gateway devices with the Foundation-Base capacity subscription can support up to 75 client devices per branch.

When the client capacity reaches the threshold:

- Aruba Central triggers the **Gateway base license capacity limit exceeded** alert.
- If the notification options for the **Gateway base license capacity limit exceeded** alert is configured, the Aruba sends an email notification with a list Aruba Gateways that exceed the client capacity threshold. You can also configure alerts to trigger an incident using Webhook.
- **Advanced**—This subscription is available for all Aruba Gateways. It allows users to avail advance features and services such as SaaS Express and Overlay Tunnel Orchestrator.
- **Advanced-Base Capacity**—This subscription is available for Aruba 7005, Aruba 7008, and Aruba 9004 Series Gateways.

Assigning Subscriptions to Gateways

To assign subscription to a Gateway, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Subscription Assignment**.
The **Subscription Management** page is displayed.
2. Under **Gateway Subscriptions**, select the device to which you want to assign a subscription.
3. Expand the drop-down in the **Assignment** column for the selected device.
4. Select the subscription; for example, **Foundation**.
5. To assign subscription to multiple devices:

- a. Select the devices in the table.
- b. Click **Batch Assignment**.
- c. Select the subscription that you to assign.

When a subscription assigned to a Gateway expires, Aruba Central automatically assigns a valid subscription from the same subscription category.

Virtual Gateway Subscriptions

Aruba Virtual Gateway is a virtual instance of headend gateway for SD-WAN. Aruba Central supports licenses are based on the bandwidth capacity for Virtual Gateways. SKUs are available for various for bandwidth and time-based combinations.

When the client capacity reaches the threshold:

- Aruba Central triggers the **Gateway base license capacity limit exceeded** alert.
- If the notification options for the **Gateway base license capacity limit exceeded** alert is configured, the Aruba sends an email notification with a list Aruba Virtual Gateways that exceed the client capacity threshold. You can also configure alerts to trigger an incident using Webhook.



For Paid licenses email notifications are sent out in 30 day intervals starting at 90th day before expiration and the last notification 1 day before the expiry of the license.

For Evaluation licenses email notifications are sent out on the 30th day before expiration and 1 day before the expiry of the license.

Assigning Subscriptions to Virtual Gateways

To assign subscription to a Virtual Gateway, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Subscription Assignment**.
The **Subscription Management** page is displayed.
2. Under **Virtual Gateway**, select the device to which you want to assign a subscription.
3. Expand the drop-down in the **Assignment** column for the selected device.
4. Select the subscription SKU; for example, **VGW-500MB**.
5. To assign subscription to multiple devices:
 - a. Select the devices in the table.
 - b. Click **Batch Assignment**.
 - c. Select the subscription that you to assign.

When a subscription assigned to a Virtual Gateway expires, Aruba Central automatically assigns a valid subscription from the same subscription category.



For more information on available SKUs, contact your Aruba Sales Specialist.

Removing Subscriptions from Devices

To remove the subscriptions from the devices, complete the following actions:

Removing a Device Subscription from a Device

1. On the **Global Settings > Subscription Assignment** page, ensure that the **Auto Subscribe** toggle is turned off. The devices that have the subscriptions assigned are selected and highlighted in green.
2. Clear the **Subscribed** check box for the device from which you want to unassign the subscription and click **Update Subscription**. The **Confirm Action** pop-up window with the **Do you want to modify the subscription for selected devices** message opens.
3. Click **Yes** to confirm. The subscription is unassigned and the **Subscribed** status for the device is marked as **No** in the devices table.

Removing a Network Service Subscription from a Device

To remove network service subscription from a device:

1. On the **Global Settings > Subscription Assignment** page, under **Network Service Subscriptions**, select a subscription from the table on the left.
2. From the table on the right, select the devices from which you want to unassign the subscription.
3. Click **Batch Remove Subscriptions**. The subscription is unassigned from the selected devices.

Acknowledging Subscription Expiry Notifications

The **Key Management** page under the **Global Settings** menu displays the expiration date for each subscription. As the subscriptions expiration date approaches, users receive expiry notifications. The users with evaluation subscription receive subscription expiry notifications on the 30th, 15th and 1 day before the subscription expiry and on day 1 after the subscription expires.

The users with paid subscriptions receive subscription expiry notifications on the 90th, 60th, 30th, 15th, and 1 day before expiry and two notifications per day on the day 1 and day 2 after the subscription expiry.

Acknowledging Notifications through Email

If the user has multiple subscriptions, a consolidated email with the expiry notifications for all subscriptions is sent to the user. The users can also acknowledge these notifications by clicking **Acknowledge** or **Acknowledge All** links in the email notification.

Acknowledging Notifications in the UI

If a subscription has already expired or is about to expire within 24 hours, a subscription expiry notification message is displayed in a pop-up window when the customer logs in to Aruba Central.

To prevent Aruba Central from generating expiry notifications, click **Acknowledge**.

Renewing Subscriptions

To renew your subscription, contact your Aruba Central sales specialist.

Assigning Devices to Sites

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 BranchA or CampusA, 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**.
The dashboard context for the filter is displayed.

2. Under **Maintain**, click **Organization > Sites and Labels**
The **Sites and Labels** page is displayed.
3. 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.
4. To view devices that are not assigned to any site, click **Unassigned**.
5. Select one or several devices from the list of devices.
6. Drag and drop the devices to the site on the left.
7. Click **Yes** to confirm action.

Assigning Labels

In Aruba Central, 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**.
The dashboard context for the filter is displayed.
2. Under **Maintain**, click **Organization > Sites and Labels**.
The **Sites and Labels** page is displayed.
3. Use the toggle switch to access the **Labels** page.
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 *Labels* in Aruba Central documentation.

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**.
The dashboard context for the filter is displayed.
2. Under **Maintain**, click **Organization**.
By default, the **Groups** page is displayed.
3. Under **Manage Groups**, click **New Group**.

4. Select the **AP and Gateway** checkbox or **Switch** checkbox to use a template based group.
5. Enter a password for the group in the **Password** text box.
6. Retype the password in the **Confirm Password** text box.
7. Click **Add Group**. The newly added group is displayed under the **Group Name** filter bar.

Assigning Gateways to a Group

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 that have similar configuration requirements. Aruba gateways are used in the tunnel mode topology of AOS 10.x deployments. In the tunnel mode topology, APs forward user traffic to a gateway cluster through a secure tunnel.

The Aruba gateways running ArubaOS 10.0.0.0 can form a cluster automatically when they are assigned to an UI group. Therefore, when you assign devices to a group, you must consider the following feature limitations:

- A cluster can be made up of different gateway platform models. For instance, a combination of Aruba7210, 7220, 7240 series gateways are allowed in the same cluster.
- Based on the hardware platform type, a single cluster can consist of up to 12 Aruba7200 Series gateways. Similarly, if the group consists of Aruba 7000 Series gateways, only four devices can form a cluster.
- You can combine 7200 Series and 7000 Series gateways in the same cluster with a maximum size of four devices with reduced AP client capacity on 7000 Series gateways.
- The groups in Aruba Central are not device-specific, so you can provision gateways, Switches, and APs in a single group. However, based on your deployment topology, you can assign these devices to the same or different groups.
- A device can be part of only one group at any given time.

To assign Aruba gateways to a group:

1. In the **Network Operations** app, set the filter to **Global**.
The dashboard context for the filter is displayed.
2. Under **Maintain**, click **Organization**.
By default, the **Groups** page is displayed.
3. From the devices table on the right, select the gateway 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.
5. Click **Yes** to confirm action.
6. If the group is not available in the list, click **New Group** to create a new group, and then drag and drop the gateways to the group that you just created.

For more information on clustering gateways, see [Gateway Cluster and Tunnel Orchestration](#).

Parent topic: [Getting Started with the Deployment](#)

Assigning APs to a Group

Aruba Central supports 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 assign APs to a group, complete the following procedure:

1. In the **Account Home** page, under **Global Settings**, click **Manage Groups**.
The **Groups** page is displayed.
2. To view a list of unassigned devices, click **Unassigned Devices**.
A list of unassigned devices is displayed in the devices table.
3. Select the group to which you want to assign the AP.
4. From the devices table on the right, select one or several APs to assign.
5. Drag and drop the APs to the group that you selected.

Connecting Aruba APs to Aruba Central

The Aruba APs have the ability to automatically provision themselves and connect to Aruba Central once they are powered on. The APs support zero touch provisioning (ZTP) using which devices can download their provisioning parameters from the Aruba Activate server.

To provision APs:

1. Connect your AP 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 *AP Installation Guide*.
 - If the device has factory default configuration, it receives an IP address through DHCP, connects to Aruba Activate, and downloads the provisioning parameters.
When an AP identifies Aruba Central as its management entity, it connects to Aruba Central and shows up as a connected device in Aruba Central.
 - If the AP is running a software version that is not compatible with Aruba Central, upgrade the AP to a supported software version and wait for it to connect to Aruba Central.

Connecting Aruba Gateways to Aruba Central

The Aruba Gateways have the ability to automatically provision themselves and connect to Aruba Central once they are powered on. The Gateways also support multiple active uplinks for ZTP (also referred to as automatic provisioning). The supported ZTP ports for different hardware platforms are listed in the following table. All these ZTP ports are assigned to VLAN 4094.

Table 5: *ArubaOS Hardware Platforms and Supported ZTP Ports*

ArubaOS Hardware Platform	Supported ZTP Ports
Aruba7005 Gateway	ALL ports except 0/0/1
Aruba7008 Gateway	ALL ports except 0/0/1
Aruba7010 Gateway	ALL ports except 0/0/1
Aruba7030 Gateway	ALL ports except 0/0/1
Aruba7024 Gateway	ALL ports except 0/0/1
Aruba7210 Gateway	ALL ports except 0/0/1

Table 5: ArubaOS Hardware Platforms and Supported ZTP Ports

ArubaOS Hardware Platform	Supported ZTP Ports
Aruba7220 Gateway	ALL ports except 0/0/1
Aruba7240 Gateway	ALL ports except 0/0/1
Aruba7280 Gateway The minimum software version required for 7280 Gateway is ArubaOS 8.5.0.0 - 1.0.6.0.	ALL ports except 0/0/1
Aruba9004 Gateway NOTE: The minimum software version required for 9004 Gateway is ArubaOS 8.5.0.0 - 1.0.7.0.	ALL ports except 0/0/1

To automatically provision the Gateways:

1. Connect your Gateway to the provisioning network.
2. Wait for the device to obtain an IP address through DHCP. Gateways support multiple uplink ports. The first port to receive the DHCP IP connects to the Activate server and completes the provisioning procedure:
 - If the device has factory default configuration, it receives an IP address through DHCP, connects to Aruba Activate, and downloads the provisioning parameters. When a devices identifies Aruba Central as its management entity, it automatically connects to Aruba Central.
3. Observe the LED indicators. Table 2 describes the LED behavior.

Table 6: LED Indicators

LED Indicator	LCD Text	Description
Solid Amber	Getting DHCP IP	Indicates that the uplink connection is UP, but DHCP IP is yet to be retrieved.
Blinking Amber	Activate Wait	Indicates that the device was able to reach the DHCP server and the connection to the Activate server is yet to be established.
Solid Green	Activate OK	Indicates that the device was able to retrieve provisioning parameters from the Activate server.
Alternating Solid Green and Amber	Activate Error	Indicates that the device was not able to retrieve provisioning parameters.

After successfully connecting to Aruba Central, the Gateways download the configuration from Aruba Central and reload.



The Gateways also include service ports that the technicians can use for manually provisioning devices in the event of ZTP failure. For more information on ports available for Aruba 7000 Series Mobility Controllers and Aruba 7200 Series Mobility Controllers, see *ArubaOS User Guide*.

Viewing Configuration Status

Aruba Central provides an audit dashboard for reviewing configuration changes for the devices provisioned in UI and template groups. The **Configuration Audit** page is available for APs, switches, and gateways.

The Configuration Audit page and the Auto Commit feature is available for Foundation and Advanced licenses for APs, switches, and gateways.

Viewing the Configuration Audit Page

To view the **Configuration Audit** page, complete the following steps:

- For APs:
 - a. In the **Network Operations** app, set the filter to a group that contains at least one AP.
The dashboard context for the selected group is displayed.
 - b. Under **Manage**, click **Devices > Access Points**.
 - c. Click the **Config** icon.
The tabs to configure access points are displayed.
 - d. Click **Show Advanced**, and click the **Configuration Audit** tab.
The Configuration Audit details page is displayed.
- For Aruba switches:
 - a. In the **Network Operations** app, set the filter to a group that contains at least one switch.
The dashboard context for the selected group is displayed.
 - b. Under **Manage**, click **Devices > Switches**.
 - c. Click the **Config** icon.
The tabs to configure switches are displayed.
 - d. Click **Configuration Audit**.
The Configuration Audit details page is displayed.
- For Aruba gateways:
 - a. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.
The dashboard context for the selected group is displayed.
 - b. Under **Manage**, click **Devices > Gateways**.
 - c. Click the **Config** icon.
The tabs to configure gateways are displayed.
 - d. Click **Show Advanced**, and click the **Configuration Audit** tab.
The Configuration Audit details page is displayed.

Applying Configuration Changes

Aruba Central supports a two-staged configuration commit workflow for APs and switches. Aruba Central now supports the auto commit feature at a group level. When auto commit state is enabled for a group, the configuration changes are instantly applied to all devices where auto commit state is enabled.

In the **Configuration Audit** page of the group, the **Auto Commit State** section allows administrators to switch their preference for committing configuration changes to the devices within the group.

- To enable auto commit, click **Change to Auto commit state ON**. When auto commit state is enabled for a group, the configuration changes are instantly applied to all devices where auto commit state is enabled.

- To disable auto commit, click **Change to Auto commit state OFF**. When auto commit state is disabled for a group, an administrator can build a candidate configuration, save it on cloud, review it, and then commit the configuration changes to all devices within the group.

Aruba Central resets the auto commit state, when a device moves to another group. The device inherits the auto commit state of the group to which the device is moved.

When auto commit state is disabled for a group, Aruba Central restricts modification to the auto commit state at a device level. When auto commit state is enabled for a group, Aruba Central allows modification to the auto commit state at a device level.

The auto commit at a group level is not applicable for Aruba MAS switches and Aruba gateways in the **Configuration Audit** page. Auto commit state is always enabled for Aruba MAS switches and Aruba gateways.



Viewing and Editing

To modify the auto commit state of devices within the group, when **Auto Commit State** for a group is enabled, complete the following steps:

1. Click **View & Edit** under **Auto Commit State: ON** tile.
2. Select a device name, click **Disable Auto Commit**, and then click **OK**.
3. Click **Yes** in the **Confirm Action** dialog box.

To modify the auto commit state of devices within the group, when **Auto Commit State** for a group is disabled, complete the following steps:

1. Click **View & Edit** under **Auto Commit State: OFF** tile.
2. Select a device name, click **Enable Auto Commit**, and then click **OK**.
3. Click **Yes** in the **Confirm Action** dialog box.



When auto commit state for a group is disabled, the **View & Edit** link is disabled to restrict modifications to the auto commit state of the devices within the group. When auto commit state for a group is enabled, the **View & Edit** link allows you to modify the auto commit state of the devices within the group.

Auto Commit Workflow

To enable Aruba Central to commit configuration changes instantly, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one AP and a switch.
The dashboard context for the selected group is displayed.
2. Under **Manage**, click **Devices > Access Points**.



In Aruba Central, the auto commit workflow for a group can be implemented either from the switch configuration audit page or AP configuration audit page. Alternatively, you can navigate to **Devices > Switches**.

3. Click the **Config** icon.
The tabs to configure access points are displayed.
4. Click **Show Advanced**, and click the **Configuration Audit** tab.
The Configuration Audit details page is displayed.

5. Ensure that the **Auto Commit State** for the group is set to **ON**.
6. Based on configuration mode set for the devices in the group, use either the UI workflows or a configuration template to complete the configuration workflow and save the changes. Aruba Central automatically commits the configuration changes to all devices where auto commit state is enabled.
7. View the **Local Overrides and Configuration Sync Issues**, if any.



Aruba Central does not support the two-staged configuration commit workflow for Aruba MAS switches and Aruba gateways.

The tenant accounts in the MSP deployments do not inherit the **Auto Commit State** configured at the MSP level. The tenant account users can enable or disable **Auto Commit** state for the devices in their respective accounts.

Manual Commit Workflow


To build configuration and review it before committing the configuration changes, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one AP and a switch. The dashboard context for the selected group is displayed.
2. Under **Manage**, click **Devices > Access Points**.




In Aruba Central, the manual commit workflow for a group can be implemented either from the switch configuration audit page or AP configuration audit page. Alternatively, you can navigate to **Devices > Switches**.

3. Click the **Config** icon.
The tabs to configure access points are displayed.
4. Click **Show Advanced**, and click the **Configuration Audit** tab.
The Configuration Audit details page is displayed.
5. Ensure that the **Auto Commit State** for the group is set to **OFF**.
6. Based on configuration mode set for the device, use either the UI workflows or a configuration template to complete the configuration workflow and save the changes. When you try to save the save changes, Aruba Central displays the following warning message:

 Auto commit configuration is disabled for this device.
After saving all the changes, go to Config Audit page to commit changes to this device.

7. When the auto commit state for a group is set to **OFF**, and changes are configured to the devices at a group level, Aruba Central displays the following warning message when you try to save the changes:

 Auto commit configuration is disabled for some devices.
After saving all the changes, go to Config Audit page of these devices to commit changes.

8. View the **Local Overrides and Configuration Sync Issues**, if any.
9. Click **Commit Now** to commits the configuration changes to all devices within the group.

Viewing Configuration Overrides and Errors

The **Configuration Audit** page allows you to view the configuration push errors, template synchronization errors, configuration sync, and device level configuration overrides. Some of notable status indicators available on the page includes:

- **Configuration Status**—Provides details of the number of devices with configuration sync errors. To view the devices with configuration sync errors, click **View Details**. The **Config Difference** window is displayed. You can view configuration differences for each device within the group.
- **Local Overrides**—Provides details of the number of devices with local overrides. To view a complete list of overrides, click **Manage Local Overrides**. The **Local Overrides** window is displayed. You can view configuration differences for each device within the group. 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.
To preserve the overrides, click **Close**. To remove the overrides, select the group name with local override, type **REMOVE** in the text box and click **OK**.
- **Configuration Conflicts**—Provides details of the number of devices with configuration conflict errors. To view a complete list of configuration conflicts, click **Manage Configuration Conflicts**. The **Configuration Conflict** window is displayed. To resolve the configuration conflicts, enable the checkbox against each conflict, and then click **Remove** to remove the conflict.
- **Template Errors**—Provides the details of the number of devices with template errors. To view a complete list of configuration template errors, click **View Template Errors**. The **Template Errors** window is displayed. You can view a list of templates with errors.
- **Move Failures**—Aruba Central supports moving a device from one group to another. If the move operation fails, Aruba Central logs such instances as **Move Failures**.

Viewing Configuration Status for Devices at the Group Level (Template Configuration Mode)

When you select a template group from the filter, the **Configuration Audit** page displays the following information.

Table 7: 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.</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 synced with the switch. ■ Device Running Configuration—Displays the running configuration on the switch.

Table 7: Configuration Audit Status for a Template Group

Data Pane Content	Description
	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.
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 Errors—Indicator showing configuration template errors for the devices deployed in template groups.

Viewing Configuration Status for a Device (Template Configuration Mode)

When you select a device that is provisioned in a template group, the **Configuration Audit** page displays the following information:

Table 8: 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. <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>
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 .

Viewing Configuration Status for Devices at the Group Level (UI-based Configuration Mode)

When you select an UI group, the **Configuration Audit** page displays the following information:

Table 9: 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 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 devices with local overrides. To view a complete list of overrides, click Manage Local Overrides. 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, select the group name with local override, type REMOVE in the text box and then click OK.
All Devices	<p>The All Devices table provides the following device information for the selected group:</p> <ul style="list-style-type: none"> ■ MAC Address—MAC address of the device. ■ Name—The name of the device. ■ IP Address—IP address of the device. ■ Site—Name of the site to which the device is assigned. ■ Type—The type of the device. ■ Auto Commit—The status of the auto commit state for all the devices within the group. ■ Config Sync/Config Status—Indicator showing configuration sync errors. ■ Local Overrides—Indicator showing configuration overrides for the devices deployed in the UI groups. <p>NOTE: The MAC Address, IP Address, Site, and Config Status columns are available only for groups in which Aruba gateways are provisioned (Manage > Device > Gateways, click the Config icon. The gateway configuration page is displayed. Navigate to Configuration Audit).</p>

Viewing Configuration Status for a Device (UI-based Configuration Mode)

When you select a device assigned to a UI group, the **Configuration Audit** page displays the following information:

Table 10: Configuration Audit Status for a Device Assigned to a UI Group

Data Pane Content	Description
<p>Configuration Status</p>	<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 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>
<p>Local Overrides</p>	<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 Local Overrides, type REMOVE in the text box and then click OK.

Backing Up and Restoring Configuration Templates

Aruba Central allows you to create a backup of configuration templates and variables that you can restore in the event of a failure or loss of data. The **Configuration Backup and Restore** feature is available in the **Configuration Audit** page for devices deployed using the template-based configuration method. The **Configuration Audit** pages for AP, switch, and gateway configuration containers allow you to create and manage backed up files and restore these files when required.

The **Configuration Backup and Restore** feature enables administrators to perform the following functions:

- Back up templates and variable files applied to the devices, managed using the template-based configuration method.
- Restore an earlier known working combination of the configuration template and device variables in the event of a failure.

Important Points to Note

- The backup and restoration options are available for devices deployed using the template-based configuration method.
- When the backup or restore for a group is in progress, you cannot make configuration changes to that group.
- The restore operation restores the variables only for the devices that are currently provisioned or pre-provisioned to the group.
- The restore operation is terminated if the firmware version running on any one device in the group does not match the firmware version in the backed up file that is being restored. For example, if the configuration file was backed up when a switch was running 16.03.0003 and was later upgraded to 16.04.0003, the restore operation fails for the group.
- The restore operation deletes any templates applied to the group before the restore. It also deletes and replaces device variables with the backed up version that is being restored.

- The details pertaining to the actions carried out during the backup and restore operations are logged in the **Audit Trail** page.

Creating a Configuration Backup

To back up configuration templates and variables applied to devices:

1. In the **Network Operations** app, set the filter to one of the template group under **Groups**.
2. Navigate to the **Configuration Audit** page. See [Viewing Configuration Status](#).
3. Under **Configuration Backup and Restore**, click **New Configuration Backup**.
The **Create New Backup** window is displayed.
4. Enter a **Backup Name**.
5. Turn on **Do Not Delete** toggle switch if you do not want the backed up file to be deleted by a new backup after the threshold of 20 backups is exceeded.



You can create and maintain up to 20 backed up configuration files. If the number of backup files exceed 20, the old backed up configuration files are overwritten. However, if the backed up files are marked as **Do not Delete**, Aruba Central does not overwrite the backed up configuration files.

6. Click **OK**.
The **Confirm Backup** window is displayed.
7. Read through the information, and select the check box to confirm that configuration changes to the group cannot be done when the backup is in progress.
8. Click **Proceed**.
The backup for the group configuration is created.

Viewing Contents of a Backed Up Configuration

To view the contents of a backed up configuration:

1. In the **Network Operations** app, use the filter to select a group that uses template-based configuration method.
2. Navigate to the **Configuration Audit** page. See [Viewing Configuration Status](#).
3. Click the **Manage Backups** option.
The **Manage Backups** window is displayed.
4. Download the backup and unzip the downloaded file. The following example shows the tree structure of a typical backup download.

```
<backup-name_timestamp>
├── templates
│   ├── <hppctemplatel1.tpl>
│   ├── <iaptemplatel1.tpl>
│   └── template_meta.json
└── variables
    ├── HPPC_variables_1.json
    ├── IAP_variables_1.json
    └── devices_meta.json
```

The variables are stored according the device type, such as, Instant APs and Aruba Switches. For example, for all Instant APs, the variables are aggregated and stored together.

The aggregated file can include variables for up to 80 devices or up to 5 MB of variables data, based on whichever condition is met first. When the number of variables or the data size exceeds this limit, new aggregate files are created and added to the backup until all the variables in the selected group are backed up. The variable data limit applies only to the aggregated files. Aruba Central does not impose any limit on the number of devices or the device variables that can be backed up.



The following details are available for a backed up configuration snapshot:

- **Backups**—provides details of the number of available and allowed backup and allows you to perform the following actions:
 - Manage group configuration backups
 - Create new configuration backups
 - Modify backup delete protection
 - **Last Backup**—provides details of the status and the timestamp of the last backup.
 - **Last Restore**—provides details of the status and the timestamp of the last restore.

Restoring a Backed Up Configuration

To restore a backed up configuration snapshot:

1. In the **Network Operations** app, use the filter to select a group that uses template-based configuration method.
2. Navigate to the **Configuration Audit** page. See [Viewing Configuration Status](#).
3. Under **Configuration Backup and Restore**, click **Restore from Backup**.
The **Restore from Backup** window is displayed.
4. Select the backup name that you want to restore, from the **Backup Name** drop-down list.
5. Select the required device type from the **Device Type** drop-down list.



Selecting a device type allows you to restore the backed up configuration by the specific device type, for example, Instant APs, Aruba Switch. By default, **All** is selected. When the device type is set to **All**, configuration restore does not follow any specific order.

6. Click **OK**.
The **Confirm Configuration Restore** window is displayed.
7. Read the instructions and select the check boxes to confirm your action for configuration restore.
8. Click **Proceed**.
The selected backup configuration is restored.



Aruba recommends that the administrators take a backup of the current configuration of the group before the restore operation.

Managing Backups

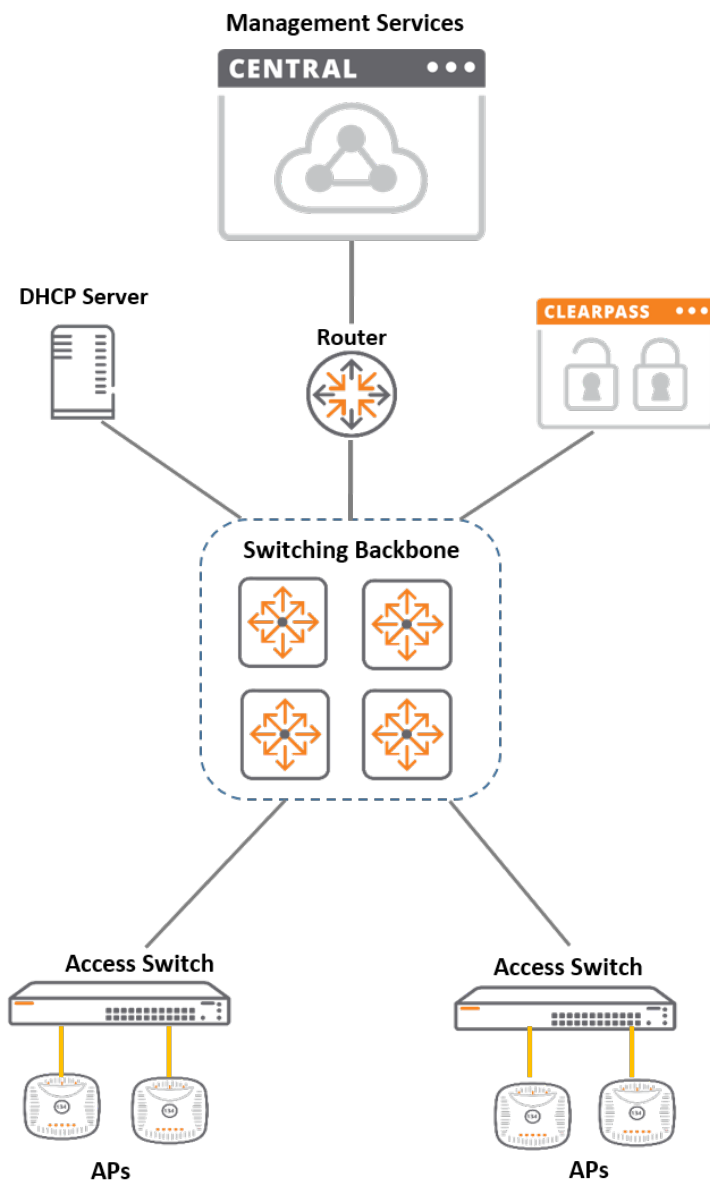
To manage the backed up configuration files:

1. In the **Network Operations** app, use the filter to select a group that uses template-based configuration method.
2. Navigate to the **Configuration Audit** page. See [Viewing Configuration Status](#).
3. Under **Configuration Backup and Restore**, click **Manage Backups**.
The **Manage Backups** window is displayed.
4. View the backup details such as date and time of backup, backup name, username, and the delete protection status for each configuration backup.
5. Click **Close**.
6. Click **Last Backup Log** to view the details of the latest backup. The **Last Backup Log** window displays the following details:
 - Group name
 - Backup name
 - Username that initiated the configuration backup
 - Details on whether templates and device variables are being saved, and completion of the configuration backup process.
7. To get the status of the last restore, click **Last Restore Log**.
8. To get the error log for a restore error event, click **Last Restore Error Log**.

The AOS 10.x allows you to establish WLAN in Bridge mode. In Bridge mode, standalone APs are connected to a switch backbone that is in-turn connected to the Aruba Cloud platform for management and configuration services. When AOS 10.x is deployed in Bridge mode, the network created acts as a physical network. All wireless traffic is terminated locally at the AP and Bridged onto the local Ethernet segment. Saturation issues in the network can be largely avoided if much of the traffic remain local. In other words, in Bridge mode, the data traffic is not tunneled back to the Gateways. In case of slow packet transfer in Bridge Mode, the heartbeat timer is set to a greater value to avoid frequent network disconnection.

The following figure illustrates the bridge-mode deployment.

Figure 4 *Bridge Mode Deployment*



AP Configuration and Client Connection Workflow

In the bridge mode topology, the AP configuration and client connection workflow includes the following steps:

1. The administrator configures a WLAN SSID in the **Bridge** mode for the AP group in AOS 10.x and the APs in the group inherit this configuration.
2. The APs in the group advertise the WLAN SSID.
3. The WLAN client connects to the SSID broadcast on an AP.
4. Based on the security profile configured for the WLAN SSID, the AP authenticates the client.
5. Based on the security and role assignment policy configured for the WLAN SSID, the AP derives the user role and VLAN information either locally or from the external authentication server.
6. Client gets an IP address from DHCP server.
7. After the client is successfully connected, the client traffic is encapsulated and sent to the AP.
8. The AP decrypts and bridges traffic on the client VLAN.
9. When the client roams from one AP to another within the VLAN, the Cloud-Assisted Roaming Services feature ensures that the client connection is seamless without the need for re-authentication.

Bridge Mode Deployment Workflow

The hardware infrastructure of the Bridge deployment requires APs with ArubaOS 10.0.0.0 or later software version.

The following sections describe the procedures for creating a WLAN SSID with the Bridge forwarding mode, assigning VLANs, and configuring security profiles, user role, and access policies.

Step 1: Follow Pre-Provisioning Procedures

Before you get started with the configuration of WLAN SSID in the Bridge Mode for LAN setup, refer the following topic to complete the pre-provisioning procedures:

[Getting Started with the Deployment](#)

For deployments with standalone AP, you must configure a WLAN SSID in the Bridge mode. Following are the steps required to configure WLAN SSID in **Bridge** mode for a LAN environment:

Step 2: Create a WLAN SSID Profile in Bridge Mode

An SSID is the primary name associated with an 802.11 wireless local area network (WLAN). Client devices use this name to identify and join wireless networks.

For more information on creating a WLAN SSID in bridge mode, see the following sections:

- [Configuring a WLAN SSID Profile in Bridge Mode](#)
- [Configuring General > Advanced Settings for a WLAN SSID Profile](#)

Step 3: Configure a VLAN for a WLAN SSID Profile in Bridge Mode

A VLAN is a group of devices on a single or multiple LANs that are logically configured to communicate seamlessly even if they are physically located on different LAN segments.

For more information on configuring VLANs in bridge mode, see the following sections:

- [Configuring VLANs for a WLAN SSID Profile in Bridge Mode](#)
- [Creating Named VLANs for Static VLAN Assignment](#)
- [Creating Named VLANs for Dynamic VLAN Assignment](#)
- [Creating VLAN Assignment Rules for Dynamic VLAN Assignment](#)

Step 4: Configure Security for a WLAN SSID Profile in Bridge Mode

AOS 10.x provides security to the following types of network profiles on a WLAN SSID in Enterprise, Personal, Captive Portal, and Open network.

For more information on configuring a security profile, see the following sections:

- [Configuring Security for a WLAN SSID Profile in Bridge Mode](#)
- [Configuring Enterprise Security for a WLAN SSID Profile](#)
- [Configuring External Authentication Servers for a WLAN SSID Profile](#)
- [Configuring Personal Security for a WLAN SSID Profile](#)
- [Configuring Captive Portal Security for a WLAN SSID Profile](#)
- [Configuring Open Security for a WLAN SSID Profile](#)

Step 5: Configure Access for a WLAN SSID Profile in Bridge Mode

A user access rule defines which users can automatically be assigned user access when logging in to the network. AOS 10.x allows you to configure access rules and roles for WLAN clients in Enterprise, Personal, and Captive Portal networks. However, access rules and user role configurations are not applicable in open security networks.

For more information on configuring access rules and roles for WLAN clients, see [Configuring Access Rules and Roles for WLAN Clients in Bridge Mode](#).

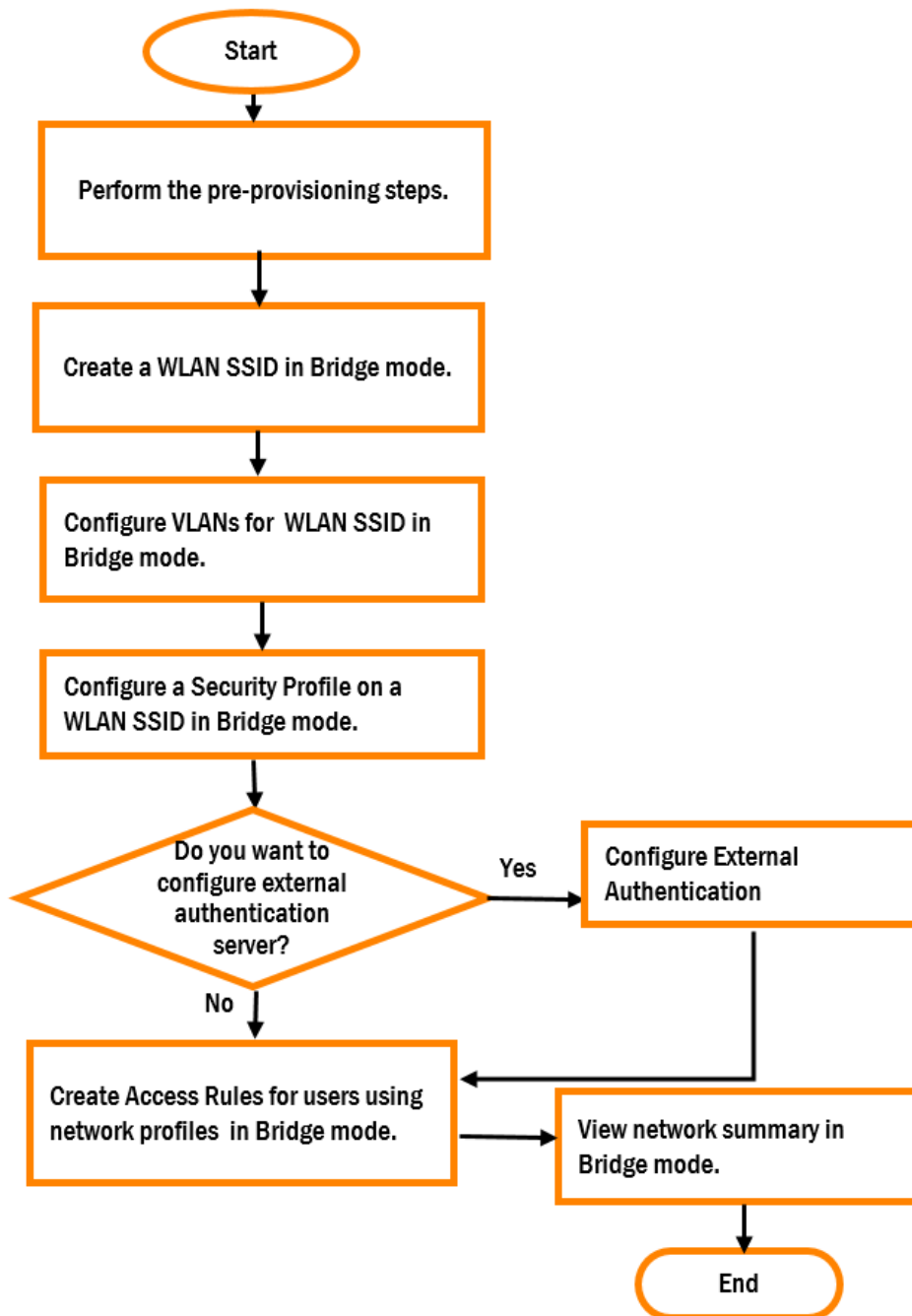
Step 6: View the Network Summary for a WLAN SSID Profile in Bridge Mode

The APs have the ability to automatically provision themselves and connect to Aruba Central after they are powered on. The APs support zero touch provisioning (ZTP) using which devices can download their provisioning parameters from the Activate server.

For more information on viewing the network summary, see [Viewing Network Summary for a WLAN SSID Profile in Bridge Mode](#).

Bridge Mode Deployment Flowchart

The following figure illustrates the procedure for setting up AOS 10.x in bridge mode.



Configuring a WLAN SSID Profile in Bridge Mode

For Bridge mode deployments, you must configure a WLAN SSID in the **Bridge** mode.

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**, go to **Device(s) > Access Points**.

3. If required, click the **Config** icon.
The second-level tabs to configure APs are displayed.
4. Go to the **WLANS** tab.
The **Wireless SSIDs** table is displayed listing the existing SSID profiles.
5. To create a new SSID profile, click **+ Add SSID**. To edit an existing SSID profile, click the row, and then click the edit icon.
The **Create a New Network** page is displayed for creating a new SSID. The **Networks** page is displayed for editing an existing SSID.
6. To create a new SSID name, enter the name of an SSID, and click **Next**.
7. (Optional) Proceed to [Configuring General > Advanced Settings for a WLAN SSID Profile](#).

Configuring VLANs for a WLAN SSID Profile in Bridge Mode

Aruba Central allows you to map VLAN name to a VLAN ID for the ease of identifying the existing VLANs.

To configure VLAN settings for an SSID, complete the following steps:

1. To access the WLAN SSID configuration wizard for a new SSID profile or an existing SSID profile, see [Configuring a WLAN SSID Profile in Bridge Mode](#) or [Creating a WLAN Profile in Tunnel and Mixed Mode](#).
2. In the WLAN SSID configuration wizard, click the **VLANs** tab.
3. Select the **Bridge** option in **Traffic Forwarding Mode** for a Bridge mode network.
In a Bridge mode SSID, all the user traffic is bridged locally. All the wireless traffic is terminated locally at the AP and bridged onto the local Ethernet segment.
4. Select one of the following options in **Client VLAN Assignment** to configure the VLAN assignment criterion for WLAN clients:
 - **Static**: Allows you to specify a VLAN ID of single VLAN. For more information, see [Creating Named VLANs for Static VLAN Assignment](#).
 - **Dynamic**: Allows you to assign the VLANs dynamically from a DHCP server. For more information, see [Creating Named VLANs for Dynamic VLAN Assignment](#).
 - **Native VLAN**: To assign the client VLAN to the native VLAN.
5. Click **Next**.

Creating Named VLANs for Static VLAN Assignment

To configure named VLANs for static VLAN assignment, complete the following steps:

1. To access the WLAN SSID configuration wizard for a new SSID profile or an existing SSID profile, see [Configuring a WLAN SSID Profile in Bridge Mode](#) or [Creating a WLAN Profile in Tunnel and Mixed Mode](#).
2. In the WLAN SSID configuration wizard, click the **VLANs** tab.
3. Select the **Bridge** option in **Traffic Forwarding Mode** for a bridge mode network.
In a bridge mode SSID, all the user traffic is bridged locally. All the wireless traffic is terminated locally at the AP and bridged onto the local Ethernet segment.
Select the **Tunnel** or **Mixed** option in **Traffic Forwarding Mode** for tunnel and mixed mode network.
4. Select **Static** in **Client VLAN Assignment** to specify a VLAN ID.
5. If a named VLAN is not available in the **VLAN ID** drop-down list, expand **Show Named VLAN** to view all the named VLANs mapped to the VLAN ID.
6. Click **+ Add Named VLAN** to add a new named VLAN.
The **Add Named VLAN** window is displayed.

7. Enter the VLAN name and VLAN ID in the **VLAN Name** and **VLAN** text boxes respectively.
8. Click **OK** to save the changes.

Creating Named VLANs for Dynamic VLAN Assignment

To assign the VLANs dynamically from a DHCP server, complete the following steps:

1. To access the WLAN SSID configuration wizard for a new SSID profile or an existing SSID profile, see [Configuring a WLAN SSID Profile in Bridge Mode](#) or [Creating a WLAN Profile in Tunnel and Mixed Mode](#).
2. In the WLAN SSID configuration wizard, click the **VLANs** tab.
3. Select the **Bridge** option in **Traffic Forwarding Mode** for a bridge mode network.
In a Bridge mode SSID, all the user traffic is bridged locally. All the wireless traffic is terminated locally at the AP and bridged onto the local Ethernet segment.
Select the **Tunnel** or **Mixed** option in **Traffic Forwarding Mode** for tunnel and mixed mode network.
4. Select **Dynamic** in **Client VLAN Assignment** to specify a VLAN ID.
5. If a named VLAN is not available in the **VLAN ID** drop-down list, expand **Show Named VLAN** to view all the named VLANs mapped to the VLAN ID.
6. Click **+ Add Named VLAN** to add a new named VLAN.
The **Add Named VLAN** window is displayed.
7. Enter the VLAN name and VLAN ID in the **VLAN Name** and **VLAN** text boxes respectively.
8. Click **OK** to save the changes.
9. (Optional) Proceed to [Creating VLAN Assignment Rules for Dynamic VLAN Assignment](#).

Creating VLAN Assignment Rules for Dynamic VLAN Assignment

To create a new VLAN assignment rule for dynamic VLAN assignment in bridge mode, complete the following steps:

1. To access the WLAN SSID configuration wizard for a new SSID profile or an existing SSID profile, see [Configuring a WLAN SSID Profile in Bridge Mode](#) or [Creating a WLAN Profile in Tunnel and Mixed Mode](#).
2. In the WLAN SSID configuration wizard, click the **VLANs** tab.
3. Select the **Bridge** option in **Traffic Forwarding Mode** for a Bridge mode network.
In a Bridge mode SSID, all the user traffic is bridged locally. All the wireless traffic is terminated locally at the AP and bridged onto the local Ethernet segment.
4. Select **Dynamic** in **Client VLAN Assignment** to specify a VLAN ID.
5. To create a new VLAN assignment rule, click **+ Add Rule** under **VLAN Assignment Rules**.
The **New VLAN Assignment Rule** window is displayed.
 - a. Select an attribute from the **Attribute** drop-down list.
 - b. Select either **equals** or **not-equals** from the **Operator** drop-down list, depending on your criteria.
 - c. Enter a string in the **String** text box.
 - d. Select a VLAN ID from the **VLAN** drop-down list.
 - e. Click **OK** to save the changes.

Configuring Security for a WLAN SSID Profile in Bridge Mode

You can configure the following types of security profiles on a WLAN SSID:

- **Enterprise**—For enterprise WLAN configuration, see [Configuring Enterprise Security for a WLAN SSID Profile](#).
- **Personal**—For personal network configuration, see [Configuring Personal Security for a WLAN SSID Profile](#).
- **Captive Portal**—For guest user access configuration, see [Configuring Captive Portal Security for a WLAN SSID Profile](#).
- **Open**—For open network with no authentication profiles, see [Configuring Open Security for a WLAN SSID Profile](#).

Configuring Enterprise Security for a WLAN SSID Profile

To configure an enterprise security profile, complete the following procedure:

1. To access the WLAN SSID configuration wizard for a new SSID profile or an existing SSID profile, see [Configuring a WLAN SSID Profile in Bridge Mode](#) or [Creating a WLAN Profile in Tunnel and Mixed Mode](#).
2. In the WLAN SSID configuration wizard, go to the **Security** tab.
3. In **Security Level**, select **Enterprise**.

4. Configure the following parameters:

Table 11: Enterprise Security Profile Configuration Parameters

Data pane item	Description
Key Management	<p>Select any of the following options from the 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, set Session Key for LEAP to Enabled. This is required for old printers that use dynamic WEP through LEAP authentication. The Session Key for LEAP feature is Disabled by default. ■ WPA-3 Enterprise(CNSA)—Select this option to use WPA-3 security employing CNSA encryption operation mode. ■ 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>
Primary Server	<p>Specify a primary authentication server for client authentication. To create a new server, see Configuring External Authentication Servers for a WLAN SSID Profile.</p>
Secondary Server	<p>Specify a secondary authentication server for client authentication. To create a new server, see Configuring External Authentication Servers for a WLAN SSID Profile.</p>
Load Balancing	<p>Enable this option to load balance between the two authentication servers.</p>

5. Click **Advanced Settings** and configure the following parameters:

Table 12: Advanced WLAN security Settings—Enterprise Security Profile

Data pane item	Description
Use Session Key for LEAP	<p>Select this option to use the session key for Lightweight Extensible Authentication Protocol (LEAP)</p>
Perform MAC Authentication Before 802.1X	<p>Allows you to use 802.1X authentication after the client completes the MAC authentication successfully. You can configure the following parameters:</p> <ul style="list-style-type: none"> ■ Delimiter Character—Specify a character as a delimiter for the MAC address string.

Data pane item	Description
	<p>When configured, the AP 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. The supported characters are : (colon), / (slash), , (comma), - (dash), and % (percent).</p> <ul style="list-style-type: none"> ■ Uppercase Support—Set to Enabled to allow the AP to use uppercase letters in MAC address string for MAC authentication. This option is available only if MAC authentication is enabled.
MAC Authentication Fail-Through	On selecting this, the 802.1X authentication is attempted when the MAC authentication of an AP client fails.
Reauth Interval	<p>Define a value for Reauth Interval. When set to a value greater than zero, APs periodically re-authenticate all associated and authenticated clients. The following events occur when the re-authentication interval is configured on WLAS SSIDs:</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 L2 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>
Denylisting	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.
Max Authentication Failures	Sets a value for the maximum allowed authentication failures. Enter a number between 1 and 10.
Enforce DHCP	<p>To enforce DHCP and to block traffic for AP clients that do not obtain IP address from DHCP, enable Enforce DHCP. When DHCP is enforced:</p> <ul style="list-style-type: none"> ■ A layer-2 user entry is created when a client associates with an AP. ■ The client DHCP state and IP address are tracked. ■ When the client obtains an IP address from DHCP, the DHCP state changes to complete. ■ If the DHCP state is complete, a layer-3 user entry is created. ■ When a client roams between the APs, the DHCP state and the client IP address is synchronized with the new AP.
Use IP for Calling Station ID	Enable this option to configure client IP address as calling station ID.
Called Station ID Type	<p>The Called Station ID Type detail can be configured even if the Use IP for Calling Station ID is set to disabled. Select any of the following options for configuring a called station ID:</p> <ul style="list-style-type: none"> ■ Access Point Group—Uses the AP's IP address as the called station ID. ■ Access Point Name—Uses the host name of the AP as the called station ID.

Data pane item	Description
	<ul style="list-style-type: none"> ■ VLAN ID—Uses the VLAN ID of as the called station ID. ■ IP Address—Uses the IP address of the AP as the called station ID.
Called Station ID Include SSID	Appends the SSID name to the called station ID.
Called Station ID Delimiter	Sets delimiter at the end of the called station ID.
Accounting	
Accounting	<p>On enabling this option, the APs post accounting information to the RADIUS server at the specified Accounting Interval. Select one of the following options from the drop-down list:</p> <p>Disabled—To disable the accounting option.</p> <p>Use authentication server—To select authentication servers and the accounting time interval in minutes.</p> <p>Use separate servers— To select specific accounting and mention the accounting interval time in minutes.</p>
Accounting Interval	Specify a number between 0 and 60 minutes.
Fast Roaming	
Opportunistic Key Caching (OKC)	Select Opportunistic key caching (OKC) to reduce the time needed for authentication. When OKC is enabled, multiple APs can share Pairwise Master Keys (PMKs) and use these keys when clients roam to a neighboring AP.
MDID	A mobility domain identifier (MDID). Enter a value between 1 and 65535. This option is available only when Opportunistic Key Caching (OKC) field is enabled.
802.11K	Select 802.11K to enable 802.11k roaming. The 802.11k protocol enables APs and clients to dynamically discover the available radio resources. When 802.11k is enabled, APs and clients send neighbor reports, beacon reports, and link measurement reports to each other.
802.11V	Select 802.11V to enable 802.11v based BSS transition. The 802.11v standard defines mechanisms for wireless network 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.

6. Click **Next**.

Authentication Servers for APs

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 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 AP 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 AP sends a RADIUS packet to the local IP address. The external RADIUS server then responds to the RADIUS packet.

Aruba Central 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 AP 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 AP has an instance of free RADIUS server operating locally. When you enable the internal RADIUS server option for the network, the client on the AP 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 AP. 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 AP. 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 AP 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 AP to send the request.
- By default, the AP uses its device certificate to establish a TLS connection with RadSec server. You can also upload your custom certificates on to AP.

Authentication Termination on AP

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 AP 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 APs to perform load balancing of authentication requests destined to authentication servers such as RADIUS or LDAP.

The load balancing in AP 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 a WLAN SSID Profile

External authentication is the use of third-party authentication sources to decide whether a user should be allowed access to a network. Also the external authentication decides the level of access to the network by the authenticated user. WLAN clients connecting to an SSID in the network can authenticate to a server based on the security profile configured on the SSID. You can create and associate an external authentication server when configuring a security profile for an WLAN SSID.



In a Bridge mode, authentication is performed at the AP level.

To add an external authentication server for the WLAN SSID, complete the following steps:

1. To access the WLAN SSID configuration wizard for a new SSID profile or an existing SSID profile, see [Configuring a WLAN SSID Profile in Bridge Mode](#) or [Creating a WLAN Profile in Tunnel and Mixed Mode](#).
2. In the WLAN SSID configuration wizard, click the **Security** tab.
3. In **Security Level**, select **Enterprise**.
4. Click + next to **Primary Server** or **Secondary Server** to add a new external authentication server. The **New Server** window is displayed. To edit an existing external authentication server, click the edit icon next to **Primary Server** or **Secondary Server**. The **Edit Server** window is displayed.
5. In the **New Server** window, select one of the following from the **Server Type** drop-down list:
 - **RADIUS**—To configure RADIUS authentication server, see [Configuring RADIUS Authentication Server for a WLAN SSID Profile](#).
 - **LDAP**—To configure LDAP authentication server, see [Configuring LDAP Authentication Server for a WLAN SSID Profile](#).
 - **Dynamic Authorization**—To configure dynamic authorization server, see [Configuring Dynamic Authorization Servers for a WLAN SSID Profile](#).
6. Click **OK**.

Configuring RADIUS Authentication Server for a WLAN SSID Profile

The following table describes the procedure to create RADIUS authentication servers for a WLAN SSID profile:

Table 13: *RADIUS 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>Select the Radsec check box to enable secure communication between the RADIUS server and AP by creating a TLS tunnel between the AP and the server.</p> <p>If Radsec is enabled, the following configuration options are displayed:</p> <ul style="list-style-type: none"> ■ Radsec Port—Communication port number for RadSec TLS connection. By default, the port number is set to 2083. ■ NAS IP Address ■ NAS Identifier ■ Dynamic Authorization ■ Service Type Framed User ■ Query Status of RADIUS Servers (RFC 5997)
Shared Key and Retype Shared Key	Shared key for communicating with the external RADIUS server.
Retry Count	The maximum number of authentication requests that can be sent to the server group by the AP. You can specify a value within the range of 1-5. The default value is 3 requests.

Type of Server	Parameters
Timeout (in secs)	The timeout duration for one RADIUS request. The AP 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.
NAS IP Address	Enter the IP address. For AP-based cluster deployments, ensure that you enter the VC IP address as the NAS IP address. For Cloud AP based Campus WLAN deployments, ensure that you enter the AP 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.
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.
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.
Service Type Framed User	Select any of the following check boxes to send the service type as Framed User in the access requests to the RADIUS server: <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)	Select any of the following check boxes to detect the server status of the RADIUS server: <ul style="list-style-type: none"> ■ Authentication—Select this check-box to ensure the AP sends a status-server request to determine the actual state of the authentication server before marking the server as unavailable. ■ Accounting—Select this check-box to ensure the AP sends a status-server request to determine the actual state of the accounting server before marking the server as unavailable.

Configuring LDAP Authentication Server for a WLAN SSID Profile

The following table describes the procedure to create LDAP authentication servers for a WLAN SSID profile:

Table 14: LDAP Authentication Server Configuration

Type of Server	Parameters
LDAP	
Name	Name of the LDAP server.
IP Address	IP address of the LDAP server.
Admin-Distinguished-Name	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.
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.
Auth Port	Authorization port number of the LDAP server. The default port number is 389.
Base-Distinguished-Name	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 .

Configuring Dynamic Authorization Servers for a WLAN SSID Profile

The following table describes the procedure to create dynamic authorization servers for a WLAN SSID profile:

Table 15: Dynamic Authorization Server Configuration

Type of Server	Parameters
Dynamic Authorization	
Name	Name of the server.
IP Address	IP address of the server.
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.
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.

Configuring Personal Security for a WLAN SSID Profile

To configure a personal security profile, complete the following procedure:

1. To access the WLAN SSID configuration wizard for a new SSID profile or an existing SSID profile, see [Configuring a WLAN SSID Profile in Bridge Mode](#) or [Creating a WLAN Profile in Tunnel and Mixed Mode](#).
2. In the WLAN SSID configuration wizard, click the **Security** tab.
3. In **Security Level**, select **Personal**.

4. Configure the following parameters:

Table 16: *Personal Security Profile Configuration Parameters*

Data pane item	Description
Key Management	Select any of the following options from Key Management drop-down list: <ul style="list-style-type: none"> ■ WPA-2 Personal ■ WPA Personal ■ Both (WPA-2 and WPA) ■ Static WEP ■ WPA-3 Personal ■ MPSK-AES ■ MPSK-Local
Passphrase Format (Applies to WPA)	Select a passphrase format. The options available are 8-63 alphanumeric characters and 64 hexadecimal characters.
Passphrase (Applies to WPA)	Enter the passphrase of length between 8 and 63 characters.
Retype (Applies to WPA)	Retype the password.
WEP Key Size (Applies to Static WEP)	Specify a value from the drop-down.
WEP Key (Applies to Static WEP)	Specify a length of 26 hexadecimal characters.
Retype WEP Key (Applies to Static WEP)	Retype the WEP key.
Primary Server (Applies to MPSK-AES)	Specify a primary authentication server for client authentication. To create a new server, see Configuring External Authentication Servers for a WLAN SSID Profile .
Secondary Server (Applies to MPSK AES)	Specify a secondary authentication server for client authentication. To create a new server, see Configuring External Authentication Servers for a WLAN SSID Profile .
Load Balancing (Applies to MPSK AES)	Enable this option to load balance between the two authentication servers.
MPSK Local (Applies to MPSK Local)	Specify an MPSK Local profile for client authentication. To create a new MPSK Local profile, see Creating an MPSK Local Profile .

5. Click **Advanced Settings** and configure the following parameters.

Table 17: Advanced WLAN Security Settings—Personal Security Profile

Data pane item	Description
MAC Authentication	To enable MAC address based authentication of clients, turn on the MAC Authentication toggle switch. When MAC authentication is enabled, you can configure Reauth Interval . NOTE: This option is not available when MPSK-AES is selected from the Key Management drop-down list.
Reauth Interval	When set to a value greater than zero, APs periodically re-authenticate all associated and authenticated clients. On an SSID performing L2 authentication (MAC or 802.1X authentication), if 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.
Denylisting	To enable denylisting of the clients with a specific number of authentication failures, select Denylisting and specify a value between 1 and 10 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.
Enforce DHCP	To enforce DHCP and to block traffic for AP clients that do not obtain IP address from DHCP, enable Enforce DHCP . When DHCP is enforced: <ol style="list-style-type: none"> 1. A layer-2 user entry is created when a client associates with an AP. 2. The client DHCP state and IP address are tracked. 3. When the client obtains an IP address from DHCP, the DHCP state changes to complete. 4. If the DHCP state is complete, a layer-3 user entry is created. 5. When a client roams between the APs, the DHCP state and the client IP address is synchronized with the new AP.
Use IP for Calling Station ID	Enable this option to configure client IP address as calling station ID.
Called Station ID Type	The Called Station ID Type detail can be configured even if the Use IP for Calling Station ID is set to disabled. Select any of the following options for configuring a called station ID: <p>Access Point Group</p> <ul style="list-style-type: none"> ■ Access Point Name—Uses the host name of the AP 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 AP as the called station ID. ■ MAC address—Uses the MAC address of the AP as the called station ID.
Called Station ID Include SSID	Appends the SSID name to the called station ID.
Called Station ID Delimiter	Sets delimiter at the end of the called station ID.

Data pane item	Description
Primary Server	Add a primary server. To create a new server, see Configuring External Authentication Servers for a WLAN SSID Profile .
Secondary Server	Add a secondary server. To create a new server, see Configuring External Authentication Servers for a WLAN SSID Profile .
Load Balancing	Enable load-balancing of the servers.
Delimiter Character	Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the AP 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 xxxxxxxxxx format is used. This option is available only when MAC authentication is enabled.
Uppercase Support	Select this option to allow the AP to use uppercase letters in MAC address string for MAC authentication. This option is available only if MAC authentication is enabled.
Accounting	
Accounting	On enabling this option, the APs post accounting information to the RADIUS server at the specified Accounting Interval . Select one of the following options from the drop-down list: <ul style="list-style-type: none"> ■ Disabled—To disable the accounting option. ■ Use authentication server—To select authentication servers and the accounting time interval in minutes. ■ Use separate servers— To select specific accounting and mention the accounting time interval in minutes.
Accounting Server1 (Applies to Use separate servers)	Specify the primary RADIUS accounting server from the drop-down list. To create a new server, see Configuring External Authentication Servers for a WLAN SSID Profile .
Accounting Server2 (Applies to Use separate servers)	Specify the secondary RADIUS accounting server from the drop-down list. To create a new server, see Configuring External Authentication Servers for a WLAN SSID Profile .
Accounting Interval	Specify a number between 0 and 60 minutes.
Fast Roaming	
802.11R	Select 802.11R to enable 802.11r roaming. Selecting this option enables fast BSS transition. The fast BSS transition mechanism minimizes the delay when a client transitions from one BSS to another within the same cluster.
MDID	A mobility domain identifier (MDID). Enter a value between 1 and 65535. NOTE: This option is available only when 802.11R field is enabled.

Data pane item	Description
802.11K	Select 802.11k to enable 802.11k roaming. The 802.11k protocol enables APs and clients to dynamically discover the available radio resources. When 802.11k is enabled, APs and clients send neighbor reports, beacon reports, and link measurement reports to each other.
802.11V	Select 802.11v to enable 802.11v based BSS transition. The 802.11v standard defines mechanisms for wireless network 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.

6. Click **Next**.

Configuring Captive Portal Security for a WLAN SSID Profile

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, the users connecting to the SSID 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 captive portal security profile for guest user access:

- To access the WLAN SSID configuration wizard for a new SSID profile or an existing SSID profile, see [Configuring a WLAN SSID Profile in Bridge Mode](#) or [Creating a WLAN Profile in Tunnel and Mixed Mode](#).
- In the WLAN SSID configuration wizard, click the **Security** tab.
- In **Security Level**, select **Captive Portal**.
- Under **Splash Page**, select one of the following from the **Captive Portal Type** drop-down list:
 - **Internal**—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. For more information, see [Configuring an Internal Captive Portal Splash Page Profile](#)
 - **External**—The guest users are required to enter the proxy server details such as IP address and captive portal proxy server port details. For more information, see [Configuring an External Captive Portal Splash Page Profile](#)
 - **Cloud Guest**—When **Cloud Guest** is enabled, the guest users are required to select the **Guest Captive Portal Profile**. For more information, see [Associating a Cloud Guest Splash Page Profile to a Guest SSID](#).
 - **None**—Select this option if you do not want to set any splash page.
 - Configure the following parameters:

Table 18: *Captive Portal Security Profile*

Parameter	Description
Captive Portal Type	Select any of the following options from the drop-down list:

Parameter	Description
	<ul style="list-style-type: none"> ■ Internal—When Internal is enabled, 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. For more information, see Configuring an Internal Captive Portal Splash Page Profile ■ External—When External is enabled, the guest users are required to enter the proxy server details such as IP address and captive portal proxy server port details. For more information, see Configuring an External Captive Portal Splash Page Profile ■ Cloud Guest—When Cloud Guest is enabled, 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.
<p>Captive Portal Profile</p>	<p>To use the default captive portal profile, select Default.</p> <p>To use a custom Splash Page profile, click + and configure the following parameters:</p> <p>Name—Enter a name for the profile.</p> <p>Type— Select any one of the following types of authentication:</p> <p>RADIUS Authentication—Select this option to enable user authentication against a RADIUS server.</p> <p>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.</p> <p>IP or Hostname—Enter the IP address or the host name of the external splash page server.</p> <p>URL—Enter the URL of the external captive portal server.</p> <p>Port—Enter the port number that is used for communicating with the external captive portal server.</p> <p>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.</p> <p>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.</p>

Parameter	Description
	<p>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.</p> <p>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.</p> <p>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.</p> <p>Redirect URL—Specify a redirect URL if you want to redirect the users to another URL.</p>
Encryption	<p>To enable encryption settings, turn on the Encryption toggle switch and select an encryption key from Key Management:</p> <p>For WPA-2 Personal, WPA Personal, Both (WPA-2&WPA), and WPA-3 keys, configure the following parameters:</p> <p>Passphrase Format: Select a passphrase format. The options are available are 8-63 alphanumeric characters and 64 hexadecimal characters.</p> <p>Enter a passphrase in Passphrase and reconfirm.</p> <p>For Static WEP, specify the following parameters:</p> <p>Select an appropriate value for WEP key size from the WEP Key Size. You can define 64-bit or 128-bit.</p> <p>Select an appropriate value for Tx key from Tx Key.</p> <p>Enter an appropriate WEP Key and reconfirm.</p>

- Click **Advanced Settings** and configure the following parameters:

Table 19: Advanced WLAN Security Settings—Captive Portal Security Profile

Data pane item	Description
Captive Portal Proxy Server IP	To configure a captive portal proxy server or a global proxy server to match your browser configuration, enter the proxy server IP address.
Captive Portal Proxy Server Port	If the captive portal proxy server IP address is configured, enter the captive portal proxy server port.
MAC Authentication	To enable MAC address based authentication of clients, turn on the MAC Authentication toggle switch. When MAC authentication is enabled, you can configure the following parameters:

Data pane item	Description
	<p>Delimiter Character—Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the AP 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.</p> <p>Uppercase Support—Set to Enabled to allow the AP to use uppercase letters in MAC address string for MAC authentication. This option is available only if MAC authentication is enabled.</p>
Reauth Interval	<p>Define a value for Reauth Interval. When set to a value greater than zero, APs periodically re-authenticate all associated and authenticated clients.</p> <p>The following events occur when the re-authentication interval is configured on WLAS SSIDs:</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>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>To enforce DHCP and to block traffic for AP clients that do not obtain IP address from DHCP, enable Enforce DHCP. When DHCP is enforced:</p> <p>A layer-2 user entry is created when a client associates with an AP.</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 APs, the DHCP state and the client IP address is synchronized with the new AP.</p>
Use IP for Calling Station	<p>Enable this option to configure client IP address as calling station ID. When this option is enabled, the following options are displayed:</p> <p>Called Station ID Type—Select any of the following options for configuring called station ID:</p> <p>Access Point Group—Uses the AP ID as the called station ID.</p> <p>Access Point Name—Uses the host name of the AP as the called station ID.</p> <p>VLAN ID—Uses the VLAN ID of as the called station ID.</p> <p>IP Address—Uses the IP address of the AP as the called station ID.</p> <p>MAC address—Uses the MAC address of the AP as the called station ID.</p> <p>Called Station Include SSID—Appends the SSID name to the called station ID.</p> <p>Called Station ID Delimiter—Sets delimiter at the end of the called station ID.</p> <p>Max Authentication Failures—Sets a value for the maximum allowed authentication failures.</p>

Data pane item	Description
Disable If Uplink Type Is	To exclude Ethernet, Wi-Fi, or cellular uplinks from authentication, select the uplink type.
Fast Roaming	<p>Enable the following fast roaming features as per your requirement:</p> <p>802.11r—Select 802.11r option to enable 802.11r roaming. Selecting this enables fast BSS transition. The fast BSS transition mechanism minimizes the delay when a client transitions from one BSS (AP) to another within the same cluster.</p> <p>When 802.11r is enabled, you can configure a mobility domain identifier (MDID). In a network of standalone APs with the same management VLAN, 802.11r roaming is not supported as MDIDs do not match across APs. They are auto-generated based on a AP key. To enable 802.11r, you can configure an MDID with the same value.</p> <p>802.11k—Select 802.11k to enable 802.11k roaming. The 802.11k protocol enables APs and clients to dynamically discover the available radio resources. When 802.11k is enabled, APs and clients send neighbor reports, beacon reports, and link measurement reports to each other.</p> <p>802.11v— Select 802.11v to enable 802.11v based BSS transition. The 802.11v standard defines mechanisms for wireless network 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.</p>

6. Click **Next**.

Configuring Open Security for a WLAN SSID Profile

To configure an open network for a WLAN SSID profile, complete the following procedure:

1. To access the WLAN SSID configuration wizard for a new SSID profile or an existing SSID profile, see [Configuring a WLAN SSID Profile in Bridge Mode](#) or [Creating a WLAN Profile in Tunnel and Mixed Mode](#).
2. In the WLAN SSID configuration wizard, click the **Security** tab.
3. In **Security Level**, select **Open**.
4. For **Open** security level, select **Open** or **Enhanced Open** from the **Key Management** drop-down list.
5. Configure the following parameters under **Advanced Settings**:

Table 20: *Advanced WLAN Security Settings—Open Network Profile*

Data pane item	Description
MAC Authentication	<p>To enable MAC address based authentication of clients, turn on the MAC Authentication toggle switch. When MAC authentication is enabled, you can configure the following parameters:</p> <ul style="list-style-type: none"> ▪ Delimiter Character—Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the AP 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.

Data pane item	Description
	<ul style="list-style-type: none"> ▪ Uppercase Support—Set to Enabled to allow the AP to use uppercase letters in MAC address string for MAC authentication. This option is available only if MAC authentication is enabled.
Reauth Interval	<p>Define a value for Reauth Interval. When set to a value greater than zero, APs periodically re-authenticate all associated and authenticated clients.</p> <p>The following events occur when the re-authentication interval is configured on WLAS SSIDs:</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 L2 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>
Denylisting	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.
Max Authentication Failures	Sets a value for the maximum allowed authentication failures. Enter a number between 1 and 10.
Enforce DHCP	To enforce DHCP and to block traffic for AP clients that do not obtain IP address from DHCP, enable Enforce DHCP .When DHCP is enforced: A layer-2 user entry is created when a client associates with an AP. The client DHCP state and IP address are tracked. When the client obtains an IP address from DHCP, the DHCP state changes to complete. If the DHCP state is complete, a layer-3 user entry is created. When a client roams between the APs, the DHCP state and the client IP address is synchronized with the new AP.
WPA3 Transition	Enable this option to allow transition from WPA3 to WPA2 and vice versa.
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> <p>Called Station ID Type—Select any of the following options for configuring called station ID:</p> <p>Access Point Group—Uses the APs IP address as the called station ID.</p> <p>Access Point Name—Uses the host name of the AP as the called station ID.</p> <p>VLAN ID—Uses the VLAN ID of as the called station ID.</p> <p>IP Address—Uses the IP address of the AP as the called station ID.</p> <p>MAC address—Uses the MAC address of the AP as the called station ID.</p> <p>Called Station Include SSID—Appends the SSID name to the called station ID.</p> <p>Called Station ID Delimiter—Sets delimiter at the end of the called station ID.</p> <p>Max Authentication Failures—Sets a value for the maximum allowed authentication failures.</p>
Called Station ID Type	<p>The Called Station ID Type detail can be configured even if the Use IP for Calling Station ID is set to disabled. Select any of the following options for configuring a called station ID:</p> <ul style="list-style-type: none"> ▪ Access Point Group—Uses the AP's IP address as the called station ID.

Data pane item	Description
	<ul style="list-style-type: none"> ■ Access Point Name—Uses the host name of the AP 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 AP as the called station ID.
Called Station ID Include SSID	Appends the SSID name to the called station ID.
Called Station ID Delimiter	Sets delimiter at the end of the called station ID.
Primary Server	Add a primary server. To create a new server, see Configuring External Authentication Servers for a WLAN SSID Profile .
Secondary Server	Add a secondary server. To create a new server, see Configuring External Authentication Servers for a WLAN SSID Profile .
Load Balancing	Enable load-balancing of the servers.
Delimiter Character	Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the AP 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 AP to use uppercase letters in MAC address string for MAC authentication. This option is available only if MAC authentication is enabled.
Accounting	
Accounting	On enabling this option, the APs post accounting information to the RADIUS server at the specified Accounting Interval . Select one of the following options from the drop-down list: <ul style="list-style-type: none"> ■ Disabled—To disable the accounting option. ■ Use authentication server—To select authentication servers and the accounting time interval in minutes. ■ Use separate servers— To select specific accounting and mention the accounting time interval in minutes.
Accounting Server1 (Applies to Use separate servers)	Specify the primary RADIUS accounting server from the drop-down list. To create a new server, see Configuring External Authentication Servers for a WLAN SSID Profile .
Accounting Server2 (Applies to Use separate servers)	Specify the secondary RADIUS accounting server from the drop-down list. To create a new server, see Configuring External Authentication Servers for a WLAN SSID Profile .

Data pane item	Description
Accounting Interval	Specify a number between 0 and 60 minutes.
Fast Roaming	<p>Enable the following fast roaming features as per your requirement:</p> <ul style="list-style-type: none"> 802.11R—Select 802.11R option to enable 802.11r roaming. Selecting this enables fast BSS transition. The fast BSS transition mechanism minimizes the delay when a client transitions from one BSS (AP) to another within the same cluster. <p>When 802.11R is enabled, you can configure a mobility domain identifier (MDID). In a network of standalone APs with the same management VLAN, 802.11r roaming is not supported as MDIDs do not match across APs. They are auto-generated based on a AP key. To enable 802.11r, you can configure an MDID with the same value.</p> <p>NOTE: The 802.11R feature is not available when you select Static WEP or WPA2-Personal options from the Key Management drop-down list.</p> 802.11K—Select 802.11K to enable 802.11k roaming. The 802.11k protocol enables APs and clients to dynamically discover the available radio resources. When 802.11k is enabled, APs and clients send neighbor reports, beacon reports, and link measurement reports to each other. 802.11V— Select 802.11V to enable 802.11v based BSS transition. The 802.11v standard defines mechanisms for wireless network 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.

6. Click **Next**.

Configuring Access Rules and Roles for WLAN Clients in Bridge Mode

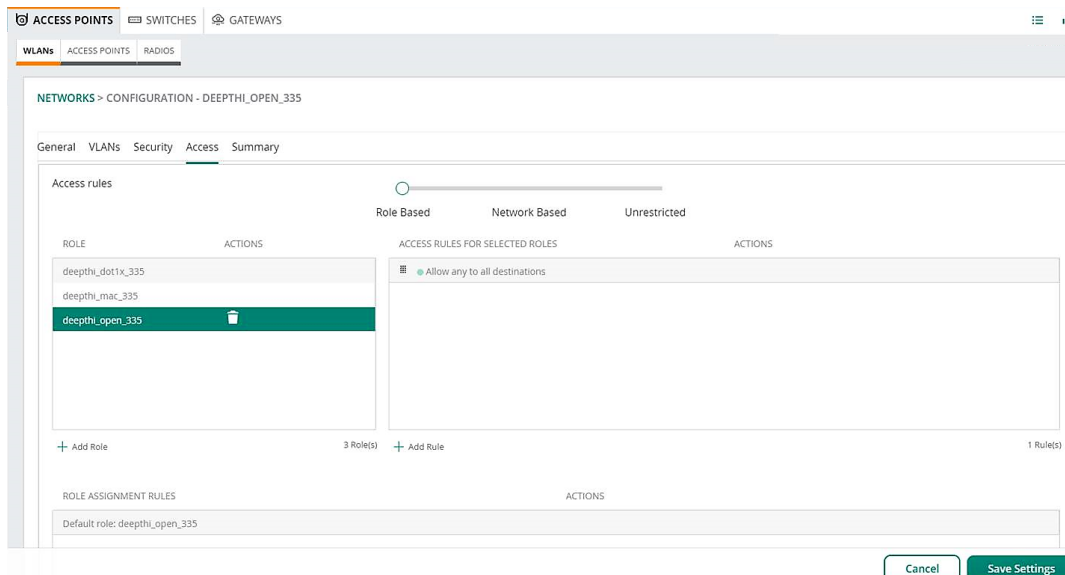
You can configure up to 64 access rules for a wireless network profile.



Configuration of ACLs for User Access is not applicable for Open network.

To configure access rules and user roles for a WLAN SSID, complete the following procedure:

1. In the WLAN SSID configuration wizard, click the **Access** tab.
The Access page is displayed.



2. 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. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. To define an access rule:
 - a. Click (+) icon.
 - b. Select appropriate options in the **New Rule** pane.
 - c. Click **Save**.
 - **Role based**—Select **Role based** to enable access based on user roles. For role-based access control:
 - Create a user role if required.



- Create access rules for a specific user role.
 - Create a role assignment rule. To configure access rules for network services, refer to the next section.
3. Click **Next**.

Configuring Access Rules

To configure access rules for network services, complete the following procedure:

1. In the WLAN SSID configuration wizard, click the **Access** tab.
The **Access** page is displayed.

2. Select the type of access control.
3. Click **Roles**.
4. Under **Access Rules For Selected Roles**, click **+ Add Rule** to add a new rule. The new rule window is displayed.

5. Under **Rule Type**, select the type of access rule. For example, **Access Control**.
6. To configure access to applications or application categories, select a service category from the following list:
 - **Network**
 - **Application Category**
 - **Application**
 - **Web Category**
 - **Web Reputation**
7. Based on the selected service category, configure the following parameters:

Table 21: Access rule configuration parameters

Data Pane Item	Description
Rule Type	Select a rule type from the list, for example Access Control .
Service	<p>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:</p> <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. <p>NOTE: If TCP and UDP uses the same port, ensure that you configure separate access rules to permit or deny access.</p>
Action	<p>Select any of following attributes:</p> <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.

Table 21: Access rule configuration parameters

Data Pane Item	Description
Destination	<p>Select a destination option. 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.
Log	<p>Select Log to create a log entry when this rule is triggered. The AOS 10.x firewall supports firewall based logging. Firewall logs on the APs are generated as security logs.</p>
Denylist	<p>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.</p>
Classify Media	<p>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:</p> <ul style="list-style-type: none"> ■ Video: Priority 5 (Critical) ■ Voice: Priority 6 (Internetwork Control)
Disable Scanning	<p>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.</p>
DSCP Tag	<p>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.</p>
802.1 priority	<p>Select 802.1 priority to specify an 802.1 priority. Specify a value between 0 and 7.</p>
Time Range	<p>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.</p>

8. Click **Save Settings**.

Viewing Network Summary for a WLAN SSID Profile in Bridge Mode

The **Network Summary** tab displays all the settings configured in the **General**, **Security**, **VLANs**, and **Access** tabs. In the **Network Operations** app, set the filter to **All Devices** to display the Global dashboard.

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

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**, go to **Device(s) > Access Points**.
3. If required, click the **Config** icon.
The second-level tabs to configure APs are displayed.
4. Go to the **WLANS** tab.
The **Wireless SSIDs** table is displayed listing the existing SSID profiles.
5. Click the row for an SSID.
The **Network Summary** page is displayed.

A Gateway cluster is a combination of multiple Aruba Gateways operating as a single entity to provide high availability and service continuity to the WLAN clients in a network. Gateway clusters provide full redundancy to APs and WLAN clients in the event of a failover.

The AOS 10.x supports Gateway clusters and provides the following features and benefits:

- **Hitless Failover**—When a Gateway device fails, APs and clients fail over to another Gateway in the cluster without any service disruption. High-value client sessions such as voice, video, FTP, and IGMP used for IPv4 multicast groups and MLD used for IPv6 multicast groups are synchronized between active and standby gateways of a cluster, thereby allowing the connected devices to fail over to the standby gateway seamlessly. However, this synchronization is supported only for the first failover. For subsequent failovers, the failover session is not synchronized to the recent standby. Instead, a new session is synchronized.
- **Load Balancing**—When there is excessive workload among the devices, the Gateways in a cluster balance AP and client loads seamlessly to ensure faster connectivity to clients.
- **Seamless roaming**—When a client roams between APs within the WLAN boundary, the clients remain anchored to the same Gateway in a cluster for seamless user experience.
- **Ease of deployment**—A Gateway cluster is automatically formed when assigned to a UI group in the Network Operations app without any manual configuration.

The automatic Gateway cluster configuration is supported on Aruba Gateways with ArubaOS 10.0.0.0 or later versions. To view a list of Aruba Gateway models and supported software versions in Aruba Unified Network Architecture, refer [Supported Devices for AOS 10.x](#)

The AOS 10.x simplifies the existing load balancing algorithm to have a more balanced distribution of load when a Gateway comes back into the cluster after its failover. This is required to streamline the entire debugging and troubleshooting process and to reduce the number of user activations during multiple cluster failover. The AOS 10.x solution leverages cluster heartbeat and fast failover detection for other features to obtain seamless failover.



In the AOS 10.x, the APs do not anchor to a Gateway. The APs are anchored to the cloud and the Gateway identifies the AP when the AP is booted. However, the Device Designated Gateway (DDG), which is an AP designated gateway, is needed to achieve multicast functionality. From the user point of view, the APs would still be aware of cluster bucket map that is used to direct the user traffic to the user designated gateway.

An AOS 10.x solution configured with Gateway clusters requires the Gateways to be onboarded to the Aruba Central. See the workflow detailed in [Gateway Cluster Architecture on page 76](#) to onboard the Gateways.

Types of Gateway Clusters

You can deploy either a homogeneous or heterogeneous cluster for Gateways.

Homogeneous Cluster

A homogeneous cluster is a cluster built with all nodes of the same platform type, and consists of the same Aruba Gateway models. A homogeneous cluster of Aruba 7200 Series Gateway supports up to 12 nodes in a cluster, whereas a homogeneous cluster of Aruba 7000 Series Gateway supports only four Gateway nodes in a cluster.

The cluster sizing depends on the number of cluster AP count required to ensure that every AP has a DDG and S-DDG with adequate capacity for all APs to failover. The recommended AP load of this cluster should be half of the total cluster capacity. Therefore, the cluster AP count should be equal to 50% of the cluster capacity.

For example, if a cluster is made up of four 7220 managed devices, the combined capacity of four 7220 managed devices is 4096 APs, hence, the AP count would be 2048.

Heterogeneous Cluster

A heterogeneous cluster allows you to combine different models of Gateways. A heterogeneous cluster with a combination of 7200 Series and 7000 Series Gateways is supported with redundancy and reduced AP or client capacity. The size of the cluster becomes four when 7000 Series Gateway is combined with 7200 Series Gateway.

Cluster AP size should be equal to the lowest value of either 50% of total cluster capacity or the worst case scenario load. The worst case scenario load is the AP load handled by the remaining nodes in a cluster in the event of highest capacity cluster member going down.

Cluster Connection Type

AOS 10.x supports L2 connection type for cluster members where the cluster members share the same user VLANs. All user VLANs on each node are also present in all nodes.



A cluster is always formed over an L2 network.

Features of Gateway Clusters

Following are the features supported for Gateway clusters:

AP Load Balancing in Gateway Clusters

The load balancing of APs is done among Gateways during initial set up. In either a homogeneous or a heterogeneous cluster, the APs are load balanced in a round robin manner among Gateways depending on the platform AP capacity. The APs are equally distributed to offload multicast handling evenly across cluster peers. Only active and standby DDG configure the multicast tunnel to the user VLAN in the datapath.

Backup Cluster Configuration for Gateway Clusters

An optional setting is introduced to configure a **Secondary Gateway Cluster**, as a failover for tunnel-mode deployments, in case the primary cluster is unavailable. Enabling the **Cluster Preemption** check-box allows the AP to switch back to the SSID of the primary gateway cluster, when it becomes available. Failover from primary cluster to secondary cluster is triggered when:

- The Primary cluster is down.
- The Primary cluster is UP but some devices are unable to reach the primary cluster. These devices would failover to backup cluster.

A secondary gateway cluster can be configured at the group-level or at the device-level and only one primary-secondary cluster can be configured per SSID. This setting be configured in a multizone environment and each zone can have it's own backup cluster. For more information, see [Configuring VLAN Settings for WLAN SSID Profile in Tunnel and Mixed Mode](#).

Multiversion Support in Gateway Clusters

The AOS 10.x supports multiple versions between Gateways in the same cluster profile by exchanging messages between Gateways in the cluster. To support multiple version for all the messages exchanged, messages are encoded in Protobuf format and sent over PAPI so that the fields that are unknown to that Gateway are ignored. The following messages are exchanged between the Gateways:

- **HELLO**: A PAPI message containing different parameters such as **platform type**, **MAC**, **IP**, **build string**, and so on. The **build string** parameter is compared to ensure that the cluster can be formed even if the Gateway version is different.
- **IKE/IPSec**: The UDP 4500 packets that are exchanged between two cluster members .
- **Heartbeat**: A PAPI message that is exchanged between every two cluster members.
- **Vlan probe**: A Layer-2 unicast packet with a special etype (0x88b5) that is used to detect if the peer is Layer-2 connected or Layer-3 connected.
- **Link map status**: A PAPI message exchanged between two cluster members to determine the overall connectivity within the cluster.
- **GSM/DDS**: A message used for object replication, activation, and de-activation.

The cluster is formed between Gateways in the same cluster profile by accepting the **HELLO** message request from peers.

Device Interface Manager in Gateway Clusters

The Device Interface Manager (DIM) is an interface between AP and the Gateway and handles the cluster related communication between them.

Cluster Support for Wired User from AP

The Gateway cluster also supports load balancing and redundancy for wired users connection to AP. This requires AP to use the bucketmap for the cluster to forward wired client traffic to appropriate Gateway. The AP uses the same GRE tunnel to forward wired and wireless client traffic and sends the same RADIUS messages to Gateway for wired users. The user is grouped as wired or wireless on the Gateway based on the NAS port type sent by the AP.

Dynamic Authorization

Dynamic authorization supports Change of Authorization (CoA) requests in a cluster. CoA requests are sent by the RADIUS servers to Gateways to dynamically modify the authorization attributes for a connected client session. Administrators can enable the dynamic authorization feature to ensure that the CoA requests are not dropped when Gateway nodes change due to load balancing or in the event of a failover.

VPN Termination

The manual cluster configuration mode also allows you to enable VPN termination to terminate the IPsec VPN tunnels originating from the APs. Administrators can enable VPN termination if the Gateways in the cluster are used as VPN endpoints.

Tunnel Orchestration

The IPsec between the AP and Gateway cluster are orchestrated by Tunnel Orchestrator for LAN Tunnels service in Aruba Central.

The Tunnel Orchestrator for LAN Tunnels service in Aruba Central automates routing between AP and the Gateway cluster provisioned in an Aruba Central account. The Tunnel Orchestrator for LAN Tunnels service also computes the cost for route between multiple data centers, so that different data centers preference can be

applied for the devices in a branch. The designated Gateway in the cluster acts a preferred VPN concentrator and aggregates routes from APs and redistributes these routes to the neighboring routers.

For Layer 2 deployments, the administrators must configure a split-tunnel policy in the access rules and apply it to the user role in the WLAN SSID. Based on the ACLs configured for an SSID and Gateway cluster, client traffic to the corporate domain is tunneled to the Gateway in the data center and traffic to the non-corporate domain is forwarded to the Internet.

Gateway Cluster Architecture

In a gateway cluster architecture, the devices form a cluster among themselves as long as they are all in the same UI group. Also, when the gateways in a group are assigned to the same site, the gateways automatically form a cluster among themselves. When all the cluster members are in a fully connected mesh, a cluster leader is elected based on the platform type or platform value, and the MAC address. The cluster leader publishes the bucket map for each cluster and balances the client load seamlessly when there is an imbalance of load among the cluster members. The bucket map is used to map bucket of clients to the active and standby User Designated Gateways (UDG).

These are used by APs to decipher the active and standby UDG for each client. A bucket map is published for every cluster. The AP calculates the Bucketindex for the client on Station Up (STA_UP) message and directs it to the UDG as per the bucketmap.

The last 3 bytes of the client's MAC address is XORed to get decimal value between 0 and 255. This value is used by the AP to look up in the bucketmap and use the corresponding index to forward the STA_UP message to the correct UDG.

The cluster leader identifies standby Gateways for clients and APs to ensure hitless failover. The client traffic is forwarded to the User Designated Gateway or to the Standby User Designated Gateway (S-UDG) based on the listing of Gateways in the AP bucket map.

The gateway cluster architecture in tunnel mode consists of the following members:

- [Device Designated Gateway \(DDG\) and Standby Device Designated Gateway \(S-DDG\)](#)
- [User Designated Gateway \(UDG\) and Standby User Designated Gateway \(S-UDG\)](#)
- [VLAN Designated Gateway \(VDG\) and Standby VLAN Designated Gateway \(S-VDG\)](#)

Device Designated Gateway (DDG) and Standby Device Designated Gateway (S-DDG)

To publish bucketmap and nodelist (A nodelist is the list of gateways in a cluster) to every device (AP), you need a designated Gateway. In the event of failure of the Active Device Designated Gateway, a standby Designated Gateway shall continue to publish the bucketmap and nodelist. Hence, every AP is assigned with a DDG and a S-DDG. The cluster leader selects the Device Designated Gateway (DDG) and the Standby Designated Gateway (S-DDG) for an AP as and when the AP details are identified as part of the initial orchestration and messaging. The Gateway station management publishes this information to the GSM channel of APs, and the cluster leader assigns the DDG and S-DDG for the AP at that point of time in a round-robin fashion based on current AP load on all Gateways in the cluster. The DDG selection sends the AP nodelist and bucket map from the Gateway to the AP. This selection also configures the VLAN Multicast table during AP bootstrapping and cluster failover.

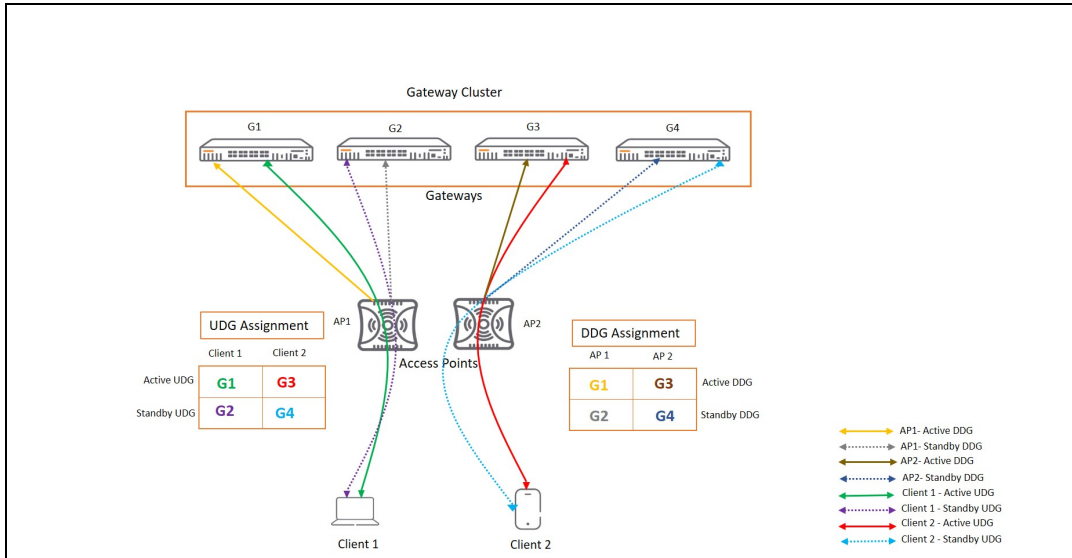
User Designated Gateway (UDG) and Standby User Designated Gateway (S-UDG)

For every client, you need a Gateway to anchor its north bound traffic. Therefore, you need a User Designated Gateway (UDG). In the event of failure of the Active User Designated Gateway, a standby User Designated

Gateway shall take over. In the Gateway Cluster architecture in Decrypt-tunnel (D-Tunnel) mode, the Gateways work as User Designated Gateway (UDG). In a D-tunnel forwarding mode, the AP decrypts and decapsulates all 802.11 frames from a client and sends the 802.3 frames through the GRE tunnel to the Gateway cluster. The forwarding mode allows a network to utilize the encryption and decryption capacity of the AP while reducing the demand for processing resources on the Gateway cluster. The UDG (User Designated Gateway) and S-UDG (Standby User Designated Gateway) bucket maps are used to forward the client traffic to the appropriate UDG. The UDG selection sends the AP nodelist and bucket map from the Gateway to the AP. This selection also configures the VLAN Multicast table during AP bootstrapping and cluster failover.

The following diagram depicts the selection of DDG and S-DDG as well as the UDG and S-UDG between two APs in a cluster setup:

Figure 5 Tunnel Mode Traffic Flow with DDG/S-DDG and UDG/S-UDG Selection



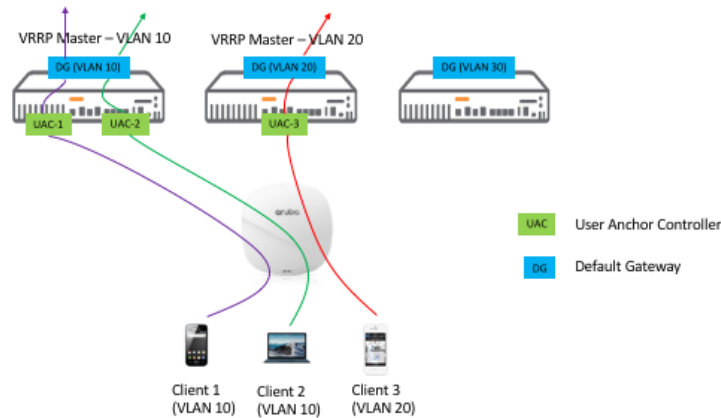
As illustrated in the above diagram, in case of a failover, the clients connect to the Gateways based on the allotment of active and standby Gateways in the bucket maps. For example, If a particular active Gateway is down, the clients are automatically moved to S-UDG since the clients have already been assigned a S-UDG.

VLAN Designated Gateway (VDG) and Standby VLAN Designated Gateway (S-VDG)

Gateways that route the traffic for every client VLAN are VLAN Designated Gateways. In the event of a failure of the Active VLAN Designated Gateway, a standby VLAN Designated Gateway shall take over. For each user VLAN, a Gateway is automatically elected by the cluster leader in a round-robin manner to function as the VLAN Designated Gateway (VDG) and is assigned the highest priority at any given time. Each VDG works with the Gateway that is anchored for communication with the APs and thus allows the cluster to manage incoming and outgoing network connection requests from the AP clients.

The following diagram depicts the VDG and S-VDG selection done by the cluster leader in a round-robin manner:

Figure 6 VDG and S-VDG Selection



Gateway Cluster Deployment

When gateways are added to a group, the gateways that are part of the UI group automatically form a cluster with the MAC address of the devices present. You must disable automatic cluster configuration if you want to configure cluster with VRRP IP and VRRP VLAN only when the gateways are in a UI group.

For **Tunnel** and **Mixed** mode SSID configuration, administrators must associate a gateway cluster for client authentication, policy enforcement, and role assignment to clients.

Based on the type of SSID configured on the APs and user VLAN, a gateway from the cluster is automatically assigned to APs. APs forward client authentication requests to gateways. The User Designated Gateway (UDG) in the cluster derives the user role either locally or from an external authentication server, and thus allows clients to connect to the network.

The tunnel orchestrator service in Aruba Central automatically establishes secure tunnels between AP and each of the gateways present in the cluster and thus allows APs to send client traffic to the tunnel mode network for role assignment and policy enforcement. For site-specific clusters, the tunnel orchestrator service automatically allows the devices on the particular site to establish tunnels among themselves.

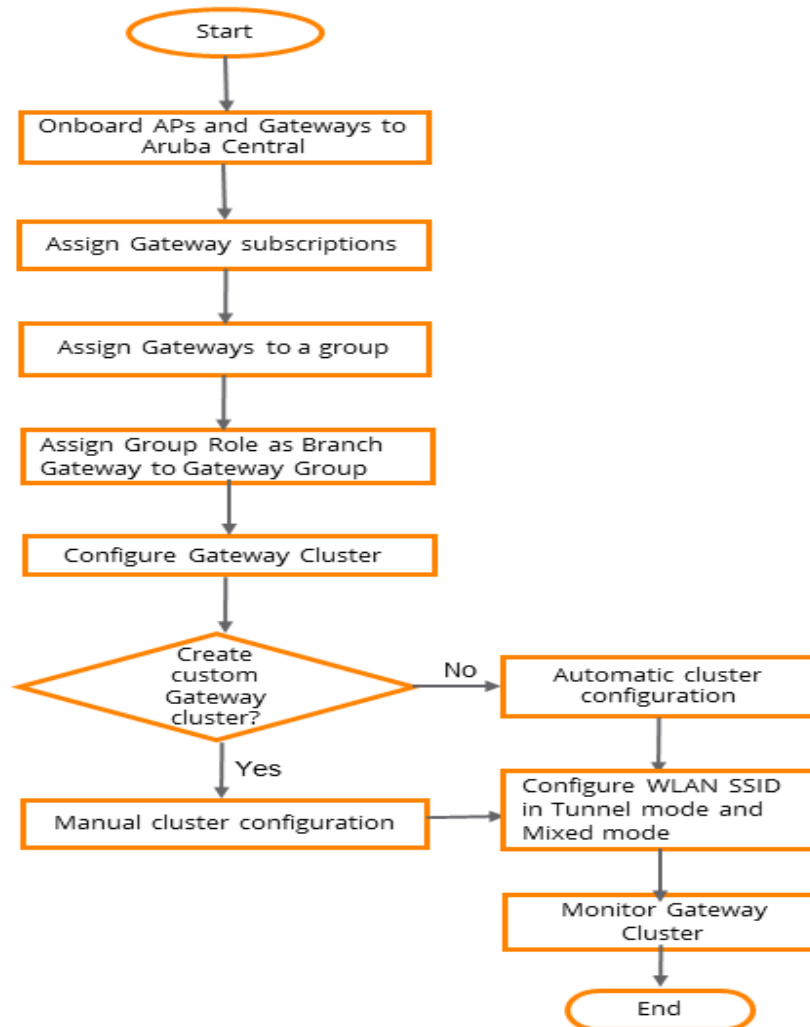
The following configuration conditions apply for gateway clusters in Aruba Central:

- To allow gateways to form a cluster, ensure that you assign gateways to the same group in Aruba Central.
- For gateways in a group assigned to the same site, a secure tunnel is established between the APs and gateways of that site.
- A gateway cluster can consist of one or several gateways.
- Gateways with ArubaOS 10.0.0.0 or later software version can automatically form a cluster when assigned to an UI group.
- When the gateways are in a template group, you must create the cluster manually using templates.

Gateway Cluster Deployment Workflow

The following flowchart illustrates the steps to deploy gateway clusters in AOS 10.x using the WebUI.

Figure 7 Gateway Cluster Deployment Flowchart



Gateway Cluster Deployment Workflow Steps

The provisioning workflow for gateway deployment includes the following steps:

Step 1: Onboard the APs and Gateways

Add the APs and gateways to Aruba Central by using an evaluation account or a paid subscription.

For more information, see [Onboarding Devices](#).

Step 2: Assign Gateway Subscriptions

You can either enable automatic assignment of subscriptions or manually assign subscriptions for the devices added in Aruba Central.

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

Step 3: Assign Gateways to a UI Group or Template Group

Aruba Central supports assigning gateways to groups for the ease of configuration and maintenance. The Aruba gateways running ArubaOS 10.0.0.0 or later versions can form a cluster automatically when they are assigned to a UI group.

Optionally, the gateways assigned to the same site can form clusters automatically among themselves.

For more information, see [Assigning Gateways to a Group](#) and [Assigning Devices to Sites](#).

Step 4: Configure the Gateway Cluster

For tunnel mode and mixed-mode SSID configuration, you must associate a gateway cluster for client authentication, policy enforcement, and role assignment to clients. The gateway clusters are created automatically at the group or at the site level. You can also manually configure the gateways in auto-group or auto-site clusters.

For more information, see [Gateway Cluster Configuration Modes](#).

Step 5: Configure a WLAN SSID for Tunnel and Mixed Mode

Client devices use service set identifier (SSID) name to identify and join wireless networks. The SSIDs distinguish a wireless network from other networks configured within a WLAN boundary.

To configure a WLAN SSID with the tunnel forwarding mode and associate the SSID to a gateway cluster, see [WLAN SSID in the Tunnel and Mixed Mode](#).

Step 6: Monitor the Gateway Cluster

AOS 10.x provides dashboards to monitor and analyze the WLAN network and health metrics for APs, gateways, and wireless clients.

For more information, see [Monitoring Gateway Clusters](#).

Gateway Cluster Configuration Modes

Aruba Central supports the following gateway cluster configuration modes:

- Cluster Group Mode (CGM)—Allows you to create gateway clusters automatically at the group or at the site level, as well as configure clusters manually.
- Cluster Configuration Mode (CCM)—Allows you to modify the parameters of an existing auto-cluster (group or site level), and add or remove gateways from a cluster.

Cluster Group Mode

In CGM, you can move gateways between the following types:

- Auto-group cluster—The gateways that are in the same group form a cluster automatically.



Only one auto-group cluster is allowed within a group.

- Auto-site cluster—The gateways that are in the respective sites within the same group form a cluster automatically.
- Manual cluster configuration—You can configure the gateways to form a cluster manually.

Configuring Automatic Gateway Cluster

Aruba gateways automatically form a cluster when they are added to a UI group in Aruba Central. Also, gateways in the same site and the same group automatically form a cluster and the APs in those sites establish a tunnel with the gateway clusters in that site.

The gateway groups must match the following criteria for automatic cluster configuration:

- There is at least one gateway in the group.
- Each group can form a cluster with up to 4 or 12 gateways depending on the gateway platform.

The automatic cluster configuration is enabled by default in the WebUI. However, if the automatic cluster configuration is disabled, complete the following steps to enable automatic configuration of gateway cluster:

1. In the **Network Operations** app, use the filter bar to select the Aruba gateway group.
2. Under **Manage**, click **Devices > Gateways**.
3. Click the **Config** icon to display the gateway configuration page.
4. Click **Advanced Mode**, and click the **High Availability** tab.
The **High Availability** details window is displayed.
5. In the **Clusters** tab, enable the **Automatic** toggle switch.
6. Select one of the following radio buttons as the mode of configuration:
 - **Auto Group**—To configure the gateways in the group to form a cluster automatically.
 - **Auto Site**—To configure the gateways in their respective site to form a cluster automatically. Ensure that the gateways in the group are added to the respective sites.

CGM creates auto-group or auto-site clusters automatically, and the **Clusters** table displays the auto-group and auto-site cluster names and the number of gateways and/or sites of that cluster.

7. (Optional) Select the **One to One Redundancy** check box to unify UDG and VDG for clusters in a branch deployment.
8. Select the auto-cluster from the **Clusters** table.
The gateways assigned to the selected cluster are displayed in the **Gateways in <group name> Cluster** table.

The following configuration conditions are applicable when CGM is moved from one mode to another in the WebUI:

- Disabled to **Auto Group/Auto Site**—The devices are added to auto-group or auto-site cluster automatically based on the group or site information. If there is a manual cluster available in the group, you must delete it to change the CGM to auto-mode.
- **Auto Group to Auto Site**—The devices mapped to the site are automatically added to the site-specific cluster. The **Auto Group to Auto Site** transition is not allowed if there are auto-group clusters mapped to an SSID in the **VLANS** tab under WLAN SSID configuration wizard. If the auto-group clusters are not mapped to any SSID, the same devices (with site mapped) form an auto-site cluster based on their site information.
- **Auto Site to Auto Group**—The devices are automatically added to auto-group cluster. The **Auto Site to Auto Group** transition is not allowed if there are auto-site clusters mapped to an SSID in the **VLANS** tab under WLAN SSID configuration wizard. If the auto-site clusters are not referenced to any SSID, the same devices form an auto-group cluster.
- **Auto Group/Auto Site to Disabled**—The existing automatic clusters at group or site level are not affected. This mode change is applicable only for manual cluster configuration.

Important Points to Note

- To change the auto-cluster configuration mode, you must first delete the referenced SSID profile from the **Wireless SSIDs** table under **Access Points > WLANS** tab.
- When **Auto Site** is enabled on a gateway group, and the gateways are part of one site, ensure that the APs are also part of the same site to establish tunnels. If the APs are not part of the same site or they are part of some other site, tunnels will not be established between the APs and the gateways within the same auto-site cluster.
- The auto-site cluster works only when the devices are assigned to the same site. For more information, see [Assigning Devices to Sites](#).

- For auto-group clusters, the cluster name is displayed in the **auto_gwcluster_<unique group ID>_0** format. For example, **auto_gwcluster_273_0**.
- For auto-site clusters, the cluster name is displayed in the **auto_gwcluster_site_<unique site ID>_<unique group ID>_0** format. For example, **auto_gwcluster_site_8_273_0**. You can modify the site name, however the unique **<site ID>** remains the same.
- You cannot add **auto_gwcluster** prefix in the manual cluster name.
- When you delete gateways from a site, the gateways from the auto-site cluster are also deleted.
- You cannot configure two auto-group clusters in the same group.
- The **One to One Redundancy** check box is available in the following scenarios:
 - When CGM is enabled and **Auto Site** radio button is selected.
 - When CGM is in manual-mode.
 - When there are no existing clusters in a group.

Cluster Configuration Mode

You must enable CCM to modify the cluster parameters for an auto-cluster or manual cluster profile.

Configuring Manual Gateway Cluster

The manual-mode also allows you to configure features such as dynamic authorization (CoA), VPN termination, multicast VLAN, and heartbeat threshold. You can configure a manual gateway cluster in the following scenarios:

- When CGM is in disabled mode—The **Automatic** toggle switch is turned off.
- When CGM is in auto-group or auto-site mode—The **Manual Cluster Configuration** toggle switch for an existing auto-group or auto-site cluster is turned on in CCM.



When you turn on the **Manual Cluster Configuration** toggle switch, the newly-added gateways do not automatically join the cluster. You must manually add the gateways to the cluster.

To manually configure gateways in a cluster when CGM is disabled, complete the following steps:

1. In the **Network Operations** app, use the filter bar to select the Aruba gateway group.
2. Under **Manage**, click **Devices > Gateways**.
3. Click the **Config** icon to display the gateway configuration page.
4. Click **Advanced Mode**, and click the **High Availability** tab.
The **High Availability** details window is displayed.
5. Turn off the **Automatic** toggle switch.



In the **Clusters** tab, the **Automatic** toggle switch is enabled by default.

6. Perform one of the following steps:
 - To edit an existing gateway cluster, select the gateway cluster from the **Clusters** table and set the CCM to manual-mode.
Also, the gateways assigned to the group are displayed in the **Gateways in <group name> Cluster** table.

- To add a new gateway to the cluster, click **+** in the **Clusters** table.

The **Manual Cluster Configuration** toggle switch is enabled.



The **+** icon is enabled only when the gateways that are not added to any cluster are available in the group.

- a. Enter the cluster name in the **Cluster Name** field.



The name of the cluster must not begin with the **auto_gwcluster** string.

- b. Click **+** in the **Gateways in <group name> Cluster** table.
 - c. Select a new gateway from the drop-down list under the **Gateway** column.
7. (Optional) To enable dynamic authorization, complete the following steps:
 - a. Turn on the **Dynamic authorization (CoA)** toggle switch.
 - b. Select a gateway in the **Gateways in <group name> Cluster** table to configure the following VRRP parameters:
 - **VRRP IP**—This is the virtual IP address of the VRRP instance. For example, for a cluster with five gateway nodes, there are five VRRP instances and five virtual IP addresses; That is, one virtual IP address for each VRRP instance. The cluster uses the virtual IP of a VRRP instance for RADIUS requests.
 - **VRRP VLAN**—VLAN for the VRRP instance.
 - (Optional) **VRRP ID**—This ID uniquely identifies a VRRP instance. The supported range of values for VRRP ID is 1-255.
 - (Optional) **VRRP Passphrase**—Passphrase to authenticate VRRP peers in a cluster. The supported range of characters for VRRP Passphrase is 1-8.
 8. (Optional) To enable VPN termination on gateways, complete the following steps:
 - a. Turn on the **VPN termination** toggle switch.

The **Public IP** column is displayed for each gateway listed in the **Gateways in <group name> Cluster** table.
 - b. Enter the public IP address for each gateway.
 9. (Optional) Enter the VLAN ID for the multicast traffic in the **Multicast VLAN** field. The supported range of values for Multicast VLAN is 0-4094.
 10. (Optional) Select one of the following radio buttons in the **Heartbeat Threshold** field:
 - **Default**—To configure a default heartbeat threshold. The default value for a port channel is 2000 ms, and the default value for a single Ethernet connection (without port channel) is 900 ms.
 - **Custom**—To configure a custom heartbeat threshold. Enter a value between 500 to 2000 ms.
 11. Click **Save Settings**.

Configuring Automatic and Manual Clusters in the Same Group

Aruba Central allows you to create multiple gateway clusters in the same group and add the desired gateways to different cluster profiles.

The following cluster combinations are supported in a single group:

- Auto-group cluster and one or more manual clusters
- Auto-site cluster and one or more manual clusters
- Multiple auto-site clusters and one or more manual clusters
- Multiple manual clusters



You cannot have two auto-group clusters or an auto-group cluster and an auto-site cluster in the same group.

Complete the following steps to configure both manual clusters and automatic clusters in the same group:

1. In the **Network Operations** app, use the filter bar to select the Aruba Gateway group.
2. Under **Manage**, click **Devices > Gateways**.
3. Click the **Config** icon to display the gateway configuration page.
4. Click **High Availability**, and then click the **Clusters** tab.
5. Turn on the **Automatic** toggle switch, if it is disabled and select either **Auto Group** or **Auto Site** radio button.
6. Create a manual cluster by following the steps in [Configuring Manual Gateway Cluster](#).

Both the auto-cluster and the manual cluster that you created are displayed in the **Clusters** table.



You cannot enable auto-cluster mode until you delete the manual cluster from the group.

Deleting a Gateway from a Cluster

You can delete gateways from a group in an auto-cluster when CGM is in either auto- or manual- mode, and the CCM is in manual-mode.

To delete a gateway from an auto-cluster, complete the following steps:

1. In the **Network Operations** app, use the filter bar to select the Aruba Gateway group.
2. Under **Manage**, click **Devices > Gateways**.
3. Click the **Config** icon to display the gateway configuration page.
4. Click **High Availability**, and then click the **Clusters** tab.
5. Select the cluster name from the **Clusters** table.
The **Automatic** toggle switch is enabled by default.
6. Turn on the **Manual Cluster Configuration** toggle switch, if it is not enabled by default.
7. Select the gateway from the **Gateways in <group name> Cluster** table, and click the delete icon on the right.
The **Confirm Removal of Gateway from Cluster** pop-up window is displayed.
8. Click **Remove Gateway**.
9. Click **Save Settings**.

The gateway is removed from the auto-cluster.

Deleting Cluster Profile

You can delete an auto-cluster profile when the CGM is in manual-mode.

To delete an auto-cluster, complete the following steps:

1. In the **Network Operations** app, use the filter bar to select the Aruba Gateway group.
2. Under **Manage**, click **Devices > Gateways**.
3. Click the **Config** icon to display the gateway configuration page.
4. Click **High Availability**, and then click the **Clusters** tab.
The **Automatic** toggle switch is enabled by default.
5. Turn off the **Automatic** toggle switch.
6. Select the auto-cluster name from the **Clusters** table, and click the delete icon on the right.
The **Delete Cluster** pop-up window is displayed.
7. Click **Yes**.
8. Click **Save Settings**.
The auto-cluster is removed from the **Clusters** table.

Monitoring Gateway Clusters

To view and monitor the gateway cluster dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage**, click **Devices > Gateways**.
3. Click the list icon to view a list of gateways provisioned in Aruba Central.
4. Click **Clusters** to view the cluster details, and the tunnels between the APs and the gateways in the cluster.
For more information, see [Monitoring Gateway Clusters](#).

Configuring Authentication Survivability on a Gateway Cluster

Authentication survivability is required when remote link failures occur between a Gateway cluster and an authentication server that is either in the cloud or a data center. If the connectivity between the gateway cluster and the authentication server is lost for a maximum duration of 7 days, authentication survivability ensures that the known users can securely join the network even if the authentication server is unavailable. This feature is currently supported in tunnel and mixed mode deployments.

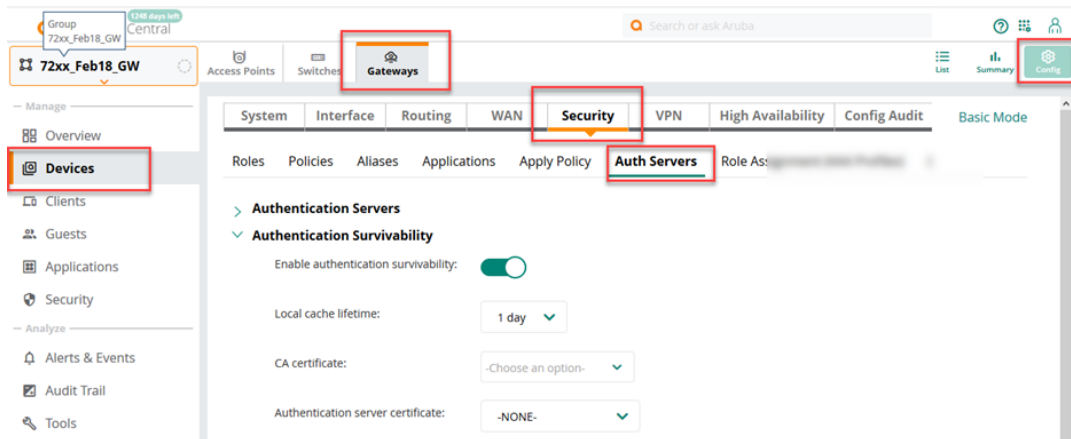
It is recommended that you configure **Authentication Survivability** only in the gateway group dashboard.

To configure authentication survivability on a gateway group, complete the following steps:

1. Configure a gateway group: Set the filter to a group containing at least one gateway. The dashboard context for a group is displayed.
 - a. Under **Manage**, click **Devices > Gateways**.
 - b. Click the **Config** icon to view the group configuration dashboard.
2. Click **Advanced Mode** and then click **Security**.
3. Under **Security**, click the third-level tab of **Auth Servers**.
4. In the resultant page, scroll to the bottom and click the **Authentication Survivability** drop-down.

- Slide the toggle switch next to **Enable authentication survivability**.

Figure 8 *Enabling Authentication Survivability*



- Select a value within the range of 1 to 7 days from the **Local cache lifetime** drop-down to set the duration after which the authenticated credentials in the cache expires. When the cache expires, the clients are required to authenticate again with the external authentication server.
- From the **CA Certificate** drop-down, select the client's CA certificate to be configured as Trusted CA cert on the Gateway device. You can add multiple CA certificates in this field.
- From the **Authentication server certificate** drop-down, select a server certificate used by the local survival server to associate EAP-TLS for 802.1X authentication.
- Click **Save Settings**.

Tunnel Orchestration for WLAN Deployments

Aruba supports automated Tunnel Orchestrator for LAN Tunnels service for APs and Gateways deployed in campus WLAN. Based on the location of the devices, the tunnel orchestrator service establishes either GRE tunnels (at the branch site) or IPsec tunnels between Gateways and APs provisioned in an Aruba Central account. The tunnel orchestrator service along with AP Tunnel Agent and Gateway Tunnel Agent creates and maintains the tunnels between APs and Gateways.

The Tunnel Orchestrator for LAN Tunnels service can be enabled either globally or on individual device groups. By default, the Tunnel Orchestrator for LAN Tunnels service is enabled for Gateways and AP devices provisioned in an Aruba Central account. The tunnel orchestrator automatically builds a tunnel mode network based on the tunnel endpoint preference that you configure in the WLAN SSID. The tunnel orchestrator selects the Gateway-AP pairs and decides the number of tunnels between the Gateway cluster and APs based on the virtual AP configuration.

To allow APs and Gateways to automatically establish tunnel modes, ensure that the following configuration tasks are completed:

- Aruba Gateways are onboarded to a group in Aruba Central.
- Aruba APs are provisioned in Aruba Central.
- Aruba Gateways and APs are upgraded to ArubaOS 10.0.0.0 or a later software version.
- A WLAN SSID with the tunnel forwarding mode is configured on the APs. When you create a new SSID, you must select the primary cluster name or Gateway where you want to establish tunnel traffic of the SSID. Optionally, you can select the backup cluster that can be used when the primary cluster goes down completely. The APs establish tunnel with the Gateways in a Gateway cluster.

- If the overlay IPsec tunnels initiated by APs to a VPN Concentrator use NAT traversal, the UDP 4500 port is enabled.

AP Tunnel Agent and Gateway Tunnel Agent

The AP Tunnel Agent (ATA) and Gateway Tunnel Agent are the tunnel management modules in APs and Gateways respectively. They are responsible for handling all GRE and IPsec tunnel configurations and maintaining the status in APs and Gateways. ATA and Gateway Tunnel Agent provide the following functions:

- Register the information of APs and Gateways with tunnel orchestrator service.
- Receive Gateway cluster and tunnel information and distribute to other processes.
- Create and maintain IPsec and GRE tunnel and survivability status.

Viewing Tunnel Orchestrator Logs


You can enable crypto and tunnelmgr process logs on the Gateways in the **Logging Levels** table of the WebUI.

To view the logging levels:

1. In the **Network Management** app, use the filter bar to select the Aruba Gateway group.
2. Under **Manage**, click **Devices > Gateways**.
3. Click the **System** tab.
4. Expand the **Logging Levels** accordion.
The **Logging Levels** table is displayed.

Monitoring Tunnel Modes

To monitor tunnel modes:

1. In the **Network Management** app, use the filter bar to select the Aruba Gateway group.
2. Under **Manage**, click **Devices > Gateways**.
3. Click the list  icon to view a list of Gateways provisioned in Aruba Central.
4. Click **Clusters**.
The **Gateway Clusters** dashboard is displayed.
5. Click the cluster name for which you want to view the tunnel mode details.
The cluster details are displayed.
6. Click the **Tunnels** tab to view the tunnel details and the operational status of the tunnels.
For more information, see [Monitoring Gateway Clusters](#).

Troubleshooting Tunnel Configuration

To perform advanced troubleshooting on tunnels, complete the following steps:

1. In the **Network Operations** app, use the filter bar to select a group, Gateway, or AP.
2. Under **Analyze**, click **Tools**.
The **Tools** page is displayed.
3. Click the **Commands** tab.
4. In the **Commands** tab, select **Access Point** or **Gateway** from the **Device Type** drop-down list.
5. From the **Available Devices** drop-down list, select the AP or Gateway based on your selection in step 4.
You can select multiple APs or Gateways from the **Available Devices** drop-down list.

Overlay Tunnel Config

Index	UAC IP	Odev	Tunnel Type	Booster	MTU	Vlan List
0	10.15.41.52	gre0	GRE	1	1500	1,30-32,41
1	10.15.41.50	gre1	GRE	1	1500	1,30-32,41

To check the connection between Tunnel Orchestrator and Gateway agent, and also check counters :

```
(host)# show crypto oto
```

```
OTO Status
Channel state:          CONNECTED
Channel UP since:      Fri Nov 1 02:44:13 2019
Last disconnect:      Fri Nov 1 02:44:10 2019
State Update Event Sent 165
Channel Up count:      165
Channel Down count:    164
Keepalive Interval:    25
#Create Channel:       168
#Delete Channel:       167
#KeepAlive Sent:       37294
#KeepAlive Received:   36802
#KeepAlive Pending:    0
Create Spec:           197
Update Spec Sent/Recv: 6/1876
Delete Spec:           111
Resync Event Sent:     1040
Ike Event Sent:        196
Peer Down DPD:         20
BG-SRC Learn/OnRekey: 133/1853
BG-SRC Err SPI/Map/Vlan: 0/0/0
Rekey Request/Done/Abort: 1874/1853/21
State Update Event Sent 165
Down Event Sent:       0/4
```

- To view the tunnels and keys on Gateways:

```
(host)# show crypto ipsec sa
```

```
IPSEC SA (V2) Active Session Information
-----
Initiator IP                               Responder IP
      SPI(IN/OUT)                Flags Start Time           Inner IP
-----
10.15.41.52                                10.15.41.50
      e926c00 /e2d35200 T2      Nov 1 01:59:58             -
10.15.41.245                               10.15.41.52
      9ea28300/5908e300 UT1t    Nov 1 03:23:03             -
10.15.41.252                               10.15.41.52
      46852b00/36c6eb00 UT1t    Nov 1 03:23:03             -
```

Flags: T = Tunnel Mode; E = Transport Mode; U = UDP Encap
L = L2TP Tunnel; N = Nortel Client; C = Client; 2 = IKEv2
l = uplink load-balance t = Tunnel Service

Total IPSEC SAs: 3

(host)# **show tunnelmgr tunnel-list**

Tunnelmgr Table Dump

```
-----  
Tunnel ID                               Map ID  Peer IP      Peer MAC  
  Type  Status  GRE ID  Start Time                Created Time  
Last Down-Time  
-----  
-----  
-----  
f9210222-3f12-4b96-84bd-7aa9234720e7  327683  10.15.41.252  
ac:a3:1e:c8:25:66 AP    UP      11      Wed Oct 30 23:18:19 2019  Fri Nov  
1 01:46:05 2019  Fri Nov 1 01:46:05 2019  
c0020760-3dde-466e-b8dd-6cefb334e876  327682  10.15.41.245  
90:4c:81:ce:08:9e AP    UP      14      Wed Oct 30 23:18:09 2019  Thu Oct  
31 23:46:35 2019  Thu Oct 31 23:44:23 2019
```

Total Tunnel Entries: 3

(host)# **show tunnelmgr counters**

Tunnelmgr Counters:
GSM AP UP/Down :147/261
Tunnel UP/Down :147/150
Map ADD/Map Del :196/114
IKE Msg Tx/Fail :0/0
GSM ADD Tx/Fail :408/0
GSM Del Tx/Fail :108/0
GSM UpdateTx/Fail :0/0

To check the tunnel IDs on Gateways:

(host)# **show datapath tunnel table**

```
Datapath Tunnel Table Entries  
#           Source           Destination  Prt  Type  MTU  VLAN  Acls  
           BSSID           Decaps      Encaps  Heartbeats  
Flags      EncapKBytes  DecapKBytes  
-----  
-----  
-----
```

```

19      10.15.41.50      10.15.41.252      47  0      1500  0      0      0      0
0      0      0      00:00:00:00:00:00      56699      3521      47475  EMSPDb

```

To check whether client traffic is going through tunnel:

```
(host)# show datapath session | include 30.30.30.252 | include 10.15.80.80
```

```

30.30.30.252      10.15.80.80      1      8011  2048      0/0      0      0      1
tunnel 19  10      1      60      FCI      28
30.30.30.252      10.15.80.80      1      8020  2048      0/0      0      0      0
tunnel 19  7      1      60      FCI      28
30.30.30.252      10.15.80.80      1      8001  2048      0/0      0      0      1
tunnel 19  1b      1      60      FCI      28

```

To check if tunnel status is changed to **Survived** on AP:

```
(host)# show ata endpoint
```

```

ATA Endpoint Status
-----
UUID                               IP ADDR      STATE        TUN
DEV  TUN SPI (OUT/IN)    PORT (SRC/DST)  VALID TIME (s)  TUNNEL TYPE  GRE VLANs
      HBT (Jiff/Missed/Sent/Rcv)  INNER IP
-----
-----
d14b436a-5173-4aad-a26a-bc200adb89c8  10.15.41.52  SM_STATE_SURVIVED  tun1
dee2a700/55631b00  4500/4500      -1455           GRE           1,30-32,41
247886/0/173525/170754      10.15.41.245
af5259fe-8350-4385-a7e5-7744eac239cf  10.15.41.50  SM_STATE_SURVIVED  tun0
f8d6d000/39dce800  4500/4500      -1455           GRE           1,30-32,41
247886/0/173323/170264      10.15.41.245
Total Endpoints Count: 2

```

To check if legacy IKE tunnel is formed with inner IP address as AP IP on Gateway:

```
(host)# show crypto ipsec sa
```

```

IPSEC SA (V2) Active Session Information
-----
Initiator IP                               Responder IP
      SPI (IN/OUT)                Flags Start Time                Inner IP
-----
-----
10.15.41.52                               10.15.41.50

```

```
c0fd8900/62784c00 T2 Nov 1 23:32:34 -
10.15.41.245 10.15.41.52
dee2a700/55631b00 UT2 Nov 1 23:15:52 10.15.41.245
```

Configuring Aruba Gateways for Campus WLAN Deployment

In overlay and mixed mode deployments, the client traffic is forwarded to a Gateway cluster for client authentication and policy enforcement. To enable Gateways to perform client authentication and derive user roles, the following configuration is required on Gateways:

- [Configuring Address Pools Gateways](#)
- [Configuring VLANs on Gateways](#)
- [Configure Authentication Profiles](#)
- [Configuring User Roles](#)
- [Configuring Firewall Policies](#)
- [Applying Policies to Ports and VLANS](#)
- [L2 Authentication](#)

You can either use the Guided Setup wizard or the advanced configuration options to configure Gateways. For more information on the Guided Setup wizard and the configuration procedures, see [Aruba Central](#) user documentation.

Tunnel and Mixed Mode Deployment

WLAN is required to establish wireless connection between devices and thereby eliminating the need for cables. WLAN helps build personal and business networks without wiring the building with Ethernet. It also provides a way for small devices, such as smartphones, tablets, laptops, and Point of Sale (POS) machines to connect to the network.

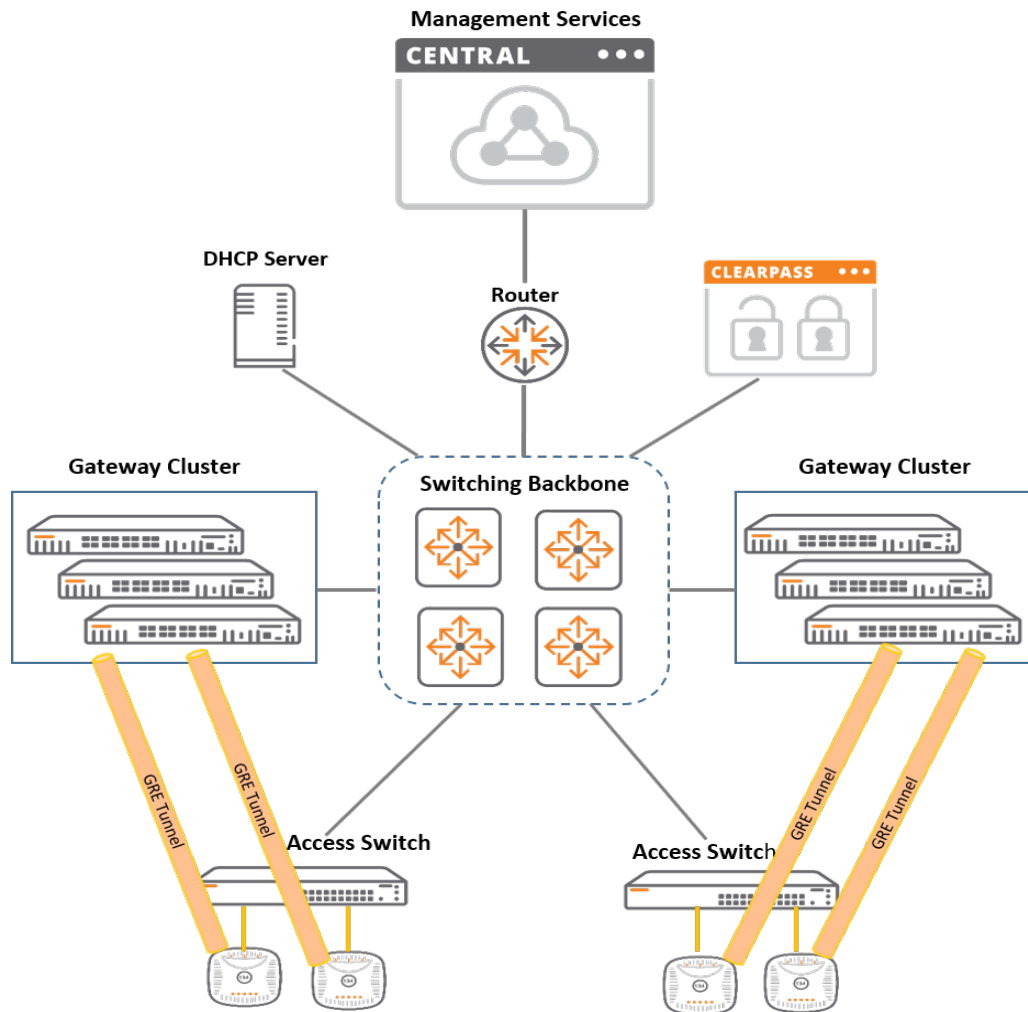
The AOS 10.x in tunnel mode consists of at least one Gateway cluster for security and network resiliency. The network created on tunnel mode or mixed mode acts as a virtual network on top of the physical network that is created on bridge mode. In the tunnel-mode of AOS 10.x, VLANs are configured on Gateway cluster and APs tunnel traffic to Gateways. APs function as authenticators and send authentication and accounting requests to the Gateway cluster.

In the Mixed mode of AOS 10.x, VLANs are configured either on the Gateway cluster or on APs which tunnel client traffic to the Gateway cluster based on the optimum traffic route.

The hardware infrastructure of the tunnel mode and mixed mode deployments require APs and Gateways with ArubaOS 10.0.0.0 or later software version.

The following figure illustrates the tunnel deployment mode:

Figure 9 Tunnel Mode Deployment



Network Setup for Tunnel and Mixed Mode Deployment

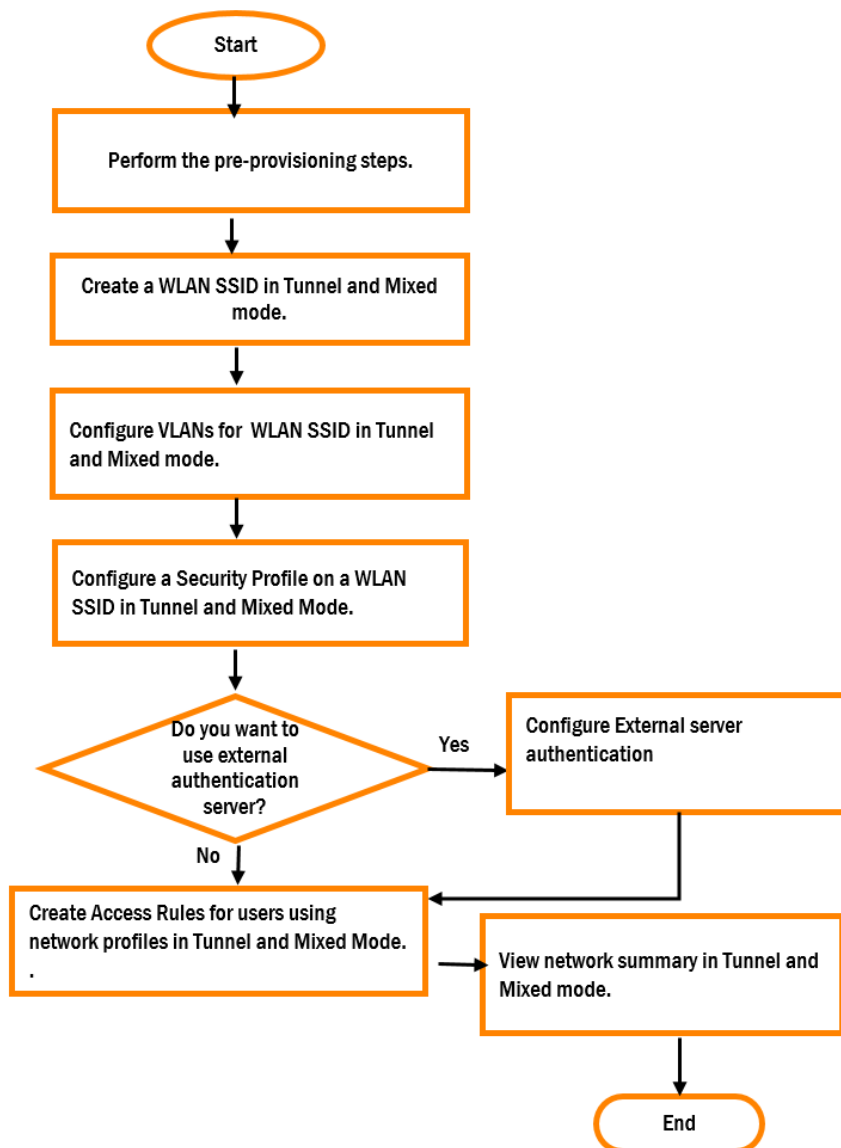
The client connection workflow in an tunnel network setup involves the following steps:

1. The administrator onboards the APs and Gateways to a group in AOS 10.x.
2. The Gateways assigned to the same group automatically form a Gateway cluster.
3. The administrator configures a WLAN SSID with the **Tunnel** or **Mixed** forwarding mode and associates the SSID to a Gateway cluster.
4. The Tunnel Orchestrator for VLAN Tunnels service in AOS 10.x establishes secure tunnels between APs and the Gateways.
5. The client connects to the SSID broadcast on the AP.
6. The AP acts as an authenticator and sends the client traffic to a Gateway in the cluster. The Gateway acts as an authentication proxy. For example, based on the VLAN to which the client is assigned, the client traffic is bridged locally or forwarded to the Gateway through a secure tunnel. This assignment is done by selecting **Bridge** or **Tunnel** as traffic forwarding mode for the VLAN in **VLAN Assignment Rules** table on the **VLANS** tab.

7. Based on the security profile and role assignment policy defined in the WLAN SSID, the Gateway forwards the request to the authentication server and derives the user role and VLAN for the client either locally or from an external authentication server.
8. After the client completes the authentication successfully, the AP applies the user role and VLAN received from the Gateway cluster.
9. The client is assigned an IP address and a user role.
10. When the client connects to the network, the traffic sent by the client is encapsulated and sent to the Gateway over GRE tunnel.
11. The Gateway bridges traffic to the client VLAN.
12. When the client roams from one AP to another across the VLANs, the Cloud-Assisted Roaming Services feature ensures that the client's wireless connection is seamless without a need for re-authentication.

Tunnel and Mixed Mode Deployment Workflow

The following flowchart illustrates the procedure for setting up AOS 10.x tunnel and mixed mode deployment for WAN Setup.



Tunnel and Mixed Mode Deployment Workflow Steps

The provisioning workflow for tunnel and mixed mode deployments includes the following steps:

Step 1: Follow the Pre-Provisioning Procedures

Before you get started with the configuration of WLAN SSID in the tunnel and mixed mode for LAN setup, refer to the following topic to complete the pre-provisioning procedures: [Getting Started with the Deployment](#)

For deployments with cluster, you must configure a WLAN SSID in the tunnel and mixed mode.

Step 2: Create a WLAN SSID Profile in Tunnel and Mixed Mode

An SSID is the primary name associated with an 802.11 wireless local area network (WLAN). Client devices use this name to identify and join wireless networks.

For more information on creating a WLAN SSID in tunnel and mixed mode, see the following sections:

- [Creating a WLAN Profile in Tunnel and Mixed Mode](#)
- [Configuring General > Advanced Settings for a WLAN SSID Profile](#)

Step 3: Configure a VLAN for a WLAN SSID Profile in Tunnel and Mixed Mode

A virtual LAN (local area network) is a group of devices on a single or multiple LANs that are logically configured to communicate seamlessly even if they are physically located on different LAN segments. In other words, a VLAN is a logical subnetwork that groups a collection of devices from different physical LANs.

For more information on configuring VLANs in tunnel and mixed mode, see the following sections:

- [Configuring VLAN Settings for WLAN SSID Profile in Tunnel and Mixed Mode](#)
- [Creating Named VLANs for Static VLAN Assignment](#)
- [Creating Named VLANs for Dynamic VLAN Assignment](#)
- [Creating VLAN Assignment Rules for Dynamic VLAN Assignment](#)

Step 4: Configure Security for a WLAN SSID Profile in Tunnel and Mixed Mode

AOS 10.x provides security for a WLAN SSID in Enterprise, Personal, and Captive Portal. There are no security policies bound with Open network profiles.

For more information on configuring a security profile, see the following sections:

- [Configuring a Security for a WLAN SSID Profile in Tunnel and Mixed Mode](#)
- [Configuring Enterprise Security for a WLAN SSID Profile](#)
- [Configuring External Authentication Servers for a WLAN SSID Profile](#)
- [Configuring Personal Security for a WLAN SSID Profile](#)
- [Configuring Captive Portal Security for a WLAN SSID Profile](#)
- [Configuring Open Security for a WLAN SSID Profile](#)

Step 5: Configure Access for a WLAN SSID Profile in Tunnel and Mixed Mode

A user access rule defines which users can automatically be assigned user access when logging in to the network. AOS 10.x allows you to configure access rules and roles for WLAN clients in Enterprise, Personal, and Captive Portal networks. However, access rules and user role configurations are not applicable in open security networks.

For more information on configuring access rules and roles, see [Configuring Access Rule for a WLAN SSID Profile in Tunnel and Mixed Mode](#).

Step 6: View the Network Summary for a WLAN SSID Profile in Tunnel and Mixed Mode

AOS 10.x displays a summary of all the basic configurations that you set for creating the WLAN SSID in tunnel and mixed mode.

For more information on network summary in tunnel and mixed mode, see [Viewing Network Summary of Tunnel and Mixed Mode](#).

MultiZone

The MultiZone feature enables you to segregate the virtual APs tunnel traffic to different gateways. MultiZone allows organizations to have multiple and separate secure networks while using the same AP. It also allows the AP to terminate SSIDs to multiple gateways that reside in different zones or clusters.

Initially, when the AP boots up, the first zone it contacts is called the primary zone. The MultiZone configuration is forwarded to the AP based on the primary cluster configuration of different SSIDs. In the same group, each SSID can choose a different primary cluster to form a different zone. The AP virtually connects to each zone independently. Hence, the tunnel traffic is segregated based on the SSIDs. Data zone is the secondary zone that an AP connects to after receiving the MultiZone configuration from the primary zone. If there are MultiZone profiles configured and associated in the AP group or AP name profile of the primary zone, then the AP enters MultiZone state and starts connecting with the specified data zones.

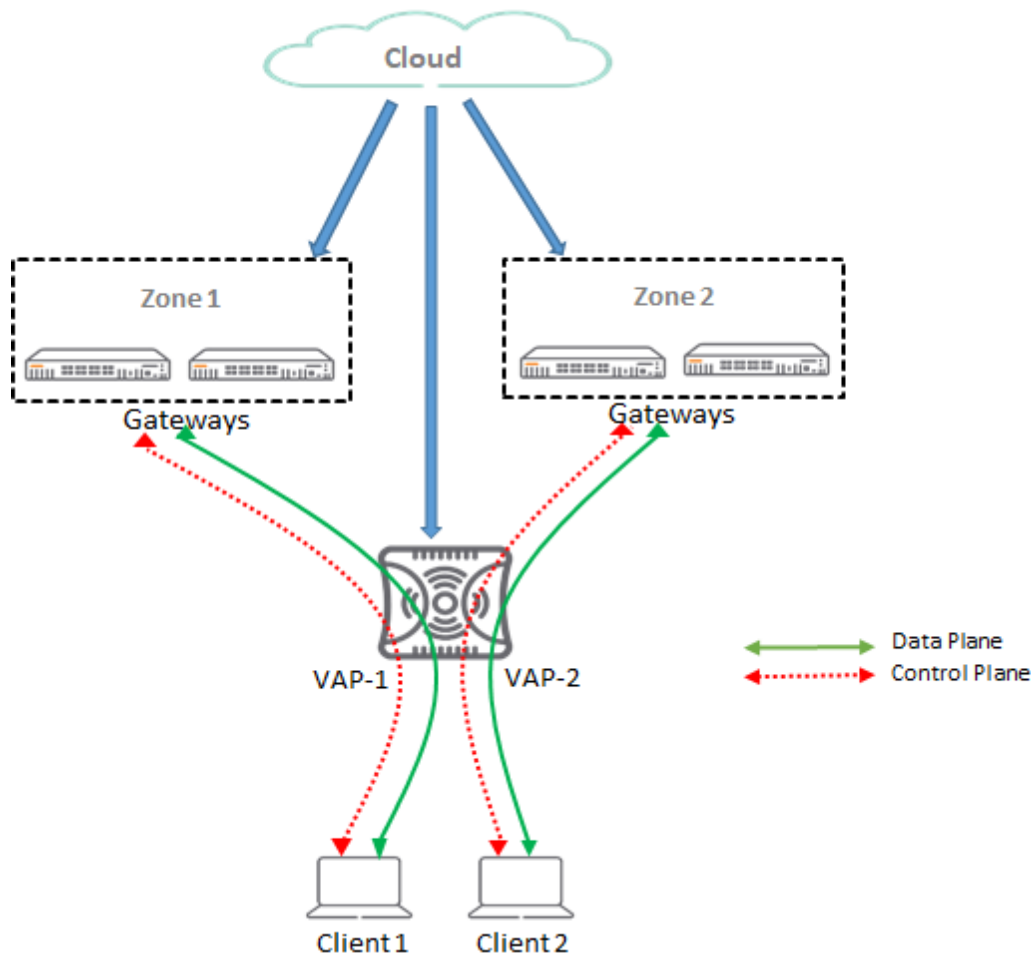
The maximum number of allowed clusters is 5 and total number of allowed gateways is 12.



The gateways in different zones are independent and do not communicate with one another.

[Figure 10](#) illustrates the configuration of MultiZone feature between two zones.

Figure 10 MultiZone Configuration



In the above diagram, Client 1 and Client 2 connect to VAP-1 and VAP-2 respectively. The MultiZone configuration segregates the tunnel traffic of VAP-1 and VAP-2 and forwards the traffic to different Gateways under Zone 1 and Zone 2.

Guidelines for MultiZone

- Different virtual APs can be mapped to different zones. For example, VAP-1 can connect to one cluster and VAP-2 can connect to another cluster.
- The AP creates the tunnels with different clusters and not with a single cluster.
- Different clients can connect to different virtual APs. For example, if one client connects to VAP-1, the AP sends client traffic to Zone 1. Similarly, if another client connects to VAP-2, the AP sends client traffic to Zone 2.
- The MultiZone feature requires an advanced license, and is disabled in the absence of the advanced license. Only an AP with advanced license can establish active SSID tunnels with data zone gateways. The AP with foundation license cannot establish active SSID tunnel with data zone gateways.

For more information on configuring MultiZone, see [Configuring VLAN Settings for WLAN SSID Profile in Tunnel and Mixed Mode](#).

Creating a WLAN Profile in Tunnel and Mixed Mode

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**, go to **Device(s) > Access Points**.
3. If required, click the **Config** icon.
The second-level tabs to configure APs are displayed.
4. Go to the **WLANs** tab.
The **Wireless SSIDs** table is displayed listing the existing SSID profiles.
5. To create a new SSID profile, click **+ Add SSID**. To edit an existing SSID profile, click the row, and then click the edit icon.
The **Create a New Network** page is displayed for creating a new SSID. The **Networks** page is displayed for editing an existing SSID.
6. To create a new SSID name, enter the name of an SSID, and click **Next**.
7. (Optional) Proceed to [Configuring General > Advanced Settings for a WLAN SSID Profile](#).

Configuring VLAN Settings for WLAN SSID Profile in Tunnel and Mixed Mode

To configure VLAN settings for an SSID, complete the following steps:

1. To access the WLAN SSID configuration wizard for a new SSID profile or an existing SSID profile, see [Configuring a WLAN SSID Profile in Bridge Mode](#) or [Creating a WLAN Profile in Tunnel and Mixed Mode](#).
2. In the WLAN SSID configuration wizard, click the **VLANS** tab.
3. In the **VLAN** tab, select any of the following options in **Traffic Forwarding Mode** to create a network in tunnel mode:
 - **Tunnel**—To forward client traffic to an Aruba gateway node in the tunnel mode network, select the **Tunnel** mode.
 - **Mixed**—To use both bridge and tunnel forwarding modes, select the **Mixed** option. To enable APs to tunnel client traffic to a gateway node in the tunnel mode network, select a gateway cluster from the **Cluster** drop-down list.
4. Select one of the following options from the **Primary Gateway Cluster** drop-down list:
 - For auto-group clusters, select **<group name:auto_gwcluster_<group ID>_0>**. For example, **Group1:auto_gwcluster_243_0**.
 - For auto-site clusters, select **<group name:auto_gwcluster_site_<site ID>_<group ID>_0>**. For example, **Group1:auto_gwcluster_site_8_243_0**.
 - For manual clusters, select **<groupname>manualclusterprofilename>**. For example, **Group2:ManualCluster123**.



The **Primary Gateway Cluster** drop-down list allows the APs to establish tunnels with the gateways in the tunnel mode network.

5. (Optional), select a secondary gateway cluster profile from the **Secondary Gateway Cluster** drop-down list.



You can use the **Secondary Gateway Cluster** drop-down list as a failover, when the primary cluster is unavailable.

- Select the **Cluster Preemption** check box to allow the AP to switch back from the SSID of secondary gateway cluster to the SSID of primary gateway cluster, when the primary gateway cluster becomes available.
6. Select the client VLAN assignment mode for WLAN clients and configure the following parameters:
 - **Static**—Allows you to specify a VLAN ID of single VLAN in the **VLAN ID** text box. You can select the VLAN name that is mapped to the VLAN ID from the **VLAN ID** drop-down list. For more information, see [Creating Named VLANs for Static VLAN Assignment](#). You can also include a large number of clients that need to be in the same subnet by specifying the configure VLAN pool. For more information on configuring VLAN pool, see [User-Based Tunneling in Dynamic Segmentation](#).
 - **Dynamic**—Allows you to assign the VLANs dynamically from a DHCP server. You can also create a new VLAN assignment rules by clicking the + sign. The **New VLAN Assignment Rule** pop-up window is displayed to enter details such as attribute, operator, string, and VLAN ID. For more information, see [Creating Named VLANs for Dynamic VLAN Assignment](#). For Mixed mode, the assignment of a client to a VLAN is done by selecting **Bridge** or **Tunnel** as traffic forwarding mode for the VLAN in **VLAN Assignment Rules** table on the **VLANs** tab.
 7. Click the **Show VLAN** section to view all the named VLANs mapped to the VLAN ID.
 8. To configure the VLAN Name and VLAN ID mapping feature, click the **Add Named VLAN** option to enter the VLAN Name and VLAN ID that is required to be mapped.
 9. Click **Next** to configure security settings.

Important Points to Note

- When you select `<group name:auto_gwcluster_site_<site ID>_<group ID>_0>` from the **Primary Gateway Cluster** drop-down list, the tunnel orchestrator service automatically allows the devices on the particular site to establish tunnels among themselves. For example, an AP in site S1 only establishes tunnel with a gateway in site S1. The AP in S1 does not establish a tunnel with the gateway in site S2.
- The following are the various scenarios applicable when you select the **Cluster Preemption** check box:
 - The reachable number of gateways in the primary cluster is equal to or more than the secondary cluster.
 - When all the tunnels are down, the tunnel that comes up first will serve the SSID profile.
 - The virtual APs wait for 5 minutes after they failover from one gateway cluster to another.
 - There is 1 minute delete time for Virtual APs when they failover from primary cluster to secondary cluster and vice versa.
 - All clients get disconnected during failover from one cluster to another.

Configuring a Security for a WLAN SSID Profile in Tunnel and Mixed Mode

You can configure the following types of security profiles on a WLAN SSID:

- **Enterprise**—For enterprise WLAN configuration, see [Configuring Enterprise Security for a WLAN SSID Profile](#).

- **Personal**—For personal network configuration, see [Configuring Personal Security for a WLAN SSID Profile](#).
- **Captive Portal**—For guest user access configuration, see [Configuring Captive Portal Security for a WLAN SSID Profile](#).
- **Open**—For open network with no authentication profiles, see [Configuring Open Security for a WLAN SSID Profile](#).

Configuring External Authentication Servers in the SSID Security Profile

WLAN clients connecting to an SSID in the network can authenticate to an external server based on the security profile configured on the SSID.

You can create and associate an external authentication server when configuring a security profile for an WLAN SSID.



In a Tunnel mode or Mixed mode, authentication is performed at the gateway cluster level.
In the Tunnel and Mixed mode, the APs act as authenticators and gateways act as authentication proxies.

The following table describes the procedure for creating external authentication servers for WLAN client authentication. You can select between **LDAP**, **RADIUS**, and **Dynamic Authorization**:

Table 22: 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	Set Radsec to Enabled to enable secure communication between the RADIUS server and AP by creating a TLS tunnel between the AP and the server. If Radsec is enabled, the following configuration options are displayed: Radsec Port —Communication port number for RadSec TLS connection. By default, the port number is set to 2083. 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.

Type of Server	Parameters
Timeout	The timeout duration for one RADIUS request. The AP 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 AP. 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 AP-based cluster deployments, ensure that you enter the VC IP address as the NAS IP address. For Cloud AP based Campus WLAN deployments, ensure that you enter the AP 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.
Dead Time	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. If Dynamic RADIUS Proxy (DRP) is enabled on the APs, configure the following parameters: 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. DRP GATEWAY —Gateway IP address of the DRP VLAN.
Service Type Framed User	Select any of the following check boxes to send the service type as Framed User in the access requests to the RADIUS server: 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)	Select any of the following check boxes to detect the server status of the RADIUS server: Authentication —Select this check-box to ensure the AP sends a status-server request to determine the actual state of the authentication server before marking the server as unavailable. Accounting —Select this check-box to ensure the AP sends a status-server request to determine the actual state of the accounting server before marking the server as unavailable.
LDAP	

Type of Server	Parameters
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-Distinguished-Name	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 .
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.
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.

Configuring Access Rule for a WLAN SSID Profile in Tunnel and Mixed Mode

You can configure up to 64 access rules for a wireless network profile.



Configuration of ACLs for User Access is not applicable for Open network.

To configure access rules for a network, complete the following steps:

1. In the WLAN SSID configuration wizard, click the **Access** tab.
2. In **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. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. To define an access rule:
 - a. Click (+) icon.
 - b. Select appropriate options in the **New Rule** pane.
 - c. Click **Save**.
 - **Role based**—Select **Role based** to enable access based on user roles. For role-based access control:
 - Create a user role if required.
 - Create access rules for a specific user role. To configure access rules for network services, refer to the *Configuring Access Rules* section.
 - Create a role assignment rule.
3. Click **Next**. The **Summary** tab displays the **Network Summary** page.

Configuring Access Rules

To configure access rules for network services, complete the following procedure:

1. In the WLAN SSID configuration wizard, click the **Access** tab. The **Access** page is displayed.
2. Select the type of access control.
3. Click **Roles**.
4. Under **Access Rules For Selected Roles**, click **+ Add Rule** to add a new rule. The new rule window is displayed.

5. Under **Rule Type**, select the type of access rule. For example, **Access Control**.
6. To configure access to applications or application categories, select a service category from the following list:
 - **Network**
 - **Application Category**
 - **Application**
 - **Web Category**
 - **Web Reputation**

7. Based on the selected service category, configure the following parameters:

Table 23: 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. <p>NOTE: If TCP and UDP uses the same port, ensure that you configure separate access rules to permit or deny access.</p>
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.
Log	Select Log to create a log entry when this rule is triggered. The AOS 10.x firewall supports firewall based logging. Firewall logs on the APs 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 23: Access rule configuration parameters

Data Pane Item	Description
802.1 priority	Select 802.1 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.

8. Click **Save Settings**.

Viewing Network Summary of Tunnel and Mixed Mode

The **Network Summary** page now displays all the settings configured in the **General**, **Security**, **VLANs**, and **Access** tabs.

See [Monitoring Network Summary](#).

User-Based Tunneling in Dynamic Segmentation

The Dynamic Segmentation feature is Aruba's security architecture that provides the ability to dynamically assign roles to a wired port based on the access method of a client and enforce application-aware policies to all devices connecting to the infrastructure. Dynamic Segmentation simplifies and secures the network by unifying policy enforcement across wired and wireless networks. When a client device is connected to a switch, it is assigned a role, either locally or by ClearPass Policy Manager (CPPM), and its traffic is tunneled through a gateway. CPPM provides robust policy management and orchestration capabilities to derive roles, based on user and device identity, device profiling, and health along with time and location- keeping traffic safe and secure. This feature also provides users the ability to segment client traffic via traditional, locally switched VLANs or to tunnel traffic back to an Aruba Mobility Controller.

User-Based Tunneling (UBT) in Dynamic Segmentation allows you to redirect specific wired users traffic from the switches to the Gateway to enforce DPI and firewall functionality, application visibility, and bandwidth control offered by Aruba Gateway. UBT implements the capability to tunnel traffic on a user role-basis or device basis, tunneling traffic of a given client or device, based on an assigned user role. The policies associated with that client could be driven through a RADIUS server such as ClearPass Policy Manager, a downloaded role from ClearPass Policy Manager, or by local MAC authentication in the switch. UBT can authenticate these devices using ClearPass Policy Manager, and tunnel the client traffic, utilizing the advanced firewall and policy capabilities in the Aruba Mobility Controller, and also provide high availability and load balancing with clustering Gateways.

Authentication is supported only from the switch, and not from the controller.



UBT is supported on Aruba switches containing 16.08.0005, 16.09.0003 or later versions.

AOS 10.x supports UBT 1.0 and 2.0 versions. UBT 1.0 and 2.0 versions provide VLAN configuration on the switch and Gateway respectively.

UBT 1.0 provides the following functions:

- Creates multicast tunnel between switch and DDG that is used to maintain multicast and broadcast traffic sent from Gateway to switch.
- The switch forwards the multicast and broadcast traffic to the UBT clients that are part of the same VLAN.
- The unicast traffic from Gateway to switch is sent through the UDG tunnel and not through multicast tunnel.
- The unicast, broadcast, or multicast traffic from switch to controller is always sent through UDG tunnel.
- The UBT user role does not have any VLAN configured on the Gateway.
- UBT 1.0 supports both tagged and untagged UBT users.

UBT 2.0 provides the following functions:

- Does not support UBT user VLAN configuration on the switch.
- Uses role-based VLAN method is used to assign VLAN for the UBT users on the Gateway.
- Gateway replicates the broadcast or multicast packet for each user on that VLAN.
- For a switch-tunneled-node port set up, you need not configure the reserved VLAN on the Gateway.
- UBT 2.0 supports only untagged UBT users.

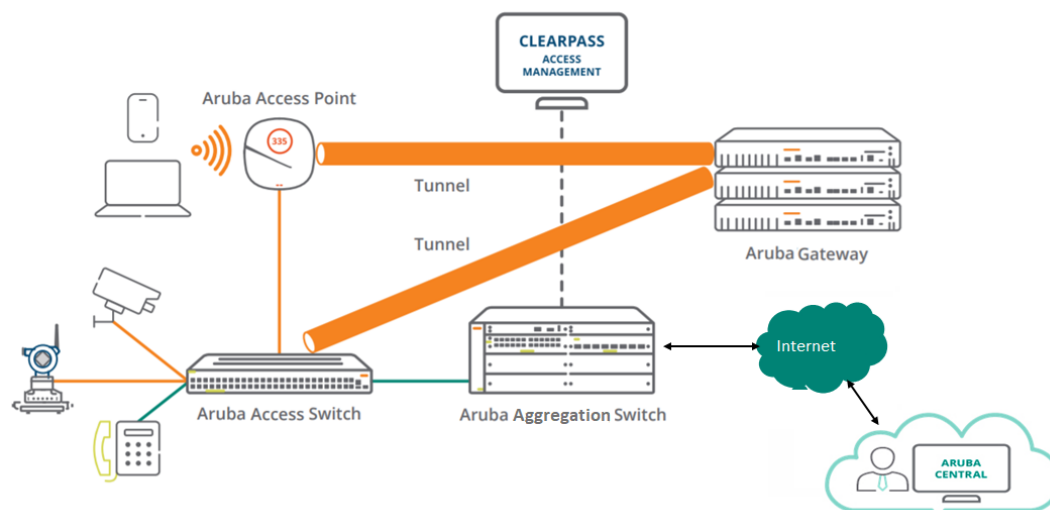


For a reserved VLAN that is configured on tunneled node port of a switch, do not configure the same reserved VLAN on the Gateway.

CPPM Downloadable User Role feature is supported for both UBT 1.0 and 2.0 versions.

The following figure illustrates the UBT deployment mode:

Figure 11 *User-Based Tunneling Deployment*



UBT Configuration Workflow

The UBT configuration workflow includes the following steps:

1. The administrator configures the DDG on the switch by issuing the **tunneled-node-server** command.
2. Once the Gateway information is available on the switch and mode is configured as role-based, the switch performs a handshake with the DDG to determine its reachability and to discover the version information.
3. The switch establishes a GRE heartbeat with the DDG by sending a bootstrap message.

4. Once acknowledged, the switch updates its local data structures with cluster information including S-DDG, node list, and bucket map.
5. After the bucket map list is downloaded to the switch, a GRE heartbeat is established between the switch and the S-DDG.
6. The switch identifies the UBT user based on the user role, and checks the bucket map to obtain the UDG information of the client.
7. The switch establishes UDG GRE tunnel, and the UDG creates the user entry and assigns the user-role and VLAN sent by the switch as part of user bootstrap.



The switch authenticates the user and sends secondary user role information to the Gateway.

Limitations

Following are the limitations of UBT:

- No support for UI Group on switch configuration. The template group is currently supported for switch configuration in Aruba Central.
- No support for cluster multicast VLAN in UBT 1.0 .
- No support for Gateway user VLAN derivation in UBT 1.0.
- No support for cluster switch load balancing, only cluster AP load balancing is supported.
- No Redirect support and VRRP IP support.



You must configure Gateway switch-ip on switch **tunneled-node-server** profile.

Supported Deployments

Aruba supports the UBT feature in the following deployment scenarios:

Standalone Gateway

This deployment includes a single primary gateway and an optional secondary gateway, which acts as a back up if the primary gateway fails. This deployment includes the following configuration conditions:

- On a single tunneled port, there can be as many as 32 clients with different user-roles.
- For each tunneled port, only one tunnel is established with the primary Gateway.
- On a single switch, if there are ten tunneled clients on ten different ports, ten tunnels are formed with the Gateway.

Gateway Cluster

This implementation utilizes the clustering of the Aruba Gateways. The objective of clustering is to provide high availability to all the clients and ensure service continuity when a failover occurs. This deployment includes the following configuration conditions:

- The 7200 Series Gateway platform supports a maximum of 12 Gateways in a cluster, where all Gateways are part of 7200 Series Gateways.
- The 7000 Series Gateway platform supports a maximum of four Gateways, where all Gateways in the cluster are part of 7000 Series Gateways.

- If there is a mix of 7000 Series and 7200 Series Gateways, a cluster can support up to a maximum of four Gateways.
- On a single tunneled port, if there are two tunneled clients which are in same or different roles, anchored to two different UACs, there will be a tunnel to each UAC.
- If the UAC is same for both the clients, there will be only a UAC tunnel from that port.

Support for Downloadable User Roles in Cluster Deployments

This feature provides a seamless redundancy for dynamic policy assignments in cluster deployments. In this deployment, each ArubaOS switch establishes a connection with the active DDG and a secondary connection to the stand-by DDG. This allows the applied client role to be automatically replicated on the secondary DDG, thus minimizing the risk of clients losing connectivity if the active DDG gets disconnected. ClearPass Policy Manager is used to define the roles and policies, which are downloaded to the devices in the cluster that is performing Dynamic Segmentation. ArubaOS switches that have Dynamic Segmentation activated on the port also have downloadable role support.

Support for Downloadable Roles for User-Based Tunneled Node Users

This feature allows the DDG to get the user role from the Aruba ClearPass Policy Manager server while tunneling wired user's traffic to the DDG. That is, the ClearPass Policy Manager downloadable role feature is integrated with user-based tunneled node users. When the user is successfully authenticated, ClearPass Policy Manager server sends two VSA attributes to the ArubaOS switch. The first VSA contains the ClearPass Policy Manager primary user role to be applied on the switch and the second VSA contains redirect attribute with secondary user role. The ArubaOS switch sends the secondary user role name to the device and once this information is provided by the switch, the DDG starts the user role download process and after a successful download, the DDG applies the user role policies.

Support for IGMP Proxy for User-Based Tunneled Node Users

IGMP proxy is supported for user-based tunneled node users in a cluster setup.



IGMP Snooping is not supported in the AOS 10.x deployment.

Licensing

AOS 10.x does not support device license for Gateways, and licensing is configured on Aruba Central. For more information, see *Aruba Central Help Center*.

AOS 10.x UBT Configuration

The UBT feature is enabled by default on the Gateway and does not require further configurations. However, you must configure UBT defined user VLAN and user role on the Gateway. The following sections describe the procedures for configuring UBT defined user VLAN and user role on the Gateway.

Configuring VLANs on Aruba Gateways

You can configure one or more physical ports on the Gateway to be a member of a VLAN. Additionally, each wireless client association constitutes a connection to a virtual port on the Gateway, with membership in a specified VLAN. You can place all authenticated wireless users into a single VLAN or into different VLANs, depending on your network requirements.

Complete the following steps to add VLANs to the Aruba Gateway and configure the VLAN parameters:

1. In the **Network Operations** app, set the filter to a group containing at least one Gateway. The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Gateways**.
3. Click the **Config** icon to view the Gateway configuration dashboard.
4. Click **Interfaces > VLANs**.
5. Click **+** from the **VLANs** table to add a new VLAN interface.
6. In the **New VLAN** window, specify the following parameters and save the changes:
 - **VLAN name**
 - **VLAN ID/Range**



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.

Configuring User Roles

A user role can contain policy and VLAN information. When the user role that is returned from the RADIUS server is applied to the user and the user based tunnel node feature status is up, the authentication sub system notifies the user-based tunnel node module, providing a secondary role where the firewall and security are applied. This secondary-role information enforces additional policies to the user's traffic based on policy configuration associated with the secondary role, and then forms the tunnel. This section includes the following topics:

- [Creating a Role](#)
- [Assigning a Policy to a Role](#)
- [Deleting a User Role](#)

Creating a Role

Complete the following steps to create a user role:

1. In the **Network Operations** app, set the filter to a group containing at least one Gateway. The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Gateways**.
3. Click the **Config** icon to view the Gateway configuration dashboard.
4. Click **Advanced Mode**, and click the **Security** tab. The Security details page is displayed.
5. Click **Roles**.
6. Click **+** from the **Roles** table to create a new role.
7. Enter a name for the new role and click **Save Settings**.

Assigning a Policy to a Role

Complete the following steps to add a policy to a role:

1. In the **Network Operations** app, set the filter to a group containing at least one Gateway. The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Gateways**.

3. Click the **Config** icon to view the Gateway configuration dashboard.
4. Click **Advanced Mode**, and click the **Security** tab.
The Security details page is displayed.
5. Click **Roles**.
6. Select the role name from the **Roles** table.
7. Click **+** under the **Policies** tab.
8. Select one of the following options:
 - **Add an existing policy**
 - **Create a new policy**
9. Select a policy type from the **Policy type** drop-down list. Select the policy type as **Route** to apply PBR policies.
10. Select a policy from the **Policy name** drop-down list.
11. Click **Save Settings**.

Deleting a User Role

Complete the following steps to delete a user role:

1. In the **Network Operations** app, set the filter to a group containing at least one Gateway.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Gateways**.
3. Click the **Config** icon to view the Gateway configuration dashboard.
4. Click **Advanced Mode**, and click the **Security** tab.
The Security details page is displayed.
5. Click **Roles**.
6. Select the role name from the **Roles** table, and click the delete icon on the right to delete the selected role.
7. Click **Yes**.
8. Click **Save Settings**.

You cannot delete an auto-generated user role from the **Gateways** configuration page. The following error message is displayed in the pop-up window: **'XXX role is in use, please use 'show references user-role XXX' to check the references.** The roles created from the **Access** tab of WLAN SSID configuration wizard can be deleted from the **Gateways** configuration page as long as they are not referenced from any WLAN. For example, if both SSID-1 and SSID-2 have a common default role, then you can delete the default role only after deleting both the SSID profiles.

You can delete a manually-configured user role from the **Gateways** configuration page. When you delete the user role, it also gets deleted from the **Access Points** configuration page automatically.



Troubleshooting UBT Configuration

To perform advanced troubleshooting on UBT configuration, complete the following steps:

1. In the **Network Operations** app, use the filter bar to select a Gateway.
2. Under **Analyze**, click **Tools**.
The **Tools** page opens.
3. Click the **Commands** tab.
4. In the **Commands** tab, select **Gateway** from the **Device Type** drop-down list.

5. From the **Available Devices** drop-down list, select the Gateway.
You can select multiple Gateways from the **Available Devices** drop-down list.
6. Select **Dynamic Segmentation** from the **Categories** pane.
The **Commands** pane displays the associated commands.
7. Click **Add>** to add the selected commands to the **Selected Commands** pane.
8. Click **Run** to view and analyze the output of the selected commands in the **Device Output** pane.
 - The following examples display the various commands used for troubleshooting switches and Gateways for UBT configuration. The relevant commands are highlighted in the following examples:
- To check the UBT feature events:

```
(host)# show tunneled-node-mgr trace-buf
```

```
TNM Trace Buffer
```

```
-----
```

```
Dec  3 19:53:53   *   TNM Process UP
Dec  3 19:54:20  gsm  Cluster Node Up   10.15.56.130 redun=1 member=1
Dec  3 19:54:34  gsm  Cluster Node Up   10.15.56.29 redun=1 member=1
Dec  3 19:54:34  gsm  Cluster Node Up   10.15.56.15 redun=1 member=1
```

- To check the switch entries:

```
(host)# show tunneled-node-mgr tunneled-nodes
```

```
No Tunneled Nodes Found.
```

- To check the user entries:

```
(host)# show tunneled-node-mgr tunneled-users
```

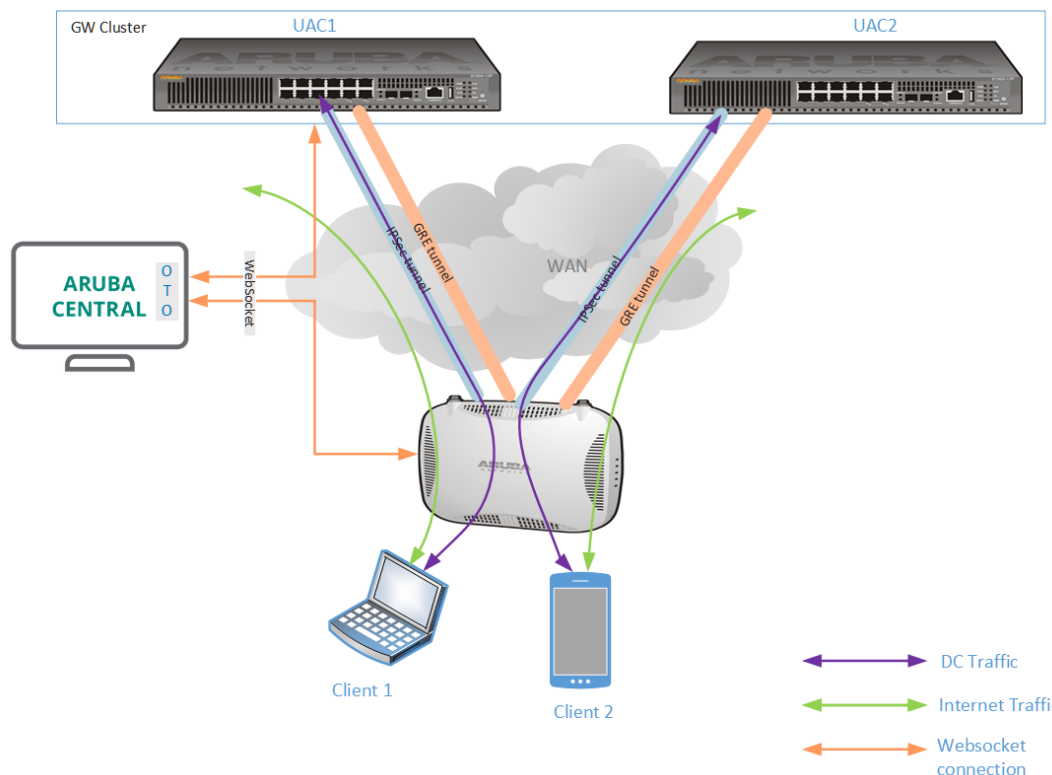
```
No Tunneled Users Found.
```

Most WLAN campus deployments typically have some remote branch site. AOS 10.x currently supports deploying a single AP as a Micro Branch AP in such remote sites such as home offices, small branch offices, retail locations, and so on.

AOS 10.x enables APs in these remote sites to be configured and managed by the Aruba cloud platform also known as Aruba Central. For Micro Branch deployments, AOS 10.x currently supports deployment of a single AP as a Micro Branch AP in remote sites. The AOS 10.x enables these APs to form an IPsec tunnel to the Gateway cluster of the parent WLAN campus. For the network administrator, configuring and managing these remote APs can be done from the same Aruba portal that manages the parent WLAN campus network. For the user at such remote sites, connecting to the WLAN campus network is a seamless experience.

The following figure is a sample representation of the AOS 10.x deployment in Micro Branch. This architecture uses a WLAN tunnel orchestration service to set up IPsec and GRE tunnels between the AP and the Gateway cluster of the parent WLAN campus network. The Micro Branch AP establish tunnels with gateway and encapsulates client's traffic in GRE over IPsec.

Figure 12 *Micro Branch Deployment Topology*



WLAN Tunnel Orchestration for Micro Branch Deployments

The WLAN tunnel orchestration service from AOS 10.x network in Micro Branch deployments automates the formation of IPsec tunnels between APs of a remote site to the Gateway cluster of the parent WLAN network. Aruba supports IPsec tunnel configuration on APs for the following deployment scenario:

- **Full Tunnel**—In this mode, the AP and Gateway cluster are managed by Aruba Central. The IPsec tunnels between the AP and Gateway cluster in a data center are orchestrated by the tunnel orchestration service. The DHCP server in the data center assigns IP addresses to clients. The firewall rules and traffic shaping policies are applied from the AP, Gateway cluster, or both.
- **Split Tunnel**—In this mode, the administrators can configure a split-tunnel policy in the access rules and apply it to the user role in the WLAN SSID. Based on the ACLs configured for an SSID, client traffic to the corporate domain is tunneled to the Gateway in the data center and traffic to the non-corporate domain is forwarded to the Internet.
- **Local Mode (NAT Layer 3)**—In this mode, a local static DHCP pool is used for client IP address assignment. Source NAT is applied to both corporate and the Internet traffic. This option is currently available only when selecting a configuration template.

Micro Branch Deployment Workflow

The provisioning workflow for Micro Branch deployment includes the following steps:

Step 1: Add the APs to Aruba Central

Add the APs to Aruba Central by using an evaluation account or a paid subscription.

For more information, see [Onboarding Devices](#).

Step 2: Assign AP Subscriptions

You can either enable automatic assignment of subscriptions or manually assign subscriptions for the devices added in Aruba Central.

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

Step 3: Create a Group

Aruba Central 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.

For more information, see [Creating a Group](#).

Step 4: Assign APs to a UI Group or Template Group

Aruba Central supports assigning APs to groups for the ease of configuration and maintenance.

For more information, see [Assigning APs to a Group](#).

Step 5: Configure a WLAN SSID for Micro Branch Mode

Client devices use service set identifier (SSID) name to identify and join wireless networks. The SSIDs distinguish a wireless network from other networks configured within a WLAN boundary.

To configure a WLAN SSID for Micro Branch mode, see [WLAN SSID for Micro Branch Deployments](#).

Step 6: Verify the Micro Branch Configuration

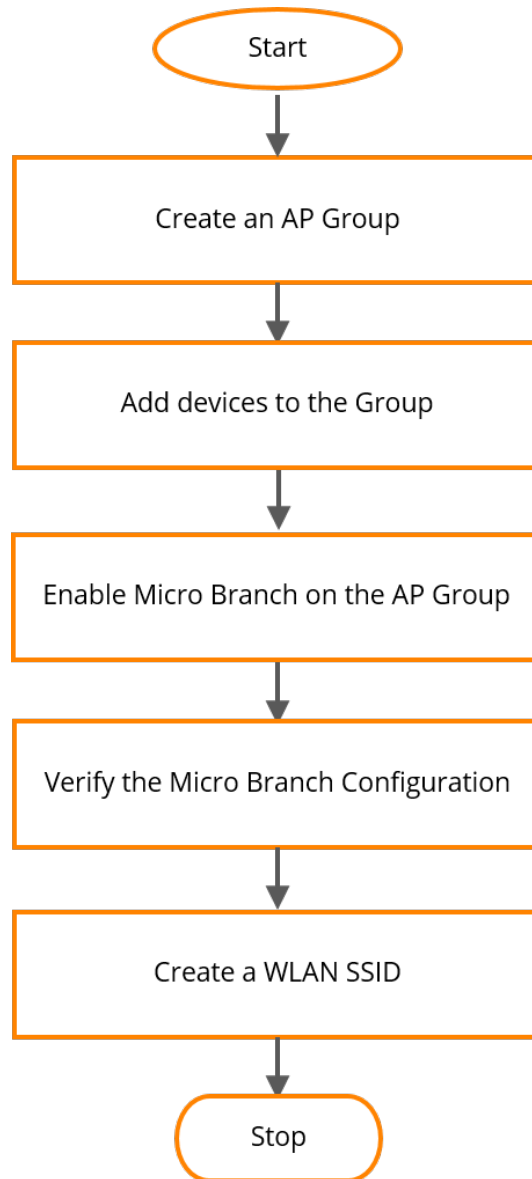
You can verify the Micro Branch configuration for each device in the AP group.

For more information, see [Verifying Micro Branch Configuration](#).

Micro Branch Deployment Flowchart

The following figure illustrates the workflow for a Micro Branch deployment in AOS 10.x:

Figure 13 *Micro Branch Deployment Flowchart*



Enabling Micro Branch on the AP Group

After you have completed the pre-provisioning procedures, you must first enable the Micro Branch setting on the AP group.

To enable Micro Branch on the AP group:

1. In the **Network Operations** app, set the filter to a group that contains at least one Micro Branch 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 APs is displayed.
4. Under the **Security** tab, expand the **Microbranch** drop-down.

5. Toggle **Enable Microbranch** to **enabled** on the slider menu.
6. After enabling the Micro Branch setting on the AP group, you must configure the Inner IP Pool on the group. The AP group then forms an IPsec tunnel with the Inner IP configured. Under **AP Inner IP Pool**, enter the **Start Address** and **End Address** of the Inner IP Pool. The IP address range for the inner IP pool is 0 to 645160.
7. Click **Save Settings**
8. Verify the status of the Micro Branch and Inner IP configuration before you reboot the AP by using the **show running-config** command.
9. Manually reboot each AP in the Micro Branch group for the Micro Branch configurations to take effect:
 - a. Go to **Access Point Details > Actions**.
 - b. Select **Reboot AP** from the drop-down menu.



At a later point in time, if you choose to add new APs to an existing Micro Branch group, ensure that you reboot each new AP manually as shown in Step 8 for the above configurations to take effect.

10. The Micro Branch deployment currently supports configuring a WLAN SSID in the tunnel mode. Once the AP is back online follow the instructions provided in [Creating a WLAN Profile in Tunnel and Mixed Mode](#) and configure the WLAN SSID settings.

Configuring WLAN SSID Settings for Micro Branch Deployments

After successfully enabling Micro Branch on a group and provisioning the APs, the next step is to create an SSID for the Micro Branch group and broadcast it in the network. Note that, all Micro Branch related configurations will be made at the group level which is then forwarded on to the individual devices.

The following sections describe the procedures for creating a WLAN SSID in the Bridge mode or tunnel mode, VLAN assignment, security profile, user role, and access policy configuration.

Creating a WLAN Profile

To configure WLAN settings, 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 **Device(s) > Access Points**.
3. Click the **Config** icon.
The tabs to configure APs is displayed.
4. Click **WLANs**.
The **Wireless SSIDs** table is displayed listing the existing SSID profiles.



You can directly edit the SSID name under the **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.

5. To create a new SSID profile, click **+ Add SSID**.
The **Create a New Network** page is displayed.
6. Under **Advanced Settings**, configure the parameters as mentioned in the [Advanced WLAN Configuration Parameters](#) table.

Table 24: Advanced WLAN Configuration Parameters

Parameter	Description
Broadcast/Multicast	
Broadcast Filtering	<p>Select any of the following values:</p> <ul style="list-style-type: none"> ■ All—The AP drops all broadcast and multicast frames except DHCP, ARP, IGMP group queries, and IPv6 neighbor discovery protocols. ■ ARP—The AP drops broadcast and multicast frames except DHCP, 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 AP is configured to ARP mode. ■ Unicast ARP Only—This option enables the AP to convert ARP requests to unicast frames and thereby sending them to the associated clients. ■ Disabled—The AP forwards all the broadcast and multicast traffic to the wireless interfaces. <p>Default value: The default value is ARP.</p>
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 AP delivers the buffered broadcast and multicast frames to the associated clients in the power save mode.</p> <p>Range: Range is 1 to 10 beacons.</p> <p>Default value: The default value is 1, which means the client checks for buffered data on the AP at every beacon. You can also configure a higher DTIM value for power saving.</p>
Dynamic Multicast Optimization (DMO)	<p>Select the check box to allow the AP 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.</p> <p>NOTE: 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 AP converts multicast streams into unicast streams as long as the channel utilization does not exceed this threshold.</p> <p>Default value: The default value is 90% and the maximum threshold value is 100%. When the threshold is reached or exceeds the maximum value, the AP sends multicast traffic over the wireless link.</p> <p>NOTE: This option will be enabled only when Dynamic Multicast Optimization is enabled.</p>
Transmit Rates (Legacy Only)	
2.4 GHz	<p>If the 2.4 GHz band is configured on the AP, specify the minimum and maximum transmission rates.</p> <p>Default value: The default value for minimum transmission rate is 1 Mbps and maximum transmission rate is 54 Mbps.</p>
5 GHz	<p>If the 5 GHz band is configured on the AP, specify the minimum and maximum transmission rates.</p> <p>Default value: The default value for minimum transmission rate is 6 Mbps and maximum transmission rate is 54 Mbps.</p>
WiFi Multimedia	

Parameter	Description
Background Wifi Multimedia Share	Allocate bandwidth for background traffic such as file downloads or print jobs. Range: 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 DHCP mapping value.
Best Effort Wifi Multimedia Share	Allocate 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	Allocate bandwidth for video traffic generated from video streaming. Range: 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	Allocate bandwidth for voice traffic generated from the incoming and outgoing voice communication. Range: Specify the appropriate DSCP mapping values within a range of 0-63 for the voice traffic in the corresponding DSCP mapping text box. NOTE: 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 if you want TSPEC for 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 for a traffic flow.
TSPEC Bandwidth	Enter the bandwidth for TSPEC.
Spectralink Voice Protocol (SVP)	Select this check box to opt for the 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-save mechanism that is an optional part of the IEEE amendment 802.11e, QoS.
Miscellaneous	
Band	Select the band of radio involved in the wireless network. The options in the drop-down include All, 2.4 GHz , and 5 GHz. Default value: Default is All .
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. Range: You can specify a value within the range of 60-3600 seconds. Default value: The default value is 1000 seconds.
Hide SSID	Select this check box if you do not want the SSID to be visible to users.

Parameter	Description
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	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. You can specify a RSSI value within range of 0-100 dB.
Min RSSI for auth request	Enter the minimum RSSI threshold for authentication requests.
Deauth Inactive Clients	Select this option to allow the AP to send a deauthentication 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.
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.
ESSID	Specify the identifier that serves as an identification and address for the device to connect to a wireless router which can then access the internet. If the ESSID value defined is not the same as the profile name, the SSID can be searched based on the ESSID value and not by its profile name.
Enable SSID When	<p>Enable the SSID based on the following OOS states of the AP:</p> <ul style="list-style-type: none"> ■ VPN down ■ Uplink down ■ Internet down ■ Primary uplink down <p>The network turns out of service when selected the event occurs and the SSID is enabled or disabled according to the configuration settings applied. For example, if you select the VPN down option from the drop-down list and set the status to Enabled, the SSID is enabled when the VPN connection is down and is disabled when the VPN connection is restored.</p> <p>Configure a hold time interval in seconds.</p> <p>Range: Range of 30-300 seconds, after which the out-of-service operation is triggered. For example, if the VPN is down and the configured hold time is 45 seconds, the effect of this out-of-service state impacts the SSID availability after 45 seconds.</p>
Disable SSID When	<p>Disable the SSID based on the following OOS states of the AP:</p> <ul style="list-style-type: none"> ■ VPN down ■ Uplink down ■ Internet down ■ Primary uplink down <p>The network turns out of service when selected the event occurs and the SSID is enabled or disabled according to the configuration settings applied. For example, if you select the VPN down option from the drop-down list and set the status to Enabled, the SSID is enabled when the VPN connection is down and is disabled when the VPN connection is restored.</p> <p>Configure a hold time interval in seconds.</p>

Parameter	Description
	Range: Range of 30-300 seconds, after which the out-of-service operation is triggered. For example, if the VPN is down and the configured hold time is 45 seconds, the effect of this out-of-service state impacts the SSID availability after 45 seconds.
Fine Timing Measurement (802.11mc) Responder Mode	Turn on the toggle switch to enable the fine timing measurement (802.11mc) responder mode.

7. Click **Next** to configure VLAN settings.

You can input the fields in Advanced Settings only for network profiles with advanced configuration options.

Configuring VLAN Settings on a WLAN SSID

To configure VLAN settings for an SSID, complete the following steps:

1. In the **VLAN** tab, select any of the following options in **Traffic Forwarding Mode** to create a micro branch network.
 - **Bridge**—To deploy APs to function as bridge between the wireless interface and the wired network deployed at a site, select the **Bridge** mode. The infrastructure layer requires only APs for a Bridge mode deployment.
 - **Tunnel**—To forward client traffic to an Aruba Gateway node in the Tunnel mode network, select the **Tunnel** mode.
2. Select a **Primary Gateway Cluster** through which the traffic from the APs is to be tunneled. This configuration is mandatory.
 - For site specific auto cluster, cluster drop-down list displays **<group name:auto site cluster>**
 - For manual cluster, cluster drop-down list displays **<groupname>manualclusterprofilename>**. For example, **Group2:TestCluster123**.
3. Optionally, you can choose to configure a **Secondary Gateway Cluster** as a failover, in case the primary cluster is unavailable. Enable the **Cluster Preemption** check-box to allow the AP to switch back to the SSID of the primary gateway cluster, when it becomes available. Skip this step, if you do not wish to configure a secondary gateway cluster.
4. Select the client VLAN assignment mode for WLAN clients and configure the following parameters:
 - **Static**—Allows you to specify a VLAN id of single VLAN, or a comma separated list of VLANS, or a range of VLANs for all clients on this network, in the **VLAN ID** text box. You can also select the VLAN name that is mapped to the VLAN id from the scroll-down list provided next to the **VLAN ID** text box. 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.
 - **Dynamic**—Assigns the VLANs dynamically from a DHCP server. You can also create a new VLAN assignment rules by clicking the + sign. The **New VLAN Assignment Rule** page is displayed to enter details such as attribute, operator, string and VLAN ID.
5. In the **Show Named VLANS** settings, you can map the VLAN ID to a VLAN name by clicking the **Add Named VLAN** option.
6. Click **Next** to configure security settings.

Configuring a Security Profile on a WLAN SSID

You can configure the following types security profiles on a WLAN SSID:

- [Enterprise](#)—For enterprise WLAN configuration
- [Personal](#)—For personal network
- [Captive Portal](#)—For guest user access
- [Open](#)—Open network with no authentication profiles.

Configuring an Enterprise Security Profile on a WLAN SSID

To configure an enterprise security profile, complete the following procedure:

1. In the WLAN SSID configuration wizard, click the **Security** tab.
2. In the **Security** tab, select the **Enterprise** security level, and configure the following parameters:

Table 25: Enterprise Security Profile Configuration Parameters

Data Pane Item	Description
Key Management	<p>For Enterprise security level, select any of the following options from Key Management</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. ■ Both (WPA-2 & WPA)—Select this option to use both WPA-2 and WPA security. ■ WPA Enterprise—Select this option to use both WPA Enterprise. ■ Dynamic WEP with 802.1X—If you do not want to use a session key from the RADIUS Server to derive pairwise unicast keys, set Session Key for LEAP to Enabled. This is required for old printers that use dynamic WEP through LEAP authentication. The Session Key for LEAP feature is Disabled by default. ■ 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. <p>NOTE: 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>
Authentication Server	<p>Specify an authentication server for client authentication.</p> <ul style="list-style-type: none"> ■ Primary Server—Allows you to configure a primary authentication server. Select one of the following options from the drop-down list: <ul style="list-style-type: none"> ● To add a new server, click +.

3. Click **Advanced Settings** and configure the following parameters:

Table 26: Advanced WLAN security Settings—Enterprise Security Profile

Data pane item	Description
Use Session Key for LEAP	Select this option to use the session key for Lightweight Extensible Authentication Protocol (LEAP)
Opportunistic Key Caching (OKC)	Select the Opportunistic key caching (OKC) checkbox to reduce the time needed for authentication. When OKC is enabled, multiple APs can share Pairwise Master Keys (PMKs) and use these keys when clients roam to a neighboring AP. OKC is available only for the WPA2-based security profiles.
Reauth Interval	<p>Define a value for Reauth Interval. When set to a value greater than zero, APs periodically re-authenticate all associated and authenticated clients.</p> <p>The following events occur when the re-authentication interval is configured on WLAS SSIDs:</p> <ul style="list-style-type: none"> ■ 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

Data pane item	Description
	<p>a post-authentication role only after a successful re-authentication. If re-authentication fails, the client retains the pre-authentication role.</p> <ul style="list-style-type: none"> ■ On an SSID performing both L2 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.
Denylisting	<p>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>To enforce DHCP and to block traffic for AP clients that do not obtain IP address from DHCP, enable Enforce DHCP. When DHCP is enforced:</p> <ul style="list-style-type: none"> ■ A layer-2 user entry is created when a client associates with an AP. ■ The client DHCP state and IP address are tracked. ■ When the client obtains an IP address from DHCP, the DHCP state changes to complete. ■ If the DHCP state is complete, a layer-3 user entry is created. ■ When a client roams between the APs, the DHCP state and the client IP address is synchronized with the new AP.
Accounting	<p>To enable accounting, select the Accounting option. On enabling this option, the APs post accounting information to the RADIUS server at the specified Accounting Interval. Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> ■ Disabled—To disable the accounting option. ■ Use authentication server—To select authentication servers and the accounting time interval in minutes. ■ Use separate servers— To select specific accounting and mention the accounting interval time in minutes.
Use IP for Calling Station	<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 APs IP address as the called station ID. ● Access Point Name—Uses the host name of the AP 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 AP as the called station ID. ● MAC address—Uses the MAC address of the AP as the called station ID. ■ Called Station Include SSID—Appends the SSID name to the called station ID. ■ 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.
Fast Roaming	<p>Enable the following fast roaming features as per your requirement:</p> <ul style="list-style-type: none"> ■ 802.11r—Select 802.11r option to enable 802.11r roaming. Selecting this enables fast BSS transition. The fast BSS transition mechanism minimizes the delay when a client transitions from one BSS (AP) to another within the same cluster. When 802.11r is enabled, you can configure a mobility domain identifier (MDID). In a network of standalone APs with the same management VLAN, 802.11r roaming is not supported as MDIDs do not match across APs. They are auto-generated based on a AP key. To enable 802.11r, you can configure an MDID with the same value. ■ 802.11k—Select 802.11k to enable 802.11k roaming. The 802.11k protocol enables APs and clients to dynamically discover the available radio resources. When 802.11k is enabled, APs and clients send neighbor reports, beacon reports, and link measurement

Data pane item	Description
	<p>reports to each other.</p> <ul style="list-style-type: none"> ■ 802.11v– Select 802.11v to enable 802.11v based BSS transition. The 802.11v standard defines mechanisms for wireless network 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.

4. Click **Next**.

Configuring Personal Security Settings for a WLAN SSID

To configure a personal security profile, complete the following procedure:

1. In the WLAN SSID configuration wizard, click the **Security** tab.
2. In the **Security** tab, select the **Personal** security level.
3. From the **Key Management** drop-down, select one of the following encryption settings on the SSID:
 - For **WPA-2 Personal**, **WPA Personal**, **Both (WPA-2&WPA)**, and **WPA-3 Personal** keys, specify the following parameters:
 - **Passphrase Format**: Select a passphrase format. The options available are 8-63 alphanumeric characters and 64 hexadecimal characters.
 - Enter a passphrase in **Passphrase** and reconfirm.
 - For **Static WEP**, specify the following parameters:
 - Select an appropriate value for WEP key size from the **WEP Key Size**. You can specify 64-bit or 128-bit.
 - Select an appropriate value for Tx key from **Tx Key**.
 - Enter an appropriate **WEP Key** and reconfirm.
 - For **MPSK-AES**, configure authentication server.
 - **Primary Server**–Sets a primary authentication server. The **Primary Server** option appears only for Enterprise security level and external captive portal types. Select one of the following options from the drop-down list:
 - To add a new server, click +.
 - **Secondary Server**–To add another server for authentication, configure another authentication server.
 - 4. Click **Advanced Settings** and configure the following parameters:

Table 27: *Advanced WLAN Security Settings–Personal Security Profile*

Data pane item	Description
MAC Authentication	<p>To enable MAC address based authentication of clients, turn on the MAC Authentication toggle switch. When MAC authentication is enabled, you can configure the following parameters:</p> <ul style="list-style-type: none"> ■ Delimiter Character–Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the AP uses the delimiter in the MAC authentication request. For example, if you specify the colon as a delimiter, MAC

Data pane item	Description
	<p>addresses in the xx:xx:xx:xx:xx:xx format are used. If the delimiter is not specified, the MAC address in the xxxxxxxxxx format is used. This option is available only when MAC authentication is enabled.</p> <ul style="list-style-type: none"> ■ Uppercase Support—Set to Enabled to allow the AP to use uppercase letters in MAC address string for MAC authentication. This option is available only if MAC authentication is enabled.
Reauth Interval	<p>Define a value for Reauth Interval. When set to a value greater than zero, APs periodically re-authenticate all associated and authenticated clients.</p> <p>The following events occur when the re-authentication interval is configured on WLAS SSIDs:</p> <ul style="list-style-type: none"> ■ 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. ■ On an SSID performing both L2 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.
Denylisting	<p>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>To enforce DHCP and to block traffic for AP clients that do not obtain IP address from DHCP, enable Enforce DHCP. When DHCP is enforced:</p> <ul style="list-style-type: none"> ■ A layer-2 user entry is created when a client associates with an AP. ■ The client DHCP state and IP address are tracked. ■ When the client obtains an IP address from DHCP, the DHCP state changes to complete. ■ If the DHCP state is complete, a layer-3 user entry is created. ■ When a client roams between the APs, the DHCP state and the client IP address is synchronized with the new AP.
WPA3 Transition	<p>This option appears when you select WPA3-Personal option in the Key Management drop-down list. This option allows the encryption format from WPA3 to WPA2.</p>
Use IP for Calling Station	<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 AP's IP address as the called station ID. ● Access Point Name—Uses the host name of the AP 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 AP as the called station ID. ● MAC address—Uses the MAC address of the AP as the called station ID. ■ Called Station Include SSID—Appends the SSID name to the called station ID. ■ 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.

Data pane item	Description
Delimiter Character	Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the AP 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 AP to use uppercase letters in MAC address string for MAC authentication. This option is available only if MAC authentication is enabled.
Accounting	To enable accounting, select the Accounting option. On enabling this option, the APs post accounting information to the RADIUS server at the specified Accounting Interval . Select one of the following options from the drop-down list: <ul style="list-style-type: none"> ■ Disabled—To disable the accounting option. ■ Use authentication server—To select authentication servers and the accounting time interval in minutes. ■ Use separate servers—To select specific accounting and mention the accounting interval time in minutes.
Fast Roaming	Enable the following fast roaming features as per your requirement: <ul style="list-style-type: none"> ■ 802.11r—Select 802.11r option to enable 802.11r roaming. Selecting this enables fast BSS transition. The fast BSS transition mechanism minimizes the delay when a client transitions from one BSS (AP) to another within the same cluster. When 802.11r is enabled, you can configure a mobility domain identifier (MDID). In a network of standalone APs with the same management VLAN, 802.11r roaming is not supported as MDIDs do not match across APs. They are auto-generated based on a AP key. To enable 802.11r, you can configure an MDID with the same value. ■ 802.11k—Select 802.11k to enable 802.11k roaming. The 802.11k protocol enables APs and clients to dynamically discover the available radio resources. When 802.11k is enabled, APs and clients send neighbor reports, beacon reports, and link measurement reports to each other. ■ 802.11v— Select 802.11v to enable 802.11v based BSS transition. The 802.11v standard defines mechanisms for wireless network 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.

5. Click **Next**.

Configuring Captive Portal Security Profile for Guest User Access

To configure captive portal security profile for guest user access:

1. In the WLAN SSID configuration wizard, click the **Security** tab.
2. In the **Security** tab, select the **Captive Portal** security level.
3. Configure the following parameters:

Table 28: *Captive Portal Security Profile*

Parameter	Description
Splash Page > Captive Portal Type > None	To configure a captive portal security profile with no Splash Page, select the None for Captive Portal Type .
Splash Page > Captive Portal Type > External	<p>To configure captive portal authentication with a Splash Page using an external captive portal authentication profile, select External from the Captive Portal Type drop-down. The external captive portal serves are used for authenticating guest users in a WLAN.</p> <p>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, the users connecting to the SSID 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.</p>
Captive Portal Profile	<p>To use the default captive portal profile, select Default. To use a custom Splash Page profile, click + and configure the following parameters:</p> <ul style="list-style-type: none"> ■ 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. ■ Automatic URL Allowlisting—On enabling this for the external captive portal authentication, the URLs

Parameter	Description
	<p>that are allowed for the unauthenticated users to access are automatically allowlisted.</p> <ul style="list-style-type: none"> ■ 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. ■ Redirect URL—Specify a redirect URL if you want to redirect the users to another URL.
Encryption	<p>To enable encryption settings, turn on the Encryption toggle switch and select an encryption key from Key Management:</p> <p>For WPA-2 Personal, WPA Personal, Both (WPA-2&WPA), and WPA-3 keys, configure the following parameters:</p> <ul style="list-style-type: none"> ■ Passphrase Format: Select a passphrase format. The options are available are 8-63 alphanumeric characters and 64 hexadecimal characters. ■ Enter a passphrase in Passphrase and reconfirm. <p>For Static WEP, specify the following parameters:</p> <ul style="list-style-type: none"> ■ Select an appropriate value for WEP key size from the WEP Key Size. You can define 64-bit or 128-bit. ■ Select an appropriate value for Tx key from Tx Key. ■ Enter an appropriate WEP Key and reconfirm.

4. Click **Advanced Settings** and configure the following parameters:

Table 29: *Advanced WLAN Security Settings—Captive Portal Security Profile*

Data pane item	Description
Captive Portal Proxy Server IP	To configure a captive portal proxy server or a global proxy server to match your browser configuration, enter the proxy server IP address.
Captive Portal Proxy Server Port	If the captive portal proxy server IP address is configured, enter the captive portal proxy server port.
MAC Authentication	<p>To enable MAC address based authentication of clients, turn on the MAC Authentication toggle switch. When MAC authentication is enabled, you can configure the following parameters:</p> <ul style="list-style-type: none"> ■ Delimiter Character—Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the AP 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

Data pane item	Description
	<p>MAC address in the xxxxxxxxxxxx format is used. This option is available only when MAC authentication is enabled.</p> <ul style="list-style-type: none"> ■ Uppercase Support—Set to Enabled to allow the AP to use uppercase letters in MAC address string for MAC authentication. This option is available only if MAC authentication is enabled.
Reauth Interval	<p>Define a value for Reauth Interval. When set to a value greater than zero, APs periodically re-authenticate all associated and authenticated clients.</p> <p>The following events occur when the re-authentication interval is configured on WLAS SSIDs:</p> <ul style="list-style-type: none"> ■ 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. ■ On an SSID performing both L2 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.
Denylisting	<p>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>To enforce DHCP and to block traffic for AP clients that do not obtain IP address from DHCP, enable Enforce DHCP. When DHCP is enforced:</p> <ul style="list-style-type: none"> ■ A layer-2 user entry is created when a client associates with an AP. ■ The client DHCP state and IP address are tracked. ■ When the client obtains an IP address from DHCP, the DHCP state changes to complete. ■ If the DHCP state is complete, a layer-3 user entry is created. ■ When a client roams between the APs, the DHCP state and the client IP address is synchronized with the new AP.
Use IP for Calling Station	<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 AP's IP address as the called station ID. ● Access Point Name—Uses the host name of the AP 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 AP as the called station ID. ● MAC address—Uses the MAC address of the AP as the called station ID. ■ Called Station Include SSID—Appends the SSID name to the called station ID. ■ 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.
Disable If Uplink Type Is	<p>To exclude Ethernet, Wi-Fi, or cellular uplinks from authentication, select the uplink type.</p>
Fast Roaming	<p>Enable the following fast roaming features as per your requirement:</p> <ul style="list-style-type: none"> ■ 802.11r—Select 802.11r option to enable 802.11r roaming. Selecting this enables fast BSS transition. The fast BSS transition mechanism minimizes the delay when a client transitions from one BSS (AP) to another within the same cluster.

Data pane item	Description
	<p>When 802.11r is enabled, you can configure a mobility domain identifier (MDID). In a network of standalone APs with the same management VLAN, 802.11r roaming is not supported as MDIDs do not match across APs. They are auto-generated based on a AP key. To enable 802.11r, you can configure an MDID with the same value.</p> <ul style="list-style-type: none"> ■ 802.11k—Select 802.11k to enable 802.11k roaming. The 802.11k protocol enables APs and clients to dynamically discover the available radio resources. When 802.11k is enabled, APs and clients send neighbor reports, beacon reports, and link measurement reports to each other. ■ 802.11v— Select 802.11v to enable 802.11v based BSS transition. The 802.11v standard defines mechanisms for wireless network 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.

5. Click **Next**.

Configuring an Open Network

1. In the WLAN SSID configuration wizard, click the **Security** tab.
2. In the **Security** tab, select the **Open** security level.
3. For **Open** security level, the Key Management includes **Open**, and **Enhanced Open** options. No encryption policy is required for both **Open** and **Enhanced Open** options,
4. Click **Advanced Settings** and configure the following parameters:

Table 30: *Advanced WLAN Security Settings—Open Network Profile*

Data pane item	Description
MAC Authentication	<p>To enable MAC address based authentication of clients, turn on the MAC Authentication toggle switch. When MAC authentication is enabled, you can configure the following parameters:</p> <ul style="list-style-type: none"> ■ Delimiter Character—Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the AP 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—Set to Enabled to allow the AP to use uppercase letters in MAC address string for MAC authentication. This option is available only if MAC authentication is enabled.
Reauth Interval	<p>Define a value for Reauth Interval. When set to a value greater than zero, APs periodically re-authenticate all associated and authenticated clients. The following events occur when the re-authentication interval is configured on WLAN SSIDs:</p> <ul style="list-style-type: none"> ■ 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

Data pane item	Description
	<p>role.</p> <ul style="list-style-type: none"> ■ On an SSID performing L2 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.
Denylisting	<p>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>To enforce DHCP and to block traffic for AP clients that do not obtain IP address from DHCP, enable Enforce DHCP.When DHCP is enforced:</p> <ul style="list-style-type: none"> ■ A layer-2 user entry is created when a client associates with an AP. ■ The client DHCP state and IP address are tracked. ■ When the client obtains an IP address from DHCP, the DHCP state changes to complete. ■ If the DHCP state is complete, a layer-3 user entry is created. ■ When a client roams between the APs, the DHCP state and the client IP address is synchronized with the new AP.
Use IP for Calling Station	<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 APs IP address as the called station ID. ● Access Point Name—Uses the host name of the AP 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 AP as the called station ID. ● MAC address—Uses the MAC address of the AP as the called station ID. ■ Called Station Include SSID—Appends the SSID name to the called station ID. ■ 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.
Disable If Uplink Type Is	<p>To exclude Ethernet, Wi-Fi, or cellular uplinks from authentication, select the uplink type.</p>
Fast Roaming	<p>Enable the following fast roaming features as per your requirement:</p> <ul style="list-style-type: none"> ■ 802.11r—Select 802.11r option to enable 802.11r roaming. Selecting this enables fast BSS transition. The fast BSS transition mechanism minimizes the delay when a client transitions from one BSS (AP) to another within the same cluster. When 802.11r is enabled, you can configure a mobility domain identifier (MDID). In a network of standalone APs with the same management VLAN, 802.11r roaming is not supported as MDIDs do not match across APs. They are auto-generated based on a AP key. To enable 802.11r, you can configure an MDID with the same value. ■ 802.11k—Select 802.11k to enable 802.11k roaming. The 802.11k protocol enables APs and clients to dynamically discover the available radio resources. When 802.11k is enabled, APs and clients send neighbor reports, beacon reports, and link measurement reports to each other. ■ 802.11v— Select 802.11v to enable 802.11v based BSS transition. The 802.11v standard defines mechanisms for wireless network 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,

Data pane item	Description
	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.

Configuring ACLs for User Access to a WLAN

You can configure up to 64 access rules for a wireless network profile.



Configuration of ACLs for User Access is not applicable for Open network.

To configure access rules for a network, complete the following steps:

1. In the WLAN SSID configuration wizard, click the **Access** tab.
2. In **Access Rules**, select any of the following types of access control:

Viewing Network Summary

The **Network Summary** page now displays all the settings configured in the **General**, **Security**, **VLANs**, and **Access** tabs.

Viewing WLAN SSIDs Summary Table

You can view the list of wireless SSIDs that have been configured in the **Wireless Management > Wireless SSIDs** page. The table includes the list of wireless SSIDs with the following details:

- **Name**—This column displays the name provided to the SSID profile.
- **Type**—This column indicates the type of wireless SSIDs, for example, **Mixed Traffic**, or **Voice**.
- **Security**—This column displays the encryption mode configured for wireless SSIDs such as **WPA2-AES**, **WPA-3**, **MPSK-AES**, and so on.
- **Access Type**—This column displays scope of access to the SSID profile, for example, **Unrestricted**, or **Restricted**.
- **Zone**—This column displays the input provided in the **Zone** field of **General > Advanced Settings**.
- **Network Enabled**—This column displays the status of the network configured in the **General > Advanced Settings > Miscellaneous > Disable Network** option.
- **Actions**—This column includes actions to enable or disable the Wi-Fi, edit the SSID profile, and delete the SSID profile.

Configuring External Authentication Servers in an SSID Security Profile

WLAN clients connecting to an SSID in the network can authenticate to an external server based on the security profile configured on the SSID.

You can create and associate an external authentication server when configuring a security profile for an WLAN SSID.



In a Tunnel mode, authentication is performed at the gateway cluster level.

The following table describes the procedure for creating external authentication servers for WLAN client authentication:

Table 31: 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 AP by creating a TLS tunnel between the AP and the server.</p> <p>If Radsec is enabled, the following configuration options are displayed:</p> <ul style="list-style-type: none"> ● Radsec Port—Communication port number for RadSec TLS connection. By default, the port number is set to 2083. ● 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 AP 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 AP. 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	<p>Enter the IP address.</p> <ul style="list-style-type: none"> ● For AP-based cluster deployments, ensure that you enter the VC IP address as the NAS IP address. ● For Cloud AP based Campus WLAN deployments, ensure that you enter the AP 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.
Dead Time	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.

Type of Server	Parameters
	<ul style="list-style-type: none"> ■ If Dynamic RADIUS Proxy (DRP) is enabled on the APs, configure the following parameters: <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. ● DRP GATEWAY—Gateway IP address of the DRP VLAN.
Service Type Framed User	Select any of the following check boxes to send the service type as Framed User in the access requests to the RADIUS server: <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)	Select any of the following check boxes to detect the server status of the RADIUS server: <ul style="list-style-type: none"> ● Authentication—Select this check-box to ensure the AP sends a status-server request to determine the actual state of the authentication server before marking the server as unavailable. ● Accounting—Select this check-box to ensure the AP sends a status-server request to determine the actual state of the accounting server before marking the server as unavailable.
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 .
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.

Type of Server	Parameters
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	<ul style="list-style-type: none"> ■ 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.

Type of Server	Parameters
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.
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.

Configuring Traffic Forwarding for Micro Branch APs

The DHCP traffic in Micro Branch deployments is tunneled through three different modes— full tunnel, split-tunnel, or Local (NAT Layer-3) mode. In the full-tunnel and split-tunnel modes, the DHCP server is configured externally on the Gateway. In the Local DHCP mode, the DHCP IP addresses are handled locally by the AP. The following sections describe the configuration modes that are currently supported for Micro Branch deployments:

- [Configuring Full Tunnel and Split Tunnel Mode on page 136](#)
- [Configuring Traffic Forwarding for Micro Branch APs on page 136](#)

Configuring Full Tunnel and Split Tunnel Mode

The centralized DHCP scope supports L2 full tunnel and split tunnel configuration modes.

Full Tunnel Mode

For full tunnel clients, the AP bridges the DHCP traffic to the Gateway cluster over the IPsec or GRE tunnel. The IP address is obtained from the DHCP server behind the Gateway cluster serving the IPsec or GRE of the client. This DHCP assignment mode also allows you to add the DHCP option 82 to the DHCP traffic forwarded to the Gateway cluster. In this mode, 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.

Split Tunnel Mode

For split tunnel clients, the client is able 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 software client to connect to file servers, database servers, mail servers, and other servers on the corporate network through the IPsec tunnel network. 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 tunnel

functionality intercepts DNS requests from clients for non-corporate domains and forwards to the AP's own DNS server.

The following ACL rule configures the split tunnel mode on the Micro Branch group:

- rule any any match udp any 67 permit
- rule any any match udp any 68 permit
- rule 192.168.0.0 255.255.0.0 match any any any permit
- rule any any match any any any src-nat

DHCP Ports 67 and 68 are permitted to send over the tunnel for client DHCP requests. The 192.168.0.0 IP address is configured for the corporate network. The rest of the traffic corresponds to internet traffic which is source natted out using the br0 interface IP of the AP.

Configuring Local (NAT Layer-3) Mode

Micro Branch deployments currently support the Local (NAT Layer-3) configuration mode as a template based configuration.

In this mode, the AP acts as both the DHCP Server and default gateway. The configured subnet and the corresponding DHCP scope are independent of subnets configured. The AP 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. The traffic that is destined to the corporate network is source-natted with it's tunnel inner IP, and tunneled to the interface. The traffic that is destined to the internet is source-natted with it's br0 IP address and forwarded to the management VLAN's default Gateway. This DHCP assignment mode is used for the NAT forwarding mode.

The following ACL rule configures the Local mode on a Micro Branch group:

- rule any any match udp any 67 permit
- rule 172.40.1.0 255.255.255.0 match any any any src-nat tunnel
- rule 172.50.1.0 255.255.255.0 match any any any src-nat tunnel
- rule any any match any any any src-nat

Verifying Micro Branch Configuration

To run troubleshooting or diagnostics commands on the devices managed from Aruba Central, use the troubleshooting utilities available in the **Tools** page.

To access the **Tools** page, in the **Network Operations** app, go to **Analyze > Tools**.

For more information on how to run troubleshooting commands for analyzing device and network health issues, see [Using Troubleshooting Tools](#).

To verify the Micro Branch configuration for each device in the AP group:

1. In the **Network Operations** app, go to **Analyze > Tools**.
2. In the **Commands** window, select the **Device Type** as **Access Point**.
3. Select the AP(s) from the list of **Available Devices**.
4. Select System from the **Categories** menu, and then select **Show running-config** from the **Commands** menu.
5. Click the **Add >** button to move the command to the **Selected Commands** window.
6. Click **Run**.
7. Verify the Micro Branch configuration settings for the device in the **Device Output** screen.

You can configure an AP in the **Network Operations** app by setting the filter to a group containing at least one AP.

In the group or device dashboard, the 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

Viewing AP Configuration Options

You can configure an AP in the Network Operations app by setting the filter to a group containing at least one AP.

In the group or device dashboard, the 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

Deploying a Wireless Network Using APs

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).

For more information on AP configuration, see the following topics:

- [Configuring Device Parameters for an AP](#)
- [Configuring Network Profiles on APs](#)
- [Configuring a Time Range Profile for a WLAN SSID](#)
- [Configuring RF Parameters on APs](#)
- [Configuring Authentication and Security Profiles on APs](#)
- [Configuring DHCP Pools and Client IP Assignment Modes on APs](#)
- [Configuring Systems](#)
- [Configuring Enterprise Domains](#)
- [Configuring Syslog and TFTP Servers for Logging Events](#)

Setting the Country Code for an AP

The initial Wi-Fi setup of an AP requires you to specify the country code for the country in which the AP operates. This configuration sets the regulatory domain for the radio frequencies that the AP uses. The available 20 MHz, 40 MHz, or 80 MHz channels are dependent on the specified country code.

If you provision a new AP without the country code, Aruba Central exhibits the following behavior:

Table 32: AP Provisioned To Aruba Central

Country Code Configured at AP	Country Code Configured in Group	Behavior
No	Yes	The country code of the group is pushed to the newly added AP.
No	No	Aruba Central 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 AP. To set the country code, perform the following actions: <ol style="list-style-type: none"> 1. Click Set Country Code now link on the notifications pane. The Set Country Code pop up is displayed. 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 AP has a country code and joins Aruba Central using ZTP configuration, then the country code of the AP is retained. In this case, Aruba Central will not push the group country code.

Setting the Country Code in the AP Group Dashboard

To set the country code of the AP at the group level, 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 APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced** (if required), and click the **System** tab.
The System details page is displayed.
5. Click **General**.
6. In the **Set Country code for group** drop-down list, select the country code for the AP.
7. Click **Save Settings**.
8. Reboot AP for changes to take effect.



By default, the value corresponding to the **Set Country** code for group field is empty. This indicates that any 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 also will be updated.

Configuring General > Advanced Settings for a WLAN SSID Profile

Configuring the advanced settings is part of creating the WLAN SSID profile either in [Bridge mode](#) or [Mixed and Tunnel mode](#).

To configure the **Advanced Settings** under the **General** tab:

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**, go to **Device(s) > Access Points**.
3. If required, click the **Config** icon.
The second-level tabs to configure APs are displayed.
4. Go to the **WLANS** tab.
The **Wireless SSIDs** table is displayed listing the existing SSID profiles.
5. To create a new SSID profile, click **+ Add SSID**. To edit an existing SSID profile, click the row, and then click the edit icon.
The **Create a New Network** page is displayed for creating a new SSID. The **Networks** page is displayed for editing an existing SSID.
6. Under **General > Advanced Settings**, configure the following parameters:

Table 33: *Advanced Settings Parameters*

Parameter	Description
Broadcast/Multicast	

Parameter	Description
Broadcast filtering	<p>Select any of the following values:</p> <ul style="list-style-type: none"> ■ All—The AP drops all broadcast and multicast frames except DHCP and ARP, IGMP group queries, and IPv6 neighbor discovery protocols. ■ ARP—The AP 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 AP is configured to ARP mode. ■ Unicast ARP Only—This option enables AP to convert ARP requests to unicast frames thereby sending them to the associated clients. ■ Disabled—The AP 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 AP delivers the buffered broadcast and multicast frames to the associated clients in the power save mode. Range is 1 to 10 beacons.</p> <p>The default value is 1, which means the client checks for buffered data on the AP at every beacon. You can also configure a higher DTIM value for power saving.</p>
Dynamic Multicast Optimization (DMO)	<p>Select the check-box to allow AP 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.</p> <p>NOTE: 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 AP 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 AP sends multicast traffic over the wireless link.</p> <p>NOTE: This option will be enabled only when Dynamic Multicast Optimization is enabled.</p>
DMO Client Threshold	Specify a value between 2 and 255 to set the DMO client threshold.
Transmit Rates (Legacy Only)	
2.4 GHz	If the 2.4 GHz band is configured on the AP, specify the minimum and maximum transmission rates. The default value for minimum transmission rate is 1 Mbps and maximum transmission rate is 54 Mbps.
5 GHz	If the 5 GHz band is configured on the AP, specify the minimum and maximum transmission rates. The default value for minimum transmission rate is 6 Mbps and maximum transmission rate is 54 Mbps.
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.

Parameter	Description
Downstream	<p>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.</p> <p>NOTE: The bandwidth limit set in this method is implemented at the device level and not cluster level.</p>
Upstream	<p>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.</p> <p>NOTE: The bandwidth limit set in this method is implemented at the device level and not cluster level.</p>
Each Radio	<p>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.</p>
Enable 11n	<p>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 AP, it is automatically enabled for all SSIDs configured on an AP. By default, HT is enabled on all SSIDs.</p> <p>NOTE: If you want the 802.11ac APs to function as 802.11n APs, clear this check-box to disable VHT on these devices.</p>
Enable 11ac	<p>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 AP, it is automatically enabled for all SSIDs configured on an AP. By default, VHT is enabled on all SSIDs.</p> <p>NOTE: If you want the 802.11ac APs to function as 802.11n APs, clear this check-box to disable VHT on these devices.</p>
Enable 11ax	<p>When this option is selected, VHT is enabled on the 802.11ax devices. If VHT is enabled for a radio profile on an AP, it is automatically enabled for all SSIDs configured on an AP. By default, VHT is enabled on all SSIDs.</p>
WiFi Multimedia	
Background Wifi Multimedia Share	<p>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 DHCP mapping value.</p>
Best Effort Wifi Multimedia Share	<p>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.</p>
Video Wifi Multimedia Share	<p>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.</p>
Voice Wifi Multimedia Share	<p>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.</p>

Parameter	Description
	<p>NOTE: 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.</p>
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.
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.
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	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. You can specify a RSSI value within range of 0-100 dB.
Min RSSI for auth request	Enter the minimum RSSI threshold for authentication requests.
Deauth inactive clients	Select this option to allow the AP to send a de-authentication frame to the inactive client and the clear client entry.

Parameter	Description
Can be used without uplink	Select this check-box if you do not want the SSID profile to use the uplink.
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	Turn on the toggle switch to disable intra VLAN traffic. It enables the client isolation and disables 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 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 toggle switch to provide high network security by maintaining data confidentiality of management frames. For more information, see Configuring 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 a Time Range Profile for a WLAN SSID .

Configuring Device Parameters for an AP

To configure device parameters on an access point (AP), 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 one of the options under **Groups**. Ensure that the filter selected contains at least one active 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.

- To select an AP in the filter:
 - a. Set the filter to **Global**.
 - 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 **Device > Access Point**.
- 2. Click the **Config** icon.
The tabs to configure 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.

- Configure the parameters described below.

Table 34: *Access Points Configuration Parameters*

UI	Parameters	Description
System	Name	Configures a name for the AP. For APs running 8.7.0.0 or later versions, you can enter up to 128 ASCII or non-ASCII characters. For APs running 8.6.0.0 or earlier versions, you can enter up to 32 ASCII or non-ASCII characters.
	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 APs obtain IP address from a DHCP server. ■ Static—You can also assign a static IP address to the AP. To specify a static IP address for the AP, complete the following steps: Enter the new IP address for the AP in the IP Address text-box. Enter the subnet mask of the network in the Netmask text-box. Enter the IP address of the default gateway in the Default Gateway text-box. Enter the IP address of the DNS server in the DNS Server text-box. <p>NOTE: 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> <p>Enter the domain name in the Domain Name text-box.</p>
	LACP Mode	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> ■ Active ■ Passive ■ Disabled <p>If LACP is enabled, you must specify if the ports on the gateway operate in Active or Passive mode. Passive enables LACP only when a LACP peer device is detected. For the port-channel to become active, one side must be operating in an Active mode.</p>
WLANS		From the WLANS table, specify one or more group WLANS that the selected AP will advertise.

UI	Parameters	Description
Radio	Enable Radio	Select the Enable Radio check-box under 2.4GHz Band and 5 GHz Band to enable the radio.
	Mode	<p>Select any of the following options:</p> <ul style="list-style-type: none"> ■ Access—In the Access mode, the AP serves clients, while also monitoring for rogue APs in the background. ■ Monitor—In the Monitor mode, the AP acts as a dedicated monitor, scanning all channels for rogue APs and clients. ■ Spectrum—In the Spectrum mode, the AP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference, whether from the neighboring APs or from non-Wi-Fi devices such as microwaves and cordless phones. <p>NOTE: In the Monitor and Spectrum modes, the APs do not provide access services to clients.</p> <p>NOTE: In the dual 5 GHz band, the Mode remains as Access and is non-editable. This dual 5 GHz band is only supported on AP-344 and AP that runs on ArubaOS 8.3.0.0. See Dual 5 GHz Radio Mode for more information.</p> <p>NOTE: To get accurate monitoring details and statistics, it is highly recommended to reboot the APs once the APs are toggled from the 2.4/5 GHz mode to dual 5 GHz radio mode or vice-versa.</p>
		You can configure a radio profile on an AP manually. See Configuring Radio Parameters for more information.
	Channel Assignment	<p>Select one of the following buttons:</p> <ul style="list-style-type: none"> ■ Automatic—Assign the channel settings automatically. ■ Manual—Select the number of channels from the drop-down list.
	Transmit Power Assignment	<p>Select one of the following buttons:</p> <ul style="list-style-type: none"> ■ Automatic—Assign the power settings automatically. ■ Manual—Enter the signal strength measured in dBm.
Uplink		Create the PEAP user credentials for certificate-based authentication. Enter the user name, password, and retype password in the Username , Password , and Retype Password fields to create the PEAP user.



You can now specify WLAN groups and radio profile for multiple APs in bulk. Select more than one APs from the **Access Points** table and click the edit icon on the pop-up window. In the new window, specify multiple WLAN groups from the **WLANs** table and select the radio profile from the **Radio Profile** drop-down list.

6. Click **Save Settings** and reboot the AP.

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 AP.

Configuring External Antenna

If the AP 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 AP is deployed. You can also measure or calculate additional attenuation between the device and antenna before configuring the antenna gain. To know, if the AP device supports external antenna connectors, see the *Installation Guide* that is shipped along with the AP 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 35: *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 APs with external connectors, 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 APs is displayed in the **List** view.

- To select an AP in the filter:
 - a. Set the filter to **Global**.
 - 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 **Device > Access Point**.
- 2. Click the **Config** icon.
The tabs to configure 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 **Radio** tab and select **External Antenna** to configure the antenna gain value. This option is available only if the selected AP supports external antennas.
- 6. Enter the **Antenna Gain** values in dBm for the **2.4GHz Band** and **5GHz Band**.
- 7. Click **Save Settings**.

Configuring Intelligent Power Monitoring

The Intelligent Power Monitoring (IPM) feature actively measures the power utilization of an 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.

To configure Intelligent Power Monitoring, 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 **Show Advanced**, and click the **System** tab.
The **System** details page is displayed.
5. Click the **IPM** accordion.
6. Select the **IPM Activation** check box to enable IPM.
7. Click the + icon in the **IPM Power Reduction Steps With Priorities** pane.
The **IPM Power Reduction Steps With Priorities** window is displayed.

8. In the **IPM Step Priority** field, enter a value from 1 to 16 to define IPM priority.
9. From the **IPM Step** drop-down list, select a setting as described in the following table:

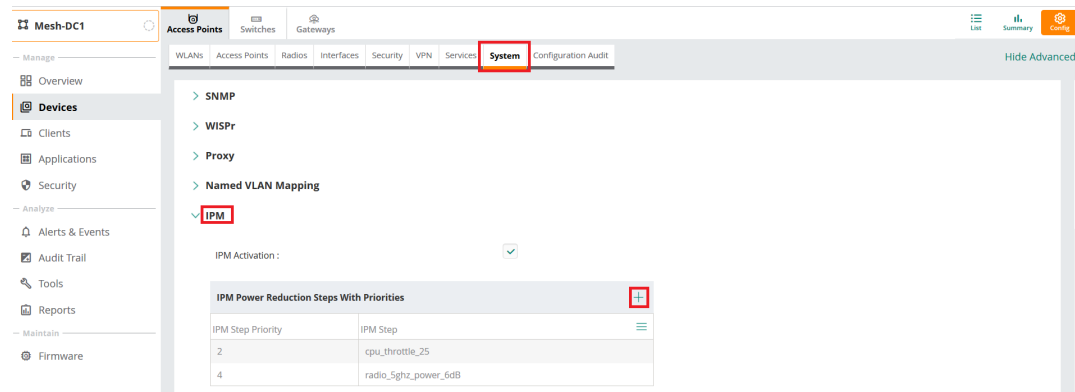
Table 36: Intelligent Power Monitoring Step Parameters

	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.
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.

10. Click **OK**.
The **IPM Power Reduction Steps With Priorities** table in the **IPM** section lists all the IPM settings.
11. Click **Save Settings**.
12. Reboot the AP 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 14 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, IPM is disabled.
- When enabled, IPM enables all AP 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 AP.

Support for Automatic Dual 5 GHz Mode

Aruba Central 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 access point (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, 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 second-level tabs to configure APs are displayed.

4. Click the second-level **Access Points** tab.
The **Access Points** table is displayed.
5. To edit an AP, select the AP and click the edit icon for that AP.
The edit pane for modifying the AP parameters is displayed.
6. Click the third-level **Radio** tab.
The **Radio** page is displayed.
7. Set **Dual 5G Mode** to **Automatic**.
8. Optionally, specify the manual channel by setting **Channel Assignment** to **Manual**.
9. Optionally, specify the transmit power by setting **Transmit Power Assignment** to **Manual**.

Configuring System > General Parameters for an AP Group

To configure system parameters for an AP, 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 APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced** (if required), and click the **System** tab.
The System details page is displayed.
5. Click the **General** accordion and configure the following parameters:

Table 37: System Parameters

Data Pane Item	Description
Set Country code for group	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. 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	This parameter allows you to configure NTP servers for the AP. Up to four NTP servers can be configured for the AP, each one separated by a comma. 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: <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.

Table 37: System Parameters

Data Pane Item	Description
	<p>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> <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>
<p>DHCP Option 82 XML</p>	<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 master 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 master 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_dhcpt82_1.xml ■ default_dhcpt82_2.xml <p>For more information, see Configuring DHCP Scopes on APs.</p>
<p>Login Session Timeout</p>	<p>Allows you to set a timeout for login session.</p>
<p>Console Access</p>	<p>When enabled, the users can access AP through the console port.</p>
<p>WebUI Access</p>	<p>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.</p>
<p>Telnet Server</p>	<p>When enabled, the users can start a Telnet session with the AP CLI.</p>
<p>LED Display</p>	<p>Enables or disables the LED display for all APs in a cluster.</p> <p>The LED display is always enabled during the AP reboot.</p>
<p>Deny Inter User Bridging</p>	<p>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.</p> <p>To disable inter-user bridging, turn off the Deny Inter User Bridging toggle switch.</p>
<p>Deny Local Routing</p>	<p>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.</p> <p>To disable local routing, move the slider to the right.</p>

Configuring HTTP Proxy on an AP

If your network requires a proxy server for Internet access, ensure that you configure the HTTP proxy on the AP to download the image from the cloud server. After setting up the HTTP proxy settings, the AP connects to the Activate server, Aruba Central, or OpenDNS server through a secure HTTP connection. You can also exempt certain applications from using the HTTP proxy (configured on an AP) by providing their host name or IP address under exceptions. Aruba Central allows the user to configuring HTTP proxy on an AP.

To configure HTTP proxy on AP through Aruba Central, 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 APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**, and click the **System** tab.
The System details page is displayed
5. 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.
 - c. Enter the user name and password in the **Username** and **Password** text boxes.
 - d. Retype the password in the **Retype Password** text box.
6. Click **Save Settings**.

Configuring Network Profiles on APs

This section describes the following procedures:

- [Configuring General > Advanced Settings for a WLAN SSID Profile](#)
- [Configuring Wireless Networks for Guest Users on APs](#)
- [Configuring Wired Port Profiles on APs](#)
- [Editing a WLAN SSID Profile](#)
- [Deleting a WLAN SSID Profile](#)
- [Editing a Wired Port Profile](#)
- [Disconnecting a Network from a WLAN SSID Profile](#)

Configuring General > Advanced Settings for a WLAN SSID Profile

Configuring the advanced settings is part of creating the WLAN SSID profile either in [Bridge mode](#) or [Mixed and Tunnel mode](#).

To configure the **Advanced Settings** under the **General** tab:

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**, go to **Device(s) > Access Points**.
3. If required, click the **Config** icon.
The second-level tabs to configure APs are displayed.
4. Go to the **WLANs** tab.
The **Wireless SSIDs** table is displayed listing the existing SSID profiles.
5. To create a new SSID profile, click **+ Add SSID**. To edit an existing SSID profile, click the row, and then click the edit icon.
The **Create a New Network** page is displayed for creating a new SSID. The **Networks** page is displayed for editing an existing SSID.
6. Under **General > Advanced Settings**, configure the following parameters:

Table 38: *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 AP drops all broadcast and multicast frames except DHCP and ARP, IGMP group queries, and IPv6 neighbor discovery protocols. ■ ARP—The AP 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 AP is configured to ARP mode. ■ Unicast ARP Only—This option enables AP to convert ARP requests to unicast frames thereby sending them to the associated clients. ■ Disabled—The AP 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 AP delivers the buffered broadcast and multicast frames to the associated clients in the power save mode. Range is 1 to 10 beacons.</p> <p>The default value is 1, which means the client checks for buffered data on the AP at every beacon. You can also configure a higher DTIM value for power saving.</p>
Dynamic Multicast Optimization (DMO)	<p>Select the check-box to allow AP 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.</p> <p>NOTE: 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 AP 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 AP sends multicast traffic over the wireless link.</p> <p>NOTE: This option will be enabled only when Dynamic Multicast Optimization is enabled.</p>

Parameter	Description
DMO Client Threshold	Specify a value between 2 and 255 to set the DMO client threshold.
Transmit Rates (Legacy Only)	
2.4 GHz	If the 2.4 GHz band is configured on the AP, specify the minimum and maximum transmission rates. The default value for minimum transmission rate is 1 Mbps and maximum transmission rate is 54 Mbps.
5 GHz	If the 5 GHz band is configured on the AP, specify the minimum and maximum transmission rates. The default value for minimum transmission rate is 6 Mbps and maximum transmission rate is 54 Mbps.
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. NOTE: 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. NOTE: 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 AP, it is automatically enabled for all SSIDs configured on an AP. By default, HT is enabled on all SSIDs. NOTE: If you want the 802.11ac APs to function as 802.11n APs, 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 AP, it is automatically enabled for all SSIDs configured on an AP. By default, VHT is enabled on all SSIDs. NOTE: If you want the 802.11ac APs to function as 802.11n APs, 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 AP, it is automatically enabled for all SSIDs configured on an AP. 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 DHCP 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	<p>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.</p> <p>NOTE: 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.</p>
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.
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.

Parameter	Description
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	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. You can specify a RSSI value within range of 0-100 dB.
Min RSSI for auth request	Enter the minimum RSSI threshold for authentication requests.
Deauth inactive clients	Select this option to allow the AP 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.
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	Turn on the toggle switch to disable intra VLAN traffic. It enables the client isolation and disables 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 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 toggle switch to provide high network security by maintaining data confidentiality of management frames. For more information, see Configuring 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 a Time Range Profile for a WLAN SSID .

Configuring Client Isolation

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 AP.

This feature enhances the security of the network and protects it from vulnerabilities. When **Client Isolation** is configured, the AP 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 AP. All other data packets are dropped.

Enabling Client Isolation for Wireless Networks

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**.

Configuring Management Frames Protection

Aruba Central supports the Management Frame Protection (MFP) feature that 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 AP.

Enabling Management Frames Protection for Wireless Networks in Aruba Central

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 **WLAN** 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 Wireless Networks for Guest Users on APs

APs 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 AP 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 AP.

The AP 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

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 an Internal Captive Portal Splash Page Profile](#)
- [Configuring an External Captive Portal Splash Page Profile](#)
- [Configuring Wireless Networks for Guest Users on APs](#)
- [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 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** 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 39: VLANs Assignment

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 AP 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 APs. 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 APs. 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.

Parameter	Description
<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"> <p>■ 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> <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"> 1. Click +Add Named VLAN. <p>The Add Named VLAN window is displayed.</p> <ol style="list-style-type: none"> 2. Enter the VLAN Name and VLAN details, and then click OK. <p>■ Dynamic—Assigns the VLANs dynamically from a DHCP server.</p> <p>To add a new VLAN assignment rule, complete the following steps:</p> <ol style="list-style-type: none"> 1. Click +Add Rule in the VLAN Assignment Rules window. <p>The New VLAN Assignment Rule page is displayed.</p> <ol style="list-style-type: none"> 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 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"> 1. Click +Add Named VLAN. <p>The Add Named VLAN window is displayed.</p> <ol style="list-style-type: none"> 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> <p>■ Native VLAN—Assigns the client VLAN is assigned to the native VLAN.</p> <p>For more information, see Configuring VLAN Assignment Rule.</p>

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 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. Configure the following parameters under **Splash Page**:

Table 40: *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. To create a new captive portal splash page, click Customize Captive Portal . For more information, see Configuring a Captive Portal Splash Page
Primary Server	Specify a primary authentication server for guest authentication. To create a new server, see Configuring External Authentication Servers for a WLAN SSID Profile .
Secondary Server	Specify a secondary authentication server for guest authentication. To create a new server, see Configuring External Authentication Servers for a WLAN SSID Profile .
Encryption	By default, this field is disabled. Turn on the toggle switch to enable and configure the following encryption parameters: 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	Turn on the MAC Authentication toggle switch to enable MAC address based authentication for Captive Portal security level.
Delimiter Character (Applies only to MAC Authentication)	Specify a character as a delimiter for the MAC address string. When configured, the AP 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. The supported characters are : (colon), / (slash), , (comma), - (dash), and % (percent).
Use IP for Calling Station ID	Enable this option to configure client IP address as calling station ID.
Called Station ID Type	The Called Station ID Type detail can be configured even if the Use IP for Calling Station ID is set to disabled. Select any of the following options for configuring a called station ID: <ul style="list-style-type: none"> ■ Access Point Group—Uses the AP's IP address as the called station ID. ■ Access Point Name—Uses the host name of the AP as the called station

Table 40: Internal Captive Portal Configuration Parameters

Parameter	Description
	<p>ID.</p> <ul style="list-style-type: none"> ■ VLAN ID—Uses the VLAN ID of as the called station ID. ■ IP Address—Uses the IP address of the AP as the called station ID.
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.
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	Sets a value for the maximum allowed authentication failures. Enter a number between 1 and 10.
Enforce DHCP	To enforce DHCP and to block traffic for AP clients that do not obtain IP address from DHCP, enable Enforce DHCP . When DHCP is enforced: <ul style="list-style-type: none"> ■ A layer-2 user entry is created when a client associates with an AP. ■ The client DHCP state and IP address are tracked. ■ When the client obtains an IP address from DHCP, the DHCP state changes to complete. ■ If the DHCP state is complete, a layer-3 user entry is created. ■ When a client roams between the APs, the DHCP state and the client IP address is synchronized with the new AP.
WPA3 Transition	This option appears when you select WPA3-Personal option in the Key Management drop-down list. This option allows the encryption format from WPA3 to WPA2.
Called Station ID Include SSID	Appends the SSID name to the called station ID.
Called Station ID Delimiter	Set delimiter at the end of the called station ID.
Uppercase Support	Set to Enabled to allow the AP to use uppercase letters in MAC address string for MAC authentication. This option is available only if MAC authentication is enabled.
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.
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 .

8. Click **Next**.

You can create and customize 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.

Complete the following steps to customize the splash page design:

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 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 either **Authenticated** or **Acknowledged** from the **Captive Portal Location** drop-down list.
8. Click **Customize Captive Portal**.
The **Splash Page Properties** page is displayed.
9. Configure the following parameters:

Table 41: *Splash Page Parameters*

Parameter	Description
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 .
Logo image	To upload a custom logo, click Browse to upload. Ensure that the image file size does not exceed 16 KB. To delete an image, click Delete Logo . To preview the captive portal page, click Preview . NOTE: 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 under Advanced Settings .

10. Click **Save**.

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 that contains 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. Configure the following parameters under **Splash Page**:

Table 42: External Captive Portal Configuration Parameters

Parameter	Description
Captive Portal Type	Select External from the drop-down list.
Captive Portal Profile	Select a profile from the drop-down list. To add a new profile, click + . For more information, see Configuring New External Captive Portal Profile
Primary Server	Specify a primary authentication server for guest authentication. To create a new server, see Configuring External Authentication Servers for a WLAN SSID Profile .
Secondary Server	Specify a secondary authentication server for guest authentication. To create a new server, see Configuring External Authentication Servers for a WLAN SSID Profile .
Encryption	By default, this field is disabled. Turn on the toggle switch to enable and configure the following encryption parameters: 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	

Table 42: External Captive Portal Configuration Parameters

Parameter	Description
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	Turn on the MAC Authentication toggle switch to enable MAC address based authentication for Captive Portal security level.
Delimiter Character (Applies only to MAC Authentication)	Specify a character as a delimiter for the MAC address string. When configured, the AP 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. The supported characters are : (colon), / (slash), , (comma), - (dash), and % (percent).
Use IP for Calling Station ID	Enable this option to configure client IP address as calling station ID.
Called Station ID Type	The Called Station ID Type detail can be configured even if the Use IP for Calling Station ID is set to disabled. Select any of the following options for configuring a called station ID: <ul style="list-style-type: none"> ■ Access Point Group—Uses the AP's IP address as the called station ID. ■ Access Point Name—Uses the host name of the AP 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 AP as the called station ID.
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.
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. Set a threshold for denylisting clients based on the number of failed authentication attempts. This is applicable for WLAN SSIDs only.
Max Authentication Failures	Sets a value for the maximum allowed authentication failures. Enter a number between 1 and 10.
Enforce DHCP	To enforce DHCP and to block traffic for AP clients that do not obtain IP address from DHCP, enable Enforce DHCP . When DHCP is enforced: <ul style="list-style-type: none"> ■ A layer-2 user entry is created when a client associates with an AP. ■ The client DHCP state and IP address are tracked. ■ When the client obtains an IP address from DHCP, the DHCP state changes to complete. ■ If the DHCP state is complete, a layer-3 user entry is created. ■ When a client roams between the APs, the DHCP state and the client IP address is synchronized with the new AP.
WPA3 Transition	This option appears when you select WPA3-Personal option in the Key Management drop-down list. This option allows the encryption format from WPA3 to WPA2.

Table 42: External Captive Portal Configuration Parameters

Parameter	Description
Called Station ID Include SSID	Append the SSID name to the called station ID.
Called Station ID Delimiter	Set delimiter at the end of the called station ID.
Uppercase Support	Set to Enabled to allow the AP to use uppercase letters in MAC address string for MAC authentication. This option is available only if MAC authentication is enabled.
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.
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 .

8. (Optional) 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 under **Advanced Settings**.
9. Click **Next**.

To add a new external captive portal profile page , 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 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**, click + next to **Captive Portal Profile**.
The **External Captive Portal-New** page is displayed.

- Configure the following parameters:

Table 43: New External Captive Portal Profile Configuration Parameters

Data Pane Item	Description
Name	Enter a name for the profile.
Authentication Type	Select any one of the following types of authentication: 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.
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.
Server Offload	Enable this option 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	Enable this option to prevent the overlay of frames. When enabled, the frames display only those pages that are in the same domain as the main page.
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 when Authentication Text is selected from Authentication Type drop-down list.
Use VC IP in Redirect URL	Enable this option to send the IP address of the virtual controller in the redirection URL when external captive portal servers are used. This option is disabled by default.
Redirect URL	Specify a redirect URL if you want to redirect the users to another URL.

- Click **OK**.

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. For more information, see Aruba Central Help Center.

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 that contains 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:
 - i. **Key Management**—Specify an encryption and authentication key.
 - ii. **Passphrase format**—Specify a passphrase format.
 - iii. **Passphrase**—Enter a passphrase.
 - iv. **Retype**—Retype the passphrase to confirm.
 - v. To exclude uplink, expand **Disable if uplink type is** and select an uplink type. For example, **Ethernet, Wi-Fi, and 3G/4G**.
 - vi. 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 that contains 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:

- 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, 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**.
8. To assign pre-authentication role, select the **Assign Pre-Authentication Role** check-box and select a pre-authentication role from the drop-down list.
 9. 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 that contains 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 44: 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. <p>To create a profile, click the + icon and enter the following information in the External Captive Portal window.</p> <ul style="list-style-type: none"> ■ 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. ■ Server offload—Turn on the toggle switch to offload the server.

Table 44: Access Rule Configuration Parameters

Data Pane Item	Description
	<ul style="list-style-type: none"> ■ 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 that contains 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 Wired Port Profiles on APs

If the wired clients must be supported on the APs, configure wired port profiles and assign these profiles to the ports of an AP.

The wired ports of an AP 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 AP, 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 APs is displayed in the **List** view.

3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**, and click the **Interfaces** tab.
The Interfaces details page is displayed.
5. Click the **Wired** accordion.
6. 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](#)
- [Configuring VLAN Network Profile Settings](#)
- [Configuring Security Settings](#)
- [Configuring Access Settings](#)
- [Configuring Network Port Profile Assignment](#)

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 APs 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 APs that support a minimum of 8.4.0.0 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 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.
 - **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.
2. 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.
 - **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 APs](#).
 - **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 [External RADIUS Server](#).
 - **Secondary Server**—To add another server for authentication, configure another authentication server.
 - **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 AP 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 AP as the called station ID.
 - **MAC address**—Uses the MAC address of the AP 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.



The **Downloadable Role** feature is optional, and is available only for networks that include APs that run a minimum of 8.4.0.0 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 APs](#).

2. Click the action corresponding to the server.
The **Edit Server** page is displayed.



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**.



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 that contains 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**, and click the **Interfaces** tab.
The Interfaces details page is displayed.

5. Click the **Wired** accordion.
The **Wired Port Profiles** page is displayed.
6. 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 AP 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.
7. 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 Wired Networks for Guest Users on APs

APs 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 AP 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 AP.

The AP 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

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.

For information on how to create splash page profiles, see the following sections:

- [Creating a Wired Network Profile for Guest Users](#)
- [Configuring an External Captive Portal Splash Page Profile](#)
- [Associating a Cloud Guest Splash Page Profile to a Guest SSID](#)
- [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 that contains 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**, and click the **Interfaces** tab.
The Interfaces details page is displayed.
5. Click the **Wired** accordion.
6. To create a new wired SSID profile, click **+Add Port Profile**.
The **Create a New Network** pane is displayed.
7. Under **General**, enter the following information:
 - a. **Name**—Enter a name.
 - b. **ports**—Select port(s) from the drop-down list.
8. Click **Next** to configure the **VLANs** settings.
The VLANs details are displayed.
9. In the **VLANs** tab, select a type of mode from the **Mode** drop-down list.
10. Select any of the following options for **Client IP Assignment**:

Table 45: *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.

Parameter	Description
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 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 46: *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.

Data Pane Item	Description
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.

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 a WLAN SSID Profile](#).
 - **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 AP 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 AP 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, APs 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**.

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. For more information, see Aruba Central Help Center.

To associate a Cloud Guest splash page profile to a guest SSID, 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.
 - a. Select **Cloud Guest** from the **Splash Page Type** 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 encryption parameters.
 - d. To exclude uplink, select **3G/4G**, **Wi-Fi**, or **Ethernet** option from **Disable If Uplink Type Is** accordion.
 - e. Click **Next**.
3. Click **Save Settings**.

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 that contains 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**.

Editing a WLAN SSID 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 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 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.

Deleting a WLAN SSID 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 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 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.

Editing a Wired Port Profile

To edit a wired port 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 APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced** (if required), 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**.

Disconnecting a Network from a WLAN SSID Profile

You can disable the network from a WLAN SSID profile, so that the connected clients are disconnected from the network,

To disconnect a network from a WLAN SSID 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 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 the network that you want to disconnect, and then click the disconnect icon under the **Actions** column.
6. Click **Yes** in the confirmation dialog box.

Configuring a Time Range Profile for a WLAN SSID

You can 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.

APs 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](#)
- [Configuring a Time Range Profile for a WLAN SSID](#)

Before You Begin

Before you configure time-based services, ensure that the NTP server connection is active.

Creating a Time Range Profile

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 APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**, and click the **System** tab.
The System details page is displayed.
5. Click the **Time-Based Services** accordion.
6. Click **+** in the **Time Based Profiles** table.
7. The **New Profile** window for creating a time range profile is displayed.
8. Configure the parameters that are listed in the following table.

Table 47: 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	Applicable to Periodic Type only. 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: <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> ■ For weekly occurrence—If the Repeat option is set to Weekly, this field allows you to select the start and end days of a week and time range. <p>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.</p> </p>
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 that contains at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, go to **Device(s) > Access Points**.

3. If required, click the **Config** icon.
The second-level tabs to configure APs are displayed.
4. Go to the **WLANs** tab.
The **Wireless SSIDs** table is displayed listing the existing SSID profiles.
5. To create a new SSID profile, click **+ Add SSID**. To edit an existing SSID profile, click the row, and then click the edit icon.
The **Create a New Network** page is displayed for creating a new SSID. The **Networks** page is displayed for editing an existing SSID.
6. To create a new SSID name, enter the name of an SSID, and click **Next**.
7. (Optional) Proceed to [Configuring General > Advanced Settings for a WLAN SSID Profile](#).
8. In **General > Advanced Settings**, click **Time Range Profiles**.
9. In the **Time Range Profiles** section, enter the following information:
 - a. Select a time range profile from the **Time Range Profile** list.
 - b. Select a value from the **Status** drop-down list.
 - When a time range profile is enabled on the 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.
10. Click **Save**.

Configuring RF Parameters on APs

This section provides the following information:

- [Configuring Radio Parameters](#)
- [Retrieving Radio Numbers for Clients Connected to APs](#)

Configuring Radio Parameters

To configure RF parameters for the 2.4 GHz and 5 GHz radio bands on an AP, 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 APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click the **Radios** tab.
5. In the RF Coverage page, perform one of the following steps:

- To configure existing radio parameters, select a profile from the **Radio Profiles** table and click the edit icon on the right.
- Click **+ Add Profile** to configure a new radio profile as described in the following table:

Table 48: Radio Configuration Parameters

Data Pane Item	Description
Name	Enter a name for the 2.4 GHz or 5 GHz radio profile.
Under 2.4 GHz Radio , 5 GHz Radio , or both, configure the following parameters:	
Allowed Channels	<p>Allows you to customize valid channels for 2.4 GHz and 5 GHz bands. By default, the AP uses valid channels as defined by the Country Code (regulatory domain). When you click on the default channels from the Allowed Channels field, a pop-up window is displayed containing a list of valid channels for both 2.4 GHz and 5 GHz.</p> <p>In the Allowed Channels - 2.4 GHz pop-up window, you can select the Allow 40 MHz Channel Bandwidth check box to allow 40 MHz bandwidth for the valid channels listed for 2.4 GHz band.</p> <p>In the Allowed Channels - 5 GHz pop-up window, you can specify the bandwidth range for the valid channels listed for 5 GHz band by selecting one of the following from the Minimum and Maximum drop-down lists:</p> <ul style="list-style-type: none"> ■ 20 MHz ■ 40 MHz ■ 80 MHz ■ 160 MHz
Allowed Transmit Power	Specify the minimum and maximum transmission power. The value specified indicates the minimum and maximum EIRP that can range from -51 dBm to 51 dBm. If the minimum and maximum transmission EIRP setting configured on an AP is not supported by the AP model, this value is reduced to the highest supported power setting.

6. Click **Show advanced settings** and configure the following additional parameters:

Table 49: Advanced Radio Configuration Parameters

Data Pane Item	Description
Advertise 802.11d & 802.11h	When enabled, the radios advertise their 802.11d (Country Information) and 802.11h (Transmit Power Control) capabilities. This option is disabled by default.
Scan All Channels	Allows the AP 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. This option is enabled by default.
ARM/WIDS Override	<p>Select one of the following from the drop-down list:</p> <ul style="list-style-type: none"> ■ Dynamic—If an AP is heavily loaded with client traffic and the CPU utilization exceeds the threshold limit, the WIDS processing is suspended. This causes more CPU cycles to handle the client traffic. When the CPU utilization is within the threshold limit, the WIDS processing is resumed. ■ On—When ARM/WIDS Override is enabled, the AP stops processing frames for

Table 49: Advanced Radio Configuration Parameters

Data Pane Item	Description
	<p>WIDS.</p> <ul style="list-style-type: none"> Off—When ARM/WIDS Override is disabled, the AP always processes 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.
High Noise Backoff Time	<p>The duration, in minutes, for not selecting Noise prone channel after 2 consecutive high noise detections on a channel. Setting the value to 0 from the drop-down list disables the backoff window. The default value is 720 minutes.</p>
Radar Backoff Time	<p>The duration, in minutes, for not selecting Radar prone channel after 2 consecutive radar detections on a channel. Setting the value to 0 disables the backoff window. The default value is 720 minutes.</p> <p>NOTE: This option is not applicable to 2.4 GHz Radio.</p>
Very High Throughput	<p>Select this check box to enable VHT (Very High Throughput) on 802.11ac devices with 5 GHz radio. If VHT is enabled for the 5 GHz radio profile on an AP, it is automatically enabled for all SSIDs configured on a AP. By default, VHT is enabled on all SSIDs. If you want the 802.11ac APs to function as 802.11n APs, clear the check box to disable VHT on these devices.</p> <p>NOTE: This option is not applicable to 2.4 GHz Radio.</p>
Set second radio differently	<p>Select this check box to use the second radio differently than the first radio.</p> <p>NOTE: This option is applicable only to AP-345 and AP-555 access points.</p>
Allowed transmit power	<p>Move to sliders to set the range of power transmitted on the second radio.</p> <p>NOTE: This option is applicable only to AP-345 and AP-555 access points.</p>

7. Click **Save Settings**.

Retrieving Radio Numbers for Clients Connected to APs

Aruba Central provides an option to retrieve the radio numbers of APs through the APIs. It also provides an option to filter AP details using radio numbers in the AP monitoring dashboard.



For regular APs 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.
3. In the **All Published APIs** window, click the any url link listed under the **Documentation** column.
The **Central Network Management APIs** page is displayed.

- On the left navigation pane, select **Monitoring** from the **URL** drop-down list.
- Click **API Reference > AP**.

The following APIs allow you to retrieve the radio number for the total number of clients connected:

Table 50: 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.

- 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 51: 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>.

Configuring IDS Parameters on APs

Aruba Central supports the IDS feature that monitors the network for the presence of unauthorized APs and clients. 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. 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**.
5. Click **Security**. The **Security** details page is displayed.
6. 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 52: Infrastructure Detection Policies

Detection level	Detection policy
Off	All detection policies are disabled.
Low	<ul style="list-style-type: none"> ■ Detect Windows Bridge ■ Signature Deassociation Broadcast ■ Signature Deauthentication Broadcast ■ Detect AP Spoofing
Medium	<ul style="list-style-type: none"> ■ Detect Windows Bridge ■ Signature Deassociation Broadcast ■ Signature Deauthentication Broadcast ■ Detect AP Spoofing ■ Detect adhoc using VALID SSID ■ Detect malformed large duration
High	<ul style="list-style-type: none"> ■ Detect Windows Bridge ■ Signature Deassociation Broadcast ■ Signature Deauthentication Broadcast ■ Detect AP Spoofing ■ Detect adhoc using VALID SSID ■ Detect malformed large duration ■ Detect Overflow EAPOL key ■ Detect Invalid Address Combination ■ Detect AP Impersonation ■ Detect AP Flood ■ Detect Beacon Wrong Channel ■ Detect ht Greenfield ■ Detect Overflow IE ■ Detect RTS Rate Anomaly ■ Detect Malformed HT IE ■ Detect CTS Rate Anomaly ■ Detect Malformed Frame Auth. ■ Detect devices with invalid MAC OUI ■ Detect Malformed Association Request ■ Detect Bad WEP ■ Detect Wireless Bridge ■ Detect HT 40 MHz intolerance ■ Detect Valid SSID Misuse ■ Detect Adhoc Network ■ Detect Client Flood
Custom	Allows you to select custom detection policies. To select, click the check box of respective detection policy.

Table 53: Client Detection Policies

Detection level	Detection policy
Off	All detection policies are disabled.
Low	Detect Valid Station Mis-association

Detection level	Detection policy
Medium	<ul style="list-style-type: none"> ■ Detect Valid Station Mis-association ■ Detect Hotspotter Attack ■ Detect Power Save DOS Attack ■ Detect Omerta Attack ■ Detect Disconnect Station ■ Detect unencrypted Valid ■ Detect Block ACK Attack ■ Detect FATA-Jack
High	<ul style="list-style-type: none"> ■ Detect Valid Station Mis-association ■ Detect Hotspotter Attack ■ Detect Power Save DOS Attack ■ Detect Omerta Attack ■ Detect Disconnect Station ■ Detect unencrypted Valid ■ Detect Block ACK Attack ■ Detect FATA-Jack ■ Detect Rate Anomaly ■ Detect Chop Chop Attack ■ Detect EAP Rate Anomaly ■ Detect TKIP Replay Attack ■ Signature – Air Jack ■ Signature – ASLEAP
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.

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 54: *Infrastructure Protection Policies*

Protection level	Protection policy
Off	All protection policies are disabled
Low	<ul style="list-style-type: none"> ■ Protect SSID ■ Rogue Containment
High	<ul style="list-style-type: none"> ■ Protect SSID ■ Rogue Containment ■ Protect AP Impersonation

Protection level	Protection policy
	<ul style="list-style-type: none"> ■ Protect from Adhoc Networks
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 55: *Client Protection Policies*

Protection level	Protection policy
Off	All protection policies are disabled
Low	Protect Valid Station
High	<ul style="list-style-type: none"> ■ Protect Valid Station ■ Protect Windows Bridge
Custom	Allows you to select custom detection policies. To select, click the check box of respective protection policy.

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**



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. is not liable for any claims, sanctions, or other direct, indirect, special, consequential or incidental damages related to your use of containment functionality.

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 Aruba Central Help Center.

1. To add multiple subnets, repeat step 2.
2. 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.

Management access to the AP is allowed irrespective of the inbound firewall rule.

The inbound firewall is not applied to traffic coming through the GRE tunnel.



NOTE

Configuring Authentication and Security Profiles on APs

This section describes the authentication and security parameters to configure on an AP:

- [Supported Authentication Methods](#)
- [Authentication Servers for APs](#)
- [Configuring Guest and Employee User Profiles on APs](#)
- [Important Points to Note](#)
- [Enabling ALG Protocols on APs](#)
- [Denylisting AP Clients](#)
- [Configuring a Wired Server with the IP Address](#)

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 APs managed through Aruba Central 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 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 AP. The wireless client can pass data traffic only after successful 802.1X authentication.



NOTE

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.

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 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 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 AP 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 AP 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.

To configure MAC authentication for a wireless 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 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**.

Captive Portal Authentication

Captive portal authentication is used for authenticating guest users. For more information, see [Configuring Wireless Networks for Guest Users on APs](#).

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 APs](#).

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 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 APs are displayed.
4. Click **Show Advanced**, and click the **Security** tab.
The **Security** details for the selected group or the device are displayed.
5. In the **Authentication Server** panel, click **+** to create a new server.
6. Select any of the following server types and configure the parameters for your deployment scenario.

Table 56: *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 AP by creating a TLS tunnel between the AP and the server.</p> <p>If Radsec is enabled, the following configuration options are displayed:</p> <ul style="list-style-type: none"> ● Radsec Port—Communication port number for RadSec TLS connection. By default, the port number is set to 2083. ● NAS Identifier

Type of Server	Parameters
	<ul style="list-style-type: none"> ● 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 AP 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 AP. 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. <ul style="list-style-type: none"> ● For AP-based cluster deployments, ensure that you enter the VC IP address as the NAS IP address. ● For Cloud AP based Campus WLAN deployments, ensure that you enter the AP 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.
Dead Time	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. <ul style="list-style-type: none"> ■ If Dynamic RADIUS Proxy (DRP) is enabled on the APs, configure the following parameters: <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. ● DRP GATEWAY—Gateway IP address of the DRP VLAN.
Service Type Framed User	Select any of the following check boxes to send the service type as Framed User in the access requests to the RADIUS server: <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.

Type of Server	Parameters
Query Status of RADIUS Servers (RFC 5997)	Select any of the following check boxes to detect the server status of the RADIUS server: <ul style="list-style-type: none"> ●Authentication—Select this check-box to ensure the AP sends a status-server request to determine the actual state of the authentication server before marking the server as unavailable. ●Accounting—Select this check-box to ensure the AP sends a status-server request to determine the actual state of the accounting server before marking the server as unavailable.
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 .
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.

Type of Server	Parameters
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	<ul style="list-style-type: none"> ■ 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.

Type of Server	Parameters
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.

7. 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.

Configuring Users Accounts for the AP Management Interface

You can configure RADIUS or TACACS authentication servers to authenticate and authorize the management users of an AP. 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 APs 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, the AP management user passwords are stored and displayed as hash instead of plain text. The **hash-mgmt-user** command is enabled by default on the APs provisioned in the template and UI groups. If a pre-configured AP 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 AP. In other words, Aruba Central hashes management user passwords irrespective of the management user configuration settings running on an AP.

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 that contains 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**, and click the **System** tab.
The System details page is displayed.

- Click the **Administrator** accordion and configure the following parameters:

Table 57: Configuration Parameters for the AP 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 APs .
	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**.

Support for MPSK in WLAN SSID

Aruba Central allows you to configure Multi-Pre-Shared Key (MPSK) in WLAN network profiles that include APs running a minimum of 8.4.0.0 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 AP.

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 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 AP 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 AP 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 AP stores the MPSK passphrase in its local cache for client roaming. The cache is shared between all the APs within a single cluster. The cache can also be shared with standalone APs in a different cluster provided the APs belong to the same multicast VLAN. Each AP first searches the local cache for the MPSK information. If the local cache has the corresponding MPSK passphrase, the AP 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

To configure multiple PSK for wireless networks, 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 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**.

MPSK Local

The MPSK Local operating mode allows to configure 24 pre-shared keys per SSID without an external policy engine like ClearPass Policy Manager. These local PSKs serve as an extension of the base pre-shared key functionality. MPSK Local operating mode is supported on the SSID profile to allow individual users or group of users to authenticate with per-device or per-group passphrase respectively. MPSK Local works only with wpa2-psk-aes encryption and not with any other PSK-based encryption.

The workflow is as follows:

1. The user creates the MPSK Local profile on the AP with the passphrase and key-name value.
2. By using WLAN SSID configuration wizard, the user creates the SSID profile with MPSK Local as the opmode.
3. The user attaches the MPSK Local profile created in step 1 to the SSID profile.
4. The MPSK Local profile is sent to the gateway during SSID creation as a UDR rule attached to AAA profile.
5. When the wireless client connects to the AP, the key-name value (Aruba-MPSK-Key-Name) identified is sent to the gateway as a TLV (Type-Length-Value).
6. The gateway processes the TLV to configure role and VLAN derivation-rules by matching the UDR rule.



MPSK Local only supports passphrases in the form of strings. It does not support passphrases in the form of hexadecimal characters.

To create an MPSK Local 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 APs are displayed.
4. Click **Show Advanced**, and click the **Security** tab.
The Security details page is displayed.
5. Click the **MPSK Local** accordion.
6. In the **MPSK Local** table, click **+** and enter a name for the MPSK Local profile.
7. To create an MPSK Local passphrase, click **+** and enter the following information in the **MPSK Local Passphrase** window, and then click **OK**.
 - a. **Name**—Enter a unique name for each profile.
 - b. **Passphrase**—Enter a passphrase.
 - c. **Retype Passphrase**—Retype the passphrase to confirm.
 - d. **Role**—Select a user role from the drop-down list.

8. In the **MPSK Local Passphrase** window, select an MPSK Local passphrase name, and then click **OK**.
9. Click **Save Settings**.

To edit an MPSK Local 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 APs are displayed.
4. Click **Show Advanced**, and click the **Security** tab.
The Security details page is displayed.
5. Click the **MPSK Local** accordion.
6. In the **MPSK Local** table, select an MPSK Local profile that you want to edit, and then click the edit icon.
7. In the **MPSK Local Passphrase** table, click **+** and enter the following information to add a new MPSK Local passphrase, and then click **OK**.
 - a. **Name**—Enter a unique name for each profile.
 - b. **Passphrase**—Enter a passphrase.
 - c. **Retype Passphrase**—Retype the passphrase to confirm.
 - d. **Role**—Select a user role from the drop-down list.
8. (Optional) To delete an MPSK Local passphrase, select the MPSK Local passphrase name from the **MPSK Local Passphrase** table, and then click the delete icon.
9. Click **OK**.
10. Click **Save Settings**.

To delete an MPSK Local 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 APs are displayed.
4. Click **Show Advanced**, and click the **Security** tab.
The Security details page is displayed.
5. Click the **MPSK Local** accordion.
6. In the **MPSK Local** table, select an MPSK Local profile that you want to delete, and then click the delete icon.
7. Click **Save Settings**.

To enable MPSK Local for wireless networks, 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 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 **MPSK Local**.
9. From the **MPSK Local** drop-down list, select an MPSK Local profile.
10. Click **Save Settings**.

WPA3 Encryption

Aruba Central supports WPA3 encryption for security profiles in SSID creation for networks that include APs running Aruba Instant 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 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.



WPA3-Enterprise is supported 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.

Configuring WPA3 for Enterprise Security for Wireless Network

To configure WPA3 for enterprise security, 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 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 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 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**.

Configuring Guest and Employee User Profiles on APs

The local database of an AP 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 AP is configured as an internal RADIUS server.

The local user database of APs can support up to 512 user entries except IAP-92/93. IAP-92/93 supports only 256 user entries. If there are already 512 users, IAP-92/93 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 that contains 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**, and click the **Security** tab.
The Security details page is displayed.
5. Click **User For Internal Server**.
6. In the **Users** pane, click the **+** icon.
7. In the **Add User** window, enter the following information:
 - 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.
 - Click **OK**.
8. 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**.
9. To delete a user:
 - a. In the **Users** pane, select the username to delete.
 - b. Click the delete icon.
 - c. Click **OK**.
10. 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.

Intra VLAN Traffic Allowlist

The Intra VLAN Traffic Allowlist is a global allowlist for all wired networks and WLAN SSIDs configured with the feature. For servers to serve the network, you must add them to Intra VLAN Traffic Allowlist using their IP or MAC address. When you configure wired servers with their IP address or MAC address, the AP allows client traffic to the destination MAC addresses.

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 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 APs are displayed.
4. Click **Show Advanced**, and click the **Security** tab.
The Security details page is displayed.
5. Click the **Intra VLAN Traffic Allowlist** accordion.
6. In the **Wired Server IP** window, click **+** and enter the IP address of the server.
7. Click **OK**.
8. 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.

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 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 APs are displayed.
4. Click **Show Advanced**, and click the **Security** tab.
The Security details page is displayed.
5. Click the **Intra VLAN Traffic Allowlist** accordion.
6. In the **Wired Server MAC** window, click **+** and enter the MAC address of the server.
7. Click **OK**.
8. 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.

Enabling GRE over IPsec for Tunnel and Mixed Modes

The Tunnel Orchestrator service establishes either IPsec tunnels or GRE tunnels between the AP and each of the Gateways present in the cluster. The IPsec tunnels provide end-to-end encryption of data traffic between the AP and the Gateway cluster. Based on the tunnel type to client's UAC, the AP can encapsulate client traffic in either GRE over IPsec or GRE without IPsec.

To configure secure data tunnels between AP and Gateway cluster, 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 APs are displayed.
4. Click **Show Advanced**, and click the **Security** tab.
The Security details page is displayed.
5. Click the **Data Handling** accordion.
6. To enable IPsec tunnel for data traffic, turn on the **Data Encryption** toggle button.
7. Click **Save Settings**.



The **Data Encryption** toggle button is disabled by default. When this toggle button is enabled, the AP sends client traffic to Gateway through GRE over IPsec. When this toggle button is disabled, the AP sends client traffic to Gateway through GRE only.

Configuring Roles and Policies on APs for User Access Control

APs support identity-based access control to enforce application-layer security, prioritization, traffic forwarding, and network performance policies for wired and wireless networks. Using the AP 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.

APs support a role-based stateful firewall. In other words, the firewall can recognize flows in a network and keep track of the state of sessions. The firewall logs on the APs 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 AP. 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 AP clients are associated with user roles, which determine the client's network privileges and the frequency at which clients re-authenticate. AP 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.

AP 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.

Netdestination and Alias

The netdestination feature allows you to create an alias for a specific host, network, IP address range, DNS name, or a combination of all of them on APs. To use netdestination, you must configure an IPv4 address or DNS name. The netdestination feature simplifies configuration of session or route ACLs by grouping a set of network destinations, and using the netdestinations as aliases in ACL policies.

You can use aliases to allow or block specific host, network, or both. When you have multiple hosts or networks to allowlist or denylist, you can create a single alias and add the list of hosts or network's IP addresses to it. This helps in allowing or blocking multiple entries at the same time.

You can use an alias when specifying the traffic source and/or destination in multiple session ACLs or route ACLs. Once you configure an alias, you can use it to manage network and host destinations from a central configuration point, because all policies that reference the alias are updated automatically when you change the alias.



AOS 10.2.0.0 does not support netdestination for IPv6 address.

The following commands configure an alias for an IPv4 network host, subnetwork, or range of addresses:

```
(host) [mynode] (config) #netdestination test
(host) [mynode] (config-submode) #description exampleConfiguration
(host) [mynode] (config-submode) #host 10.17.72.5
(host) [mynode] (config-submode) #network 1.1.1.0 255.255.255.240
(host) [mynode] (config-submode) #range 2.1.1.69 2.1.1.72
(host) [mynode] (config-submode) #name hpe.com
```

The following are the various commands used to troubleshoot netdestination profile:

- To view the configured and pre-defined aliases:

```
COMMAND=show netdestination
```

```
Name:          :test
Description:   :exampleConfiguration
Destination ID: :1
Position  Type      IP addr      Mask-Len/Range
-----  ----      -
1        host       10.1.1.41    32
2        name       0.0.0.2      www.baidu.com
3        network    10.65.155.0  255.255.255.192
```

```
COMMAND=show netdestination test
Name:          :test
Destination ID: :1
Position  Type      IP addr      Mask-Len/Range
-----  ----      -
1        host       10.1.1.41    32
2        name       0.0.0.2      www.baidu.com
3        network    10.65.155.0  255.255.255.192

Destination ID = 1, start-index = 1
1: 0 10.1.1.41 255.255.255.255
2: 1 0.0.0.2 255.255.255.255
3: 3 10.65.155.0 255.255.255.0

Total netdestination entries in use = 1
Total free netdestination entries = 1023
Available netdestination entries at bottom = 1023
Next netdestination entry to use = 1 (table 0)
```

- To view the netdestination profile configuration in datapath table:

```
COMMAND=show datapath netdest-id
Datapath Netdest Table
-----
ID  Type  Count  Start Index
--  ----  -
2   v4    6      1
```

```
COMMAND=show datapath netdest-id 2
Datapath Netdest Entries for netdest id 2
-----
Index  Type      Value
-----  ----      -
0      Host      10.1.1.41
```

```

2     NAME (DNS list id)  2
3     Range                1.1.1.4 to 1.1.1.9
5     Subnet                10.65.155.0 255.255.255.192

```

- To check if the domain name is configured under netdestination:

```
COMMAND=show acl domains
```

```
role-domain
```

```
-----
```

```

ID  role-domain                inused
--  -----
1   device.arubanetworks.com    used(1)
2   device-smoke1.arubathena.com used(2)
3   activate-frm5-cf.arubathena.com used(1)
4   smoke1-cgqa-elb.arubathena.com used(1)

```

```
COMMAND=show datapath dns-id-map
```

```
entry:0 id:9 yoda-cgqa.arubathena.com
```

```
entry:1 id:2 licdn.com
```

```
entry:2 id:3 twimg.com
```

- The maximum number of IPv4 addresses that are allowed in IP address range is 16.
- A netdestination definition can have a maximum of 256 netdestination entries.
- A maximum of 1024 netdestination entries are allowed on the AP.

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 that contains 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**, and click the **Security** tab.
The Security details page is displayed.
5. Click the **Roles** accordion.
6. Under **Access Rules For Selected Roles**, click **+** to add a new rule.
The **Access Rule** window is displayed.
7. Under **Rule Type**, select **Access Control**.
8. To configure access to applications or application categories, select a service category from the following list:

- Network
- App Category
- Application
- Web Category
- Web Reputation

9. Based on the selected service category, configure the following parameters:

Table 58: Access Rule Configuration Parameters

Data Pane Item	Description
Rule Type	Select a rule type from the list, for example Access Control .
Service	<p>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:</p> <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. <p>NOTE: If TCP and UDP uses the same port, ensure that you configure separate access rules to permit or deny access.</p>
Action	<p>Select any of following attributes:</p> <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	<p>Select a destination option. 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 AP is allowed. After selecting this option, specify the domain name in the IP text box. ■ To AP Network—Traffic to the specified AP network is allowed. After selecting this option, specify the domain name in the IP text box. ■ To master IP—Traffic to the specified master AP 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 APs are generated as security logs.

Table 58: Access Rule Configuration Parameters

Data Pane Item	Description
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.
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.

10. 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**.
3. Click the **Config** icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click the **Security** tab.
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 Reputation
 - Web Category

10. Based on the selected service category, configure the following parameters:

Table 59: 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.</p> <p>To specify a bandwidth limit:</p> <ol style="list-style-type: none"> 1. Select the Application Throttling check box. 2. 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 AP is allowed. After selecting this option, specify the domain name in the IP text box. ■ To AP Network—Traffic to the specified AP network is allowed. After selecting this option, specify the domain name in the IP text box. ■ To master IP—Traffic to the specified master AP 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. AP supports firewall based logging. Firewall logs on the 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 as Auth failure denylist time on the Denylisting tab of the Security window. For more information, see Denylisting AP Clients .

Table 59: Access Rule Configuration Parameters

Service category	Description
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. 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.
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. For more information on time range profiles, see Configuring a Time Range Profile for a WLAN SSID .

11. Click **Save**.

Configuring ACLs on APs for Website Content Classification

You can configure web policy enforcement on an 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 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 to display the AP configuration dashboard.
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. If required, select the following check boxes:
12. 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.
 - **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 APs are generated as security logs.
 - **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 AP 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 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 AP involves the following procedures:

- [Creating a User Role](#)
- [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 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 APs are displayed.
4. Click **Show Advanced**, and click the **Security** tab.
The Security details page is displayed.
5. Click the **Roles** accordion.
6. In the **Roles** pane, click **+**.
7. 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.

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 AP) or downstream (AP 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 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 APs are displayed.
4. Click **Show Advanced**, and click the **Security** tab.
The Security details page is displayed.
5. Click the **Roles** accordion.
6. [Create a user role](#) or select an existing role.
7. In the **Access Rues For Selected Roles** pane, click **+**.
8. In the **Access Rule** window, select **Bandwidth Contract** under **Rule Type**.
9. Specify the downstream and upstream rates in Kbps. If the assignment is specific for each user, select **Per User**.
10. 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 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.

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 that contains 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**.

To configure VLAN assignment rules for an SSID profile:

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 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.
9. From the **Rule Type** drop-down list, select **VLAN Assignment** option.
10. Enter the VLAN ID in the **VLANID** 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**.



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.

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 that contains 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 that contains 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**, and click the **Security** tab.
The Security details page is displayed.
5. Click the **Wireless IDS/IPS** accordion.
6. Under **Firewall Settings**, turn on the toggle switch to enable **SIP, VOCERA, ALCATEL NOE, Auto Topology Rules, Restrict Corporate Access**, and **CISCO Skinny** protocols.
7. 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 Firewall Parameters for Inbound Traffic

APs support an enhanced inbound firewall for the traffic that flows into the network through the uplink ports of an AP. You can configure firewall rules for the inbound traffic in the **Security > Inbound Firewall** section.

To configure the firewall rules, 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 APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**, and click the **Security** tab.
The Security details page is displayed.
5. Click the **Wireless IDS/IPS** accordion.
6. Click **Firewall Settings**.
7. In the **Access Rule** section, click the **+** icon.

The **Inbound Firewall** page is displayed.

8. In the **Inbound Firewall** page, enter the following information:

Table 60: 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 the IP address and netmask of the destination network. ■ 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

Parameter	Description
	<p>name in the Domain Name text box.</p> <ul style="list-style-type: none"> ■ To AP IP—Traffic to the specified AP is allowed. After selecting this option, specify the domain name in the IP text box. ■ To AP Network—Traffic to the specified AP network is allowed. After selecting this option, specify the domain name in the IP text box. ■ To master IP—Traffic to the specified master AP 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.

You can configure subnets to ensure that the AP 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 that contains 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**, and click the **Security** tab. The Security details page is displayed.
5. Click the **Wireless IDS/IPS** accordion.
6. Click **Firewall Settings**.
7. Under **Management Subnets** pane, to add a new management subnet, complete the following steps:
 - Enter the subnet address in **Subnet**.
 - Enter the subnet mask in **Mask**.
 - Click **Add**.

8. Click **Save Settings**.

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 master AP, including clients connected to a slave AP.

To configure restricted corporate access, 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 APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**, and click the **Security** tab.
The Security details page is displayed.
5. Click the **Wireless IDS/IPS** accordion.
6. Click **Firewall Settings**.
7. To restrict corporate access, turn on the **Restrict Corporate Access** toggle switch.
8. Click **Save Settings**.

Configuring Custom Redirection URLs for AP Clients

You can create a list of URLs to redirect users to when they access 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.

To create a list of error page URLs, 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 to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click the **Security** tab.
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**.

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 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 to display the AP configuration dashboard.
4. Click **Show Advanced**.

5. Click the **Security** tab.
6. Under **Roles**, select the role for which you want to configure access rules.
7. Click **+** in the Access Rules section. The **New Rule window** is displayed.
8. 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

APs support an enhanced inbound firewall for the traffic that flows into the network through the uplink ports of an AP.

To configure the firewall rules, 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 APs is displayed in the **List** view.
3. Click the **Config** icon. The tabs to configure the APs are displayed.
4. Click **Show Advanced**, and click the **Security** tab. The Security details page is displayed.
5. Click the **Wireless IDS/IPS** accordion.
6. Click **Firewall Settings**.
7. In the **Access Rule** section, click the **+** icon. The **Inbound Firewall** page is displayed.
8. In the **Inbound Firewall** page, enter the following information as described below:

Table 61: *Inbound Firewall Rule Configuration Parameters*

Parameter	Description
Service	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: <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	Select any of following actions: <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	Select any of the following options: <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.

Parameter	Description
	<ul style="list-style-type: none"> ■ 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 the IP address and netmask of the destination network. ■ 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 AP is allowed. After selecting this option, specify the domain name in the IP text box. ■ To AP Network—Traffic to the specified AP network is allowed. After selecting this option, specify the domain name in the IP text box. ■ To master IP—Traffic to the specified master AP or virtual controller is allowed. After selecting this option, specify the domain name in the IP text box.
Log	<p>Select the Log check box if you want a log entry to be created when this rule is triggered. Aruba supports firewall-based logging function. Firewall logs on the APs are generated as security logs.</p>
Denylist	<p>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.</p>
Classify Media	<p>Select the Classify Media check box to classify and tag media on HTTPS traffic as voice and video packets.</p>
Disable scanning	<p>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.</p>

Parameter	Description
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.

9. Click **Ok**.
10. 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.

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 master AP, including clients connected to a slave AP.

To configure restricted corporate access, 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 APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**, and click the **Security** tab.
The Security details page is displayed.
5. Click the **Wireless IDS/IPS** accordion.
6. Click **Firewall Settings**.
7. To restrict corporate access, turn on the **Restrict Corporate Access** toggle switch.
8. Click **Save Settings**.

Enabling ALG Protocols on APs

To configure protocols for ALG, 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 APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**, and click the **Security** tab.
The Security details page is displayed.

5. Click the **Wireless IDS/IPS** accordion.
6. 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.
7. 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 AP and the client, or wait a few minutes for changes to take effect.

Denylisting AP Clients

The client denylisting denies connection to the denylisted clients. When a client is denylisted, it is not allowed to associate with an AP 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 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 **Security** tab.
The Security details page is displayed.
5. Click the **Denylisting** accordion.
6. Under **Manual Denylisting**, click **+** and enter the MAC address of the client to be denylisted.
7. Click **OK**.
8. 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 General > Advanced Settings for a WLAN SSID Profile](#).

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 AP.

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 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 **Security** tab.
The Security details page is displayed.
5. Click the **Denylisting** accordion.
6. 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 Firewall**, enter the duration after which the clients can be denylisted due to an ACL rule trigger.
7. 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 General > Advanced Settings for a WLAN SSID Profile](#).



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](#).

Mapping AP Certificates

When an AP joins a group that does not have a certificate, the AP's existing certificate is retained. When an AP joins a group that already has a certificate, the AP's certificate is overwritten by the group certificate.

To map an AP 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**—To verify the identity of the TLS server.
 - **RadSec Certificate Authority**—To verify the authentication between the AP and the TLS server.
 - **Clearpass**—To verify the identity of the ClearPass server.
8. Click **Save Settings**.



To enable certificates for the **Cloud Guest Service**, contact the Aruba Central support team.

AP VPN Overview

As APs use a virtual controller architecture, the AP 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 AP networks at branch locations or data centers, where the Arubacontroller acts as a VPN Concentrator.

When the VPN is configured, the AP acting as the virtual controller creates a VPN tunnel to ArubaMobility Controller in your corporate office. The controller acts as a VPN endpoint and does not supply the AP 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

APs support the following VPN protocols for remote access:

Table 62: *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 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 AP 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 APs support IPsec only with ArubaControllers.</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. APs support the configuration of L2 GRE (Ethernet over GRE) tunnel with an Aruba Controller to encapsulate the packets sent and received by the AP. You can use the GRE configuration for L2 deployments when there is no encryption requirement between the AP and controller for client traffic.</p> <p>APs 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 AP, 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 AP 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.

Table 62: *VPN Protocols*

VPN Protocol	Description
	NOTE: APs support manual and Aruba GRE configuration only for L2 mode of operations. Aruba GRE configuration is supported only with ArubaControllers.
L2TP	The L2TP version 3 feature allows AP 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 AP gets the IP address from the DHCP server running on LNS. For this, AP has to transparently allow DHCP transactions through the L2TPv3 tunnel.

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.

To configure an IPsec tunnel from virtual controller, 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 APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**, and click the **VPN** tab.
The VPN details page is displayed.
5. Click the **Controller** accordion.
6. In the **Protocol** drop-down list, select **Aruba IPsec**.
7. In the **Primary host** field, enter the IP address or FQDN for the main VPN/IPsec endpoint.
8. 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.
9. Specify the following parameters.
 - a. To allow the VPN tunnel to switch back to the primary host when it becomes available again, select the **Preemption** check-box. 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. To allow the AP to create a backup VPN tunnel to the controller along with the primary tunnel, and maintain both the primary and backup tunnels separately, select the **Fast Failover** check-box. When fast failover is enabled and if the primary tunnel fails, the AP 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 AP can verify if an active VPN connection is available. The default value is 5 seconds, which means that the AP 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 AP can determine that the VPN connection is unavailable. The default value is 2.
 - e. 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** check-box.
 - f. To configure an interval for which wired and wireless users are disconnected during a VPN tunnel switch, specify a value in seconds for **Reconnect Time On Failover** within a range of 30-900 seconds. 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.
10. When the IPsec tunnel configuration is completed, the packets that are sent from and received by an AP 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, you can configure an access point (AP) to automatically set up a GRE tunnel from the AP to the controller.

To configure an AP to automatically set up a GRE tunnel, 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 APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**, and click the **Interfaces** tab.
The Interfaces details page is displayed.
5. Click the **GRE** accordion.
6. In the **Protocol** drop-down list, select **Aruba GRE**.
7. In the **Primary host** field, enter the IP address or FQDN for the main VPN/IPsec endpoint.
8. 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.
9. Select the **Per-AP-Tunnel** check-box.
The administrator can enable this option to create a GRE tunnel from each AP to the VPN/GRE Endpoint rather than the tunnels created just from the master AP. When enabled, the traffic to the corporate network is sent through a Layer-2 GRE tunnel from the AP itself and need not be forwarded through the master AP.



By default, the **Per-AP tunnel** option is disabled.

10. Specify a value in seconds for **Seconds Between Test Packets**.
Based on the configured frequency, the AP can verify if an active VPN connection is available. The default value is 5 seconds, which means that the AP sends one packet to the controller every 5 seconds.
11. Enter a value for **Max Allowed Test Packet Loss**, to define a number for lost packets, after which the AP can determine that the VPN connection is unavailable. The default value is 2
12. Click **Save Settings**.

Configuring a GRE VPN Tunnel

You can also manually configure a GRE tunnel by configuring the GRE tunnel parameters on the AP and controller. This procedure describes the steps involved in the manual configuration of a GRE tunnel from virtual controller by using Aruba Central.

During the manual GRE setup, you can either use the virtual controller IP or the AP IP to create the GRE tunnel at the controller side depending upon the following AP 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 AP 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 that contains 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**, and click the **Interfaces** tab.
The Interfaces details page is displayed.
5. Click the **GRE** accordion.
6. In the **Protocol** drop-down list, select **Manual GRE**.
7. 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. **GRE Type**—Enter a value for the parameter.
 - d. **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.
 - e. **Per-AP-Tunnel**—The administrator can enable this option to create a GRE tunnel from each AP to the VPN/GRE endpoint rather than the tunnels created just from the master AP. When enabled, the traffic to the corporate network is sent through a Layer-2 GRE tunnel from the AP itself and need not be forwarded through the master AP.



By default, the **Per-AP tunnel** option is disabled.

- f. 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**.
8. When the GRE tunnel configuration is completed on both the AP and Controller, the packets sent from and received by an AP are encapsulated, but not encrypted.

Configuring an L2TPv3 VPN Tunnel

The Layer 2 Tunneling Protocol version 3 (L2TPv3) feature allows AP 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 AP 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, 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 APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**, and click the **VPN** tab.
The VPN details page is displayed.
5. Click the **Controller** accordion.
6. In the **Protocol** drop-down list, select **L2TPv3**.
7. To configure a tunnel profile, complete the following steps:
 - a. Turn on the **Enable Tunnel Profile** toggle switch.
 - b. Enter the profile name.
 - c. Enter the primary server IP address.
 - d. Enter the remote end backup tunnel IP address. This is an optional field and is required only when backup server is configured.
 - e. Enter the peer UDP and local UDP port numbers. The default value is 1701.
 - f. Enter the interval at which the hello packets are sent through the tunnel. The default value is 60 seconds.
 - g. Select the message digest as MD5 or SHA used for message authentication.
 - h. Enter a shared key for the message digest. This key should match with the tunnel end point shared key.
 - i. If required, set the failover mode. The following two failover modes are supported:
 - **Preemptive**—In this mode, if the primary comes up when the backup is active, the backup tunnel is deleted and the primary tunnel resumes as an active tunnel. If you configure the tunnel to be preemptive, and when the primary tunnel goes down, it starts the persistence timer which tries to bring up the primary tunnel.
 - **Non-Preemptive**—In this mode, when the backup tunnel is established after the primary tunnel goes down, it does not make the primary tunnel active again.
 - j. Set an interval between every failover retry. The default value is 60 seconds.

- k. Configure a number of retries before the tunnel fails over.
- l. Ensure that **Checksum** is disabled.
- m. Specify a value for the tunnel MTU value if required. The default value is 1460.
- n. Click **Save Settings**.

Configuring Routing Profiles for AP VPN

Aruba Central can terminate a single VPN connection on ArubaMobility 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 APs is displayed in the **List** view.
3. Click the **Config** icon. The tabs to configure the APs 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 AP 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 APs

This section provides the following information:

- [Configuring DHCP Scopes on APs](#)
- [Configuring DHCP Server for Assigning IP Addresses to AP Clients](#)

Configuring DHCP Scopes on APs

The VC supports the following types of DHCP address assignments:

- [Configuring Distributed DHCP Scopes on page 237](#)
- [Configuring a Centralized DHCP Scope on page 239](#)
- [Configuring Local DHCP Scopes on page 241](#)

Configuring Distributed DHCP Scopes

Aruba Central 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 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 that contains 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**, and click the **System** tab.
The System details page is displayed.
5. Click the **DHCP** accordion.
6. To configure distributed DHCP scope, click **+** under **Distributed DHCP Scopes**.
The **New Distributed DHCP Scopes** pane is displayed.
7. Based on the type of distributed DHCP scope, configure the following parameters:

Table 63: *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.

Table 63: Distributed DHCP Scope Configuration Parameters

Data pane item	Description
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	<p>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.</p> <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. <p>NOTE: You can allocate multiple branch IDs (BID) per subnet. The AP 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.</p>
DHCP Reservation	<p>Displays the total number of DHCP reservations. Click the number to view the list of DHCP reservations.</p> <p>NOTE: You can configure DHCP reservation only on virtual controllers.</p> <p>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> <p>To delete a DHCP reservation, click the delete icon.</p>
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.

8. 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 AP does not allow the administrators to assign the remaining IP addresses to another branch, although a lower value is configured for the client count.

9. Click **Next**. The **Static IP** tab is displayed. Specify the number of first and last IP addresses to reserve in the subnet.
10. 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 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 **System** tab. The System details page is displayed.
5. Click the **DHCP** accordion.
6. To configure centralized DHCP scopes, click **+** under **Centralized DHCP Scopes**.
7. The **New Centralized DHCP Scope** data pane is displayed.
8. Based on type of centralized DHCP scope, configure the following parameters:

Table 64: *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

Table 64: *DHCP mode configuration parameters*

Data pane item	Description
VLAN	Specify a VLAN ID or multiple VLAN IDs by entering a list of comma separated digits or ranges, for example 1,2,5, or 1- 4, or all. You can enter the VLAN ID in the range of 1-4093. To use this subnet, ensure that the VLAN ID(s) 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 Instant AP'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> <p>NOTE: When split tunnel is enabled, you can specify only a single VLAN ID in the VLAN field. When split tunnel is disabled, you can enter multiple VLAN IDs separated by commas in the VLAN field.</p>
DHCP Relay	Select the DHCP Relay check-box to allow the APs 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	<p>Select one of the following options:</p> <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 XML drop-down list. ■ 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 > General Parameters for an AP Group</p>

9. Click **Save Settings**.

The following table describes the behavior of the DHCP Relay Agent and Option 82 in the AP.

Table 65: *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 AP:

- **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 AP 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 AP.
- **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 AP 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 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 **System** tab.
The System details page is displayed.
5. Click the **DHCP** accordion.
6. To configure local DHCP scopes, click **+** under **Local DHCP Scopes**.
7. The **New DHCP Scopes** data pane is displayed.

8. Based on type of local DHCP scope, configure the following parameters:

Table 66: 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 AP. 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. <p>NOTE: You can configure DHCP reservation only on virtual controllers.</p> <p>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> <p>To delete a DHCP reservation, click the delete icon.</p>
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.
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 AP Clients

The DHCP server is a built-in server, used for networks in which clients are assigned IP address by the 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 AP automatically determines a suitable DHCP pool for **Virtual Controller Assigned** networks. The AP typically selects the 172.31.98.0/23 subnet. If the IP address of the AP is within the 172.31.98.0/23 subnet, the AP 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 that contains 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**, and click the **System** tab.
The System details page is displayed.
5. Click the **DHCP** accordion.
6. 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. 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 on APs

This section describes how to configure location services, Lawful Intercept, OpenDNS, SIP phones, and Firewall services on APs:

- [Configuring an AP for RTLS Support](#)
- [Configuring an AP for ALE Support](#)
- [Managing BLE Beacons](#)
- [Configuring OpenDNS Credentials on APs](#)
- [Creating a CALEA Profile](#)
- [Configuring an AP for Network Integration](#)
- [Configuring XML API Interface](#)
- [Configuring SIP Phones with Source-NAT](#)
- [AppRF and Deep Packet Inspection](#)

Configuring an AP 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. In the **IP/FQDN** and **Port** fields, specify the IP address and port number of the RTLS server, to which location reports must be sent.
8. In the **Passphrase** field, enter the passphrase required for connecting to the RTLS server.
9. Retype the passphrase in the **Retype Passprahrse** field.
10. Specify the update interval within the range of 6-60 seconds in the **Update every** field.
The default interval is 30 seconds.
11. Click **3rd Party** and select **Aeroscout** to send reports on the stations to a third-party server.
12. In the **IP/FQDN** and **Port** fields, specify the IP address and port number of the third party server.
13. Select **Include Unassociated Stations** to send reports on the stations that are not associated to any AP.
14. Click **Save Settings**.

Configuring an AP 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 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 AP sends client information and all status information to the ALE server.

To integrate AP with ALE, the ALE server address must be configured on an AP. 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 AP

To configure an AP 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 AP sends messages to the ALE server at the specified interval. The default interval is 30 seconds.
9. Click **Save Settings**.

Managing BLE Beacons

APs 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 AP 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

AP assets can be tracked using BLE tags, AP beacons scan the network. When a tag is detected, the AP 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 67: BLE Operation Modes

Mode	Description
beaconing	The built-in BLE chip in the AP functions as an iBeacon combined with the beacon management functionality.
disabled	The built-in BLE chip of the AP is turned off. The BLE operation mode is set to Disabled by default.
dynamic-console	The built-in BLE chip of the AP functions in the beaconing mode and dynamically enables access to AP console over BLE when the link to LMS is lost.
persistent-console	The built-in BLE chip of the AP provides access to the AP 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.
11. Enter the URL of BLE HTTPS management server in **Server URL**.
12. Enter the authorization token in **Authorization token**.
13. Enter the location ID in **Location ID**.
14. Click **Save Settings**.

Configuring OpenDNS Credentials on APs

APs 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 APs

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 AP in a hierarchical and flat topology, mesh AP 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 AP to CALEA server, see *Aruba Instant User Guide*.

To enable an AP to communicate with the CALEA server, complete the following steps:

- [Creating a CALEA Profile](#)
- [Creating ACLs for CALEA Server Support](#)

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.
7. Click **Save Settings**.

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 APs for Palo Alto Networks Firewall Integration

APs maintains the network (such as mapping IP address) and user information for its clients in the network. To integrate the AP network with a third-party network, you can enable an AP to provide this information to the third-party servers.

To integrate an AP with a third-party network, you must add a global profile. This profile can be configured on an AP with information such as IP address, port, user name, password, firewall enabled or disabled status.

To configure an AP 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**.

AppRF and Deep Packet Inspection

Application Visibility (AppRF) is a custom built Layer 7 firewall capability supported for APs managed by Aruba Central. It consists of an on-board deep packet inspection and a cloud-based Web Policy Enforcement service that allows creating firewall policies based on types of application.

APs with Deep Packet Inspection (DPI) capability analyze data packets to identify applications in use and allow you to create access rules to determine client access to applications, application categories, web categories and website URLs based on security ratings. You can also define traffic shaping policies such as bandwidth control and QoS per application for client roles. For example, you can block bandwidth monopolizing applications on a guest role within an enterprise.

The DPI feature is supported on APs running 6.4.3.x-4.1.x.x or later releases. The AppRF feature is not supported on IAP-104/105 and IAP-134/135 devices.

You can configure APs to send URL information for the blocked HTTP and HTTPS sessions to ALE. The URL information can be extracted for the associated clients for DPI, analytics, and data mining through the Northbound APIs. To enable URL information logging and extraction, enable the URL Visibility parameter in the AP UI or CLI.



For more information on DPI and application analytics, see the following topics:

- [Enabling AppRF on APs](#)
- [Configuring ACLs for Deep Packet Inspection](#)
- [Configuring ACLs on APs for Website Content Classification](#)
- [Creating a List of Error Page URLs](#)

Enabling AppRF on APs

To view application usage metrics for WLAN clients, enable the AppRF service on APs.

To enable the AppRF 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**.
3. Click the **Config** icon to display the AP configuration dashboard.
4. If you select the device, click **Device** under **Manage**.
5. Click **Show Advanced**.
6. Click **Services**. The **Services** page is displayed.
7. Click **AppRF**.
8. 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.
9. Click **Save Settings**.

Configuring SIP Phones with Source-NAT

Aruba Central allows to use SIP phones with source-NAT function using centralized Gateway service. SIP ALG is supported in bridge mode along with the use of NAT on APs.



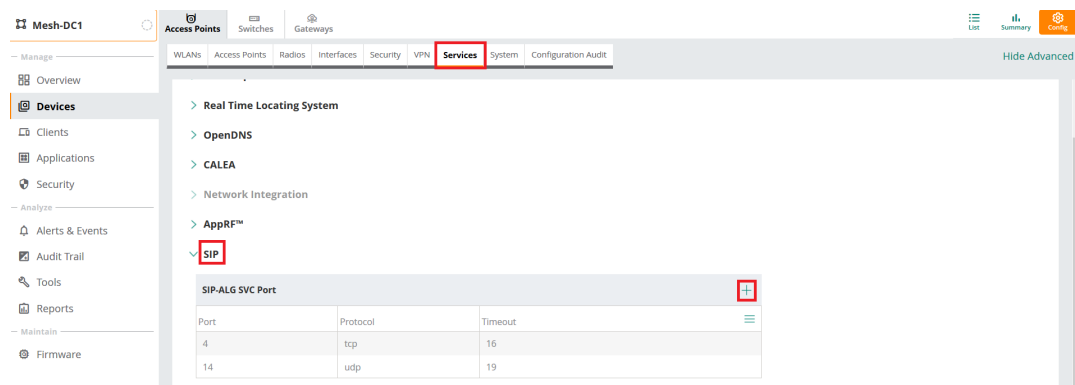
The SIP phones with source-NAT supported only on AP devices running Aruba Instant 8.6.0.3.

To configure SIP phones with source-NAT function, 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 **Show Advanced**, and click the **Services** tab.
The **Services** details page is displayed.
5. Click the **SIP** accordion.
6. Click the **+** icon in the **SIP** pane.
The **SIP-ALG SVC Port** window is displayed.
7. In the **Port** field, enter the port number within the range of 1–65535.
8. Select **TCP** or **UDP** from the **Protocol** drop-down list.
9. In the **Timeout** field, enter the timeout value in seconds.
The value should be between 15 to 30 seconds.
10. Click **OK**.
11. The **SIP-ALG SVC Port** table in the **SIP** section lists the configured SIP settings.
12. Click **Save Settings**.

The following figure displays the SIP configuration page:

Figure 15 SIP Configuration



Configuring XML API Interface

The XML API interface allows Instant APs to communicate with an external server. The communication between AP 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 slave AP.
- 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 *ArubaInstant User Guide*.

Enabling AirSlice on Access Points

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 a limited availability feature in Aruba Central. If you wish to enable the feature, contact your Aruba Representative.

The AirSlice feature is available for only Advanced AP 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 access points (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 Enterprise Domains

The enterprise domain names list displays the DNS domain names that are valid on the enterprise network. This list is used to determine how client DNS requests are routed. When **Content Filtering** is enabled, the DNS request of the clients is verified and the domain names that do not match the names in the list are sent to the OpenDNS server.

To configure an enterprise domain, 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 APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs are displayed.
4. Click **Show Advanced**, and click the **System** tab.
The System details page is displayed.
5. Click the **Enterprise Domains** accordion.
6. Click **+** in the **Enterprise Domains** pane, and enter a name in the **New Domain Name** window.
7. Click **OK**.
8. 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:

- [SNMP Configuration Parameters on page 253](#)
- [Configuring Community String for SNMP on page 253](#)
- [Configuring SNMP Trap Receivers on page 254](#)

SNMP Configuration Parameters

Aruba Central supports SNMPv1, SNMPv2c, and SNMPv3 for reporting purposes only. An AP cannot use SNMP to set values in an Aruba system.

You can configure the following parameters for an AP:

Table 68: *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 AP, 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 that contains 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**, and click the **System** tab.
The System details page is displayed.
5. Click the **SNMP** accordion.
6. Under **SNMP**, click **+** to add a new community string.
7. In the **New SNMP** window, enter a name for the community string.
8. Click **OK**.
9. 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 that contains 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**, and click the **System** tab.
The System details page is displayed.
5. Click the **SNMP** accordion.
6. Under **User for SNMPV3**, click **+** to add a new community string for **SNMPv3**.
7. 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**.
8. To edit the details for a particular user, select the user, and then click the edit icon.
9. To delete a particular user, select the user, and then click the delete icon.

Configuring SNMP Trap Receivers

Aruba Central supports the configuration of external trap receivers. Only the 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 that contains 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**, and click the **System** tab.
The System details page is displayed.

5. Click the **SNMP** accordion.
6. Under **SNMP Traps Receivers**, click **+** to add a new community string for **SNMP Traps Receivers**.
7. 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 APs on page 255](#)
- [Configuring TFTP Dump Server on page 256](#)

Configuring Syslog Server on APs

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 that contains 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**, and click the **System** tab.
The System details page is displayed.
5. Click the **Logging** accordion.
6. In the **Servers** section, enter the IP address of the syslog server in the **Syslog Server** text-box.
You can enter up to three IP addresses in the **Syslog Server** text box for logging events. Separate each value with a comma.
7. 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 AP 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 AP 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 69](#) describes the logging levels in order of severity, from the most severe to the least.

Table 69: 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.

8. Click **Save Settings**.

Configuring TFTP Dump Server

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 that contains 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**, and click the **System** tab. The System details page is displayed.
5. Click the **Logging** accordion.
6. In the **Servers** section, enter the IP address of the TFTP server in the **TFTP Dump Server** text-box.
7. Click **Save Settings**.

Mobility and Client Management

This section provides the following information on Layer-3 Mobility for AP clients:

- [Layer-3 Mobility on page 256](#)
- [Configuring L3 Mobility Domain on page 257](#)

Layer-3 Mobility

APs form a single Aruba Central 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 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 APs in a given Aruba Central network can roam to APs in a foreign Aruba Central 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 AP cluster.

Configuring L3 Mobility Domain

To configure a mobility domain, you have to specify the list of all Aruba Central 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 or VC IP address, so that the same configuration can be used across all Aruba Central 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 that contains 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**, and click the **System** tab.
The System details page is displayed.
5. Click the **Layer-3 Mobility** accordion.
6. Turn on the **Home Agent Load Balancing** toggle switch. By default, home agent load balancing is disabled.
7. 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.
8. 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.
- e. Click **OK**.

Configuring Routing Profiles for AP VPN

Aruba Central can terminate a single VPN connection on ArubaMobility 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 APs is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the APs 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 AP 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**.

Enterprise Mesh Network with Mesh APs

The Aruba secure mesh solution is an effective way to expand and configure network coverage for outdoor and indoor enterprise environments in a wireless environment. Using mesh, you can bridge multiple Ethernet LANs or extend your wireless coverage. The mesh network automatically reconfigures broken or blocked paths when traffic traverses across mesh AP. This self-healing feature provides increased reliability and redundancy by allowing the network to continue operating even when an AP is non-functional or if the device fails to connect to the network.

Mesh APs detect the environment when they boot up, and they locate and associate with their nearest neighbor to determine the best path to the mesh portal. The mesh functionality is supported only in dual-radio APs. On dual-radio APs, the 2.4 GHz radio is always used for client traffic, while both 2.4 GHz and 5 GHz radios are used for both mesh-backhaul and client traffic.

The mesh network must be provisioned for the first time by plugging into the wired network. After that, the mesh service works on APs like it does on any other regulatory domain.

Mesh Portals

A mesh portal is a gateway between the wireless mesh network and the enterprise wired LAN. The mesh roles are automatically assigned based on the AP configuration. You can deploy multiple mesh portals to support redundant mesh paths (mesh links between neighboring mesh points that establish the best path to the mesh portal) from the wireless mesh network to the wired LAN.

The mesh portal broadcasts an MSSID or mesh cluster name to advertise the mesh network service to available mesh points in the network. Neighboring mesh points that have been provisioned with the same MSSID authenticate to the portal and establish a secure mesh link over which traffic is forwarded. The authentication process requires secure key negotiation, common to all APs, and the mesh link is established and secured using AES encryption.



The mesh portal reboots after 5 minutes when it loses its uplink connectivity to a wired network.

Mesh Points

The mesh point is an Aruba AP configured for mesh and assigned the mesh point role. Depending on the AP model, configuration parameters, and how it was provisioned, the mesh point can perform multiple tasks. 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.

Mesh points use one of their wireless interfaces to carry traffic and reach the wired LAN. Mesh points are also aware of potential neighbors, and can form new mesh links if the current mesh link is no longer preferred or available.



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, you can convert the Eth0 uplink port to a downlink port by enabling port-bonding.

There can be a maximum of eight mesh points per mesh portal in a mesh network. When mesh APs boot up, they detect the environment to locate and associate with their nearest neighbor. The mesh APs determine the best path to the mesh portal ensuring a reliable network connectivity.

AOS 10.x provides support to configure a prioritized list of mesh portals that a mesh point should use. The mesh point then chooses the available mesh portal to connect to from that prioritized list.

Automatic Mesh Role Assignment

AOS 10.x supports enhanced role detection during AP boot-up and AP 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. This function is effective only when the mesh-role is configured as mesh-auto.

Mesh Role Detection during System Boot-Up

If the Ethernet link is down during AP boot-up, the AP acts as a mesh point. If the Ethernet link is up, the AP continues to detect if the network is reachable in the following scenarios:

- In a static IP address scenario, the AP acts as a mesh portal if it successfully pings the gateway. Otherwise, it acts as a mesh point.
- In case of DHCP, the AP acts as a mesh portal when it obtains the IP address successfully. Otherwise, it acts as a mesh point.
- In case of IPv6, APs do not support the static IP address but only support DHCP for detection of network reachability.

Mesh Role Detection during System Running Time

When a mesh point detects whether its Ethernet link is up, it continues to use Loop Protection (based on the Loop Protection for Secure Jack Port feature), to check if the loop has been detected. If the loop is detected, the AP reboots. Otherwise, the AP does not reboot and the mesh role continues to act as a mesh point.

Setting up Mesh Network

To configure APs as mesh APs:

1. Connect the APs to a wired switch.
2. Ensure that Aruba Central is synchronized and the country code is configured.
3. Configure mesh parameters in Aruba Central and ensure that the AP synchronizes with the mesh configuration.
4. Reboot APs to make the mesh configuration effective.
5. Disconnect the APs that you want to deploy as mesh points from the switch, and place the APs at a remote location. The APs come up without any wired uplink connection and function as mesh points. The APs with valid uplink connections function as mesh portals.

Mesh Uplink

Aruba provides centralized configuration and management for APs in a mesh environment where local mesh APs provide encryption and traffic forwarding for mesh links.



A mesh network requires at least one valid wired or 3G uplink connection.

Mesh APs are either configured as mesh portals or mesh points based on the uplink type. Any mesh-configured AP that has a valid uplink (wired or 3G) functions as a mesh portal, and the AP without an Ethernet link functions as a mesh point. Mesh portals and mesh points are also known as mesh nodes, a generic term used to describe APs configured for mesh.

Redundancy is observed in the mesh network when two mesh portals have valid uplink connections and APs are connected to the first mesh portal. In case of uplink failure in the first mesh portal, all the mesh points failover to the second mesh portal. However, depending on the actual deployment and RF environment, some mesh points may mesh through other intermediate mesh points.

Mesh Cluster Profile

Mesh clusters are grouped and defined by a mesh cluster profile, which provides the framework of the mesh network. The mesh cluster contains the MSSID, authentication methods, security credentials, and cluster priority required for mesh nodes to associate with their neighbors and join the cluster. You can also configure and apply multiple mesh clusters to an individual AP or an AP group. If you configure multiple cluster profiles with different cluster priorities, the mesh portal uses the profile with the highest priority to bring up the mesh network. The mesh portal stores and advertises that profile to neighboring mesh points to build the mesh network. This profile is known as the primary cluster profile.

Mesh points, in contrast, go through the list of configured mesh cluster profiles in order of priority to decide which profile to use to associate themselves with the network. The mesh cluster priority determines the order by which the mesh cluster profiles are used. Once the primary profile is identified, the other profiles are considered backup cluster profiles.

Since the mesh cluster profile provides the framework of the mesh network, you must define and configure the mesh cluster profile before configuring an AP to operate as a mesh node. You can use either the default cluster profile or create your own. If you find it necessary to define more than one mesh cluster profile, you must assign priorities to each profile to allow the mesh AP group to identify the primary and backup mesh cluster profiles. The primary mesh cluster profile and each backup mesh cluster profile must be configured to use the same RF channel.

The following CLI commands configure multiple mesh cluster profiles on an AP:

```
(AP) (config) # mesh-cluster <cluster_name_1> wpa2-psk <cluster_key_1> priority
<number_1>
(AP) (config) # mesh-cluster <cluster_name_2> wpa2-psk <cluster_key_2> priority
<number_2>
(AP) (config) # mesh-cluster <cluster_name_3> wpa2-psk <cluster_key_3> priority
<number_3>
```

The following CLI commands display the mesh cluster with the highest priority:

```
(AP) # show ap mesh cluster status
(AP) # show ap mesh cluster configuration
```

Mesh Recovery

The mesh recovery is based on a PSK, and mesh nodes use the recovery mechanism to establish a link to the managed device if the mesh link is broken and no other mesh clusters are available. The mesh recovery is automatically generated based on the customer ID.

Configuring Mesh APs

To configure APs as mesh nodes to bridge multiple Ethernet LANs or extend wireless coverage, 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 APs is displayed.
4. Click **Show Advanced**, and click the **System** tab.
The **System** details page is displayed.
5. Click the **Mesh** accordion.
6. Select one of the following from the **Mesh Role** drop-down list:
 - **auto**—an AP that automatically detects the mesh role and configures mesh portal or mesh point.
 - **portal**—an AP that uses its wired interface to reach the enterprise wired LAN.
 - **point**—an AP that establishes a path to the wired LAN using the mesh portal.

7. Select one of the following from the **Mesh Band** drop-down list:
 - **2.4 GHz**
 - **5 GHz**
8. Click + if you want to add a new mesh node to the network.
The **Mesh** window is displayed.
9. Configure the following parameters:
 - **Name**—Specify a name for the mesh node. The value must be between 8 to 32 characters.
 - **Key**—Specify a key for the mesh node, which is unique to each node. The value must be between 8 to 64 characters.
 - **Priority**—Specify a priority for the mesh node. The priority values range from 1-16, 1 being the highest and 16 being the lowest.
10. Click **OK**.
11. Click **Save Settings**.
12. Reboot the AP for the configuration to take effect.

Mobility Mesh

AOS 10.2.0.0 supports Mobility Mesh feature that provides fast roaming for APs deployed in a wireless mesh network. The mesh points for which fast roaming is enabled are called mobility mesh points. The mobility mesh points can dynamically reselect and reconnect to a new selected mesh point based on detection of RF conditions, such as beacon frames and RSSI value.

The Mobility Mesh feature involves the following steps:

1. **Detecting roaming condition**—The mesh points identify fast moving environments such as buses or the subway to apply fast roaming.
2. **Background scanning**—The mesh points perform fast scanning of other mesh points in the background. In fast scanning, the radio immediately initiates another channel scan request when the current scan request is complete. The background scan implies that when mesh is connected, the mesh point collects information about surrounding radio channels. The background scan is triggered due to missed beacon frames or low RSSI value below the threshold.
3. **Roaming or reconnection**—The mesh points rapidly choose the best mesh point neighbor to connect from all the neighbors.



The mobility mesh point scan time between radio channels is altered to be faster than the mesh point scan in a regular mesh network.

The following CLI command enables Mobility Mesh on the AP:

```
(AP) # mesh-mobility [high|low|<number>]
```



-
- This feature is currently supported on 300 Series, 303 Series, 303H Series, 310 Series, 318 Series, 320 Series, 330 Series, 360 Series, 370 Series, and 370EX Series access points.
 - A mesh point only connects to MPP (A mesh portal with hop count = 0).
 - A mesh point's hop count is always 1.
-

Radio Selection for Mesh Links

The radio used for the mesh link can be configured in dual 5 GHz or split 5 GHz enabled access points. When dual 5 GHz radio or split 5 GHz radio is enabled on the access point, the operations on the 5 GHz band is split and carried out by two separate radios—lower 5 GHz radio and upper 5 GHz radio. The lower 5 GHz radio operates on channels 32-64 and the upper 5 GHz radio operates on channels 100-173. With two active 5 GHz radios, the mesh link functions can be dedicated to one radio while the other radio can be used to service clients.



This feature is currently supported only on 340 Series and 550 Series access points.

The radio used for the mesh link can be configured using the **rf-split5G-band-range** command and can be configured only using the CLI. This configuration can only be applied on dual-5 GHz radio or split-5 GHz radio enabled APs. Apply the configuration and reboot the AP for the changes to take effect.

The following CLI command configures the radio for mesh link:

```
(host) [mynode] (config) #ap mesh-cluster-profile cluster1
(host) [mynode] (Mesh Cluster profile "cluster1") rf-split5G-band-range { first |
full | lower | upper }
```

The radio assignment and operating band information is listed in the following table:

Table 70: *Radio Assignment and Band Information*

Radio Mode	Radio	Operating Band
Dual 5 GHz (340 Series access points)	Radio 0	Upper 5 Ghz band
	Radio 1	Lower 5 Ghz band
Split 5 GHz (550 Series access points)	Radio 0	Lower 5 Ghz band
	Radio 2	Upper 5 Ghz band

Migrating APs to ArubaOS 10.x

You can migrate access points (APs) to ArubaOS 10.0.0.0 or later versions in AOS 10.x. The migration to ArubaOS 10.x involves the following two scenarios:

- Converting Instant AP from Aruba Instant 8.x to ArubaOS 10.x
- Converting Campus AP from ArubaOS 8.x to ArubaOS 10.x



The direct migration of APs running ArubaOS/Aruba Instant 6.x to ArubaOS 10.x is currently not supported. Instead, migrate the APs running ArubaOS/Aruba Instant 6.x to ArubaOS /Aruba Instant 8.7 and then follow the steps in this section to migrate the APs running ArubaOS/Aruba Instant 8.7 to ArubaOS 10.x.

Converting Instant AP from 8.x to ArubaOS 10.x

Before you convert Instant AP 8.x to ArubaOS 10.x, ensure that the following condition is met:

- Instant AP cluster is deployed in flat topology (single-subnet IP network)

Following are the high-level steps to convert Instant APs running 8.7.0.0 or later versions to ArubaOS 10.0.0.0:

1. Create a customer account having special permission to manage both 8.7.0.0 and 10.0.0.0 configurations simultaneously in Aruba Central.
2. Copy existing Instant AP groups in 8.7.0.0 to new groups, and configure 10.0.0.0 firmware compliance on the AP groups.
3. Move all Instant APs of a site to a new group in ArubaOS 10.0.0.0.
Aruba Central initiates upgrade from Instant AP to ArubaOS 10.0.0.0. The Instant AP boots up in ArubaOS 10.0.0.0 version and reconnects with Aruba Central by removing most of the configurations and retaining only the following uplink configurations:
 - Running configuration parameters:
 - ap1x uplink configuration (ap1x peap, and ap1x tls)
 - proxy server
 - mesh-cluster
 - all configurations in the pppoe-uplink-profile, wired-port-profile, enet0-port-profile, and enet1-port-profile
 - Per-AP env parameters:
 - static IPv4 address, static IPv6 address, netmask, gateway, DNS, and domain name
 - uplink-vlan
 - ap1x-peap-user and password
 - lacp-mode

Aruba Central performs configuration audit and forwards the 10.0.0.0 configurations from the new AP group.

Instant AP currently does not support migration for the following scenarios: Wi-Fi uplink, cellular uplink, and hierarchy mode.

The Aruba Central WebUI currently does not support the following per-AP env parameters: uplink-vlan, enet0-bridge, ap1x-peap-user and password, and IPv6 address. To perform migration in these scenarios, you must use Aruba Central template.



For more information on the various uplink configurations, see [Configuring Uplinks](#).

Converting Campus AP from 8.x to ArubaOS 10.x

When a Campus AP is migrated to an AP in AOS 10.x, you must ensure that the AP is able to reach the cloud. The uplink configuration between the different AP deployment modes must be aligned so that appropriate configuration parameters are chosen. This is to enable the AP to have a working uplink. In particular, the following uplink parameters must be configured for Campus AP migration:

- Static IP settings of uplink port
- AP1X settings on Eth01 uplink
- Mesh uplink parameters
- Wi-Fi uplink parameters

You can convert a Campus AP running ArubaOS 8.7.0.0 or later versions to ArubaOS 10.0.0.0 using the **ap convert** command. You can convert the AP using local-flash or local image server options like ftp, tftp, http, https, or scp by copying the downloaded image from Aruba support to the local ftp/tftp/scp server. From that server, the managed device downloads the image to its ftp or tftp folder and then distributes the ftp or tftp URLs to Campus APs.

For more information on the **ap convert** command, see [ap convert](#).

Following are the high-level steps to convert Campus APs running 8.7.0.0 or later versions to ArubaOS 10.0.0.0:

1. Create a customer account with special permission to manage both 8.7.0.0 and 10.0.0.0 configurations simultaneously in Aruba Central.
2. Copy existing AP groups in 8.7.0.0 to new groups, and configure 10.0.0.0 firmware compliance on the AP groups.
3. Reboot the Campus AP to upgrade it to the ArubaOS 10.0.0.0.
4. Issue the **ap convert active all-aps server ftp/http/https/scp/tftp** command on the managed device to initiate upgrade of Campus AP to ArubaOS 10.0.0.0 AP. The managed device obtains the ArubaOS 10.0.0.0 AP image, and notifies the APs to download it.
Apart from mesh and Wi-Fi uplink, the remaining uplink parameters are saved in **ap-env** parameter in Campus AP. When the AP boots up with ArubaOS 10.0.0.0 image, the uplink parameters saved before in **ap-env** are read and configured temporarily. This is to ensure that the AP boots up and connects to Aruba Central to access the new configuration successfully.
5. Issue the **no ap-env** command to remove the uplink parameters that are supported in AOS 10.x AP. For the parameters that are not supported in AOS 10.x AP, the uplink parameters in **ap-env** are cleared when AP makes configuration changes and the current uplink configuration is disabled. Once the Campus AP converts to 10.0.0.0 AP, there should not be any existing AP configurations but the AP should use Campus AP parameters. Hence, AP should recognize these Campus AP parameters and connect to the cloud. Once the APs are managed by cloud, they are provisioned with new parameters and the older Campus AP parameters are removed.

The Aruba Central WebUI currently does not support the following per-AP env parameters: uplink-vlan, enet0-bridge, ap1x-peap-user and password, and IPv6 address. To perform migration in these scenarios, you must use Aruba Central template.

The preferred uplink port is configured using the **preferred-uplink** command. The preferred uplink command is a per-AP setting and can only be configured manually on the AP through the CLI. The preferred uplink configuration can be viewed using the **show ap-env** command.

The following is the syntax for configuring the preferred uplink:

preferred-uplink <0,1>, where 0 is the Ethernet port and 1 is the fiber port.

The following example displays the configuration of Eth01 port as the preferred uplink:

```
(host)# preferred-uplink 1
```

The **show ap-env** command displays the status of preferred uplink configuration:

```
(host)# show ap-env
Antenna Type: Internal
Need usb field:No
uap_controller_less:1
preferred_uplink:eth1
```

[Table 71](#) provides a list of various Ethernet uplink parameters in **ap-env** that are configured to migrate Campus AP to 10.0.0.0 AP:

Table 71: Uplink Parameters to Migrate Campus AP to AOS 10.x AP

Uplink Type	Campus AP Parameter	AOS 10.x AP Parameter
Static IP	■ IPv4 address–	■ IPv4 address–

Table 71: Uplink Parameters to Migrate Campus AP to AOS 10.x AP

Uplink Type	Campus AP Parameter	AOS 10.x AP Parameter
	ipaddr, netmask, gatewayip, dnsip <ul style="list-style-type: none"> ■ IPv6 address—ip6addr, ip6prefix, gatewayip6, dnsip6 	ipaddr, netmask, gatewayip, dnsip <ul style="list-style-type: none"> ■ IPv6 address—ip6addr, ip6prefix, gatewayip6, dnsip6
PPPoE	pppoe_user pppoe_passwd pppoe_service_name pppoe_chap_secret	pppoe_user pppoe_passwd pppoe_service_name pppoe_chap_secret NOTE: When PPPoE uplink is not configured, the AP removes the uplink parameters by issuing the no ap-env command.
AP1X	ap1xuser, ap1xpasswd	ap1xuser, ap1xpasswd NOTE: When AOS 10.x AP boots up, it automatically enables ap1x peap parameter. This is to ensure that AP1X uplink connects to Aruba Central to obtain the required configuration.
Mesh	mesh_role	NA
Wi-Fi	wifi_uplink	NA

The Aruba Central WebUI currently does not support the following per-AP env parameters: uplink-vlan, enet0-bridge, ap1x-peap-user and password, and IPv6 address. To perform migration in these scenarios, you must use Aruba Central template.

To convert APs using local-flash option, upload the images in flash before executing the following commands:

```
(host) [mynode] #ap convert active specific-aps local-flash <images>
(host) [mynode] #ap convert active all-aps local-flash <images>
```

To convert APs using image servers, execute one of the following commands depending on the mode:

```
(host) [mynode] #ap convert all-aps server ftp: <ftphost> <user> <images >
(host) [mynode] #ap convert specific-aps server ftp: <ftphost> <user> <images>
(host) [mynode] #ap convert all-aps server scp: <scphost> <user> <images >
(host) [mynode] #ap convert specific-aps server scp: <scphost> <user> <images>
(host) [mynode] #ap convert all-aps server tftp: <tftphost> <images >
(host) [mynode] #ap convert specific-aps server tftp: <tftphost> <images>
```

To add specific AP groups or AP names to convert, execute the following command:

```
(host) [mynode] #ap convert add ap-group <ap-group>
(host) [mynode] #ap convert add ap-name <ap-name>
```

To remove specific AP groups or AP names from list of conversion, execute the following command:

```
(host) [mynode] #ap convert delete ap-group <ap-group>
(host) [mynode] #ap convert delete ap-name <ap-name>
```

To clear all the APs from the list of conversion, execute the following command:

```
(host) [mynode] #ap convert clear-all
```

To abort the conversion of APs:

```
(host) [mynode] #ap convert cancel
```

Configuring Uplinks

Most network devices such as APs, wireless routers, switches, and hubs are usually connected to a network backbone using Ethernet. In enterprise networks, APs normally connect to a switch with an Ethernet uplink and at homes, an AP normally connects to an ISP modem or a small switch using Ethernet. Though Ethernet is the most common and widespread uplink used for APs, some remote networks in particular have certain special uplink requirements. The following are some of the factors that require the need for an alternative to the standard Ethernet uplink of APs:

- Redundancy—In remote deployments, organizations have limited or no IT support and require the network to be always up to ensure productivity. Such organizations often require a backup link when the primary uplink fails. Some examples of organizations that require uplink redundancy include:
 - Energy companies having unmanned remote sites that have to be remotely accessible for monitoring purposes.
 - Healthcare and retail companies having remote and satellite offices that are required to be always up and accessible to carry out business.
 - Organizations with remote offices where employees depend heavily on centralized or cloud based services.
 - Lack of Ethernet uplink—Sometimes, extending an Ethernet uplink to a location is expensive or impossible due to geographical factors. In such situations, organizations require alternative uplink capabilities to connect to the internet and corporate resources. Some examples where an alternate uplink is required include:
 - Remote site where wired broadband services such as DSL and ADSL are expensive or unavailable.
 - Road warriors who need an AP to connect multiple devices but have limited or no access to Ethernet uplinks.
 - Mall Kiosks, mobile clinics, first response camps, and other emergency camps during catastrophic disasters.

Uplink Types

AOS 10.x provides the following types of uplinks to address the aforementioned deployment scenarios:

- [Ethernet Uplink](#)
- [Wi-Fi Uplink](#)

Ethernet Uplink

The Eth0 port on an AP is enabled as an uplink port by default. In most Campus and Remote AP networks, an AP connecting using an Ethernet uplink is usually assigned an IP using DHCP or static IP. However, in certain remote deployments, there is an additional possibility of ISPs assigning IP using PPPoE in addition to DHCP and static IP.

Ethernet uplink on AOS 10.x supports the following types of configuration:

- DHCP—This is the default method to receive an IP address on the Ethernet uplink.
- Static—When configuring a static IP for the AP, it is recommended to configure a valid DNS server.
- PPPoE—In networks where the ISP uplink uses PPPoE, the uplink can be configured for PPPoE. The AP can establish a PPPoE session with a PPPoE server at the ISP and get authenticated using username/password in Password Authentication Protocol (PAP) PAP or shared secret in Challenge Handshake Authentication Protocol (CHAP). After configuring PPPoE, reboot the AP for the PPPoE configuration to take effect. The PPPoE configuration is checked during AP boot and if the configuration is correct, Ethernet is used for the uplink connection. An SSID created with default VLAN is also not supported with PPPoE uplink.



After the PPPoE settings are configured, PPPoE has the highest priority for the uplink connections.

Configuring PPPoE Uplink Profile

To configure PPPoE settings from the WebUI, 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 APs is displayed.
4. Click **Show Advanced**, and click the **Interfaces** tab.
The **Interfaces** details page is displayed.
5. Click the **Uplink** accordion.
6. Perform the following steps in the **PPPoE** section:
 - a. Enter the PPPoE service name provided by your service provider in the **Service name** field.
 - b. Enter the secret key used for CHAP authentication in the **CHAP Secret** and **Retype CHAP Secret** fields.



You can use a maximum of 34 characters for the CHAP secret key.

- c. Enter the username for the PPPoE connection in the **User** field.
- d. Enter a password for the PPPoE connection and confirm the password in the **Password** and **Retype Password** fields.
- e. Select a value from the **Local Interface** drop-down list to set a local interface for the PPPoE uplink connections.
The selected DHCP scope will be 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 allows the entire Local L3 DHCP subnet to be allocated to clients.



The options in the **Local Interface** drop-down list are displayed only when a Local L3 DHCP scope is configured on the AP.

- f. Click **Save Settings**.
- g. Reboot the AP for the configuration to take effect.

The following example configures the PPPoE uplink on an AP in the CLI:

```
(AP) (config) # pppoe-uplink-profile
(AP) (pppoe-uplink-profile) # pppoe-username User1
(AP) (pppoe-uplink-profile) # pppoe-passwd Password123
(AP) (pppoe-uplink-profile) # pppoe-svcname internet03
(AP) (pppoe-uplink-profile) # pppoe-chapsecret 8e87644deda9364100719e017f88ebce
(AP) (pppoe-uplink-profile) # pppoe-unnumbered-local-l3-dhcp-profile dhcpProfile1
```

```
(AP) (pppoe-uplink-profile)# end
(AP) # commit apply
```

Configuring AP1X

To configure 802.1X authentication on uplink ports of an AP, complete the following steps in the WebUI:

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 APs is displayed.
4. Click **Show Advanced**, and click the **Interfaces** tab.
The **Interfaces** details page is displayed.
5. Click the **Uplink** accordion.
6. In the **AP1X** section, specify one of the following 802.1X authentication protocol to be used under the **AP1X Type** drop-down list:
 - If **TLS** authentication type is selected, specify the certificate type to be used in the **Certificate type** drop down list.
 - If **PEAP** authentication type is selected, enter the user credentials in the **Username** and **Password** text box.
7. Toggle the **Validate Server** button to enable or disable server certificate verification by the AP.
8. Click **Save Settings**.
9. Reboot the AP for the configuration to take effect.

The modem parameters are loaded during the AP boot process. Hence, the AP must be rebooted after configuring or reconfiguring any USB parameters. For plug and play modems, the modem must be plugged in during AP boot up. If the modem is plugged in after the AP is up, the AP must be rebooted to load the drivers. Once the drivers is loaded, the AP failovers between uplinks without any reboot.



Wi-Fi Uplink

AOS 10.x supports the use of existing Wi-Fi network as an uplink, when Ethernet or cellular uplinks are not available. Wi-Fi uplink allows you to connect to SSIDs with open, CCMP, TKIP, PSK-CCMP, and PSK-TKIP encryption. When Wi-Fi uplink is used, the AP uses MAC Address Translation (MAT) to bridge traffic between wireless and wired users of the AP and the uplink network. Wi-Fi uplink can also be used to connect the AP to another Wi-Fi service, such as a hospital wireless network. To enable or disable Wi-Fi uplink on the AP, the AP must be rebooted. Some examples where the Wi-Fi uplink is used are as follows:

- Mobile users who do not have an Ethernet or cellular uplink can use the Wi-Fi uplink to connect to hotel networks or other hotspots and securely connect to corporate resources and Internet using the VPN capabilities of AOS 10.x. This also allows the user to easily connect multiple devices to a hotspot because the MAC and IP addresses of the APs are used for the hotspot captive portal page and the user devices are hidden from the hotspot network.
- Mall Kiosks and certain devices in mobile clinics that support only Ethernet uplinks can connect to the existing Wi-Fi network through an AP. In this case, the device can connect to the additional Ethernet port on AP and the AP in turn can connect to the existing Wi-Fi network using the Wi-Fi uplink feature.



-
- Wi-Fi uplink is applicable to 802.11ax AP platforms and 802.11ac wave2 AP platforms except 340 Series access points.
 - Wi-Fi uplink is not supported on RAP-155 Series, 200 Series, 210 Series, 220 Series, and 270 Series access points.
 - Wi-Fi uplink is not supported on AP-555 access points when split 5 GHz mode is enabled.
 - 802.1X authentication is not supported in 802.11n AP platforms.
-

The following configuration conditions are applicable to Wi-Fi uplink:

- For single-radio APs, the radio serves wireless clients and the Wi-Fi uplink and for dual-radio APs, both radios can be used to serve clients but only one of them can be used for Wi-Fi uplink.
- It is recommended to use NAT mode when some clients are unable to obtain the IP address due to third-party DHCP servers. This is because the third-party DHCP servers may assign multiple IP addresses for one MAC address, when Wi-Fi uplink is configured in bridge mode.
- Mesh configuration is not supported when Wi-Fi uplink is configured on the 5 GHz band. If Wi-Fi uplink is enabled on the 5 GHz band, mesh is disabled.
- Mesh configuration is supported when Wi-Fi uplink is configured on the 2.4 GHz band. When Wi-Fi uplink is configured on the 2.4 GHz radio of an AP in a mesh, that AP automatically assumes the role of mesh portal.

Configuring Wi-Fi Uplink

To configure Wi-Fi uplink from the WebUI, 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 APs is displayed.
4. Click **Show Advanced**, and click the **Interfaces** tab.
The **Interfaces** details page is displayed.
5. Click the **Uplink** accordion.
6. In the **Wi-Fi** section, enter the name of the wireless network that is used for the Wi-Fi uplink in the **Name (SSID)** field.
7. Select the band in which the Virtual Controller currently operates, from the **Band** drop-down list.
The following options are available:
 - **2.4 GHz** (default)
 - **5 GHz**
8. Select the type of key for uplink encryption and authentication from the **Key Management** drop-down list.
If the uplink wireless router uses mixed encryption, **WPA-2 Personal** or **WPA-2 Enterprise** is recommended for the Wi-Fi uplink.
9. Select a passphrase format from the **Passphrase Format** drop-down list.
The following options are available:
 - 8-63 alphanumeric characters
 - 64 hexadecimal characters
10. Enter a PSK passphrase in the **Passphrase** field.

11. Click **Save Settings**.
12. Reboot the AP for the configuration to take effect.

The following example configures the Wi-Fi uplink profile in the CLI:

```
(AP) (config) # wlan sta-profile corpnet
(AP) (sta uplink)# uplink-band dot11a
(AP) (sta uplink)# cipher-suite wpa-tkip-psk
(AP) (sta uplink)# wpa-passphrase user@123
```

Uplink Preferences and Switching

This section includes the following topics:

- [Enforcing Uplinks](#)
- [Uplink Priority](#)
- [Uplink Preemption](#)
- [Switching Uplinks Based on VPN and Internet Availability](#)

Enforcing Uplinks

The enforce uplink parameter is used to specify an uplink that an AOS 10.x network must use even if other higher priority uplinks are available. When enforce uplink parameter is configured, an AP uses the specified uplink irrespective of the current status of the uplink configured in the enforce uplink parameter. When disabled, an AOS 10.x network selects an uplink based on the uplink status, uplink priority, and preemption settings.

To enforce a specific uplink on an AP from the WebUI, 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 APs is displayed.
4. Click **Show Advanced**, and click the **Interfaces** tab.
The **Interfaces** details page is displayed.
5. Click the **Uplink** accordion.
6. In the **Management** section, select the type of uplink from the **Enforce Uplink** drop-down list.
If the Ethernet uplink is selected, the **Port** text box is displayed.
7. Specify the Ethernet interface port number.
8. Click **Save Settings**.
9. Reboot the AP for the configuration to take effect.

To enforce an uplink, use the following CLI commands::

```
(host) (config)# uplink
```

```
(host) (uplink)# enforce {cellular|ethernet | wifi | none}
```

Uplink Priority

The uplink priority configuration allows you to define the uplink priority order when multiple uplinks are available. The uplink priority determines the uplink that the AP chooses during uplink failover and preemption.

To set an uplink priority from the WebUI, 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 APs is displayed.
4. Click **Show Advanced**, and click the **Interfaces** tab.
The **Interfaces** details page is displayed.
5. Click the **Uplink** accordion, and expand the **Management** section.
6. In the **Uplink Priority List** window, select the uplink, and drag the hand icon to increase or decrease the priority.
By default, the **Eth0** uplink is set as a high-priority uplink.
7. Click **Save Settings**.
The selected uplink is prioritized over other uplinks.

To set an uplink priority, use the following CLI commands:

```
(host) (config)# uplink
```

```
(host) (uplink)# uplink-priority {cellular <priority> | ethernet <priority> | [port  
<Interface-number> <priority>] | wifi <priority>}
```

Uplink Preemption

The preemption parameter determines whether an AP fails back to a higher priority link when it becomes available. When multiple uplink are available, an AP fails over to a lower priority link if the current link fails and if enforce uplink is disabled. When preemption is enabled, an AP that failed over to a lower priority link periodically checks to see if the higher priority link is available again and switches back to the higher priority uplink even if the current uplink is active. When preemption is disabled and the current uplink goes down, the AP tries to find an available uplink based on the uplink priority configuration.

To enable uplink preemption from the WebUI, 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 APs is displayed.
4. Click **Show Advanced**, and click the **Interfaces** tab.
The **Interfaces** details page is displayed.
5. Click the **Uplink** accordion.
6. In the **Management** section, select **None** from the **Enforce Uplink** drop-down list.
7. Toggle the **Pre-emption** switch to enable.
8. Click **Save Settings**.

To configure the Internet failover IP address for a cellular 3G/4G uplink, use the following CLI commands:

```
(host) (config)# uplink
```

```
(host) (uplink)# failover-internet-ip-for-cellular-uplink
```

Switching Uplinks Based on VPN and Internet Availability

The default priority for uplink switchover is Ethernet and the next preference is 3G/4G. The AP can switch to the lower-priority uplink if the current uplink is down.

AOS 10.x supports switching uplinks based on the VPN status when deploying multiple uplinks (Ethernet, 3G/4G, and Wi-Fi). When VPN is used with multiple backhaul options, the AP switches to an uplink connection based on the VPN connection status, instead of only using the Ethernet or the physical backhaul link.

The following configuration conditions apply to uplink switching:

- If the current uplink is Ethernet and the VPN connection is down, the AP tries to reconnect to VPN. The retry time depends on the fast failover configuration and the primary or backup VPN tunnel. If this fails, the AP waits for the VPN failover timeout and selects a different uplink such as 3G/4G or Wi-Fi.
- If the current uplink is 3G or Wi-Fi, and Ethernet has a physical link, the AP periodically suspends user traffic to try and connect to the VPN on the Ethernet. If the AP succeeds, it switches to Ethernet. If the AP does not succeed, it restores the VPN connection to the current uplink.

To configure uplink switching based on VPN status, 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 APs is displayed.
4. Click **Show Advanced**, and click the **Interfaces** tab.
The **Interfaces** details page is displayed.
5. Click the **Uplink** accordion.
6. In the **Management** section, specify the duration in the **VPN Failover Timeout** field to wait for an uplink switch.
By default, this duration is set to 180 seconds. When **VPN Failover Timeout** is set to 0, the uplink does not switch over.
7. Click **Save Settings**.

To enable uplink switching based on VPN status, use the following CLI commands:

```
(host) (config)# uplink
```

```
(host) (uplink)# failover-vpn-timeout <seconds>
```

You can configure AOS 10.x to switch uplinks based on Internet availability. When the uplink switchover based on Internet availability is enabled, the AP continuously sends Internet Control Management Protocol 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 public Internet is not reachable from the current uplink, the AP switches to a different connection. To configure uplink switching based on Internet availability, 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 APs is displayed.
4. Click **Show Advanced**, and click the **Interfaces** tab.
The **Interfaces** details page is displayed.
5. Click the **Uplink** accordion.
6. Under **Management** section, specify a value for **Failover Internet IP**.
7. Enable **Internet Failover**.
8. Specify values for **Failover Internet Packet Send Frequency**, **Failover Internet Packet Lost Count**, and **Internet Check Timeout**.
9. Click **Save Settings**.



When **Internet Failover** is enabled, the AP ignores the VPN status, although uplink switching based on VPN status is enabled.

To enable uplink switching based on Internet availability, use the following CLI commands:

```
(host) (config)# uplink
```

```
(host) (uplink)# failover-internet
```

```
(host) (uplink)# failover-internet-ip <ip>
```

```
(host) (uplink)# failover-internet-pkt-lost-cnt <count>
```

```
(host) (uplink)# failover-internet-pkt-send-freq <frequency>
```

Aruba Central allows the enablement of AOS10 at a Group Level. This involves conversion of the group type from ArubaOS 8.x to AOS 10.x. This feature is available only for Aruba Central customers that have been allow-listed for AOS 10.x. To begin the conversion process, you need to first create a group. By default, the group operates on the ArubaOS 8.x version. This newly created group can then be converted to AOS 10.x version.


An existing ArubaOS 8.x group in Aruba Central can also be converted to AOS 10.x, provided there are no APs or Gateways mapped to it. The current configuration in the group will be replaced with the default AOS 10.x configuration.

Important Points to Remember

- This conversion process is currently the only method to create AOS 10.x groups in Aruba Central.
- Once the group is converted to AOS 10.x, you cannot downgrade the group to ArubaOS 8.x or earlier versions.
- After an AP is added to an ArubaOS 8.x group, it cannot be upgraded to AOS 10.x. Similarly, an AP added to an AOS 10.x group, cannot be downgraded to ArubaOS 8.x. However, this logic does not apply to Gateways, as they are allowed to upgrade or downgrade, irrespective of the type of group they are in.
- By default, a newly created group in Aruba Central operates on ArubaOS 8.x, even if the devices imported to the group are AOS 10.x devices.

Converting a Group to AOS 10.x

To convert a group from ArubaOS 8.x to AOS 10.x, complete the following procedure in Aruba Central:

1. Ensure that the Aruba Central account is allow-listed to support AOS 10.x.
2. Create a new group. For more information, see [Creating a Group](#).
3. In the **Network Operations** app, set the filter to **Global**. The dashboard context for the filter is displayed.
4. Under **Maintain**, click **Organization**. By default, the **Groups** page is displayed.
5. Hover over the newly created group in the list, and click the  icon. The **Convert to AOS 10** window displayed.



The  icon is displayed only for ArubaOS 8.x groups that are not mapped to any device.

6. Click **Convert to AOS 10**, to convert the group to AOS 10.x.



This operation will discard the current configuration on the group, and replace it with a default AOS 10.x configuration. After the groups are upgraded to AOS 10.x, the conversion cannot be undone.

To check whether the upgrade to AOS 10.x is successful, see the event logs in the **Audit trail**.


Converting to AOS 10.x in MSP Mode

Aruba Central also supports migration of UI-based and template-based groups from ArubaOS 8.x to AOS 10.x, in the MSP mode. The MSP group can be upgraded to AOS 10.x only when there are no existing configurations in the group, and the group is not mapped to any tenant. An MSP group operating on AOS 10.x can be mapped to a tenant, only if the default group of the tenant is updated and converted from ArubaOS 8.x to AOS 10.x.



The default group of the tenant can be converted to AOS 10.x only if it does not have any devices, and a group-mapping relationship does not exist with MSP.

To convert a group in MSP mode, to AOS 10.x, complete the following procedure in Aruba Central:

1. Ensure that the MSP account is allow-listed to support AOS 10.x.
2. Create a new MSP group. For more information, see [Groups in MSP Mode](#).
3. In the **Network Operations** app, set the filter to **Global**. The dashboard context for the filter is displayed.
4. Under **Maintain**, click **Organization**. By default, the **Groups** page is displayed.
5. Hover over the newly created group in the list, and click the  icon. The **Convert to AOS 10** window is displayed.



The  icon is displayed only for ArubaOS 8.x groups that are not mapped to any tenants.

6. Click **Convert to AOS 10**, to convert the MSP group to AOS 10.x.



This operation will discard the current configuration for the group, and replace it with a default AOS 10.x configuration. After the groups are upgraded to AOS 10.x, the conversion cannot be undone.


Mapping a Tenant to an AOS 10.x MSP Group

The default group of the tenant must also be converted to AOS 10.x, before mapping it to an AOS 10.x MSP group. To convert the default group of the tenant to AOS 10.x, complete the following procedure in Aruba Central:

1. From the **Network Operations** app, filter **All Groups**.
2. Under **Manage**, click **Overview**. The **Dashboard** is displayed.
3. Hover over the tenant you want to convert to AOS 10.x, and click **expand**. The summary page for the tenant is displayed.



The tenant should not be associated to an existing MSP group.

4. Under **Maintain**, click **Organization**. By default, the **Groups** page is displayed.
5. Hover over the **default** group for the tenant and click the  icon. The **Convert to AOS 10** window is displayed.
6. Click **Convert to AOS 10**, to upgrade the default group of the tenant to AOS 10.x.
7. Click **Return to MSP View**.
8. In the **Customers | Overview** table, hover over the tenant account name, and click **edit**.
9. Turn on the **Add to Group** toggle switch and select the AOS 10.x MSP group from the **Group** drop-down list.



The **Groups** drop-down list will only include AOS 10.x MSP groups. The ArubaOS 8.x groups will no longer be displayed in the list once the default group of the tenant is converted to AOS 10.x.

10. Click **Save**. The tenant is now mapped to the AOS 10.x MSP group.
11. To check whether the upgrade to AOS 10.x is successful, see the event logs in the **Audit trail**.

RF Optimization	279
Monitoring Radios in Summary View	280
Monitoring Radios in List View	283
Dual 5 GHz Radio Mode	285
Support for Automatic Dual 5 GHz Radio Mode	286

AirMatch is a Radio Resource Management service. Aruba Central monitors radio resources on APs and also supports bandwidth and Effective Isotropic Radiated Power (EIRP) optimization for WLAN deployments. Aruba Central supports the AirMatch service on APs to enable networks to quickly adapt to changing RF conditions, such as a higher density, co-channel interference (CCI), coverage gaps, and roaming.

Aruba Central periodically analyzes RF data across the entire network to derive configuration changes for every AP deployed in a given network. The APs receive regular updates based on changing environmental conditions, using which the channel allocation is optimized plan on a regular basis. For example, when a local RF event is detected, such as an increase in the noise floor or when a radar detection event occurs, APs automatically change channels.

In addition to radio resource management and channel allocation, the AirMatch service performs the following functions:

- Compute channel bandwidth and EIRP for APs
- The AirMatch service in Aruba Central can also automatically adjust channel widths between 20MHz, 40MHz and 80MHz to maximize system capacity and overall network efficiency. If device density increases, the channel width will automatically change to either 40MHz or 20MHz. If it decreases, channel width will revert to a wider channel.
- It can also fine-tune power settings to minimize large EIRP swings across neighboring APs to ensure a seamless user experience.
- Provide a neighboring AP list to track client mobility and provide seamless roaming experience.

RF Optimization

By default, RF optimization is enabled on APs, and the channel and power transmission settings are static on AP radios. When RF optimization is enabled on APs, the AirMatch service on Aruba Central collects sample data about the RF environment from each AP in a network, and automatically tunes the transmission power and channel allocation on APs in a dynamic way.

Enabling RF Optimization

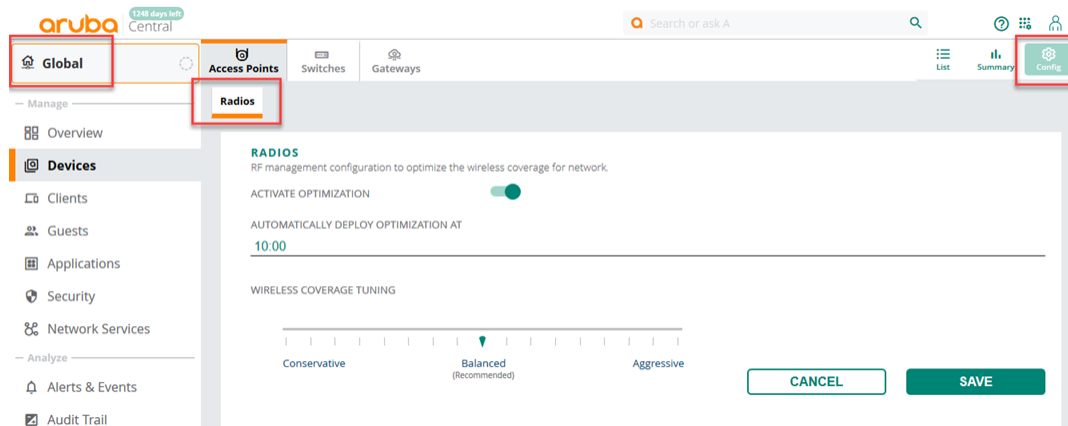
To enable RF optimization on APs, complete the following procedure:

1. In the **Network Operations** app, set the filter to **Global** to select the global dashboard.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the **Config** icon.

The **Radios** page is displayed.

4. To enable RF optimization, turn on the **Activate Optimization** toggle switch.

Figure 16 *Enabling RF Optimization*



1. Select the time at which you want to deploy automatic optimization.
2. Under **Wireless Coverage Tuning**, set one of the following wireless coverage tuning options:
 - a. **Unreactive**—Takes no or very few corrective actions for channel and power adjustments. Allows algorithm to prioritize preserving network settings over optimal RF health.
 - b. **Adaptive**—Allows to dynamically adjust radio channels and power while keeping a balance between preserving network settings, and finding optimal RF settings. This is the recommended option.
 - c. **Aggressive**—Allows to prioritize change of radio channels and power, over preserving network settings.



When you apply the RF optimization changes to a live network, it may impact the clients that are currently connected to the network. Therefore, Aruba recommends that you exercise caution when applying RF optimization on all APs in the network.

3. Click **Save**.

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. 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:

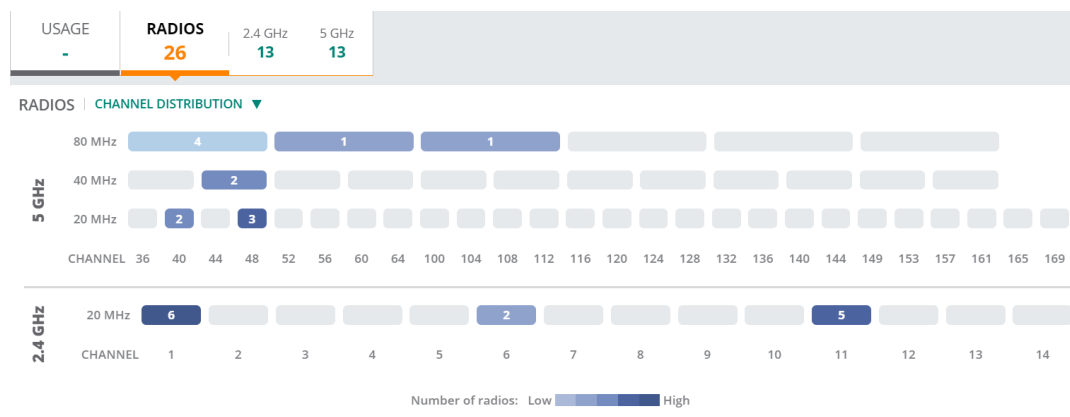
Radios

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.

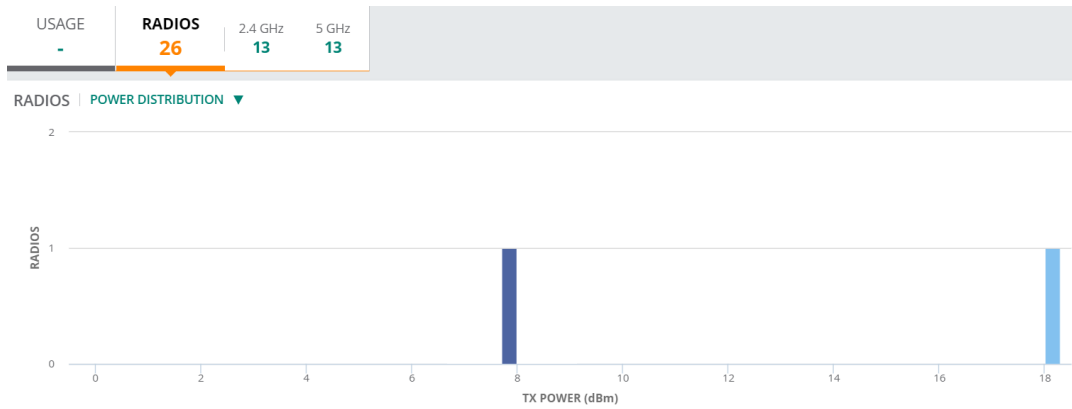
Figure 17 *Channel Distribution*



Power Distribution

From the drop-down list, select **Power Distribution** to display the power distributed across each of the radios.

Figure 18 *Power Distribution*

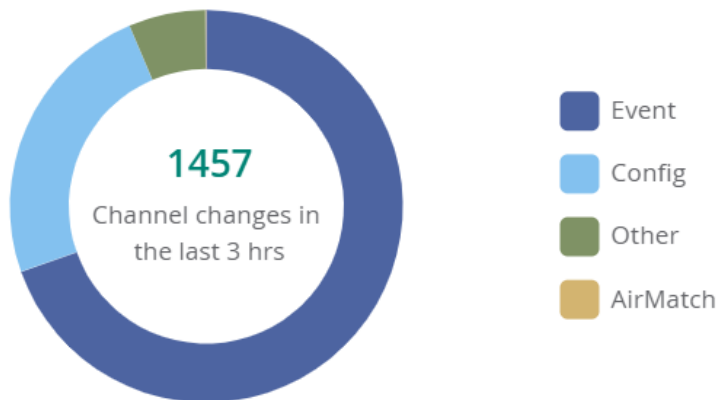


Channel Changes

The **Channel Changes** graph displays the number of channel changes that has occurred in the radios.

Figure 19 *Channel Changes*

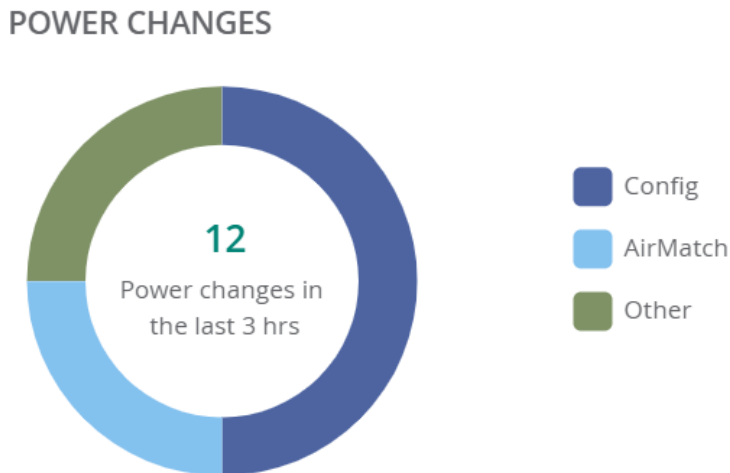
CHANNEL CHANGES



Power Changes

The **Power Changes** graph indicates the power change by each of the radios, from ARM to AirMatch EIRP.

Figure 20 Power Changes



Monitoring Radios in List View

The **Radios** tab in the access point (AP) List page provides information associated with the radios provisioned and managed in Aruba Central. When you click the **Radios** tab, the **2.4 GHz** and **5 GHz** tabs are displayed.

Viewing the Radios List Page

To navigate to the Radios 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.
3. Click the **Radios** tab.
A list of radios is displayed in the **List** view.

When you click the **Radios** tab, it displays the following information:

- **Radios**—Displays the total number of radios. When you click the **Radios** tab, it provides information about all the 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](#).

Radios Table

When you click the **Radios**, **2.4 GHz**, and **5 GHz** tab, the **Radios** table provides 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. Certain type of interferences, though not all, may affect or increase:
 - Noise at the radio receivers of the radios
 - Thermal noise
 - Noise floorNoise 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.

Figure 21 Radios Tab in List View

ACCESS POINT	RADIO MAC ADDRESS	BAND	BANDWIDTH	CHANNEL	UTILIZATION	CHANNEL CHANGES	POWER (dBm)	POWER CHANGES	NOISE FLOOR (dBm)
325-2	ac a3 1e 53 c1 d0	5 GHz	-	-	-	-	-	-	-
325-2	ac a3 1e 53 c1 d0	2.4 GHz	-	-	-	-	-	-	-
04bd88:ca:2c:26	04 bd 88 22 c2 60	2.4 GHz	-	-	-	-	-	-	-
04bd88:ca:2c:26	04 bd 88 22 c2 70	5 GHz	-	-	-	-	-	-	-
c8b5ad:c3:bc:98	c8 b5 ad bb bc 90	5 GHz	-	-	-	-	-	-	-
c8b5ad:c3:bc:98	c8 b5 ad bb bc 90	2.4 GHz	-	-	-	-	-	-	-
a8bd27:ee:df:40	a8 bd 27 ee df 40	2.4 GHz	-	-	-	-	-	-	-
a8bd27:ee:df:40	a8 bd 27 ee df 50	5 GHz	-	-	-	-	-	-	-

Figure 22 2.4 GHz Radios Tab in List View

ACCESS POINT	RADIO MAC ADDRESS	BAND	BANDWIDTH	CHANNEL	UTILIZATION	CHANNEL CHANGES	POWER (dBm)	POWER CHANGES	NOISE FLOOR (dBm)
a8bd27:ee:df:40	a8 bd 27 ee df 40	2.4 GHz	-	-	-	-	-	-	-
04bd88:ca:2c:26	04 bd 88 22 c2 60	2.4 GHz	-	-	-	-	-	-	-
c8b5ad:c3:bc:98	c8 b5 ad bb bc 90	2.4 GHz	-	-	-	-	-	-	-
325-2	ac a3 1e 53 c1 d0	2.4 GHz	-	-	-	-	-	-	-

Figure 23 5 GHz Radios Tab in List View

ACCESS POINT	RADIO MAC ADDRESS	BAND	BANDWIDTH	CHANNEL	UTILIZATION	CHANNEL CHANGES	POWER (dBm)	POWER CHANGES	NOISE FLOOR (dBm)
04bd88:ca:2c:26	04 bd 88 22 c2 70	5 GHz	-	-	-	-	-	-	-
c8b5ad:c3:bc:98	c8 b5 ad bb bc 90	5 GHz	-	-	-	-	-	-	-
325-2	ac a3 1e 53 c1 d0	5 GHz	-	-	-	-	-	-	-
a8bd27:ee:df:40	a8 bd 27 ee df 50	5 GHz	-	-	-	-	-	-	-

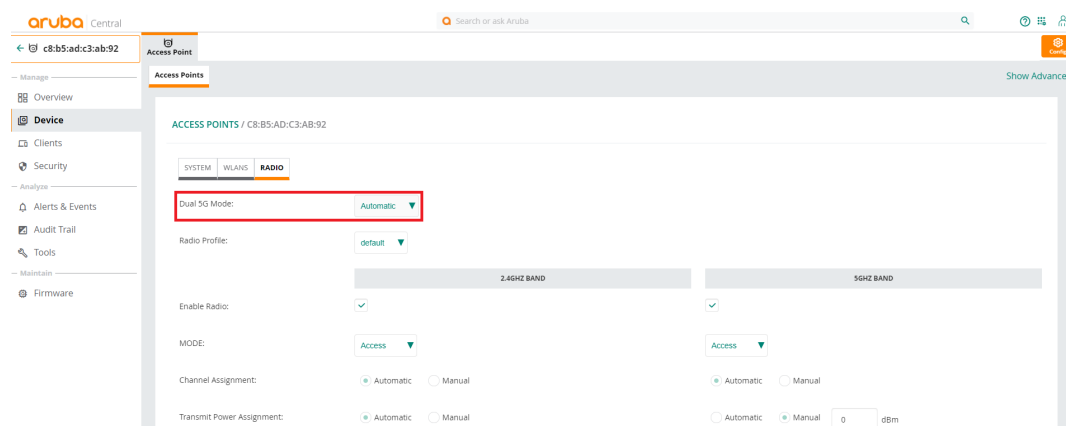
Dual 5 GHz Radio Mode

The dual 5 GHz radio mode feature of AirMatch allows the 340 Series APs to configure two radio interfaces, both running 5 GHz channel. The APs have two radios, one operating on 2.4 GHz band, and the other on 5 GHz band. AP-345 APs support upgrade of the 2.4 GHz radio interface to a 5 GHz radio interface, which effectively doubles the throughput in 5 GHz band. Hence, both radio interfaces can operate on 5 GHz band in dual 5 GHz radio mode. You can configure the dual 5 GHz radio mode using the WebUI.

To configure a dual 5 GHz radio, 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 second-level tabs to configure APs are displayed.
4. Click the second-level **Access Points** tab.
The **Access Points** table is displayed.
5. To edit an AP, select the AP and click the edit icon for that AP.
The edit pane for modifying the AP parameters is displayed.
6. Click the third-level **Radio** tab.
The **Radio** page is displayed.
7. Select **Enable** from the **Dual 5G Mode** drop-down list.
The default option is **Automatic**.
8. Click **Save Settings** and reboot the AP.

Figure 24 *Dual 5 GHz Radio*



The dual 5 GHz radio mode feature is supported only on AP-344 and AP-345.

For more information on the other fields in the **Radio** section, see [Configuring Device Parameters for an AP](#).

Support for Automatic Dual 5 GHz Radio Mode

There is an automatic opmode selection available for dual 5 GHz AP. When the opmode is set to automatic, AirMatch determines whether to convert a 2,4 GHz 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 supported only on AP-345, and not 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, 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 second-level tabs to configure APs are displayed.
4. Click the second-level **Access Points** tab. The **Access Points** table is displayed.
5. To edit an AP, select the AP and click the edit icon for that AP. The edit pane for modifying the AP parameters is displayed.
6. Click the third-level **Radio** tab. The **Radio** page is displayed.
7. Set **Dual 5G Mode** to **Automatic**.
8. Optionally, specify the manual channel by setting **Channel Assignment** to **Manual**.
9. Optionally, specify the transmit power by setting **Transmit Power Assignment** to **Manual**.

The guest management feature allows guest users to connect to the network and at the same time, allows the administrator to control guest user access to the network.


Aruba Central allows administrators to create a splash page profile for guest users. Guest users can access the Internet by providing either the credentials configured by the guest operators or their respective social networking login credentials. For example, you can create a splash page that displays a corporate logo, color scheme and the terms of service, and enable logging in from a social networking service such as Facebook, Google, Twitter, and LinkedIn.

Businesses can also pair their network with the Facebook Wi-Fi service, so that the users logging into Wi-Fi hotspots are presented with a business page, before gaining access to the network.

To enable logging using Facebook, Google, Twitter, and LinkedIn credentials, ensure that you create an application (app) on the social networking service provider site and enable authentication for that app. The social networking service provider will then issue a client ID and client secret key that are required for configuring guest profiles based on social logins.

Guest operators can also create guest user accounts. For example, a network administrator can create a guest operator account for a receptionist. The receptionist creates user accounts for guests who require temporary access to the wireless network. Guest operators can create and set an expiration time for user accounts. For example, the expiration time can be set to 1 day.

Guest Access Dashboard

The  **Summary** page in the **Manage > Guest Access** application provides a dashboard displaying the number of guests, guest SSID, client count, type of clients, and guest connection for the selected group.

[Table 72](#) describes the contents of the **Guest Access Overview** page:

Table 72: *Guest Access Overview Page*

Data Pane Item	Description
Time Range	Time range for the graphs and charts displayed on the Overview pane. You can choose to view graphs for a time period of 1 day, 1 week, and 1 month.
Guests	Number of guests connected to the SSIDs with Cloud Guest splash page profiles.
Guest SSID	Number of guest SSIDs that are configured to use the Cloud Guest splash page profiles.
Avg. Duration	The average duration of client connection on the SSIDs with Cloud Guest splash page profiles.
Max Concurrent Connections	Maximum number of client devices connected concurrently on the guest SSIDs.
Guest Connection (graph)	Time stamp for the client connections on the cloud guest for the selected time range.

Data Pane Item	Description
Guest Count by Authentication	Number of client devices based on the authentication type configured on the cloud guest SSIDs.
Guest Count by SSID	Number of guest connections per SSID.
Client Type	Type of the client devices connected on the guest SSIDs.

Creating Apps for Social Login

The following topics describe the procedures for creating applications to enable the social login feature:

- [Creating a Facebook App](#)
- [Creating a Google App](#)
- [Creating a Twitter App](#)
- [Creating a LinkedIn App](#)

Creating a Facebook App

Before creating a Facebook app, ensure that you have a valid Facebook account and you are registered as a Facebook developer with that account.

To create a Facebook app, complete the following steps:

1. Visit the Facebook app setup URL at <https://developers.facebook.com/apps>.
2. From **My Apps**, select **Add a New App**.
3. Enter the app name and your email address in the **Display Name** and **Contact Email** text boxes, respectively.
4. Click **Create App ID**.
5. Hover the mouse on **Facebook Login** and select **Setup**.
6. Click **Web** (that is, the WWW platform).
7. Enter the website URL in the **Site URL** box.

This URL is the same as the server URL mapped in the splash page configuration.

8. Click **Save**.
9. Read through the Next Steps section for further information on including Login Dialog, Access Tokens, Permissions, and App Review.
10. Go to **PRODUCTS > Facebook Login > Settings** from the left navigation menu.
11. Click the **Client OAuth Login** toggle switch to turn to **Yes**.
12. Enter the OAuth URI in the **Valid OAuth redirect URIs** box.

The URI is the server URL mapped in the splash configuration with **/oauth/reply** appended to it. To get the valid OAuth redirect URL, go to the **Guest Access > Splash Pages** path and click the eye (👁) icon available against the specific splash page name in the **Splash Pages** table.



Ensure that the URL is an HTTPS URL with a domain name and not the IP address. For example, <https://example1.cloudguest.arubanetworks.com/oauth/reply>.

13. From the left navigation menu, select **App Review**.
14. Select the **Make <App Name> Public** toggle switch to make your app available to public.
15. Click **Category**.
16. In the **Choose a Category** pop-up window, select a category.
17. Click **Confirm**.
18. Select other extra permissions you want to provide for the users of your app.
There are 41 permissions available for you to select from.
19. Click **Add xx Items**, where x represents the number of permissions you selected.
20. Enter the reason for providing specific permissions and click **Save**.
21. Click **Submit for Review**.
22. On the left navigation pane, click the **Settings** icon.
Note the app ID and app secret key. Use the app ID and secret key when configuring Facebook login in the Aruba Central UI.
23. Under **App Domains**, enter the server URL.

Creating a Google App

Before creating a an app for Google based login, ensure that you have a valid Google account.

To create a Google app, complete the following steps:

1.
 - a. Access the Google Developer site at <https://code.google.com/apis/console>.
 - b. To select an existing project, click **Select a project** and select the desired project.
 - c. If the project is not created, click **Create a project**, enter the project name and click **Create**.
 - d. Click **Enable APIs and Services**.
 - e. Navigate to **Social** category, and then click **Google API**. The **Google API** window opens.
 - f. To enable the API, click **Enable**.
 - g. Click **Create Credentials**. If the credentials are already created, click **Go to credentials**.
 - h. In the **Credentials** pane, perform the following actions:
 - Under the **Where will you be calling the API from** section, select **Web Browser**.
 - Under the **What data you will be accessing** section, select **User Data**.
 - Click **What Credentials do I need**.
2. Under **Create an OAuth 2.0 client ID**. Enter the **OAuth 2.0 Client ID Name**.
3. Under **Authorized JavaScript Origins**, enter the base URL with FQDN of the cloud guest instance that will be hosting the captive portal. For example, `https://%hostname%/.`
4. Under **Authorized Redirect URIs**, enter the cloud server OAuth reply URL that includes the FQDN of the cloud server instance with `/oauth/reply` appended at the end of the URL.



Ensure that the URL is an HTTPS URL with a domain name and not the IP address. For example, `https://example1.cloudguest.exemplenetworks.com/oauth/reply`.

5. Click **Create Client ID**.
Under **Set up the OAuth 2.0 consent screen**, provide your **Email Address** and product name, and then click **Continue**. The client ID is displayed.

6. Click **Done**. A page showing the OAuth Client IDs opens.
7. Click the **OAuth client ID** to view the client ID and client secret key.
Use this client ID and client secret key when configuring Google login in the Aruba Central UI.

Creating a Twitter App

Before creating a Twitter app, ensure that you have a valid Twitter account.

To create a Twitter app, complete the following steps:

1. Visit the Twitter app setup URL at <https://apps.twitter.com>.
2. Click **Create New App**. The **Create an application** web page is displayed.
3. Enter the application name and description.
4. For OAuth 2.0 Redirect URLs, enter the HTTPS URL of the cloud guest server to which you want to connect this social authentication source, and append `/oauth/reply` at the end of the URL.



Ensure that the URL is an HTTPS URL with a domain name and not the IP address. For example, <https://exa.example.com/oauth/reply>.

5. Select **Yes, I agree** to accept the Developer Agreement terms.
6. Click **Create a Twitter application**.
7. Click **Manage Keys and Access Tokens**.
The **Keys and Access Tokens** tab opens. The consumer key (API key) and consumer secret (API key) are displayed.
8. Note the ID and the secret key. The consumer key and consumer secret key when configuring Twitter login in Aruba Central UI.

Creating a LinkedIn App

Before creating a LinkedIn app, ensure that you have a valid LinkedIn account.

To create a LinkedIn app, complete the following steps:

1. Visit the LinkedIn app setup URL at <https://developer.linkedin.com>.
2. Click **My Apps**. You will be redirected to <https://www.linkedin.com/secure/developer/apps>.
3. Click **Create Application**. The **Create a New Application** web page is displayed.
4. Enter your company name, application name, description, website URL, application logo with the specification mentioned, application use, and contact information.
5. Click **Submit**. The **Authentication** page is displayed.
6. Note the client ID and client secret key displayed on the **Authentication** page.
7. For **OAuth 2.0 Redirect URLs**, enter the HTTPS URL of the cloud guest server to which you want to connect this social authentication source and append `/oauth/reply` at the end of the URL.
8. Click **Add** and then click **Update**. The API and secret keys are displayed.
9. Note the API and secret key details. Use the API ID and secret key when configuring LinkedIn login in the Aruba Central UI.

Configuring a Cloud Guest Splash Page Profile

Aruba Central allows administrators to create a splash page profile for guest users. Guest users can access the Internet by providing either the credentials configured by the guest operators or their respective social networking

login credentials. For example, you can create a splash page that displays a corporate logo, color scheme and the terms of service, and enable logging in from a social networking service such as Facebook, Google, Twitter, and LinkedIn.

This topic describes the following procedures:

- [Adding a Cloud Guest Splash Page Profile](#)
- [Customizing a Splash Page Design](#)
- [Configuring a Cloud Guest Splash Page Profile](#)
- [Localizing a Cloud Guest Portal](#)
- [Associating a Splash Page Profile to an SSID](#)

Adding a Cloud Guest Splash Page Profile

To create a splash page profile:

1. From the **Network Operations** app, select a group from the filter.
2. Under **Manage**, click **Guests** to display the **Splash Page**.
You can create splash page profiles only for the individual groups.
3. To create a new Splash page, click the **+** icon.
The **New Splash Page** pane is displayed.
4. On the **Configuration** tab, configure the parameters described in the following table:

Table 73: *Splash Page Configuration*

Data Pane Content	Description
Name	Enter a unique name to identify the splash profile. NOTE: If you attempt to enter an existing splash profile's name, Aruba Central displays a message stating that Splash page with this name already exists .
Type	Configure any of the following authentication methods to provide a secure network access to the guest users and visitors. <ul style="list-style-type: none"> ■ Anonymous ■ Authenticated ■ Facebook Wi-Fi
Anonymous	Configure the Anonymous login method if you want to allow guest users to log in to the Splash page without providing any credentials. For anonymous user authentication, you can also enable a pre-shared key to allow access. To enable a pre-shared key based authentication, set the Guest Key to ON and specify a password.
Authenticated	Configure authentication and authorization attributes, and login credentials that enable users to access the Internet as guests. You can configure an authentication method based on sponsored access and social networking login profiles. The authenticated options available for configuring the cloud guest splash page are described in the following rows.

Table 73: Splash Page Configuration

Data Pane Content	Description
Username/Password	<p>The Username/Password based authentication method allows pre-configured visitors to obtain access to wireless connection and the Internet. The visitors or guest users can register themselves by using the splash page when trying to access the network. The password is delivered to the users through print, SMS or email depending on the options selected during registration.</p> <p>To allow the guest users to register by themselves:</p> <ol style="list-style-type: none"> 1. Enable Self-Registration. 2. Set the Verification Required to ON if the guest user account must be verified. 3. Enable the Bypass Apple Captive Network Assistant (CNA) to bypass the CNA on the iOS devices. Enabling CNA bypass allows users to bypass the Apple Captive Network Assistant pop-up on their iOS devices. However, users still need to verify their credentials with a browser. When the CNA bypass is disabled, the iOS clients have to enter the credentials in the CNA pop-up on their devices. The Bypass Apple Captive Network Assistant (CNA) toggle button is displayed only when Verification Required is enabled. Users can either enable or disable CNA bypass based on their requirement. 4. Specify a verification criteria to allow the self-registered users to verify through email or phone. <ul style="list-style-type: none"> ■ If email-based verification is enabled and the Send Verification Link is selected, a verification link is sent to the email address of the user. The guest users can click the link to obtain access to the Internet. ■ If phone-based verification is enabled, the guest users will receive an SMS. The administrators can also customize the content of the SMS by clicking on Customize SMS. 5. Specify the duration within the range of 1-60 minutes, during which the users can access free Wi-Fi to verify the link. The users can log in to the network for the specified duration and click the verification link to obtain access to the Internet. <p>By default, the expiration date for the accounts of self-registered guest users is set to infinite during registration. The administrator or the guest operator can set the expiration date after registration.</p>
Social Login	<p>Social Login—Enable this option to allow guest users to use their existing login credentials from social networking profiles such as Facebook, Twitter, Google, or LinkedIn and sign into a third-party website. When a social login based profile is configured, a new login account to access the guest network or third-party websites is not required.</p> <ul style="list-style-type: none"> ■ Facebook—Allows guest users to use their Facebook credentials to log in to the splash page. To enable Facebook integration, you must create a Facebook app and obtain the app ID and secret key. For more information on app creation, see Creating a Facebook App. Enter the app ID and secret key for client ID and client Secret respectively to complete the integration. ■ Twitter—Allows guest users to use their Twitter credentials to log in to the splash page. To enable Twitter integration, you must create a Twitter app and obtain the app ID and secret key. For more information, see Creating a Twitter App. Enter the app ID and secret key for client ID and client secret respectively to complete the integration. ■ Google—Allows guest users to use their Google credentials to log in to the splash page. To enable Google integration, you must create a Google app and obtain the app ID and secret key. For more information, see Creating a Google App. <ol style="list-style-type: none"> 1. Enter the app ID and secret key for client ID and client secret respectively. 2. To restrict authentication attempts to only the members of a Google hosted domain, enter the domain name in the Gmail for Work Domain text box. Ensure that you have a valid domain account licensed by Google Domains or Google Apps. For more information see: <ul style="list-style-type: none"> ■ https://apps.google.com/intx/en_in/ ■ https://domains.google.com/about/ 3. Specify a text for the Sign-In button.

Table 73: Splash Page Configuration

Data Pane Content	Description
	<ul style="list-style-type: none"> ■ LinkedIn—Allows guest user to use their LinkedIn credentials to log in to the splash page. To enable LinkedIn integration, you must create a LinkedIn app and obtain the app ID and secret key. For more information, see Creating a LinkedIn App. Enter the app ID and secret key for client ID and client secret respectively to complete the integration.
Facebook Wi-Fi	<p>If you want to enable network access through the free Wi-Fi service offered by Facebook. Select the Facebook Wi-Fi option. The Facebook Wi-Fi feature allows you to pair your network with a Facebook business page, thereby allowing the guest users to log in from Wi-Fi hotspots using their Facebook credentials.</p> <p>If the Facebook Wi-Fi business page is set up, when the users try to access the Internet, the browser redirects the user to the Facebook page. The user can log in with their Facebook account credentials and can either check in to access free Internet or skip checking in and then continue.</p>
Facebook Wifi Configuration	<p>After selecting the Facebook Wi-Fi option, complete the following steps to continue with the Facebook Wi-Fi configuration.</p> <ol style="list-style-type: none"> 1. Click the Configure now link. 2. Sign in to your Facebook account. 3. If you do not have a business page, click Create Page. For more information on setting Facebook Wi-Fi service, see Setting up Facebook Wi-Fi for Your Business at https://www.facebook.com/help/126760650808045. <p>NOTE: Instant AP devices support Facebook Wi-Fi services on their own, without Aruba Central. However, for enabling social login based authentication, the guest splash pages must be configured in Aruba Central. For more information on Facebook Wi-Fi configuration on an Instant AP, see the <i>Aruba Instant User Guide</i>.</p>
Allow Internet In Failure	<p>To allow users access the Internet when the external captive portal server is not available, click the Allow Internet In Failure toggle switch. By default, this option is disabled.</p>
Override Common Name	<p>To override the default common name, click the Override Common Name toggle switch and specify a common name. The common name is the web page URL of the guest access portal. By default, the common name is set to securelogin.arubanetworks.com. The guest users can override this default name by adding their own common name.</p> <p>If your devices are managed by AirWave and you want to use your own certificate for the captive portal service, ensure that the captive portal certificate is pushed to the Instant AP from the AirWave management system. When the appropriate certificate is loaded on the AP, perform the following actions:</p> <ol style="list-style-type: none"> 1. Run the show captive-portal-domains command at the Instant AP command prompt. 2. Note the common name or the internal captive portal domain name. 3. Add this domain name in the Override Common Name field on the Splash Page configuration page. 4. Save the changes.
Guest Key	<p>To set password for anonymous users, enable the Guest Key and enter a password.</p>
Authentication Success Behavior	<p>If Anonymous or Authenticated option is selected as the guest user authentication method, specify a method for redirecting the users after a successful authentication. Select one of the following options:</p> <ul style="list-style-type: none"> ■ Redirect to Original URL— When selected, upon successful authentication, the user is redirected to the URL that was originally requested. ■ Redirect URL— Specify a redirect URL if you want to override the original request of users and redirect them to another URL.

Table 73: Splash Page Configuration

Data Pane Content	Description
Authentication Failure Message	If the Authenticated option is selected as the guest user authentication method, enter the authentication failure message text string returned by the server when the user authentication fails.
Session Timeout	Enter the maximum time in Day(s): Hour(s): Minute(s) format for which a client session remains active. The default value is 0:8:00. When the session expires, the users must re-authenticate. If MAC caching is enabled, the users are allowed or denied access based on the MAC address of the connective device.
Share This Profile	Select this check box if you want to allow the users to share the Splash Page profile. The Splash Page profiles under All Devices can be shared across all the groups.
Daily Usage Limit	<p>Use this option to set a data usage limit for authenticated guest users, anonymous profiles, and Facebook Wi-Fi logins. By default, no daily usage limit is applied.</p> <p>To set a daily usage limit, use one of the following options:</p> <ul style="list-style-type: none"> ■ By Time– Specify the time limit in hours and minutes for data usage during a day. When a user exceeds the configured time limit, the device is disconnected from the network until the next day begins; that is, until 00.00 hours in the specified time zone. ■ By Data– Specify a limit for data usage in MB. You can set this limit to either Per User, Per Session, or Per Device. When the data usage exceeds the configured limit, the user device is disconnected from the network until the next day begins; that is, until 00.00 hours in the specified time zone. <ul style="list-style-type: none"> ● Per User– This option applies the data usage limit based on authenticated user credentials. ● Per Session– This option applies the data usage limit based on user sessions. ● Per Device– This option applies the data usage limit based on the MAC address of the client device connected to the network. <p>Important Points to Note</p> <ul style="list-style-type: none"> ■ The values configured for this feature do not serve as hard limits. There might be a slight delay in enforcing daily usage limits due to the time required for processing information. ■ For anonymous and Facebook Wi-Fi logins, the daily usage limit is applied per MAC address of the client device connected to the network.
Allowlist URL	To allow a URL, click + and add the URL to the allowlist. For example, if the terms and conditions configured for the guest portal include URLs, you can add these URLs to the allowlist, so that the users can access the required web pages.

Customizing a Splash Page Design

1. From the **Network Operations** app, select a group from the filter.
2. Under **Manage**, click **Guests** to display the **Splash Page**.
You can create splash page profiles only for the individual groups.
3. To create a new splash page, click the + icon.

The **New Splash Page** pane is displayed.

To customize a splash page design, on the **Guest Access > Splash Page > New Splash Page > Customization** pane, configure the parameters described in the following table:

Table 74: Splash page customization

Data Pane Content	Description
Layout	<p>To customize the page layout based on the device type. Specify a layout by selecting one of the following options:</p> <ul style="list-style-type: none"> ■ Horizontal, better for computers ■ Vertical, better for phones <p>The horizontal layout is selected by default. To change the layout, click the drop-down list and select the required layout type.</p>
Background color	<p>To change the color of the splash page, select a color from the Background Color palette.</p>
Button color	<p>To change the color of the sign in button, select a color from the Button Color palette.</p>
Header fill color	<p>Select the fill color for the splash page header from the Header fill color palette.</p>
Page font color	<p>To change the font color of the text on the splash page, select a color from the Page font color palette.</p>
Page font Color	<p>Select the font color of the splash page from the palette.</p>
Logo	<p>To upload a logo, click Browse, and browse the image file. Ensure that the image file size does not exceed 256 KB.</p>
Background Image	<p>Click Browse to upload a background image. Ensure that the background image file size does not exceed 512 KB.</p>
Terms & Conditions	<p>Enter the terms and conditions to be displayed on the splash page. Ensure that the terms and conditions text does not exceed 20000 characters.</p> <p>The text box also allows you to use HTML tags for formatting text. For example, to highlight text with italics, you can wrap the text with the <code><i> </i></code> HTML tag.</p> <p>Specify an acceptance criteria for terms and condition by selecting any of the following options from the Display "I Accept" Checkbox:</p> <ul style="list-style-type: none"> ■ No, Accept by default ■ Yes, Display Checkbox <p>If the I ACCEPT check box must be displayed on the Splash page, select the display format for terms and conditions.</p> <p>Ensure that Display Option For Terms & Conditions has the Inline Text option auto-selected and displayed as an uneditable text.</p>
Ad Settings	<p>If you want to display advertisements on the splash page, enter the URL in the Advertisement URL.</p> <p>For Advertisement Image, click Browse and upload the image.</p>

4. Click **Next** to configure the **Localization** settings for the Guest Portal.

Localizing a Cloud Guest Portal

1. From the **Network Operations** app, select a group from the filter.
2. Under **Manage**, click **Guests** to display the **Splash Page**.
You can create splash page profiles only for the individual groups.
3. To create a new splash page, click the **+** icon.
The **New Splash Page** pane is displayed.

To localize or translate the Cloud Guest portal content, on the **Guest Access > Splash Page > New Splash Page > Localization** pane, configure the parameters described in the following table:



These are optional settings unless specified as a required parameter explicitly.

Table 75: Cloud Guest Portal Localization

Data Pane Content	Description	Allowed Length of Text
Login Section		
Login button title	Enter the custom label text to be localized for the Login button.	1-255 characters
Network login title	Enter the custom title text that you want to localize for the Network Login page.	1-255 characters
Login page title	Enter the custom text for title in the Login page.	1-255 characters
Access denied page title	Enter the custom title text for the Access Denied page.	1-255 characters
Logged in title	Enter the custom Logged in title text for the page that allows access.	1-255 characters
Username label	Enter the custom text for Username label.	1-255 characters
Username placeholder	Enter the custom text to show in in the Username placeholder.	1-255 characters
Password placeholder	Enter the custom text to show in in the Password placeholder.	1-255 characters
Email address placeholder	Enter the custom text to show in in the Email Address placeholder.	1-255 characters
Register button title	Enter the custom title text for Register button.	1-255 characters
Network login button title	Enter the custom title text for Network Login button.	1-255 characters
Terms and Conditions title	Enter the custom text to show in the Terms and Conditions title.	1-255 characters
'I accept the Terms and Conditions' text	Enter the custom text to show for the 'I accept the Terms and Conditions' text adjacent to the check box.	Up to 20000 characters
Welcome Text	Enter a custom Welcome text to the cloud guest portal user.	Up to 20000 characters

Table 75: Cloud Guest Portal Localization

Data Pane Content	Description	Allowed Length of Text
Login failed message	Enter a custom text to show for the Login Failed message when a user's login attempt gets denied or fails.	Up to 20000 characters
Logged in message	Enter a custom text to show for the Logged in message in the access allowed page.	Up to 20000 characters
Register Section		
Phone help message	Enter a custom help message to show for the Phone help field.	Up to 20000 characters
Phone number placeholder	Enter the custom placeholder text for the Phone Number input UI control.	1-255 characters
'Back' button text	Enter the custom text label to show for the Back button control.	1-255 characters
'Continue' button text	Enter the custom text label to show for the Continue button control.	1-255 characters
Email radio button	Enter a custom text label for the Email option.	–
Phone radio button	Enter a custom label text for the Phone option.	–
Register page title	Enter a custom title text for the Register page.	1-255 characters
Accept button title	Enter a custom title text for the Accept button.	1-255 characters
Register Page instructions	Enter a custom message to show in the Register page.	Up to 20000 characters
Verification Section		
Verification code label	Enter a custom text to show for the Verification code label.	1-255 characters
Verification code placeholder	Enter a custom text to show for the Verification code placeholder.	1-255 characters
Verification email check message	Enter a custom text for the Verification Email Check message. This is shown in the verification pending page.	Up to 20000 characters
Verification email notice message	Enter a custom text for the Verification Email Notice message. This is the message notifying the user when the email will be sent.	Up to 20000 characters
Verification email sent message	Enter a custom text for the Verification Email Sent message.	Up to 20000 characters
Verification phone notice message	Enter a custom text for the Verification Phone Notice message. This is the message notifying the user that an SMS has been sent.	Up to 20000 characters

Table 75: Cloud Guest Portal Localization

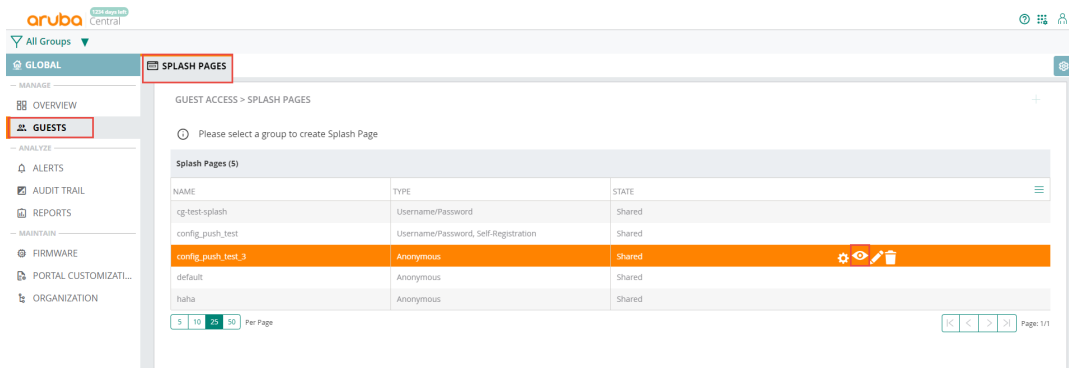
Data Pane Content	Description	Allowed Length of Text
Verified account message	Enter a custom text for the Verified Account message. This is the message that will be shown in the Verified page.	Up to 20000 characters
Verify account message	Enter a custom text for the Verify Account message. This is the message that will be shown in the Verify page.	Up to 20000 characters
Verify button title	Enter a custom label text for the Verify button.	1-255 characters
Verify title	Enter a custom text for Verify title.	1-255 characters
Network login message	Enter a custom text message to show in the Network Login page.	Up to 20000 characters

4. Click **Preview** to preview the localized cloud guest portal page or click **Finish**.

Previewing and Modifying a Splash Page Profile

To preview a splash page profile, complete the following steps:

1. From the **Network Operations** app, select a group from the filter.
2. Under **Manage**, click **Guests** to display the **Splash Page**.
A list of splash page profiles is displayed.
3. Ensure that the pop-up blocker on your browser window is disabled.
4. Hover over the splash profile you want to preview and click the preview icon. The Splash Page is displayed in a new window.




The **Splash Pages** page also allows you to perform any of the following actions:

- To view the Splash Page configuration text in an overlay window, click the settings icon next to the profile. You can copy the configuration text and apply it to AirWave managed APs using configuration templates.
- To modify a splash page profile, click the edit icon ext to the profile form list of profiles displayed in the Splash Page Profiles pane.
- To delete a profile, select the profile and click the delete icon next to the profile.

Associating a Splash Page Profile to an SSID

To associate a splash page profile with an SSID, complete the following steps:

1. From the **Network Operations** app, select a group from the filter.
2. Under **Manage**, click **Device > Access Points**.
3. Click the configuration icon  to open the configuration window.
4. Under **WLANs**, click **+Add SSID**.
5. The **Create a New Network** pane is displayed.
6. Refer to the AP configuration page for Aruba Central Online Help for more detailed information on how to create the network .

Configuring Visitor Accounts

The **Visitors** pane displays information on the session and account details of the visitors who access the splash page. It helps you monitor the guest sessions.

The MSP does not support creating or modifying guest visitor accounts. To configure visitors for WLAN networks and view visitor connection details, the administrators must drill down to the customer account and access it.

Adding a visitor

To add a new visitor:

1. From the MSP view, drill down to a customer account.
2. In the **Network Operations** app, navigate to **Manage > Guests > Visitors**.
The **Guest Access > Visitors** page is displayed.
3. Click on the **Account** tab, and then click **Add Visitor**.
The **Add Visitor** pane is displayed.
4. Configure the parameters described in the following table:

Table 76: *Adding Visitors*

Data Pane Content	Description
Name	Enter a unique name to identify the visitor.
Company	Enter the company name of the visitor.
Email	Enter the email ID of the visitor.
Phone	Enter the phone number of the visitor.
Password	<ul style="list-style-type: none">■ Click Generate. The automatically generated password is displayed in the PASSWORD text box.■ Select Send Access Code to send the access code by email or SMS.
Valid Till	Specify the duration for the visitor account to expire in Day(S): Hour(s): Minute(s) format. To allow users to access the network for unlimited period of time, select Unlimited .

Data Pane Content	Description
Enable	Select this check box to activate the user account.

- Click **Save**.
- Click **Save and Print** to print the details of the visitor.

To view the guest or visitor sessions:

- From the MSP view, drill down to a customer account.
- In the **Network Operations** app, navigate to **Manage > Guests > Visitors**.
The Guest Access > Visitors page is displayed.
- From the **Show visitors for network** drop-down list, select a network.

The following table displays the session details of the visitor:

Table 77: *Visitor Sessions Pane*

Data Pane Content	Description
Visitors	Displays the name of the visitor.
Login Type	Displays the login type of the client (Anonymous, Username/Password, Self-Registration, Facebook Wi-Fi).
Browser	Displays the type of browser that the client is connected.
MAC Address	Displays the MAC address of the connected client device.
Device Type	Displays the type of the device.
OS Name	Displays the OS on the client device.
Login Time	Displays the login time of the client.
Session Time (Secs)	Displays the duration for which the client is connected.

The following table displays the account details of a visitor:

Table 78: *Visitor Accounts Pane*

Data Pane Content	Description
Name	Displays the name of the visitor.
Email	Displays the email ID of the visitor.
Phone	Displays the contact number of the visitor.
Company	Displays the company name of the visitor.
Status	Indicates if the user account is in active or inactive state.

Data Pane Content	Description
Creation	Displays the date and time on which the visitor account is created.
Expiration	Displays the date and time on which the visitor account expired.
Actions	Allows you to edit a specific visitor account.



You can filter the visitors displayed in the **Account List** by visitor status. Select **Active**, **Inactive**, or **Show All** from the drop-down list.

Deleting Visitors

To delete one or more visitors:

1. Select the visitor or visitors you want to delete using the **Multiselect** box option.
2. Click **Delete**. The selected visitors get deleted.

Downloading Visitor Account Details

To download the visitor account details:

1. Click **Download** to download the visitor account details available in the **Accounts** tab.

AirGroup Changes	303
AirGroup Licensing	304
AirGroup Features	304
AirGroup Services	304
AirGroup Limitations	305
Enabling AirGroup	305
Configuring AirGroup Services	305
Monitoring AirGroup	306
Troubleshooting AirGroup	308

AirGroup is a unique enterprise-class capability that leverages zero-configuration networking and allows devices to communicate over complex access network topologies. AirGroup supports Bonjour-supported and DLNA-supported services on Apple and Android devices respectively. Apple devices constantly send mDNS packets to locate Bonjour services. Similarly, Android devices constantly send SSDP packets to locate DLNA services.

In simple networks, like a home network, discovering devices and services is easier because there is just one subnet. If a network includes a large number of client devices sending mDNS or SSDP queries, more bandwidth is consumed and therefore, the network performance is affected. In large universities and enterprise networks, it is common for devices to connect to the network across VLANs. As a result, client devices on a specific VLAN cannot discover a service that resides on another VLAN. The IP addresses in such networks are link-local scope multicast addresses and each query or advertisement can only be forwarded on its respective VLAN, but not across different VLANs. Broadcast and multicast traffic are usually filtered out from a WLAN network to preserve the airtime and battery life. This inhibits the performance of services that rely on multicast traffic.

Aruba addresses this challenge with AirGroup. AirGroup allows administrators to set policy-based discovery and enables client devices to be location-aware. Zero-configuration networking enables service discovery, address assignment, and name resolution for desktop computers, mobile devices, and network services.

AirGroup also supports DLNA, a network standard that is derived from UPnP for Android devices. AirGroup adds mDNS or SSDP proxy capabilities to campus WLANs, so that Bonjour or DLNA messages can be served across subnets or VLANs. DLNA uses SSDP for discovering services available on the network. DLNA provides the ability to share digital media between multimedia devices running Android or Windows operating systems. SSDP multicasts and advertises the services and queries managed by AirGroup without affecting the advertisement or discovery process of SSDP devices.



Availability of AirGroup is limited. Contact Aruba Support for access to AirGroup.

AirGroup Changes

The following changes are introduced in AirGroup from the previous release:

- AirGroup can be enabled at per group level.
- AirGroup can be configured at group level.

- AP Foundation license is applicable to AirGroup.
- Monitoring is available at group level.
- Visibility is available at site level and label level.
- Disallow role configuration is supported.

AirGroup Licensing

The following table lists the availability of AirGroup services based on the type of license.

Table 79: *AirGroup Licensing*

Function	Foundation License	Advanced License
Availability of AirPlay service	Yes	Yes
Availability of AirPrint service	Yes	Yes
Availability of DIAL service	Yes	Yes
Availability of GoogleCast service	Yes	Yes
Availability of DLNA Media service	No	Yes
Availability of DLNA Print service	No	Yes
Availability of Amazon FireTV service	No	Yes
Monitoring visibility	Yes	Yes
Troubleshooting assistance	Yes	Yes
Services available in deployments with bridge mode and in tunnel mode	Yes	Yes

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 based on user roles or VLANs.

AirGroup Services

AirGroup supports discovery and management of the following services.

- 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.
- Amazon Fire TV –The Amazon Fire TV allows you to stream music, video, and games to television.

- Google Cast – The Google Cast service allows you to play audio or video content on a high-definition television by streaming content through Wi-Fi from the Internet or local network.



Google Cast does not respond to application ID-based wildcard queries from Aruba Central.

- 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.

AirGroup Limitations

AirGroup has the following limitations:

- Template groups are not supported.
- Wired AirGroup servers or users are not supported.
- Custom-based AirGroup services are not supported.

Enabling AirGroup

AirGroup runs on provisioned devices and it uses the OpenFlow infrastructure to receive the signaling messages from devices and installs or deletes flows on the devices.

Pre-requisites

Ensure that the following pre-requisites are met before enabling AirGroup:

- Customer ID should be allow-listed.
- A 10.x group should be used. For additional information, see [Creating a Group](#).
- In WLAN configuration, the broadcast-multicast filter should be disabled or set to unicast-ARP for AirGroup. For additional information, see [Configuring General > Advanced Settings for a WLAN SSID Profile](#).
- After Aruba Central is upgraded to version 2.5.3, re-enable AirGroup.
- All AirGroup services that worked in Aruba Central 2.5.2 will not work in Aruba Central 2.5.3 with a foundation license.

To enable AirGroup, complete the following procedure:

1. In the **Network Operations** app, set the filter to a group.
2. Under **Manage**, click **Applications > AirGroup**.
3. Click the **Config** icon.
4. Under **Settings**, move the **AirGroup Service** slider to the right.

Configuring AirGroup Services

To enable AirGroup services, complete the following procedure:

1. In the **Network Operations** app, set the filter to a group.
2. Under **Manage**, click **Applications > AirGroup**.
3. Click the **Config** icon.
4. On the required AirGroup service, click the **Edit** icon under **Action**.

5. Hover over the required AirGroup service and move the slider to the right.
6. To disallow the AirGroup service on the required roles:
 - a. Select the **Disallow service on selected roles** check box.
 - b. Select the check-box next the required roles.



Disallowing an AirGroup service on roles is optional. If configured, the AirGroup service is not available on the specified roles.

7. To disallow the AirGroup service on the required VLANs, select the **Disallow service on selected vlans** check box and enter comma separated VLAN IDs.



Disallowing an AirGroup service on VLANs is optional. If configured, the AirGroup service is not available on the specified VLANs.

8. Click **Save**.

Monitoring AirGroup

AirGroup allows monitoring of services, servers, clients, and suppressed services. To monitor AirGroup:

1. In the **Network Operations** app, set the filter to a group, site, or label that contains at least one AP.
2. Under **Manage**, click **Applications > AirGroup**.
3. To monitor the AirGroup services, click **Services**. The following table lists the columns in the services table.

Table 80: *AirGroup Services*

Column	Description
Name	Name of the AirGroup service
State	Status of the AirGroup service
Type	Type of the AirGroup service
Disallowed Roles	Roles disallowed for the AirGroup service
Disallowed VLANs	VLANs disallowed for the AirGroup service
Auto Associate	Status of auto association
Service ID	Service IDs associated with the AirGroup service

4. To monitor the AirGroup servers, click **Servers**. The following table lists the columns in the servers table.

Table 81: *AirGroup Servers*

Column	Description
Hostname	Name of the AirGroup server
MAC Address	MAC address of the AirGroup server
IP Address	IP address of the AirGroup server
Role	Role of the AirGroup server
Service	Services running on the AirGroup server
VLAN	VLAN of the AirGroup server
Connected To	MAC address of the device to which the AirGroup server is connected
Status	Connection status of the AirGroup server
Link	Link of the AirGroup server
Usage	Data usage of the AirGroup server

5. To monitor the AirGroup clients, click **Clients**. The following table lists the columns in the clients table.

Table 82: *AirGroup Clients*

Column	Description
Name	Name of the AirGroup client
MAC Address	MAC address of the AirGroup client
IP Address	IP address of the AirGroup client
Role	Role assigned to the AirGroup client
VLAN	VLAN assigned to the AirGroup client

Column	Description
Connected To	MAC address of the device to which the AirGroup client is connected
Status	Connection status of the AirGroup client
Link	Link of the AirGroup client
OS	Operating System running on the AirGroup client
Band	Band used by the AirGroup client
Channel	Channel used by the AirGroup client
Capabilities	Capabilities of the AirGroup client
Client health	Health status of the AirGroup client

- To monitor the suppressed AirGroup services, click **Suppressed Services**. A list of suppressed services is displayed.

Troubleshooting AirGroup

This topic describes the procedures to troubleshoot AirGroup.

Check Openflow

To check the presence of the openflow flow ID, 63000, for AirGroup, complete the following procedure:

- In the **Network Operations** app, set the filter to a group.
- Under **Analyze**, click **Tools**.
- Click the **Commands**.
- Use the **Commands** filter to select the **show openflow flow-table** command.
- Click **Add**.
- Click **Run**.
- Analyze the output of the command. In the following sample, the words or lines of relevance are highlighted:

```
(host) # show openflow flow-table
```

```
Flow: <Add at Wed Nov 11 09:00:03 2020> <bytes:0, pkts:0, idletmo:0, hardtmo:0  
last:1605103203> Match:<17, x.x.x.x, x.x.x.x, 63000, 63000> Cookie:<1099511629259>,  
Action:<out:controller >
```

Check AirGroup Status

To check the status of AirGroup, complete the following procedure:

1. In the **Network Operations** app, set the filter to a group.
2. Under **Analyze**, click **Tools**.
3. Click the **Commands**.
4. Use the **Commands** filter to select the **show airgroup status** command.
5. Click **Add**.
6. Click **Run**.
7. Analyze the output of the command. In the following sample, the words or lines of relevance are highlighted:

```
(host) # show airgroup status
```

```
AirGroup Information
```

```
-----
```

```
Feature Status
```

```
-----
```

```
AirGroup status Enabled
```

```
IPV6 Disabled
```

Check AirGroup Debug Statistics

The AirGroup debug statistics counters maintain to record the number of mDNS or SSDP packets (response and query packets are maintained separately) that are forwarded or dropped. The counters for the packet filtering statistics are:

- `mdns_query_pkt_dropped_count`
- `ssdp_query_pkt_dropped_count`
- `mdns_query_pkt_forwarded_count`
- `ssdp_query_pkt_forwarded_count`
- `mdns_response_pkt_forwarded_count`

- ssdp_response_pkt_forwarded_count
- mdns_papi_send_to_ofa_failure

To check the AirGroup debug statistics, complete the following procedure:

1. In the **Network Operations** app, set the filter to a group.
2. Under **Analyze**, click **Tools**.
3. Click the **Commands**.
4. Use the **Commands** filter to select the **show airgroup debug statistics** command.
5. Click **Add**.
6. Click **Run**.
7. Analyze the output of the command. In the following sample, the words or lines of relevance are highlighted:

```
(host)# show airgroup debug statistics
```

```
My ip address :x.x.x.x
```

```
AirGroup Debug Statistics
```

```
-----
```

```
Key Value
```

```
--- ----
```

```
network cache init counter 1(0)
```

```
mdns apdb init counter 1(0)
```

```
airgroup restore count 1(0)
```

```
unsupported mdns query pkt dropped count 169(159)
```

```
unsupported ssdp query pkt dropped count 178(124)
```

```
supported mdns query pkt forwarded count 379(239)
```



```
supported ssdp query pkt forwarded count 270 (178)
```

```
mdns response pkt forwarded count 635 (371)
```

```
ssdp response/notify pkt forwarded count 94 (40)
```

```
dropped as init not done rx 13 (0)
```

```
mdns recieved bonjour pkt from device 1183 (769)
```

```
mdns recieved dlna pkt from device 542 (342)
```



The value outside the brackets indicates the collective counter from the time AirGroup was enabled. The value inside the bracket indicates the new count of packets from the time the command was last executed.

Check mDNS Trace Logs

Use the mDNS trace logs to analyze the packet type or content and how it is processed by the mDNS process in the AP. The mDNS trace logs can also be used to see if the packet is forwarded to Aruba Central based on the allowed service filtering.

To enable the mDNS trace logs, complete the following procedure:

1. In the **Network Operations** app, set the filter to a group.
2. Under **Analyze**, click **Tools**.
3. Click the **Commands**.
4. Use the **Commands** filter to select the **trace component mdns sub-component all** command.
5. Click **Add**.
6. Click **Run**.

To see the mDNS trace logs, complete the following procedure:

1. In the **Network Operations** app, set the filter to a group.
2. Under **Analyze**, click **Tools**.
3. Click the **Commands**.
4. Use the **Commands** filter to select the **show trace logs mdns 1000** command.
5. Click **Add**.
6. Click **Run**.
7. Analyze the output of the command. In the following sample, the words or lines of relevance are highlighted:

```
Query packet :
```

```
Mar 11 06:15:31|---:--:--:--:--:--|---.---.---.---|GENERAL|rx_mdns_pkt_from_
asap:2982|vlan : 1, client_type : 0
```

```
Mar 11 06:15:31|f4:30:b9:11:6a:18|---.---.---.---|HOST|print_mdns_pkt_
ether:1555|ethhdr: src_mac=f0:5c:19:cb:19:a2, dst_mac=f0:5c:19:cb:19:a2, proto=4400
```

```
Mar 11 06:15:31|f4:30:b9:11:6a:18|---.---.---.---|HOST|print_mdns_pkt_ether:1633|udp
hdr: not-present
```

```
Mar 11 06:15:31|f4:30:b9:11:6a:18|---.---.---.---|HOST|mdns_parse_packet_from_
sos:1150|pkt from SOS: vlan 1, mac f4:30:b9:11:6a:18 ip 10.17.141.154
```

```
Mar 11 06:15:31|f4:30:b9:11:6a:18|---.---.---.---|HOST|mdns_parse_
packet:2928|***** mdns query packet received *****- info;
mac=f4:30:b9:11:6a:18, ip=10.17.141.154, origin=1
```

```
Mar 11 06:15:31|---:--:--:--:--:--|---.---.---.---|GENERAL|mdns_query_queue_
enqueue:175|Number of elements after insert 1, thread_num =0
```

```
Mar 11 06:15:31|---:--:~:~:~:~:~:~|---.---.---.---|GENERAL|mdns_queue_
dequeue:194|Number of Elements in the Queue 1 thread_num 0
```

```
Mar 11 06:15:31|19:cb:19:a2:f4:30|---.---.---.---|HOST|print_mdns_pkt_
ether:1555|ethhdr: src_mac=01:00:00:00:f0:5c, dst_mac=01:00:00:00:f0:5c, proto=800
```

```
Mar 11 06:15:31|19:cb:19:a2:f4:30|---.---.---.---|HOST|print_mdns_pkt_ether:1633|udp
hdr: not-present
```

```
Mar 11 06:15:31|f4:30:b9:11:6a:18|---.---.---.---|HOST|mdns_parse_query_packet_from_
queue:1298|Parsing Queued Packet
```

```
Mar 11 06:15:31|f4:30:b9:11:6a:18|---.---.---.---|HOST|mdns_parse_query_packet_from_
queue:1306|pkt from SOS: vlan 1, mac f4:30:b9:11:6a:18 ip 10.17.141.154
```

```
Mar 11 06:15:31|f4:30:b9:11:6a:18|---.---.---.---|HOST|mdns_parse_query_
packet:2106|mid_googlecast._tcp.local : normal query
```

```
Mar 11 06:15:31|f4:30:b9:11:6a:18|---.---.---.---|HOST|mdns_parse_query_
packet:2110|mdns_sid_status : 4
```

Mar 11 06:15:31|f4:30:b9:11:6a:18|---.---.---.---|HOST|mdns_parse_query_packet:2135|mid _googlecast._tcp.local : forwarding the pkt to ofald

Mar 11 06:15:31|e4:50:a9:be:18:f3|---.---.---.---|HOST|mdns_parse_query_packet_from_queue:1525|Query Handler, free Data and go back; ret_status:0

Mar 11 06:15:31|---:---:---:---:---:---|---.---.---.---|GENERAL|mdns_send_pkt_to_ofa:224|vlan : 1, client_flag : 0

Mar 11 06:15:31|---:---:---:---:---:---|---.---.---.---|GENERAL|mdns_send_pkt_to_ofa:251|Send 90 byte pb to ofa

Mar 11 06:15:31|---:---:---:---:---:---|---.---.---.---|GENERAL|mdns_send_papi_to_ofa:189|PAPI Send to OFA successful, msgtype 5012, msglen 110

Response packet :

Mar 13 05:33:45|---:---:---:---:---:---|---.---.---.---|GENERAL|rx_mdns_pkt_from_asap:2982|vlan : 1, client_type : 0

Mar 13 05:33:45|f4:30:b9:11:6a:18|---.---.---.---|HOST|print_mdns_pkt_ether:1555|ethhdr: src_mac=01:00:5e:00:00:fb, dst_mac=01:00:5e:00:00:fb, proto=9a02

Mar 13 05:33:45|f4:30:b9:11:6a:18|---.---.---.---|HOST|print_mdns_pkt_ether:1633|udp_hdr: not-present

Mar 13 05:33:45|f4:30:b9:11:6a:18|---.---.---.---|HOST|mdns_parse_packet_from_sos:1150|pkt from SOS: vlan 1, mac f4:30:b9:11:6a:18 ip 10.17.141.169

Mar 13 05:33:45|f4:30:b9:11:6a:18|---.---.---.---|HOST|mdns_parse_packet:2949|***** mdns response packet received *****
mac=f4:30:b9:11:6a:18, ip=10.17.141.169, origin=1

Mar 13 05:33:45|---:---:---:---:---:---|---.---.---.---|GENERAL|mdns_send_pkt_to_ofa:224|vlan : 1, client_flag : 0

Mar 13 05:33:45|---:---:---:---:---:---|---.---.---.---|GENERAL|mdns_send_pkt_to_ofa:251|Send 689 byte pb to ofa

```
Mar 13 05:33:45|---:--:--:--:--:--|---.---.---.---|GENERAL|mdns_send_papi_to_
ofa:189|PAPI Send to OFA successful, msgtype 5012, msglen 709
```

Check if Filtered Packets are Forwarded

To enable the openflow logs, complete the following procedure:

1. In the **Network Operations** app, set the filter to a group.
2. Under **Analyze**, click **Tools**.
3. Click the **Commands**.
4. Use the **Commands** filter to select the **openflow-logging** command.
5. Click **Add**.
6. Click **Run**.

To check if the **ofald** process forwards the filtered packets from the mDNS process to Aruba Central successfully, complete the following procedure:

1. In the **Network Operations** app, set the filter to a group.
2. Under **Analyze**, click **Tools**.
3. Click the **Commands**.
4. Use the **Commands** filter to select the **show log openflow** command.
5. Click **Add**.
6. Click **Run**.
7. Analyze the output of the command. In the following sample, the words or lines of relevance are highlighted:

```
[7639] Wed Nov 11 10:54:34 2020.410091 INFO ofald_papi_handler:804 Recvd msg unknown
from 127.0.0.1:8476, len:236
```

```
[7639] Wed Nov 11 10:54:34 2020.410260 DEBUG ofald_process_mdns_msg:660 ofald_
process_mdns_msg MDNS message 0x20000c2 236
```

```
[7639] Wed Nov 11 10:54:34 2020.410390 DEBUG ofald_process_mdns_msg:674 BSSID :
20:4c:03:0a:14:b4, hex_data_len : 226
```

```
[7639] Wed Nov 11 10:54:34 2020.410528 DEBUG ofald_process_mdns_msg:691 in_port :
8456
```

```
[7639] Wed Nov 11 10:54:34 2020.410679 DEBUG ofald_process_mdns_msg:751 OFPT_PACKET_
IN Cookie 1099511629256
```

```
[7639] Wed Nov 11 10:54:34 2020.410791 DEBUG ofmsg_tx_encode:1065
```

```
[7639] Wed Nov 11 10:54:34 2020.410966 INFO ofmsg_tx_encode:1151 Message encoded:
len:310, {type=OFPT_PACKET_IN, length=310, xid = 393628647}{buffer=4294967295,
tlen=268, reas=1, table=0, dlen=268 }
```

Capture mDNS packets

To capture the mDNS query and response packets to and from the AP, complete the following procedure:

```
mdns :
```

```
debug pkt type udp
```

```
debug pkt match port 5353
```

```
debug pkt mirror <client_laptop_ip>
```



NOTE

The client laptop should have Wireshark capturing on the interface of this IP.

```
debug pkt dump
```

Capture SSDP packets

To capture the SSDP query and response packets to and from the AP, complete the following procedure:

```
ssdp :
```

```
debug pkt type udp
```

```
debug pkt match port 1900
```

```
debug pkt mirror <client_laptop_ip>
```



NOTE

The client laptop should have Wireshark capturing on the interface of this IP.

```
debug pkt dump
```

Configuring IoT Operations	316
Creating an IoT Connector	316
Configuring AP	318
Configuring Transport Profile	318
Monitoring IoT	320

Aruba Central supports transporting IoT data over enterprise WLAN. IoT data from partners providing access control systems, Electronic Shelf Labeling (ESL), industrial and manufacturing, hospital and health management, and building management systems is supported. APs receive the data from the devices and send the dashboard metadata to Aruba Central and the IoT data to external servers through IoT connectors. The IoT connector aggregates the device data, performs edge compute, and runs business logic on the raw device data before sending the dashboard metadata to Aruba Central. Transport profiles can be defined to send the IoT data to external servers.

Aruba Central provides IoT connector control, management, and dashboard visibility. The dashboard provides a view of the IoT connectors, devices, and installed applications. An application store with applications from supported partners is integrated with Aruba Central. Aruba Central does not store or display the device data or derive insights from the IoT data.

Configuring IoT Operations

The **Applications > IoT Operations** page displays the data of IoT connectors, devices, and applications. It also allows to configure the connectors, applications, and transport profiles. Configuring IoT Operations involves:

- [Creating an IoT Connector](#)
- [Configuring AP](#)
- [Configuring Transport Profile](#)

Creating an IoT Connector

IoT connectors are available as OVA files in Aruba Central. Before creating an IoT connector, download the OVA file. For additional information, see [Downloading an OVA File](#). After downloading the OVA file, deploy it on a VM server. For additional information, see [Deploying an OVA File](#).

To create a connector, complete the following procedure:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage**, click **Applications > IoT Operations**.
3. Click **Show Connectors**.



If no IoT connector is deployed, the connector graph displays **Add Connector**. Click **Add Connector** to create an IoT connector.

4. In the **Connectors** table, click **+**.
5. In the **Data Collectors** page, click the **Data Collectors** graph.
6. In the **Managed Collectors** page, click **Create Collector**.
7. In **Give collector a name**, enter a connector name.
8. In **Select an application to install on collector**, select **IoT Connector**.
9. Click **Next**.
10. Select the collector and click **Create**.

Downloading an OVA File

To deploy an OVA file, complete the following procedure:

1. In the **Accounts Home** page, click **Global Settings > Data Collectors**.
2. In the **Managed Collectors** page, click **Download Virtual Appliance**.
3. In the **Download Virtual Appliance** page, select one of the following OVA files:
 - Small OVA file - Requires a 8-core CPU, 16 GB memory, and 256 GB disk space
 - Medium - Requires a 24-core CPU, 64 GB memory, and 480 GB disk space

Deploying an OVA File

Deploy an OVA file on a VM server. The following procedure describes how to deploy an OVA file on a VMware server:

1. Log in to the VMware server.
2. Click **File > Deploy OVF Template**.
3. Click **Browse** and select the OVA file.
4. Click **Next**.
5. After the OVA file is deployed, click **Console**.
6. Log in to the console with the following credentials:
 - Username as aruba
 - Password as aruba.
7. Change the password.
8. Configure the hostname.
9. Configure the network with static IP address, mask, gateway, and DNS server.
10. Test the network connectivity.
11. Configure the timezone.
12. Register the IoT connector to Aruba Central by using a registration token. For additional information, see [Obtaining Registration Token](#).

Obtaining Registration Token

A registration token is required to register an IoT connector to Aruba Central. The registration token is available on Aruba Central. To obtain a registration token, complete the following procedure:

1. In the **Accounts Home** page, click **Global Settings > Data Collectors**.
2. Under **Configure Appliance**, click **Registration Token**.
3. In the **Registration Token** page, click **Copy Token**.
4. Click **Close**.

Configuring AP

Configure the IoT radio profile and IoT transport profile on an AP using templates. For additional information, see [Configuring APs Using Templates](#).

Configuring Transport Profile

To configure transport profile, complete the following procedure:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage**, click **Applications > IoT Operations**.
3. In the **Connectors** graph, click **Show Connectors**.
4. In the **Connectors** table, click the name of a connector.
5. In the detailed view of the connector, under the **Transport Profiles** graph, click **Show Transport Profiles**. In the **Transport Profile on Connector** table, click **+** and configure the following transport profile parameters.



If no transport profile is configured, the **Transport Profile on Connector** table displays **Add**. Click **Add** to configure a transport profile.

Table 83: Transport Profile

Parameter	Description
Profile	Name of the transport profile.
Description	Description of the transport profile.
Stream Type	Type of the data stream. Select one of: <ul style="list-style-type: none"> ■ Periodic Telemetry - Send data stream periodically ■ Data Frames - Send each data frame when data is available
Aggregation	Type of aggregation. Aggregation consists of: <ul style="list-style-type: none"> ■ Reporting Interval (seconds) - Period to aggregate the data stream. This parameter is available when Stream Type is set to Periodic telemetry. ■ RSSI Aggregation Type - Type of RSSI aggregation. This parameter is available when Stream Type is set to Periodic telemetry. Select one of: <ul style="list-style-type: none"> • Average - Use average value when aggregating the data stream. • Latest - Use the latest value when aggregating the data stream. • Max - Use the maximum value when aggregating the data stream.
Subscriptions	Type of subscription. A subscription consists of a type and value. The supported type is device class and the available values for device class are: <ul style="list-style-type: none"> ■ ABB Sensor ■ Aruba Beacon ■ Aruba Tag ■ Eddystone ■ Google ■ HID ■ iBeacon ■ Minew ■ Mysphera ■ ZF Tag ■ Wiliot <p>Multiple subscriptions are allowed with a OR operator between subscriptions. Use + to add subscriptions.</p>
Filters	Type of filter. A filter consists of type and value. The supported type is ibeacon UUID and the value is a UUID. Multiple filters are allowed with a OR operator between filters. Use + to add filters.
Destination	Details of the destination server. A destination consists of: <ul style="list-style-type: none"> ■ Protocol Type - Type of protocol used when sending data. Select one of: <ul style="list-style-type: none"> • WS • WSS ■ URL - URL of the destination server ■ Format Type - Format of the data. Select one of: <ul style="list-style-type: none"> • JSON • PROTOBUF
Authentication	Details of the authentication method to use. Select one of:

6.

Table 83: Transport Profile

Parameter	Description
	<ul style="list-style-type: none"> ■ Use Credentials - Configure authentication URL, client ID, username, and password. ■ Use Token - Configure the authentication token.

7. Click **Create**.

Monitoring IoT

The **Applications > IoT Operations** page provides a variety of charts (**Summary** view) and lists (**List** view) that allow you to assess the status of the IoT connectors, IoT devices, and IoT applications.



In any chart, hover over any spot or segment to view additional information.

To view the status of the IoT connectors, complete the following procedure:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage**, click **Applications > IoT Operations**.
3. The **Connectors** graph displays a graph of the online and offline IoT connectors. Click **Show Connectors** to view the list of IoT connectors. The **Connectors** table lists the following additional information:

Table 84: IoT Connectors

Parameter	Description
Name	Name of the connector. Click any name to view the detailed information of the connector. The detailed information includes: <ul style="list-style-type: none"> ■ Connector banner - Status of the banner with number of IoT devices, access points, and IoT applications in the connector. ■ Installed applications - Graph of up-to-date or upgrade-available status of the applications. ■ Transport profiles - Transport profiles associated with the connector. Click Add to configure a transport profile. For additional information, see Configuring Transport Profile. ■ Statistics - Timeline with the number of IoT devices connected to the IoT connector.
Status	Status of the connector.
Reported Access Points	Number of access points collecting the data.
IoT Applications	Number of applications running on the connector.
IoT Devices	Number of devices connected to the connector.
Classified Devices	Number of devices classified by the connector.

To view the status of the IoT device, complete the following procedure:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage**, click **Applications > IoT Operations**.
3. The **IoT Devices** graph displays a graph of the IoT devices filtered by **Communication Type** and **Device Class**. Click **Show Devices** to view the list of IoT devices. The **Devices on all Connectors** table lists the following additional information:

Table 85: IoT Devices

Parameter	Description
Address	MAC address of the device.
Address Type	Type of address of the device.
Classes	Device class of the device.
Last Seen	Date and time when the device was last seen.
Last Reported By	MAC address of the last AP that saw the device.
Connector	Name of the connector.



To view the status of the IoT devices on a specific connector, navigate to the detailed view of the connector. In the detailed view of the connector, click the number displayed below IoT devices.

To view the status of the installed IoT applications or IoT applications that are available for installation on a connector, complete the following procedure:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage**, click **Applications > IoT Operations**.
3. The **IoT Applications** graph displays a graph of the installed IoT applications. Click on Click **Show App Store** to view the list of IoT applications. The **IoT Applications** page lists the following additional information:

Table 86: IoT Applications

Parameter	Description
Recommended for you	List of recommended applications.
Available apps	List of available applications.

4. Click any application to view its detailed information. In the detailed view of the application, click **Install** to install the application.

Licensing	322
Heuristics Classification	322
Protocols	323
Limitations	323
Subscribing to Unified Communications	323
Enabling Unified Communications	324
Monitoring Unified Communications	325
WebRTC Prioritization	328
Troubleshooting Unified Communications	328

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. 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 calls, video calls, and application sharing when using communication and collaboration tools. The Unified Communications service actively monitors voice, video, and application sharing sessions, provides traffic visibility, and allows you to prioritize the required sessions. The Unified Communications service leverages the functions of the service engine and provides rich visual metrics for analytical purposes.

The Unified Communications service supports the following functions based on the type of device:

- **Session visibility**—The Unified Communications application provides call session visibility correlated across the 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.
- **Session prioritization**—Based on the type of device provisioned in your network, the Aruba Central server receives call control information from devices like AP, controllers, and switches. The Unified Communications application uses this data to detect and classify the traffic type and dynamically prioritize the voice and video traffic over data traffic. The heuristics method is used for session prioritization. A built-in heuristics engine detects the Unified Communications traffic and prioritizes the require traffic. 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.

Licensing

Unified Communications is available with AP Advanced license.

Heuristics Classification

In the heuristics method, Aruba devices like APs perform deep packet inspection on the traffic to determine voice and video traffic. For the heuristics classification method, no changes or additional components are required on the Unified Communications servers.

The heuristics classification method includes the following steps:

- When the voice or video call is established, classify-media in the ACL is triggered and clients are marked as media-capable clients.
- Any subsequent UDP data flow with source/destination port numbers from or to media-capable users go through the DPI engine.
- 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.

Protocols

Unified Communications supports the following protocols:

- Facetime
- SIP
- Skype for Business
- Wi-Fi Calling

Limitations

The following is a list of Unified Communications limitations:

- WLAN and end-to-end quality metrics are not available for Wi-Fi calling and any video calls.
- Wi-Fi calling is not identified and prioritized if NAT is enabled on the user VLAN. Wi-Fi calling is not identified and prioritized if the corresponding sessions undergo NATting by gateway
- Skype with SDN is not supported.
- Unified Communication supports wired clients that are terminated on an AP.
- Unified Communication does not support wired clients that are connected to PUTN switch and gateway.
- Call data is visible 2 minutes after a call has ended.
- Live or ongoing call status is not visible in the Unified Communications dashboard.



If an infrastructure upgrade or restart takes more than 60 ms, the UCC application restarts.

Subscribing to 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.

If you have a valid subscription, follows these steps to enable the **Unified Communications** service on your devices:

1. In the **Accounts Home** page, click **Global Settings** > **Subscription Assignment**.
2. From the list of subscriptions, select **All devices**.
3. Select the device from the **Devices** table.
4. Drag and drop the device from the **Devices** table to **UCC** row in the **Subscriptions** table.
5. Click **Yes** to confirm the subscription assignment

Enabling Unified Communications

To enable Unified Communications:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage**, click **Applications > UCC**.
3. Click the **Config** icon.
4. Move the **Activate UCC** slider to the right.



UCC will be disabled if UCC is not subscribed, UCC is not subscribed but configuration is enabled, or UCC is subscribed but configuration is disabled.

Enabling Call Prioritization

To enable call prioritization:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage**, click **Applications > UCC**.
3. Click the **Config** icon.
4. Move the **Enable Call Prioritization** slider to the right.

Editing a Protocol

To edit a protocol:

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 required protocol and click the **Edit** icon under **Actions**. Unified Communications supports Facetime, SIP, Skype for Business, and Wi-Fi Calling protocols.
5. Edit the following parameters:

Table 87: *Protocol Parameters*

Parameter	Description
Facetime	
Video	Configure video priority tag.
SIP	
Voice	Configure voice priority tag.
Video	Configure video priority tag.
Skype for Business	
Voice	Configure voice priority tag.

Table 87: Protocol Parameters

Parameter	Description
Video	Configure video priority tag.
Desktop Sharing	Configure desktop sharing priority tag.
Server	Configure FQDN of Skype SDN server. NOTE: Skype with SDN is not supported.
Wi-Fi Calling	
Voice	Configure voice priority tag.

Monitoring Unified Communications

The **Applications > UCC** page provides a variety of charts (**Summary** view) and lists (**List** view) that allow you to assess the quality of calls in the network. The **Applications > UCC** page is available when the filter is set to **Global**, site, or label.

In the **Summary** view or **List** view, data is shown for all devices irrespective of the whether **All Devices** or a specific device or group is selected in the filter.

Call data is visible in the Unified Communications dashboard 2 minutes after a call has ended.

Live or ongoing call status is not visible in the Unified Communications dashboard.



Dashboard Banner

The Unified Communications dashboard banner in the **Applications > UCC** page 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.
- **Fair**—Displays the total number of fair calls. that have ended.
- **Poor**—Displays the total number of poor calls that have ended.
- **Unknown**—Displays the total number of calls whose status is unknown.

Dashboard Summary

The **Summary** view in the **Applications > UCC** page provides the following charts:

- **Calls**—Displays the chart of all, good, fair, poor, or unknown calls. Chart can be viewed by Health, SSID, Protocol, Operating System, Session Type, or Quality, In any chart, hover over any spot or segment to view additional information.
Click any spot or segment to view detailed information of the call in a **Call Detail** pop-up.
- **Access Points**—Displays the chart of APs. Chart can be viewed by Poor Quality % or Most Calls. Hover over any row in the list to view additional information.
Use **Show More** in the Access Points chart to view the following additional information:

Table 88: Access Points with Calls

Parameter	Description
Access Point Name	Displays the name of the AP.
Calls Total	Displays the total number of calls.
Calls Good	Displays the total number of good calls.
Calls Fair	Displays the total number of fair calls.
Calls Poor	Displays the total number of poor calls.
Calls Poor Percentage	Displays the percentage of poor calls.
Calls Unknown	Displays the total number of unknown calls.

- Clients—Displays the chart of clients. Chart can be viewed by Poor Quality % or Most Calls. Hover over any row in the list to view additional information.


Use **Show More** in the Clients chart to view the following additional information:

Table 89: Clients with Calls

Parameter	Description
Client Name	Displays the name of the client.
Calls Total	Displays the total number of calls from the client.
Calls Good	Displays the total number of good calls from the client.
Calls Fair	Displays the total number of fair calls from the client.
Calls Poor	Displays the total number of poor calls from the client.
Calls Poor Percentage	Displays the percentage of poor calls from the client.
Calls Unknown	Displays the total number of unknown calls from the client.

Dashboard List

The **List** view in the **Applications > UCC** page provides a variety of lists that allow you to assess the quality of calls in the network.

- Click the  icon to select additional columns, all columns, or export the information as a CSV file.
- The following is the list of available columns:
 - CDR
 - Start Time
 - Client Name
 - Call Quality

- Client Health
- SSID
- Protocol Type
- Session Type
- OS
- User Role
- Call Duration
- Call Type
- Client IP Address
- Peer IP Address
- AP Host name
- AP type
- UCC MOS
- State
- BSSID
- DSCP
- Group Name
- Label Name
- Site Name
- Quality Score
- Source Port
- Destination Port
- Delay
- Jitter
- Packet Loss
- WMM
- Priority
- Codec
 - Click on any **Client Name** to navigate to the **Summary** page of the client. Click **UCC** in the summary page of the client to view additional information of the client.
 - Click on any **AP Host Name** to navigate to the **Summary** page of the AP.

The **Calls** list displays the following details of the calls:

Table 90: Call Details

Parameter	Description
From	Displays the device originating the call.
To	Displays the device receiving the call.
Start Time	Displays the date and time when the call originated.

Table 90: Call Details

Parameter	Description
Duration	Displays the duration of the call.
State	Displays the state of the call. Possible values are: <ul style="list-style-type: none">■ Active■ Success■ Terminated
Quality	Displays the quality of the call. Possible values are: <ul style="list-style-type: none">■ Good■ Fair■ Poor■ Unknown
AP Name	Displays the name of the AP.
Client	Displays the name of the client.



Up to 400,000 CDRs are displayed in the UCC dashboard.

WebRTC Prioritization

UCC supports the WebRTC prioritization that prioritizes the media traffic from WebRTC sources. WebRTC prioritization provides better end user experience, dashboard visibility of all WebRTC applications like voice, video, and application sharing, and call quality monitoring for audio calls using upstream and downstream RTP analysis.

Troubleshooting Unified Communications

To troubleshoot an AP:

1. In the **Network Operations** app, set the filter to **Global**. The dashboard context for the group is displayed.
2. Under **Analyze**, click **Tools**.
3. Click the **Commands**.
4. Use the **Commands** filter to select the **show openflow flow-table** and **show openflow controller** commands.
5. Click **Add**.
6. Click **Run**.
7. Analyze the output of the commands. In the following sample, the lines of relevance are highlighted:

```
(host) #show openflow controller
```

Controller IP: 52.26.220.65, port:30633, **State: Msg rcv wait**, SSL: True, Send ARP: True, Logging: False

Rap config:1, status:0

Openflow Interface List

IF MAC:c8:b5:ad:ba:bc:91, port_no:8479, name:aruba001, oflow_index:0

IF MAC:c8:b5:ad:c3:ab:c8, port_no:8456, name:bond0, oflow_index:0

IF MAC:c8:b5:ad:c3:ab:c9, port_no:8453, name:eth1, oflow_index:0

OpenFlow MAC Bridge List

OpenFlow Dynamic Tunnel List

(host) #show openflow flow-table

Flow: <Add at Wed Nov 27 05:15:00 2019> <bytes:0, pkts:0, idletmo:0, hardtmo:0 last:1574831700> Match:<17, 222.173.190.239, 186.173.202.254, **60000, 60000**> Cookie:<1099511666019>, Action:<out:controller overwrite-flag:4 >

Flow: <Add at Wed Nov 27 05:15:00 2019> <bytes:0, pkts:0, idletmo:0, hardtmo:0 last:0> <aceidx:265, actidx:3>, Match< Proto:[0x806] Arp><cookie : 1099511666018>, Action:<out:normal out:controller >

Flow: <Add at Wed Nov 27 05:14:40 2019> <bytes:0, pkts:0, idletmo:0, hardtmo:0 last:0> <aceidx:268, actidx:0>, Match< ><cookie : 0>, Action:<out:normal >

```
(host) #show datapath session
```

```
Datapath Session Table Entries
```

```
-----
```

```
Flags: F - fast age, S - src NAT, N - dest NAT
```

```
D - deny, R - redirect, Y - no syn
```

```
H - high prio, P - set prio, T - set ToS
```

```
C - client, M - mirror, V - VOIP
```

```
I - Deep inspect, U - Locally destined
```

```
s - media signal, m - media mon, a - rtp analysis
```

```
E - Media Deep Inspect, G - media signal
```

```
A - Application Firewall Inspect
```

```
L - ALG session
```

```
O - Session is programmed through SDN/Openflow controller
```

```
p - Session is marked as permanent
```

```
RAP Flags: 0 - Q0, 1 - Q1, 2 - Q2, r - redirect to master, t - time based
```

Source IP Packets	Destination IP Bytes	Prot	SPort	Dport	Cntr	Prio	ToS	Age	Destination	TAge
10.15.91.244 1b8	52.26.220.65 e8a8 C	6	51203	443	0	0	0	0	local	8427
52.26.220.65 1f9	10.15.91.244 11faa	6	443	51203	0	0	8	0	local	8427
10.15.82.246 0	10.15.91.244 0 FY	17	4434	4434	0	0	0	1	local	7f
222.173.190.239 0	186.173.202.254 0 FRYHCOp	17	60000	60000	0	0	0	0	sysmsg 219	841b
10.15.91.244 1445	54.213.157.38 17321e C	6	62231	443	0	0	0	0	local	daf6
54.213.157.38 1092	10.15.91.244 4efd9	6	443	62231	0	0	0	0	local	daf6
10.15.91.244 1	10.15.82.246 2c FC	17	4434	4434	0	0	0	0	local	7f
(host) #show datapath session ucc										
C - client, M - mirror, V - VOIP										
10.15.105.91 189	10.15.105.92 3956f FHPTCIVaOp SILK	17	50016	50017	0	6	46	0	dev20	1229

10.15.105.92	10.15.105.91	17	50038	50022	0	5	34	0	dev20	1117
5fb	343eb	FHPTC	VO	p	X_	H	264	UC		

10.15.105.92	10.15.105.91	17	50017	50016	0	6	46	0	dev20	122a
188	390bd	FHPTCI	Va	O	p	SILK				

10.15.105.91	10.15.105.92	17	50022	50038	0	5	34	0	dev20	1116
14a	e05d	FHPTC	VO	p	X_	H	264	UC		

Insights Context	335
Cards	341
Baselines	343
Access Points with Excessive Number of Channel Changes	344
Access Points with High Number of Reboots	346
Access Point with High CPU Utilization	347
Access Points Impacted by High 2.4 GHz Usage	348
Access Points Radios with Frequent Transmit Power Changes	351
Access Point Transmit Power can be Optimized	352
Access Points Impacted by High 5 GHz Usage	353
Access Points with High Memory Usage	356
Clients with High Roaming Latency	357
Clients with Low SNR Minutes	359
Clients with High Number of MAC authentication Failures	362
Clients with DHCP Server Connection Problems	364
Clients with High Number of Wi-Fi Association Failures	366
Clients with High Wi-Fi Security Key-Exchange Failures	367
Clients with High 802.1X Authentication Failures	369
Clients with Captive Portal Authentication Problems	371
Clients who Roamed Excessively	373
Coverage Holes Identified	375
Dual-band (2.4/5 GHz) Clients Primarily using 2.4 GHz	376
Delayed DNS Request or Response	378
DNS Servers Rejected High Number of Queries	380
Gateways with High CPU Utilization	382
Gateways with High Memory Usage	383
Failure to Establish Gateway Tunnels	385
DNS Queries Failed to Reach or Return from the Server	387
Telemetry Information not Received from APs or Radios	389
Outdoor Clients Impacting Wi-Fi Performance	390

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 AIOps (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 collected from over huge network of data, AOS 10.x and built-in AI Insights proactively identifies and solves issues, and provides pinpoint configuration recommendations. As the data is stored in the cloud, it is easy to view the network performance across all locations from a single pane of glass. Utilizing the cloud also provides

the ability to anonymously compare a network with a peer network or the baselines for a broader perspective and optimization. All of this comes from Aruba's advantage in accessing an enormous volume and variety of data that is factored into insights. Aruba does not collect or process personal data.

In this release the insights are classified under three categories:

- **Connectivity**—Issues related to the wireless connectivity in the network.
- **Wireless Quality**—Issues related to the RF Info or RF Health in the network.
- **Availability**—Issues related to the health of your network infrastructure and the devices in the network such as, APs, switches, and gateways.

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 for the selected time range. Each insight provides specific details on the occurrences of these events for easy debugging.

To launch the **AI Insights** dashboard, 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 > AI Insights**.

The **Insights** table is displayed. AI Insights listed in the dashboard are sorted from high priority to low priority.


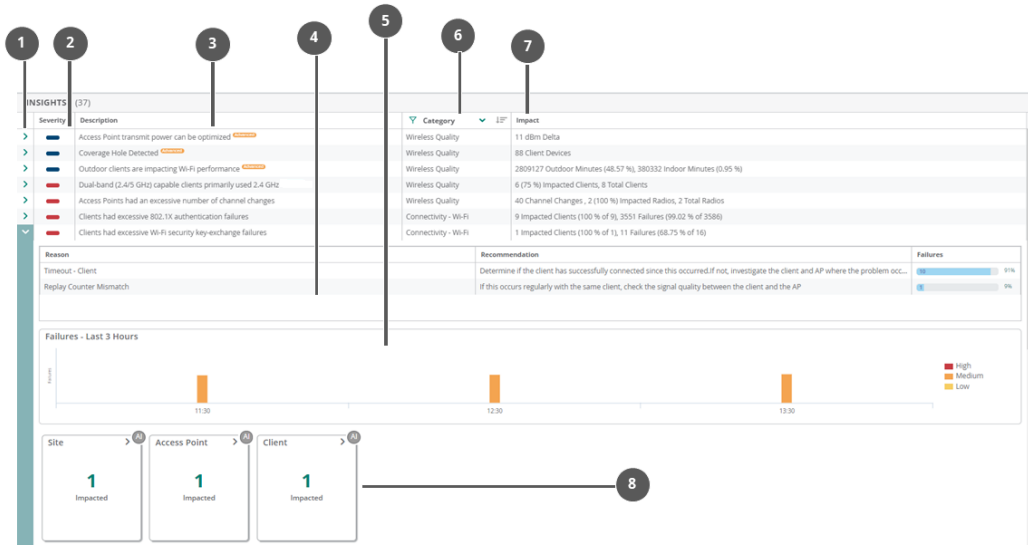





3. Click the arrow  against each insight to view the further details.

Figure 25 *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

Callout Number	Description
	<p> Orange—Medium priority</p> <p> Yellow—Low priority</p> <p>Note: The following three configuration recommendation insights are marked in blue () color in the severity column:</p> <p>Access Point Transmit Power can be Optimized</p> <p>Coverage Holes Identified</p> <p>Outdoor Clients Impacting Wi-Fi Performance</p>
3	Short description of the insight.
4	<p>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. The reasons are classified into:</p> <ul style="list-style-type: none"> ■ Static—These reasons rely on Aruba 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. The entries in each time series bar can be customized to highlight a specific entry by clicking on it. Only one specific entry can be highlighted at a time.
6	Category of the insight. Insight category can be filtered by clicking the filter  icon.
7	Short description of the impact.
8	<p>Cards display additional information specific to each insight. Cards might vary for each insight based on the context the insight is accessed from.</p> <p>For more information, see Cards.</p>

All AI Insights generated are listed in the **Global > AI Insights** dashboard. Alternatively, AI Insights for a specific site, device, or client can be viewed by selecting the respective context. For more information on available insights and the context, see [Insights 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**.

Insights 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.



In this release, all AI Insights are available irrespective of the user role or AOS 10.x subscription. In the upcoming AOS 10.x release, AI Insights marked as **Advanced** in the user interface would require an advanced subscription.

Table 91: Navigating Insights

Insights	Category	Context	Navigation
Access Point with High CPU Utilization	Availability – Access Point	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
Access Points with High Memory Usage	Availability – Access Point	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
Telemetry Information not Received from APs or Radios	Availability – Access Point	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
Access Points with High Number of Reboots	Availability – Access Point	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
Failure to Establish Gateway Tunnels	Availability – Gateway	Global	Network Operations > Global > Overview > AI Insights
		Site	Network Operations > Sites > Overview > AI Insights
		Gateways	Network Operations > Global > Devices > Gateways > Device Name > AI Insights
Gateways with High CPU Utilization	Availability – Gateway	Global	Network Operations > Global > Overview > AI Insights
		Site	Network Operations > Sites > Overview > AI Insights
		Gateways	Network Operations > Global > Devices > Gateways > Device Name > AI Insights

Insights	Category	Context	Navigation
Gateways with High Memory Usage	Availability – Gateway	Global	Network Operations > Global > Overview > AI Insights
		Site	Network Operations > Sites > Overview > AI Insights
		Gateways	Network Operations > Global > Devices > Gateways > Device Name > AI Insights
Clients who Roamed Excessively	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 Roaming Latency	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
Delayed DNS Request or Response	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
DNS Servers Rejected High Number of Queries	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 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
DNS Queries Failed to Reach or Return from the Server	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 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 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 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
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
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

Insights	Category	Context	Navigation
Access Point Transmit Power can be Optimized	Wireless Quality	Global	Network Operations > Global > Overview > AI Insights
Access Points Impacted by High 2.4 GHz Usage	Wireless Quality	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
Access Points Impacted by High 5 GHz Usage	Wireless Quality	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
Dual-band (2.4/5 GHz) Clients Primarily using 2.4 GHz	Wireless Quality	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 Low SNR Minutes	Wireless Quality	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
Coverage Holes Identified	Wireless Quality	Global	Network Operations > Global > Overview > AI Insights





Insights	Category	Context	Navigation
Access Points with Excessive Number of Channel Changes	Wireless Quality	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
Access Points Radios with Frequent Transmit Power Changes	Wireless Quality	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
Outdoor Clients Impacting Wi-Fi Performance	Wireless Quality	Global	Network Operations > Global > Overview > AI Insights












Cards


All the insights in Aruba Central 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. Few cards have further drill down option available, in the form of a drop-down. Additionally, a few cards have an expandable view option to view the graph.




The cards might vary for each insight based on the context the insight is accessed from. The following table displays the cards available in different insights:



Table 92: *Cards*

Card	Description
Site	The Site card displays the number of sites impacted by an insight. Click the arrow  to expand the card and view the most impacted sites where the issue occurred.
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 most impacted APs where the issue occurred. You can also click the drop-down list to view further details about the impacted access points.
Clients	The Client card displays the number of clients impacted by an insight. Click the arrow  to expand the card and view the most impacted 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 most impacted servers where the issue occurred.

Card	Description
RF Info	The RF Info card displays the number of channels, band, and SSID information based on the insight it is accessed from. Click the arrow  to expand the card and view the relevant information. You can also click the drop-down list to view further details about the impacted RF bands.
Wired Clients	The Wired Client card displays the number of wired clients impacted by an insight. Click the arrow  to expand the card and click the drop-down list to view further details about the impacted wired clients.
Roam	The Roam card displays the percentage of client latency roams. Click the arrow  to expand the card and click the drop-down list to view further details about the roaming latency and band.
Tunnel	The Tunnel card displays the number of gateway tunnels down. Click the arrow  to expand the card and view the reasons for the cause of tunnel down.
Gateway	The Gateway card displays the number of gateways impacted by an insight. Click the arrow  to expand the card and view the most impacted gateways where the issue occurred. You can also click the drop-down list to view further details about the impacted gateways.
VPNC	The VPNC card displays the number of VPNC gateways on which the tunnels are down. Click the arrow  to expand the card and view the reasons for the cause of VPNC tunnel down.
Outdoor Clients	The Outdoor Clients card is available only for Outdoor Clients Impacting Wi-Fi Performance insight and it displays the percentage of avoided outdoor client minutes. Click the arrow  to expand the card and view graphical representation of the data.
Outdoor Minutes	The Outdoor Minutes card is available only for Outdoor Clients Impacting Wi-Fi Performance insight and it displays the percentage of avoided outdoor clients minutes and affected indoor client minutes. Click the arrow  to expand the card and view graphical representation of the data.
CPU	The CPU card is available at the device (Gateways and Switches) context and displays the number of gateways and switches impacted by high CPU utilization in the network. Click the arrow  to expand the card and view graphical representation of the data.
Memory	The Memory card is available at the device (Gateways and Switches) context and displays the number of gateways and switches impacted by high memory utilization in the network. Click the arrow  to expand the card and view graphical representation of the data.
Power	The Power card displays the number of power changes in access points in the network. Click the arrow  to expand the card and click the drop-down list to view further details about the impacted access points.

Card	Description
Channel	The Channel card displays the number of channels changes per channel for a specific access point in the network. Click the arrow  to expand the card and click the drop-down list to view further details about the impacted channels.

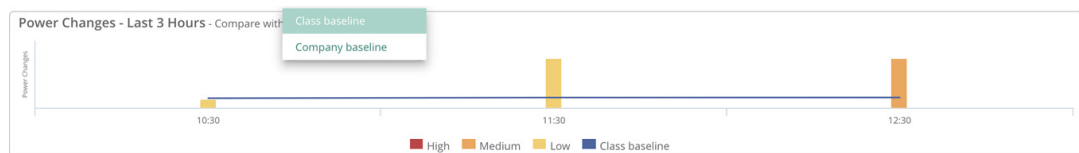
If you click on the number displayed on each card, further details specific to that card is displayed in a tabular format. The filter  icon allows you to filter data in each table columns. The  and  icon allows you to sort the columns in ascending and descending order. Few columns are displayed by default 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 columns. Click  to download the card details in a CSV format.

Baselines

Baseline enables you to compare your network performance with similar peer groups. Baseline is calculated on a weekly basis and is available in the trend chart for insights in the **Site** context only. Baseline is displayed as a blue line in the trend chart. The following two baselines are available in Aruba Central:

- **Class baseline**—Provides a comparison with similar peer groups in the networks. Peer group classification is done based on various parameters such as number of access points, neighboring devices information, and so on.
- **Company baseline**—Provides a comparison of the network within the entire customer ID (CID).



Baseline is supported for the following insights:

- [Clients with High Number of MAC authentication Failures](#)
- [Clients with High Wi-Fi Security Key-Exchange Failures](#)
- [Clients with High 802.1X Authentication Failures](#)
- [Clients with DHCP Server Connection Problems](#)
- [DNS Queries Failed to Reach or Return from the Server](#)
- [DNS Servers Rejected High Number of Queries](#)
- [Delayed DNS Request or Response](#)
- [Access Point with High CPU Utilization](#)
- [Delayed DNS Request or Response](#)
- [Access Points with High Memory Usage](#)
- [Access Points with High Number of Reboots](#)
- [Telemetry Information not Received from APs or Radios](#)
- [Access Points with Excessive Number of Channel Changes](#)
- [Access Points Impacted by High 2.4 GHz Usage](#)

- [Access Points Impacted by High 5 GHz Usage](#)
- [Access Point Transmit Power can be Optimized](#)
- [Dual-band \(2.4/5 GHz\) Clients Primarily using 2.4 GHz](#)
- [Clients with Low SNR Minutes](#)

Access Points with Excessive Number of Channel Changes

The **Access Points had an excessive number of channel changes** insight can be accessed from the **Global**, **Site**, and **Access Points** context. This insight provides information about AP radios on the network that changed channels excessively in the network. It is categorized under wireless quality as the connected clients might have to reconnect after an AP changes channel for a better network performance. This insight displays the following information:

- [Insight Summary](#)
- [Time Series Graph](#)
- [Cards](#)

Insight Summary

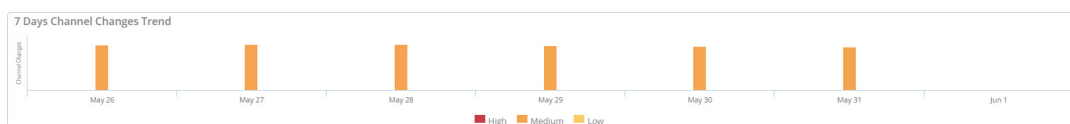
The insight summary provides the following details:

- **Reason**—Displays the possible causes for which the APs changed channels on the network.
- **Recommendation**—Displays the recommendation against each failure to resolve the same.
- **Channel Changes**—Displays the exact number and percentage of failures that occurred against each failure reason.

Time Series Graph

This bar graph displays the number of channel changes per channel for a specific AP during the selected time period. Hover your mouse on each bar graph to see the exact number of channel changes. The following graph shows data trend for seven days (1 Week).

Figure 26 Excessive AP Radio Channel Changes Data



Cards


The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 93: Cards Context

Cards	Context
Site	Global
Access Point	Global, Site


Cards	Context
Client	Global, Site, Device
Channel	Global, Site, Device

Site

Lists the number of sites that experience excessive AP radio channel changes in the network. Click the arrow  to view the pictorial graph of the **Top 5** 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.
- **Impacted Session Count**—Number of times the insight is triggered on each site.
- **Total Session Count**—Total number of session count in each site.
- **Total Channel Changes**—Total number of channel changes in each site.
- **Impacted Radio Count**—Number of radios with high airtime.
- **Total Radios**—Total number of radios in each site.

Access Point


Lists the number and details of APs that experience excessive AP radio channel changes in the network. Click the arrow  to view the pictorial graph of the **Top 5** impacted access points. Click the **Access Point** drop-down list, to view the following:

- **Model**—Pictorial graph of the channel changes classified by AP models.
- **FW Version**—Pictorial graph of channel changes classified by AP firmware versions.

Click the number displayed on the **Access Point** card to view a detailed description of the impacted access points:


- **Name**—Name of the access points and link to the **Access Point Details** page.
- **Model**—Model number of each AP.
- **Band**—Bandwidth where each AP dwells.
- **Channel Change Count**—Number of channel changes on each AP.
- **Impacted Session Count**—Number of times the insight is triggered on each AP.
- **Total Session Count**—Total number of session count in each AP.

Client

Lists the MAC Address, name, host name, auth ID, and the corresponding number of channel changes for each client. Click the arrow  to view the pictorial graph of the **Top 5** impacted clients. Click the number displayed on the **Clients** card, to view a detailed description of the impacted clients:

- **Name**—Name of the impacted client.
- **Impacted Count**—Number of channels changed on each client.

Channel

Number of channel changes per channel for a specific AP during the selected time period. Click the arrow  to expand the card and view the pictorial graph of the channel changes. Click the **Channel** drop-down list to view the following:

- **Band**— Pictorial graph of the channel changes based on both 2.4 GHz and 5 GHz.
- **Channel**—Pictorial graph of the number of channel changes per channel for a specific AP during the selected time period. It shows a comparison of the channel change between the peer network and AP.

Click the number displayed on the **Channel** card to view a detailed description of the impacted channels:

- **Channel**—Total number of channels.
- **Number of Channel Changes**—Number of channels that experienced excessive changes.

Access Points with High Number of Reboots

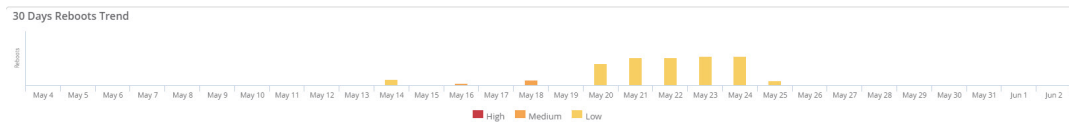
The **Access Points had a high number of reboots** insight can be accessed from the **Global**, **Site**, and **Access Points** context. This insight provides information about APs that have been rebooted the maximum times and is categorized under availability as the clients connected to these APs experience connectivity drops. This insight displays the following information:

- [Time Series Graph](#)
- [Cards](#)

Time Series Graph

This bar graph displays the number of AP reboots that occurred during the selected time period. Hover your mouse over each bar graph to see the exact number of reboots. The following graph shows data trend for the last 30 days (1 Month).

Figure 27 Excessive AP Reboots Data




Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 94: Cards Context


Cards	Context
Site	Global
Access Point	Global, Site

Site

Lists the number of sites where the APs experience excessive reboots. Click the arrow  to view the pictorial graph of the **Top 5** 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.
- **APs with Excessive Reboots**—Number of APs that experience expressive reboots in each site.
- **Reboot Count**—Number reboots that occurred in each AP in a specific site.

Access Point

Lists the number and details of reboots observed in an AP. Click the arrow  to view the pictorial graph of the **Top 5** impacted access points. Click the **Access Point** drop-down list, to view the following:

- **Time Series**—Pictorial graph of the AP reboots that occurred on different dates but similar timestamp.
- **FW Version**—Pictorial graph of AP reboots classified by AP firmware versions.
- **AP Model**—Pictorial graph of AP reboots classified by AP models.

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 **Access Point Details** page.
- **AP MAC**—MAC address of the AP.
- **AP Serial**—Serial number of the AP.
- **Firmware**—Version of the firmware running on each AP.
- **AP Model**—Model number of each AP.
- **Site**—Name of the site where the AP resides.
- **Reboot Count**—Number of reboots over time.

Access Point with High CPU Utilization

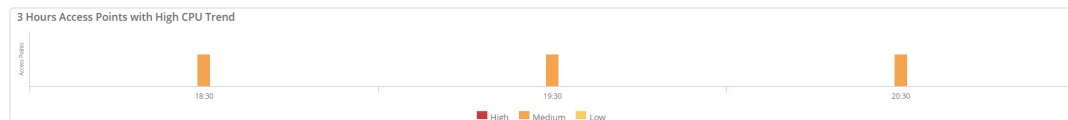
The **Access Points had unusually high CPU utilization** insight can be accessed from the **Global**, **Site**, and **Access Points** context. This insight provides information about APs that have higher than normal CPU utilization and is categorized under availability as the clients connected to these APs experience intermittent connectivity drops. This insight displays the following information:

- [Time Series Graph](#)
- [Cards](#)

Time Series Graph

This bar graph displays the number of APs that experience high CPU utilization in the network during the selected time period. Hover your mouse on each bar graph to see the exact number of APs. The following graph shows data trend for 3 hours in a day.

Figure 28 APs with High CPU Utilization Data




Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 95: Cards Context


Cards	Context
Site	Global
Access Point	Global, Site

Site

Lists the number of sites where the APs experience high CPU utilization. Click the arrow  to view the pictorial graph of the **Top 5** 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.
- **APs with High CPU**—Number of APs that experience high CPU utilization in each site.
- **Minutes with High CPU**—Time range of high CPU utilization in each site.

Access Point

Lists the number and details of APs that experience high CPU utilization in the network. Click the arrow  to view the pictorial graph of the **Top 5** impacted access points. Click the **Access Point** drop-down list, to view the following:

- **AP Model**—Pictorial graph of CPU utilization classified by AP models.
- **FW Version**—Pictorial graph of CPU utilization 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 **Access Point Details** page.
- **AP MAC**—MAC address of the AP.
- **AP Serial**—Serial number of the AP.
- **Firmware**—Version of the firmware running on each AP.
- **AP Model**—Model number of each AP.
- **Site**—Name of the site where the AP resides.
- **Minutes with High CPU**—Time range of high CPU utilization on each AP.
- **Minutes with High CPU (%)**—Percentage of high CPU utilization on each AP.

Access Points Impacted by High 2.4 GHz Usage

The **Access Points impacted by high 2.4 GHz usage** insight can be accessed from the **Global**, **Site**, and **Access Points** context. This insight provides information about AP radios whose Wi-Fi channel utilization deviated from the normal utilization range, as compared to other APs broadcasting in the same location, RF band, and time of day. It is categorized under wireless quality as the connected clients experience poor Wi-Fi performance. 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 APs experience higher airtime utilization in the network.
- **Recommendation**—Displays the possible recommendation against each failure to resolve the same.

Time Series Graph

This bar graph displays the number of APs that experience high 2.4 GHz airtime utilization in the network during the selected time period. Hover your mouse on each bar graph to see the exact number of APs. The following graph shows data trend for 3 hours in a day.

Figure 29 APs with High 2.4 GHz Utilization Data




Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 96: Cards Context


Cards	Context
Site	Global
Access Point	Global, Site
Client	Global, Site, Device
RF Info	Global, Site, Device

Site

Lists the number of sites that experience high 2.4 GHz airtime utilization in the network. Click the arrow  to view the pictorial graph of the **Top 5** 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.
- **Duration (mins)**—Time range that an AP in each site experienced high airtime utilization.
- **Clients Impacted**—Number of clients impacted by the insight.
- **APs Impacted**—Number of APs impacted by the insight in each site.
- **Reasons**—Cause of the high 2.4 GHz airtime utilization in each site.

Access Point


Lists the number and details of APs that experience high 2.4 GHz airtime utilization in the network. Click the arrow  to view the pictorial graph of the **Top 5** impacted access points. Click the **Access Point** drop-down list, to view the following:

- **Model**—Pictorial graph of the high 2.4 GHz airtime utilization percentage classified by AP models.

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 **Access Point Details** page.
- **MAC**—MAC address of the AP.
- **Serial**—Serial number of the AP.
- **Consumed Airtime (mins)**—Time range of the consumed airtime in each AP.
- **Duration (mins)**—Time range that the AP experienced high airtime utilization.
- **Reasons**—Cause of the high 2.4 GHz airtime utilization in each AP.
- **Clients Impacted**—Number of clients impacted by the insight connected to each AP.
- **Avg Channel Utilization (%)**—Average percentage of the airtime utilization in each AP.
- **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, auth ID, and the corresponding percentage of high 2.4 GHz airtime utilization of each client. Click the arrow  to view the pictorial graph of the **Top 5** impacted clients. Click the number displayed on the **Client** card, to view a detailed description of the impacted clients:

- **Client Name**—Name of the client impacted by the insight.
- **MAC**—MAC address of the client.
- **Duration (mins)**—Time range that the client experienced high airtime utilization.
- **Reason**—Cause of the high 2.4 GHz airtime utilization for each client.
- **Site**—Name of the site where the client exists.

RF Info

Number of channels impacted by high 2.4 GHz airtime utilization. Click the arrow  to view the pictorial graph of the impacted band. Click the **RF Info** drop-down list to view the following:

- **Channel**—Chart of AP radio channels that experienced excessive AP airtime utilization. It displays the channels impacted by this issue over the selected time period, sorted by airtime utilization score, which is calculated from the severity of the utilization level and the duration of time that the channel was over utilized.
- **Reason**—Pictorial graph of the percentage of causes for high 2.4 GHz airtime utilization in a channel.
- **Utilization**—Pictorial graph of the airtime utilization in each AP on a specific date and time.
- **Power Distribution**—Pictorial graph of Tx Power distribution (dBm) for both the 2.4 GHz and 5 GHz band during the time it is transmitting signal to the client.
- **Hour of Day**—Pictorial graph of which hours of the day the network was most impacted by excessive AP airtime utilization.

- **SNR Percentile**—Pictorial graph of the average Signal-to-Noise Ratio of the AP in different percentiles (25th, 50th, 75th, 90th, 99th) in 2.4 GHz band and 5 GHz band.

Click the number displayed on the **RF Info** card to view a detailed description of the impacted channels:

- **Channel**—Number of channels that experienced excessive AP airtime utilization.
- **Airtime (mins)**—Time range of the consumed airtime in each client.

Access Points Radios with Frequent Transmit Power Changes

The **Access Point radios changed their transmit power frequently** insight can be accessed from the **Global**, **Site**, and **Access Points** context. This insight provides information on AP radios that frequently changed transmission power levels and is categorized under wireless quality as the connected clients experience frequent throughput fluctuations. 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 APs experience frequent transmit power changes in the network.
- **Recommendation**—Displays the recommendation against each failure to resolve the same.

Time Series Graph

This bar graph displays the number of AP power changes in the network during the selected time period. Hover your mouse on each bar graph to see the exact number of power changes. The following graph shows data trend for 3 hours in a day.

Figure 30 *Frequent AP Transmit Power Changes Data*




Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 97: *Cards Context*


Cards	Context
Site	Global
Access Point	Global, Site
Power	Global, Site, Device

Site

Lists the number of sites that experience power transmit changes in the network. Click the arrow  to view the pictorial graph of the **Top 5** 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.
- **Power Changes**—Number of power changes occurred in each site.
- **Radio**—Number of AP radios in each site that changed transmission power level.

Access Point

Lists the number and details of APs that experience power transmit changes in the network. Click the arrow  to view the pictorial graph of the **Top 5** impacted access points. Click the number displayed on the **Access Point** card to view a detailed description of the impacted access points:

- **Name**—Name of the access points and link to the **Access Point Details** page.
- **MAC**—MAC address of the AP.
- **Serial**—Serial number of the AP.
- **Power Changes**—Number of power changes occurred in each AP.
- **Model**—Model number of each AP.
- **Firmware**—Version of the firmware running on each AP.
- **Site**—Name of the site where the AP resides.

Power

Displays the number of power changes that occurred in APs in the network. Click the arrow  to view the pictorial graph of the impacted band. Click the **Power** drop-down list to view the following:

- **Power Changes over Time**—Pictorial graphs of power transmit changes observed across time for 2.4 GHz and 5 GHz radio.
- **Power Distribution**—Pictorial graph of the percentage of time spent across power levels for the time period in the 2.4 GHz and 5 GHz band.
- **Band**—Pictorial graph of the percent of number of changes observed in the 2.4 GHz and 5 GHz bands.
- **Variance**—Pictorial graph of the percentage of variance in transmission power across number of APs in that power variance for the 2.4 GHz and 5 GHz band.

Click the number displayed on the **Power** card to view a detailed description of the impacted channels:

- **Band**—Number of power changes observed in the 2.4 GHz and 5 GHz bands.
- **Changes**—Number of power changes that occurred in each band.

Access Point Transmit Power can be Optimized

The **Access Point transmit power can be optimized** insight can be accessed only at the **Global** context. This insight generates when the transmit power is not set optimally on the radios of Access Points existing in the network. This insight detects that wireless clients are experiencing a poor Wi-Fi connectivity due to the transmit power settings of the access points. It is categorized under wireless quality as the clients connected to these APs can communicate with the APs well but, the APs have difficulty to communicate with the clients in return. This insight displays the following information:

- [Insight Summary](#)
- [Card](#)

Insight Summary

The insight summary provides the following details:

- **Reason**—Displays the possible causes for which the transmit power of APs are not set optimally.
- **Recommendation**—Displays the possible recommendation against each failure to resolve the same.

Card


The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 98: *Cards*

Context


Cards	Context
RF Info	Global
Power	Global

RF Info

Number of channels in the APs impacted by transmit power setting in the network. Click the arrow  to view the pictorial graph of the impacted band. Click the **RF Info** drop-down list to view the following:

- **Band**—Pictorial graph of power changes in both the frequency bands by the AP (2.4 GHz or 5 GHz).
- **SSID**—Pictorial graph of the percent of AP dwell bands (2.4 GHz or 5 GHz) sorted by SSIDs.

Power

Displays the number of power changes that occurred in a specific access point. Click the arrow  to expand the card to view the pictorial graph of the band and power distribution in the network. Click the **Power** drop-down list, to view the following:

- **Power Distribution**—Pictorial graph of the percentage of time spent across power levels for the time period in the 2.4 GHz and 5 GHz band.
- **Band**—Graph of the percent of number of changes observed in the 2.4 GHz and 5 GHz bands.

Click the number displayed on the **Power** card, to view a detailed description of the impacted clients:

- **Band**—Band where the maximum power changes occurred.
- **Changes**—Number of power changes that occurred in each band.

Access Points Impacted by High 5 GHz Usage

The **Access Points were impacted by high 5 GHz usage** insight can be accessed from the **Global**, **Site**, and **Access Points** context. This insight provides information about AP radios whose Wi-Fi channel utilization

deviated from the normal utilization range, as compared to other APs broadcasting in the same location, RF band, and time of day. It is categorized under wireless quality as the connected clients experience poor Wi-Fi performance. This insight displays the following information:

- [Insight Summary](#)
- [Time Series Graph](#)
- [Cards](#)

Insight Summary

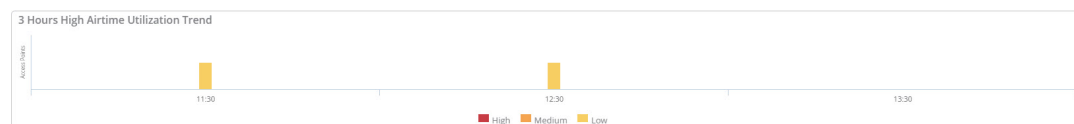
The insight summary provides the following details:

- **Reason**—Displays the possible causes for which the APs experience higher airtime utilization in the network.
- **Recommendation**—Displays the possible recommendation against each failure to resolve the same.

Time Series Graph

This bar graph displays the number of APs that experience high 5 GHz airtime utilization in the network during the selected time period. Hover your mouse on each bar graph to see the exact number of APs. The following graph shows data trend for 3 hours in a day.

Figure 31 APs with High 5 GHz Utilization Data




Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 99: Cards Context

Cards	Context
Site	Global
Access Point	Global, Site
Client	Global, Site, Device
RF Info	Global, Site, Device


Site

Lists the number of sites that experience high 5 GHz airtime utilization in the network. Click the arrow  to view the pictorial graph of the **Top 5** 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.
- **Duration (mins)**—Time range that an AP in each site experienced high airtime utilization.

- **APs**—Number of APs impacted by the insight in each site.
- **Clients**—Number of clients impacted by the insight.
- **Reason**—Cause of the high 5 GHz airtime utilization in each site.

Access Point


Lists the number and details of APs that experience high 5 GHz airtime utilization in the network. Click the arrow  to view the pictorial graph of the **Top 5** impacted access points. Click the **Access Point** drop-down list, to view the following:

- **Model**—Pictorial graph of the high 5 GHz airtime utilization percentage classified by AP models.

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 **Access Point Details** page.
- **MAC**—MAC address of the AP.
- **Serial**—Serial number of the AP.
- **Consumed Airtime (mins)**—Time range of the consumed airtime in each AP.
- **Duration (mins)**—Time range that the AP experienced high airtime utilization.
- **Reason**—Cause of the high 5 GHz airtime utilization in each AP.
- **Clients Impacted**—Number of clients impacted by the insight connected to each AP.
- **Avg Channel Utilization (%)**—Average percentage of the airtime utilization in each AP.
- **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, auth ID, and the corresponding percentage of high 5 GHz airtime utilization for each client. Click the arrow  to view the pictorial graph of the **Top 5** impacted clients. Click the number displayed on the **Client** card, to view a detailed description of the impacted clients:

- **Client Name**—Name of the client impacted by the insight.
- **MAC**—MAC address of the client.
- **Duration (mins)**—Time range that the client experienced high airtime utilization.]
- **Reason**—Cause of the high 5 GHz airtime utilization for each client.
- **Site**—Name of the site where the client exists.

RF Info

Number of channels impacted by high 5 GHz airtime utilization. Click the arrow  to view the pictorial graph of the impacted band. Click the **RF Info** drop-down list to view the following:

- **Channel**—Chart of AP radio channels that experienced excessive AP airtime utilization. It displays the channels impacted by this issue over the selected time period, sorted by airtime utilization score, which is calculated from the severity of the utilization level and the duration of time that the channel was over utilized.
- **Reason**—Pictorial graph of the percentage of causes for high 5 GHz airtime utilization in a channel.
- **Utilization**—Pictorial graph of the airtime utilization in each AP on a specific date and time.

- **Power Distribution**—Pictorial graph of Tx Power distribution (dBm) for both the 2.4 GHz and 5 GHz band during the time it is transmitting signal to the client.
- **Hour of Day**—Pictorial graph of which hours of the day the network was most impacted by excessive AP airtime utilization.
- **SNR Percentile**—Pictorial graph of the average Signal-to-Noise Ratio of the AP in different percentiles (25th, 50th, 75th, 90th, 99th) in 5 GHz band.

Click the number displayed on the **RF Info** card to view a detailed description of the impacted channels:

- **Channel**—Number of channels that experienced excessive AP airtime utilization.
- **Airtime (mins)**—Time range of the consumed airtime in each client.

Access Points with High Memory Usage

The **Access Points with unusually high memory usage were found** insight can be accessed from the **Global**, **Site**, and **Access Points** context. This insight provides information about APs that have higher than normal memory utilization and is categorized under availability as the clients connected to these APs experience intermittent connectivity drops. This insight displays the following information:

- [Time Series Graph](#)
- [Cards](#)

Time Series Graph

This bar graph displays the number of APs that experience high memory utilization in the network during the selected time period. Hover your mouse on each bar graph to see the exact number of APs. The following graph shows data trend for 3 hours in a day.

Figure 32 APs with High Memory Utilization Data




Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 100: Cards Context


Cards	Context
Site	Global
Access Point	Global, Site

Site

Lists the number of sites where the APs experience high memory utilization. Click the arrow  to view the pictorial graph of the **Top 5** 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.
- **APs with High Memory**—Number of APs that experience high memory utilization in each site.
- **Minutes with High Memory**—Time range of high memory utilization in each site.

Access Point

Lists the number and details of APs that experience high memory utilization in the network. Click the arrow  to view the pictorial graph of the **Top 5** impacted access points. Click the **Access Point** drop-down list, to view the following:

- **AP Model**—Pictorial graph of memory utilization classified by AP models.
- **FW Version**—Pictorial graph of memory utilization 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 **Access Point Details** page.
- **AP MAC**—MAC address of the AP.
- **AP Serial**—Serial number of the AP.
- **Firmware**—Version of the firmware running on each AP.
- **AP Model**—Model number of each AP.
- **Site**—Name of the site where the AP resides.
- **Minutes with High Memory**—Time range of high memory utilization on each AP.
- **Minutes with High Memory (%)**—Percentage of high memory utilization on each AP.

Clients with High Roaming Latency

The **Clients experienced high latency while roaming** insight can be accessed from the **Global**, **Site**, **Access Points**, and **Clients** context. This insight provides reports on wireless clients that have experienced long roam times to the target AP. The threshold to detect a delayed and long client roaming is set to 50 ms and all the data and analysis pattern is perceived from the target AP issues if you access this insight from the global, site, or client context. When you access this Insight from device context, data is received from the home AP issues. **Clients experienced high latency while roaming** is categorized under connectivity since it helps the network administrators to take necessary actions if there are any clients experiencing long delays to roam between APs. This insight displays the following information:

- [Time Series Graph](#)
- [Cards](#)

Time Series Graph

This bar graph displays the total number of roams and the percentage of high latency roams that occurred in the network during the selected time period. Hover your mouse on each bar graph to see the exact number and percentage of roams. The following graph shows data trend for 3 hours in a day.

Figure 33 *Clients with High Roaming Latency*




Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 101: *Cards Context*


Cards	Context
Site	Global
Access Point	Global, Site, Client
Client	Global, Site, Device
Roam	Global, Site, Device, Client

Site

Lists the number of sites where the clients have experienced high roaming latency in the network. Click the arrow  to view the pictorial graph of the **Top 5** 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.
- **High Latency Roams (%)**—Number and percentage of high latency roams in each site
- **Impacted Clients Count**—Number of clients impacted with high roaming latency in each site.

Access Point

Lists the number and details of APs where the clients have experienced high roaming latency. Click the arrow  to view the pictorial graph of the **Top 5** impacted access points. Click the **Access Point** drop-down list, to view the following:

- **Model**—Pictorial graph of high roaming latency classified by AP models.
- **FW Version**—Pictorial graph of high roaming latency 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 **Access Point Details** page.
- **Serial**—Serial number of the AP.
- **High Latency Roams (%)**—Number and percentage of high latency roams in each AP.
- **Clients From**—Number of clients that roamed in each AP.
- **Latency (min/avg/max) msec**—The minimum, average, and maximum latency that occurred in each AP.
- **AP MAC**—MAC address of the impacted AP and link to the **Access Point Details** page.
- **IP**—IP address of the impacted 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, auth ID, and the number of clients that have experience high roaming latency. Click the number displayed on the **Client** card, to view a detailed description of the impacted clients:

- **Client Name**—Name of the impacted clients and link to the **Client Details** page.
- **Client MAC**—MAC address of the impacted client and link to the **Client Details** page.
- **High Latency Roams (%)**—Number and percentage of high latency roams in each client.
- **Top AP**— AP where the client roamed maximum as compared to other APs in the network.

Roam

Displays the percentage of client latency roams in the network. This card includes the raw telemetry feed sorted based on latency at each context.

Click the arrow  to expand the **Roam** card and click the drop-down list, to view the following:

- **Latency**—Pictorial graph of latency versus concurrences.
- **Band**—Pictorial graph of clients roaming trends between 2.4 GHz and 5 GHz.

Click the number displayed on the **Roam** card, to view a detailed description of the impacted clients:

- **Timestamp**—Timestamp of the event received.
- **Latency (msec)**—Latency value in microsecond per client.
- **From AP**—Name of the home AP from the where the client roamed to the target AP.
- **To AP**—Name of the target AP to where the client roamed from the home AP.
- **From Channel**—Number of channel the client roamed from.
- **Roaming Type**—Type of the roam that occurred in each client.
- **From AP MAC**—MAC address of the home AP from the where the client roamed to the target AP.
- **From AP Serial**—Serial number of the home AP from the where the client roamed to the target AP.
- **To AP MAC**—MAC address of the target AP to where the client roamed from the home AP.
- **To AP Serial**—Serial number of the target AP to where the client roamed from the home AP.
- **RSSI (dBm)**—Received Signal Strength Indicator (RSSI) value of the client.
- **To Channel**—Number of channels the client roamed to.

Clients with Low SNR Minutes

The **Clients had a significant number of Low SNR uplink minutes** insight can be accessed from the **Global, Site, Access Points, and Clients** context. This insight provides information about access points that have a low-quality signal-strength connection and is categorized under wireless quality as the clients connecting at a Low SNR have low throughput and high retransmissions. This insight displays the following information:

- [Insight Summary](#)
- [Time Series Graph](#)
- [Cards](#)

Insight Summary

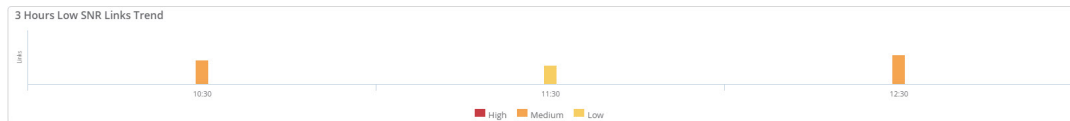
The insight summary provides the following details:

- **Reason**—Displays the possible causes for which the APs experience low-quality SNR connection in the network.
- **Recommendation**—Displays the possible recommendation against each failure to resolve the same.

Time Series Graph

This bar graph displays the number of clients with low SNR uplinks AP during the selected time period. Hover your mouse on each bar graph to see the number of SNR links. The following graph shows data trend for 3 hours in a day.

Figure 34 *Clients with Low SNR Uplink Connections*




Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 102: *Cards Context*


Cards	Context
Site	Global
Access Point	Global, Site, Client
Client	Global, Site, Device
RF Info	Global, Site, Device

Site

Lists the number of sites where the APs and clients experience low signal connection. Click the arrow  to view the pictorial graph of the **Top 5** 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.
- **APs with Low SNR**—Number of APs with low signal connection.
- **Clients with Low SNR**—Number of clients with low signal connection.
- **Uplink Minutes of Low SNR**—Duration of uplink with low signal connection in each site.
- **Downlink Minutes of Low SNR**—Duration of downlink with low signal connection in each site.

Access Point

Lists the number and details of APs that experience low signal connection in the network. Click the arrow  to view the pictorial graph of the **Top 5** impacted access points. Click the **Access Point** drop-down list, to view the following:

- **TX Power**—Pictorial graph of the percentage of Tx Power distribution (dBm) in both the 2.4 GHz and 5 GHz band during the time it is transmitting signal to the client.

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 **Access Point Details** page.
- **AP MAC**—MAC address of the AP and link to the **Access Point Details** page.
- **AP Serial**—Serial number of the AP
- **AP Model**—Model number of each AP.
- **Clients with Low SNR**—Number of clients that experience low signal connection in each AP.
- **Uplink Minutes of Low SNR**—Duration of uplink with low signal connection in each AP.
- **Uplink Low SNR Minutes in 2.4 GHz**—Duration of uplink with low signal connection in 2.4 GHz band during the time it is transmitting signal to the AP.
- **Uplink Low SNR Minutes in 5 GHz**—Duration of uplink with low signal minutes in 5 GHz band during the time it is transmitting signal to the AP.
- **Downlink Minutes of Low SNR**—Duration of downlink with low signal connection in each AP.
- **Downlink 2.4 GHz Dwell Minutes**—Duration of downlink with low signal connection in 2.4 GHz band during the time it is transmitting signal to the AP.
- **Downlink 5 GHz Dwell Minutes**—Duration of downlink with low signal connection in 5 GHz band during the time it is transmitting signal to the AP.

Client

Lists the MAC Address, name, host name, auth ID, and the number of clients experiencing low signal quality.


Click the arrow  to view the pictorial graph of the **Top 5** impacted clients. Click the **Client** drop-down list, to view the following:

- **Client Type**—Pictorial graph of the number and percentage of low SNR clients classified by vendors.

Click the number displayed on the **Client** card, to view a detailed description of the impacted clients:

- **Client Name**—Number of the impacted client and link to the **Client Details** page.
- **Client MAC**—MAC address of the client and link to the **Client Details** page.
- **Device Type**—Device type of the client.
- **Uplink Minutes of Low SNR**—Duration of uplink with low signal connection in each client.
- **Uplink 2.4 GHz Dwell Minutes**—Duration of uplink with low signal connection in 2.4 GHz band during the time it is transmitting signal to the client.
- **Uplink 5 GHz Dwell Minutes**—Duration of uplink with low signal connection in 5 GHz band during the time it is transmitting signal to the client.
- **Downlink Minutes of Low SNR**—Duration of downlink with low signal connection in each client.
- **Downlink 2.4 GHz Dwell Minutes**—Duration of downlink with low signal connection in 2.4 GHz band during the time it is transmitting signal to the client.
- **Downlink 5 GHz Dwell Minutes**—Duration of downlink with low signal connection in 5 GHz band during the time it is transmitting signal to the client.

RF Info

Number of channels impacted by low-quality signal-strength connection in the network. Click the arrow  to view the pictorial graph of the impacted band. Click the **RF Info** drop-down list to view the following:

- **Band**—Pictorial graph of devices experiencing a low signal-quality link using 2.4 GHz or 5 GHz radio bands.
- **Good vs Bad**—Pictorial graph of the amount of time (minutes) with Low SNR (Bad) and High SNR (Good) for all the clients.

Click the number displayed on the **RF Info** card to view a detailed description of the impacted channels:

- **Band**—Number of channel changes between 2.4 GHz and 5 GHz.
- **Number of Power Changes**—Number of power changes.

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. It 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

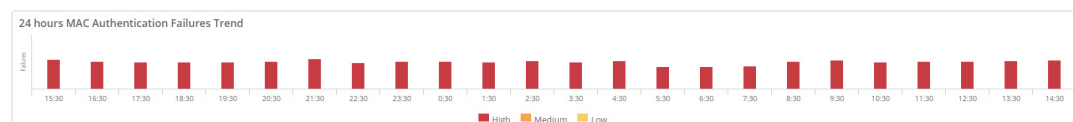
The insight summary provides the following details:

- **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

This bar graph displays the number of MAC authentication failures that occurred during the selected time period. Hover your mouse over each bar graph to see the exact number of failures. The following graph shows data trend for the last 24 hours (1 Day).

Figure 35 *MAC Authentication Failure Data*




Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 103: Cards Context


Cards	Context
Site	Global
Access Point	Global, Site, Client
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 **Top 5** 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 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 **Top 5** 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 **Access Point Details** page.
- **MAC**—MAC address of the AP and link to the **Access Point Details** page.
- **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 **Top 5** 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.
- **MAC**—MAC address of the client and link to the **Client Details** page.
- **Failures**—Number of failures occurred in each client.
- **IP**—IP address of each 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. It 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

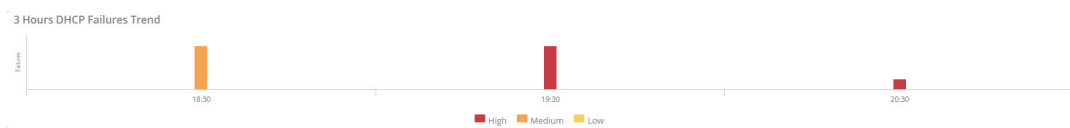
The insight summary provides the following details:

- **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

This bar graph displays the number of DHCP failures that occurred during the selected time period. Hover your mouse over each bar graph to see the exact number of failures. The following graph shows data trend for the 3 hours in a day.

Figure 36 *High DHCP Failures Data*



Cards


The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 104: *Cards Context*

Cards	Context
Site	Global
Server	Global, Site, Device, Client


Cards	Context
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 **Top 5** 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 DHCP requests.

Server

Lists the number of DHCP servers involved in this insight. Click the arrow  to view the pictorial graph of the **Top 5** impacted sites. Click the number displayed on the **Server** card, to view a detailed description of the impacted servers:

- **Name**—Name of 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 **Top 5** 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:

- **Name**—Name of the access points and link to the **Access Point Details** page.
- **MAC**—MAC address of the AP and link to the **Access Point Details** page.
- **Failures**—Number of failures occurred 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**—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 **Top 5** 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.
- **MAC**—MAC address of the client and link to the **Client Details** page.
- **Failures**—Number of failures occurred in each client.
- **Total**—Total number of DHCP requests.
- **IP**—IP address of each client.
- **OS**—OS type of the device.

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 105: *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 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. 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

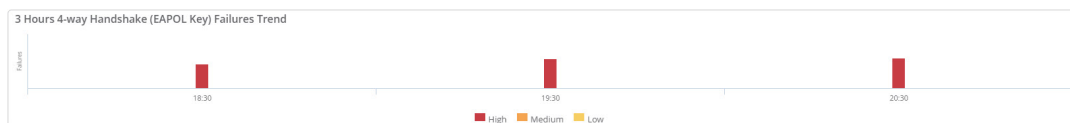
The insight summary provides the following details:

- **Reason**—Displays the possible causes 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 bar graph displays the number of Wi-Fi security key-exchange failures that occurred in the network during the selected time period. Hover your mouse on each bar graph to see the exact number of failures. The following graph shows data trend for 3 hours in a day.

Figure 37 4-Way Handshake (EAPOL Key) Failures Data




Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 106: 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 **Top 5** 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 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 **Top 5** 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:

- **Name**—Name of the access points and link to the **Access Point Details** page.
- **MAC**—MAC address of the AP.
- **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**—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 **Top 5** 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.
- **MAC**—MAC address of the client.
- **Failures**—Number and percentage of failures occurred in each client.
- **Total**—Total number of failures in each client.
- **IP**—IP address of the 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

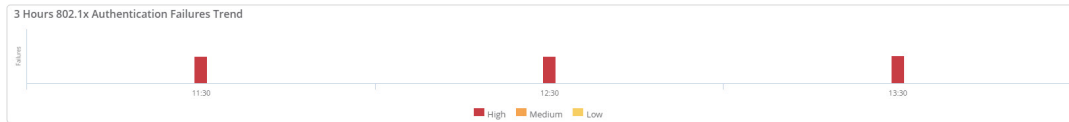
The insight summary provides the following details:

- **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

This bar graph displays the number of 802.1X authentication failures observed in the network during the selected time period. Hover your mouse over each bar graph to see the exact number of failures. The following graph shows data trend for 3 hours in a day.

Figure 38 802.1x Authentication Failure Data




Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 107: 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 **Top 5** 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 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 **Top 5** impacted sites. Click the number displayed on the **Server** card, to view a detailed description of the impacted servers:

- **Name**—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 **Top 5** 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:

- **Name**—Name of the access points and link to the **Access Point Details** page.
- **MAC**—MAC address of the AP.
- **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 **Top 5** 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.
- **MAC**—MAC address of the client.
- **Failures**—Number and percentage of failures occurred in each client.
- **Total**—Total number of failures in each client.
- **IP**—IP address of the 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 108: *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.

Clients who Roamed Excessively

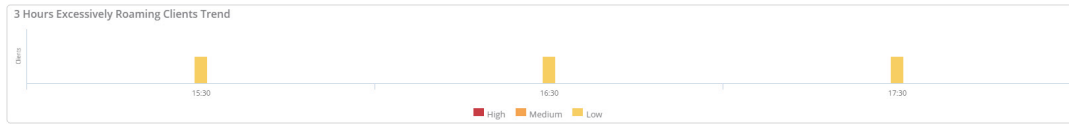
The **Clients roamed excessively** insight can be accessed from the **Global**, **Site**, **Access Points**, and **Clients** context. This insight provides reports on wireless clients that roam to the target APs more than normal from the home AP. This insight is categorized under connectivity as it helps to reduce the frequency of roaming clients in the customer network. It also helps network administrators to eliminate anonymous users and deploy additional access points in case the users get affected due to poor network performance. This insight displays the following information:

- [Time Series Graph](#)
- [Cards](#)

Time Series Graph

This bar graph displays the total number of roams and the percentage of excessive roams that occurred in the network during the selected time period. Hover your mouse on each bar graph to see the exact number and percentage of roams. The following graph shows data trend for 3 hours in a day.

Figure 39 *Clients that Roam Excessively*




Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 109: *Cards Context*


Cards	Context
Site	Global
Access Point	Global, Site, Client
Client	Global, Site, Device

Site

Lists the number of sites where the clients have experience excessive roams in the network. Click the arrow  to view the pictorial graph of the **Top 5** 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.
- **Impacted Clients**—Number and percentage of clients impacted with excessive roaming in each site.

Access Point


Lists the number and details of APs where the clients have experience excessive roams. Click the arrow  to view the pictorial graph of the **Top 5** impacted access points. Click the **Access Point** drop-down list, to view the following:

- **Model**—Pictorial graph of excessive roams classified by AP models.
- **FW Version**—Pictorial graph of excessive roams classified by AP firmware versions.

Click the number displayed on the **Access Point** card to view a detailed description of the impacted access points:

- **From AP**—The AP name from where the client roamed excessively.
- **Impacted Clients (%)**—Clients impacted by excessive roams in each AP.
- **AP MAC**—MAC address of the APs and link to the **Access Point Details** page.
- **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, auth ID, and the number of clients that have experience high roaming latency. Click the arrow  to view the pictorial graph of the **Top 5** impacted clients. Click the number displayed on the **Client** card, to view a detailed description of the impacted clients:

- **Client Name**—Name of the clients impacted by the insight and link to the **Client Details** page.
- **MAC**—MAC address of the client impacted by the insight and link to the **Client Details** page.
- **Excessive Roams**—Number of excessive roams for each client.
- **Delayed Roams**—Number of delayed roams by the client.
- **Top AP**—AP where the client roamed maximum as compared to other APs in the network.

Coverage Holes Identified

The **Coverage Holes have been detected** insight can be accessed only at the **Global** context. This insight determines the connection status of Wi-Fi clients with the APs due to poor Wi-Fi coverage. Machine learning determines when a relatively large proportion of the client minutes that consistently have low SNR links. The exact location of the coverage hole can be identified from the location of the clients listed with poor coverage and implies that there is a need to deploy one more AP which will avoid the low SNR clients in the network.

Coverage Holes have been detected is categorized under wireless quality since the clients in coverage holes have poor or intermittent Wi-Fi connectivity causing loss of productivity. This insight displays the following information:

- [Insight Summary](#)
- [Cards](#)

Insight Summary

The insight summary provides the following details:

- **Reason**—Displays the possible causes for which the clients experience poor Wi-Fi coverage in the network.
- **Recommendation**—Displays the recommendation against each failure to resolve the same.


Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 110: Cards Context


Cards	Context
Site	Global
Access Point	Global
Client	Global

Site

Lists the sites where the clients experience poor Wi-Fi coverage in the network. Click the arrow  to view the pictorial graph of the **Top 5** 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.
- **Number of APs**—Number of APs that experience coverage hole in each site.
- **Coverage Holes**—Total number APs that needs to be deployed in the network due to coverage holes.

Access Point

Lists the number and details of APs which has clients with poor connections due to a coverage hole in the network. This is measured by the amount of time the client experiences poor vs good connectivity. Click the arrow  to view the pictorial graph of the **Top 5** impacted access points. 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 **Access Point Details** page.
- **AP MAC**—MAC address of each AP and link to the **Access Point Details** page.
- **AP Serial**—Serial number of each AP.
- **Firmware**—Version of the firmware running on each AP.
- **Model**—Model number of each AP.
- **Number of Clients**—Number of clients with poor Wi-Fi coverage in each AP.
- **Poor Coverage (mins, %)**—Time range of the coverage hole detected in each AP.

Client

Lists the MAC Address, name, host name, auth ID, and the number of connected clients affected by poor connections determined by the total number of minutes spend in the coverage hole. Click the arrow  to view the pictorial graph of the **Top 5** impacted clients. Click the number displayed on the **Client** card, to view a detailed description of the impacted clients:

- **Client Name**—Name of the client and link to **Client Details** page.
- **Client MAC**—MAC address of the client and link to the **Client Details** page.
- **OS**—Operating system of the client.
- **Average SNR (dB)**—Average SNR of the client on the AP.
- **Poor Coverage (mins, %)**—Time range of the coverage hole detected in each client.

Dual-band (2.4/5 GHz) Clients Primarily using 2.4 GHz

The **Dual-band (2.4/5 GHz) capable clients primarily used 2.4 GHz** insight can be accessed from the **Global**, **Site**, **Access Points**, and **Clients** context. This insight provide reports on Dual band capable clients that spent more airtime the 2.4 GHz band instead of the 5 GHz band. It is categorized under wireless quality since the 2.4 GHz band has more interference, more clients, and less bandwidth capabilities than the 5 GHz band. Dual-band clients have a better user experience when they are on the 5 GHz band. This insight displays the following information:

- [Insight Summary](#)
- [Time Series Graph](#)
- [Cards](#)

Insight Summary

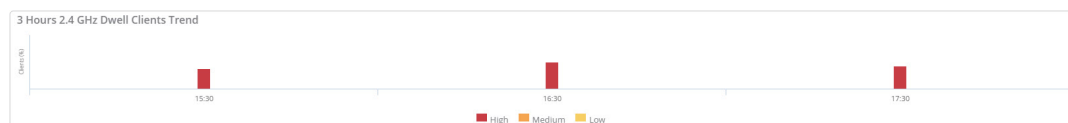
The insight summary provides the following details:

- **Reason**—Displays the possible causes for which the client is excessively dwelling in the 2.4 GHz band in the network.
- **Recommendation**—Displays the recommendation against each cause to resolve the same.

Time Series Graph

This bar graph displays the percentage of clients over dwelling in the 2.4 GHz band in the network during the selected time period. Hover your mouse on each bar graph to see the exact percentage of the dwelling time. The following graph shows data trend for 3 hours in a day.

Figure 40 *Clients with Excessive 2.4 GHz Dwell Time Data*




Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 111: *Cards Context*


Cards	Context
Site	Global
Access Point	Global, Site
Client	Global, Site, Device

Site

Lists the number of sites where the clients are dwelling excessively in the 2.4 GHz band. Click the arrow  to view the pictorial graph of the **Top 5** 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.
- **Clients Impacted**—Number of clients in each site that is excessively dwelling in the 2.4 GHz band.
- **APs Impacted**—Number of APs impacted by the insight in each site.


Access Point

Lists the number and details of APs where the clients are dwelling excessively in the 2.4 GHz band. Click the arrow  to view the pictorial graph of the **Top 5** impacted access points. 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 **Access Point Details** page.
- **AP MAC**—MAC address of the AP.
- **AP Serial**—Serial number of the AP.
- **AP Model**—Model number of each AP.

- **Site**—Name of the site where the AP resides.
- **Total Clients**—Total number of clients connected to each AP.
- **Clients with Excess 2.4 GHz Dwell**—Number of clients that is dwelling excessively on 2.4 GHz band.

Client

Lists the MAC Address, name, host name, auth ID, and the corresponding percentage of time spent for each client in the radio bands. Click the arrow  to view the pictorial graph of the **Top 5** impacted clients. Click the **Client** drop-down list, to view the following:

- **Client Type**—Pictorial graph of the percent of clients dwelling in the 2.4 GHz band sorted by client device type.

Click the number displayed on the **Client** card, to view a detailed description of the impacted clients:

- **Client Name**—Name of the client impacted by the insight.
- **Client MAC**—MAC address of the client impacted by the insight and link to the **Client Details** page.
- **Device Type**—Clients dwelling in the 2.4 GHz band sorted by client device type.
- **Site**—Name of the site where the client resides.
- **2.4 GHz Dwell Minutes**—Duration of each client dwelling in the 2.4 GHz band.
- **5 GHz Dwell Minutes**—Duration of each client dwelling in the 5 GHz band.
- **Total Dwell Minutes**—Total duration of each client dwelling on both the bands.
- **Dwell Time in 2.4 GHz (%)**—Percentage of the time of each client dwelling on 2.4 GHz band.

Delayed DNS Request or Response

The **DNS request/responses were significantly delayed** insight can be accessed from the **Global**, **Site**, **Access Points**, and **Clients** context. This insight provides information on significant delays in response from the DNS servers. It is categorized under connectivity since there is a high delay in response from the DNS server. This insight displays the following information:

- [Time Series Graph](#)
- [Cards](#)

Time Series Graph

This bar graph displays the number of delays from the DNS server that occurred during the selected time. Hover your mouse on each bar graph to see the exact number of delays. The following graph shows data trend for seven days (1 Week).

Figure 41 *Excessive DNS Delays Data*




Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 112: Cards Context


Cards	Context
Site	Global
Server	Global, Site, Device
Access Point	Global, Site

Site

Lists the number sites that experience delays from the DNS server in the network. Click the arrow  to view the pictorial graph of the **Top 5** 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.
- **Min (ms)**—Packet latency (delay) is measured. The lowest value of delay in the measurement interval is the minimum response delay.
- **Avg (ms)**—Packet latency (delay) is measured. The average value of delay in the measurement interval is the minimum response delay.
- **Max (ms)**—Packet latency (delay) is measured. The maximum value of delay in the measurement interval is the maximum response delay.

Server

Lists the number of DNS servers involved in this insight. Click the arrow  to view the pictorial graph of the **Top 5** impacted servers. Click the number displayed on the **Server** card, to view a detailed description of the impacted servers:

- **Server IP**—IP address of each server.
- **Avg (ms)**—Packet latency (delay) is measured. The average value of delay in the measurement interval is the minimum response delay.
- **Min (ms)**—Packet latency (delay) is measured. The lowest value of delay in the measurement interval is the minimum response delay.
- **Max (ms)**—Packet latency (delay) is measured. The maximum value of delay in the measurement interval is the maximum response delay.

Access Point

Lists the number and details of APs that has the most DNS response delays. Click the arrow  to view the pictorial graph of the **Top 5** impacted access points. 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 **Access Point Details** page.
- **AP MAC**—MAC address of the AP and link to the **Access Point Details** page.
- **AP Serial**—Serial number of the AP.
- **Avg (ms)**—Packet latency (delay) is measured. The average value of delay in the measurement interval is the minimum response delay.

- **Min (ms)**—Packet latency (delay) is measured. The lowest value of delay in the measurement interval is the minimum response delay.
- **Max (ms)**—Packet latency (delay) is measured. The maximum value of delay in the measurement interval is the maximum response delay.
- **Servers**—Server ID where the AP resides.
- **Model**—Model number of each AP.
- **Firmware**—Version of the firmware running on each AP.
- **Site**—Name of the site where the AP resides.

DNS Servers Rejected High Number of Queries

The **DNS server(s) rejected a high number of queries** insight can be accessed from the **Global, Site, Access Points, and Clients** context. This insight provides information on excessive request failures from the DNS servers. It is categorized under connectivity as there are high number of request failures. This insight displays the following information:

- [Insight Summary](#)
- [Time Series Graph](#)
- [Cards](#)

Insight Summary

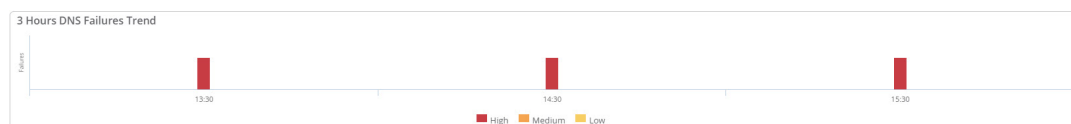
The insight summary provides the following details:

- **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

This bar graph displays the number of request failures from the DNS server that occurred during the selected time. Hover your mouse on each bar graph to see the exact number of failures. The following graph shows data trend for 3 hours in a day.

Figure 42 *Excessive DNS Request Failures Data*




Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 113: Cards Context


Cards	Context
Site	Global
Server	Global, Site, Device
Access Point	Global, Site

Site

Lists the number sites that experience request failures from the DNS server in the network. Click the arrow  to view the pictorial graph of the **Top 5** 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.
- **Total Failures(%)**—Total number of failure packets at the site multiplied by 100.
- **Query Attempts**—Number of query attempts sent to the DNS server in a site.
- **Query Success(%)**—Percentage of successful DNS queries in a site.
- **Query Format Error**—Error in the DNS query format sent to the DNS server in a site.
- **Request Failed to Complete**—DNS request failed to complete, and the server responds with an error code.
- **Domain Name Does Not Exist**—Domain name sent to the DNS server does not exist and the server responds with an error code
- **Function Not Implemented**—Function is not implemented on the DNS server and the server responds with an error code.
- **Server Refused to Answer Query**—Server refused to answer the query and responds with an error code.

Server

Lists the number of servers that has the most number of DNS request rejections. Click the arrow  to view the pictorial graph of the **Top 5** 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.
- **Total Failures(%)**—Total number of failure packets at the site multiplied by 100.
- **Query Attempts**—Number of query attempts sent to the DNS server.
- **Query Success(%)**—Percentage of successful DNS queries.
- **Query Success**—DNS server query responds successfully.
- **Query Format Error**—Error in the DNS query format sent to the DNS server in a site.
- **Request Failed to Complete**—DNS request failed to complete, and the server responds with an error code.
- **Domain Name Does Not Exist**—Domain name sent to the DNS server does not exist and the server responds with an error code
- **Function Not Implemented**—Function is not implemented on the DNS server and the server responds with an error code.
- **Server Refused to Answer Query**—Server refused to answer the query and responds with an error code.

Access Point

Lists the number and details of access points that has the most DNS request rejections. Click the arrow  to view a pictorial graph of the **Top 5** impacted access points. Click the **Access Point** drop-down list to view the following:

- **Success Rate**—Graphical representation of the total failures and total successful requests that occurred at the server.

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 **Access Point Details** page.
- **AP MAC**—MAC address of the AP and link to the **Access Point Details** page.
- **AP Serial**—Serial number of the AP.
- **Total Failures(%)**—Total number of failure packets at the site multiplied by 100.
- **Query Attempts**—Number of query attempts sent to the DNS server in each AP.
- **Query Success(%)**—Percentage of successful DNS queries in each AP.
- **Query Format Error**—Error in the DNS query format sent to the DNS server in each AP.
- **Request Failed to Complete**—DNS request failed to complete, and the server responds with an error code.
- **Domain Name Does Not Exist**—Domain name sent to the DNS server does not exist and the server responds with an error code
- **Function Not Implemented**—Function is not implemented on the DNS server and the server responds with an error code.
- **Server Refused to Answer Query**—Server refused to answer the query and responds with an error code.
- **Site**—Name of the site where the AP resides.

Gateways with High CPU Utilization

The **Gateways had unusually high CPU utilization** insight can be accessed from the **Global**, **Site**, and **Gateways** context. This insight provides information about gateways that have higher than normal CPU utilization. It is categorized under availability since the clients connected to these gateways experience intermittent connectivity drops. This insight displays the following information:

- [Time Series Graph](#)
- [Cards](#)

Time Series Graph

The time series graph displays the percentage of impacted gateways in the network during the selected time period. You can hover your mouse on each bar graph to see the percentage of impacted gateways.

Cards


The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 114: Cards

Context


Cards	Context
Site	Global
Gateway	Global, Site
CPU	Device

Site

Lists the number of sites where the gateways experience high CPU utilization. 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.
- **Number of Gateways**—Number of gateways that experience high CPU utilization in each site.
- **Duration (mins)**—Amount of time (minutes) high CPU utilization observed in each site.

Gateway


Lists the number and details of gateways that experience high CPU utilization in the network. Click the arrow  to view the pictorial graph of the **Most Impacted** gateways. Click the **Gateway** drop-down list, to view the following:

- **Gateway Model**—Pictorial graph of CPU utilization classified by gateway models.
- **FW Version**—Pictorial graph of CPU utilization classified by gateway firmware versions.
- **Mode**—Operational mode of the gateway.

Click the number displayed on the **Gateway** card to view a detailed description of the impacted gateways:

- **Serial**—Serial number of each gateway and link to the specific insight at the gateway context.
- **Gateway Name**—Name of the gateway that experience high CPU utilization.
- **Mode**—Operational mode of the gateway.
- **Max CPU**—Rate of maximum CPU utilization observed in each gateway.
- **Minutes with High CPU**—Amount of time (minutes) high CPU utilization observed in each gateway.
- **Model**—The hardware model of each gateway.
- **FW Version**—Version of the firmware running on each gateway.
- **Site**—Name of the site where the gateway resides.

CPU

CPU card is displayed only when this insight is accessed from the device context. Click the arrow  to expand the card and view the graphical representation of the time series of CPU utilization percentage in the selected gateway.

Gateways with High Memory Usage

The **Gateways had high Memory usage** insight can be accessed from the **Global**, **Site**, and **Gateways** context. This insight provides information about gateways that have higher than normal memory utilization. It is categorized under availability since the clients connected to these gateways experience intermittent connectivity drops. This insight displays the following information:

- [Time Series Graph](#)
- [Cards](#)

Time Series Graph

The time series graph displays the percentage of impacted in the network during the selected time period. You can hover your mouse on each bar graph to see the percentage of impacted gateways.

Cards


The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 115: *Cards*

Context


Cards	Context
Site	Global
Gateway	Global, Site
Memory	Device

Site

Lists the number of sites where the gateways experience high memory utilization. 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.
- **Number of Gateways**—Number of gateways that experience high memory utilization in each site.
- **Duration (mins)**—Amount of time (minutes) high memory utilization observed in each site.

Gateway


Lists the number and details of gateways that experience high memory utilization in the network. Click the arrow  to view the pictorial graph of the **Most Impacted** gateways. Click the **Gateway** drop-down list, to view the following:

- **Gateway Model**—Pictorial graph of memory utilization classified by gateway models.
- **FW Version**—Pictorial graph of memory utilization classified by gateway firmware versions.
- **Mode**—Operational mode of the gateway.

Click the number displayed on the **Gateway** card to view a detailed description of the impacted gateways:

- **Serial**—Serial number of each gateway and link to the specific insight at the gateway context.
- **Gateway Name**—Name of the gateway that experience high memory utilization.
- **Mode**—Operational mode of the mode.
- **Max Memory**—Maximum memory consumed by the gateway.
- **Minutes with High Memory**—Amount of time (minutes) high memory utilization observed in each gateway.
- **Model**—Model number of each gateway.
- **FW Version**—Version of the firmware running on each gateway.
- **Site**—Name of the site where the gateway resides.

Memory

Memory card is displayed only when this insight is accessed from the device context. Click the arrow  to expand the card and view the graphical representation of the time series of memory utilization percentage in the selected gateway.

Failure to Establish Gateway Tunnels

The **Gateway tunnels failed to get established** insight can be accessed from the **Global**, **Site**, and **Gateways** context. This insight provides information about gateway tunnels that are marked down in the network. It is categorized under availability since the clients connected to these gateways experience connectivity drops.



Gateway Tunnels Down insight is available for branch and VPNC gateways in the network.

Tunnels are marked down in the network based on the following scenarios:

- If Aruba Central receives telemetry from branch gateway that a specific tunnel is down
- If Aruba Central receives telemetry from the VPNC that a specific tunnel is down
- Lack of telemetry from both branch and VPNC gateway

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 tunnel down in the network.
- **Minutes Down**—Displays the exact number and percentage of tunnel down that occurred against each failure reason.

Time Series Graph

The time series graph displays the percentage and number of tunnels down in the network during the selected time period. You can hover your mouse on each bar graph to see the exact percentage of tunnels down.


Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 116: *Cards Context*


Cards	Context
Site	Global
Gateway	Global, Site
VPNC	Global, Site, Device
Tunnel	Global, Site, Device

Site

Lists the number of sites where the gateways experience tunnel down. Click the arrow  to expand the card and 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.
- **Number of Down Tunnels**—Number of tunnels down in each site that experience high memory utilization in each site.
- **Total Tunnels**—Total number of gateway tunnels in each site.
- **Number of Impacted Gateways**—Number of gateways impacted by tunnel down in each site.
- **Number of Impacted VPNC**—Number of VPNC gateways that experience tunnel down in each site.

Gateway

Lists the number and the reason for the cause of tunnel down in gateways. Click the arrow  to expand the card and click the number displayed on the **Gateway** card to view a detailed description of the impacted gateways:

- **Serial**—Serial number of each gateway and link to the **Gateway Details** page.
- **Gateway Name**—Name of the gateway that experience tunnel down.
- **Mode**—Operational mode of the gateway.
- **Number of Tunnels**—Number of tunnels down in each gateway.
- **Total Tunnels**—Total number tunnels in each gateway.
- **Duration (mins)**—Time range of tunnel down in each gateway.
- **Model**—The hardware model number of the gateway.
- **FW Version**—Version of the firmware running on each gateway.
- **Site**—Name of the site where the gateway resides.


VPNC

Displays the total number of VPNC gateways experiencing tunnel down. Click the arrow  to expand the card and view the amount of time (minutes) and the reasons for the cause of down tunnels on the VPNC gateways.

Click the number displayed on the **VPNC** card to view a detailed description of the impacted VPNC gateways:

- **Serial**—Serial number of each gateway and link to the specific insight at the gateway context.
- **Gateway Name**—Name of the gateway that experience tunnel down.
- **Mode**—Operation mode of the VPNC.
- **Total Number of Tunnels Down**—Number of tunnels down in each gateway.
- **Total Number of Tunnels**—Number of tunnels down in each gateway.
- **Number of Gateways**—Number of gateways impacted by tunnel down.
- **Number of Sites**—Number of site impacted by tunnel down.
- **Duration (mins)**—Time range of tunnel down in each gateway.
- **Model**—The hardware model number of the gateway.
- **FW Version**—Version of the firmware running on each gateway.
- **Site**—Name of the site where the gateway resides.

Tunnel

Displays the total number of gateways experiencing tunnel down. Click the arrow  to expand the card to view the amount of time (minutes) and the reasons for the cause of tunnel down in the network.

Click the number displayed on the **Tunnel** card to view a detailed description of the impacted tunnels:

- **Site**—Name of the site where the tunnel residee and link to the specific insight at the site context.
- **Gateway IP**—IP address of the impacted gateway.
- **VPNC IP**—IP address of the impacted VPNC gateway.
- **Duration (mins)**—Time range of tunnel down.
- **Gateway VLAN**—VLAN ID of the gateway.
- **VPNC VLAN**—VLAN ID of the VPNC.
- **Gateway Name**—Name of the gateway where the tunnel is down.
- **Gateway MAC**—MAC address of the impacted gateway.
- **VPNC Name**—Name of the VPNC gateway where the tunnel is down.
- **VPNC MAC**—MAC address of the impacted VPNC gateway.
- **Gateway Serial**—Serial number of the gateway and link to the specific insight at the gateway context.
- **VPNC Serial**—Serial number of VPNC gateway.

DNS Queries Failed to Reach or Return from the Server

The **DNS queries failed to reach or return from the server** insight can be accessed from the **Global**, **Site**, and **Access Points** context. This insight provides information about wireless APs that experience a higher than normal number of connection failures with the DNS server. It is categorized under connectivity since the wireless clients are unable to reach the destination URL. This insight displays the following information:

- [Insight Summary](#)
- [Time Series Graph](#)
- [Cards](#)

Insight Summary

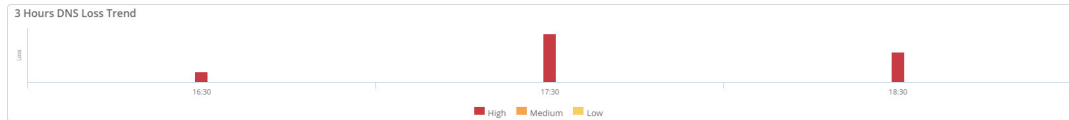
The insight summary provides the following details:

- **Reason**—Displays the possible causes for which the failure occurred.
- **Recommendation**— Displays the possible recommendation against each failure to resolve the same.

Time Series Graph

This bar graph displays the number of connection loss with the DNS server that occurred during the selected time. Hover your mouse on each bar graph to see the exact number of loss. The following graph shows data trend for 3 hours in a day.

Figure 43 High Number DNS Loss Data




Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 117: Cards Context


Cards	Context
Site	Global
Server	Global, Site, Device
Access Point	Global, Site

Site

Lists the number sites that experience connection loss with the DNS server in the network. Click the arrow  to view the pictorial graph of the **Top 5** 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.
- **Lost DNS Queries (%)**—Total count of the DNS packets that get lost in the network. DNS server does not receive these packets.
- **Denied DNS Queries**—Number of packets that reach the DNS server but, the server returns error code in a site.
- **Successful DNS Queries**—Total count of packets that reach the DNS server and responds successfully in a site
- **Total Queries**—Total number of successful DNS queries, denied DNS queries, and lost queries in the DNS server.

Server

Lists the number of servers that has higher number of DNS connection failures. Click the arrow  to view the pictorial graph of the **Top 5** 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.
- **Lost DNS Queries (%)**—Total count of the DNS packets that get lost in the network. DNS server does not receive these packets.
- **Total Queries**—Total number successful DNS queries, denied DNS queries, and lost queries in the DNS server.

Access Point

Lists the number and details of APs that has higher number of DNS connection failures. Click the arrow  to view a pictorial graph of the **Top 5** impacted access points. Click the **Access Point** drop-down list to view the following:

- **Success Rate** Graphical representation of the total failures and total successful requests that occurred at the AP.

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 **Access Point Details** page.
- **AP MAC**—MAC address of the AP and link to the **Access Point Details** page.
- **AP Serial**—Serial number of the AP.
- **Lost DNS Queries (%)**—Total count of the DNS packets that get lost in the network. DNS server does not receive these packets.
- **Total Queries**—Total number successful DNS queries, denied DNS queries, and lost queries in the DNS server.
- **Model**—Model number of each AP.
- **Firmware**—Version of the firmware running on each AP.
- **Site**—Name of the site where the AP resides.

Telemetry Information not Received from APs or Radios

The **Information (telemetry) was not received from APs/Radios** insight can be accessed from the **Global**, **Site**, and **Access Points** context. This insight provides information about AP radios that missed sending telemetry data to Aruba Central and is categorized under availability since AI insights loses visibility of the APs. This insight displays the following information:

- [Time Series Graph](#)
- [Cards](#)

Time Series Graph

This bar graph displays the number of 2.4 GHz and 5 GHz radios that failed to send telemetry data during the selected time period. Hover your mouse over each bar graph to see the exact number of missing radios. The following graph shows data trend for 3 hours in a day.

Figure 44 APs with Missing Telemetry Data




Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 118: *Cards Context*


Cards	Context
Site	Global
Access Point	Global, Site

Site

Lists the number of sites where the APs experience missing telemetry. Click the arrow  to view the pictorial graph of the **Top 5** 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.
- **Radios Impacted**—Number radio channels that missed telemetry data.
- **Minutes Missing**—Time range of missing telemetry in each site.
- **Hours Missing**—Hourly data of the missing telemetry in each site.

Access Point

Lists the number and details of APs that experience missing telemetry. Click the arrow  to view the pictorial graph of the **Top 5** impacted access points. 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 **Access Point Details** page.
- **AP MAC**—MAC address of the AP and link to the **Access Point Details** page.
- **AP Serial**—Serial number of the AP.
- **Firmware**—Version of the firmware running on each AP.
- **AP Model**—Model number of each AP.
- **Site Name**—Name of the site where the AP resides.
- **Minutes Missing in 2.4 GHz**—Time range (minutes) of missing telemetry in 2.4 GHz band.
- **Hours missing in 2.4 GHz**—Time range (hours) of missing telemetry in 2.4 GHz band.
- **Minutes missing in 5 GHz**—Time range (minutes) of missing telemetry in 5 GHz band.
- **Hours missing in 5 GHz**—Time range (hours) of missing telemetry in 5 GHz band.

Outdoor Clients Impacting Wi-Fi Performance

The **Outdoor clients are impacting Wi-Fi performance** insight can be accessed only at the **Global** context. The intention of this insight is to understand which outdoor clients are affecting the performance of the indoor network. **Outdoor clients are impacting Wi-Fi performance** insight provides information about the optimum Probe/Auth SNR Threshold value and recommended config value for Probe/Auth SNR Threshold below which APs ignore Probe Requests and Authentication Requests from far away clients. It is triggered when the Probe SNR threshold is not set optimally. Following are the recommendation scenarios:

- If the SNR Threshold value is below 8dBm, it is set back to 8dBm
- If the SNR Threshold value is anything higher than 16dBm, it is set back to 16dBm
- If the SNR Threshold is between 8dBm and 16dBm, no recommendation is provided
- If the recommended threshold value is in the range of +3 or -3, no recommendation will be provided since there might be very few clients in the network or there might be some genuine users in that range

It is categorized under wireless quality as low SNR clients (outdoor) experience poor Wi-Fi connectivity and this in return affects other clients on the AP, which have good SNR connections. This insight displays the following information:

- [Insight Summary](#)
- [Cards](#)

Insight Summary

The insight summary provides the following details:

- **Reason**—Clients connected to the wireless network at low SNR.
- **Recommendation**—Change the Probe RSSI threshold and the Auth RSSI threshold to the recommended value to improve the indoor Wi-Fi client experience.


Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 119: *Cards Context*

Cards	Context
Client	Global
Client Minute	Global

Client

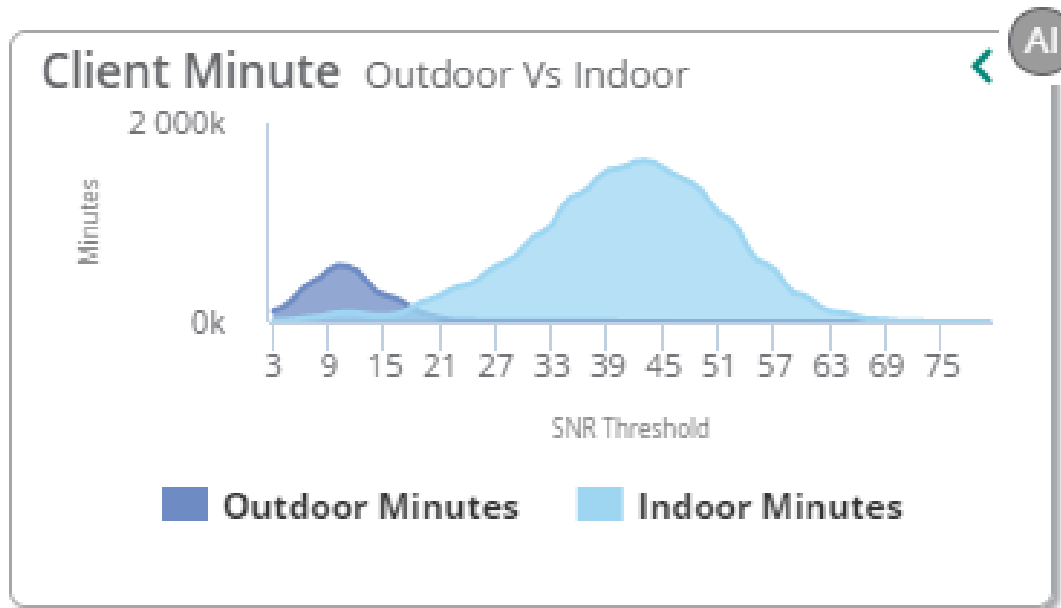
Lists the MAC Address, name, host name, auth ID, and the total number of clients below the proposed SNR threshold. Click the arrow  to view the pictorial graph of the **Top 5** impacted clients. Click the number displayed on the **Client** card, to view a detailed description of the impacted clients:

- **Client Name**—Number of the impacted client and link to the **Client Details** page.
- **Client MAC**—MAC address of the impacted client.
- **OS**—OS type of the device.
- **Site**—Name of the site where the client resides.
- **Duration (mins)**—Number of minutes client was outside below the recommended Probe SNR/ Auth threshold.

Client Minute

Display the percentage of avoided outdoor clients minutes and affected indoor client minutes in a chart. The graph also shows current and the recommended threshold (dBm) for each client type in the network. In order to rectify the issue, the Probe SNR threshold must be set to the recommended value. This frees up airtime and AP resources for indoor users.

Figure 45 Probe SNR Threshold Graph



Monitoring Gateways in List View	393
Monitoring Gateways in Summary View	394
Monitoring Gateway Clusters	395
Gateway Cluster > Overview > Summary	396
Gateways Cluster > Overview > Gateways	397
Gateway Cluster > Overview > Tunnels	398

The Network Operations app provides detailed gateway cluster monitoring pages and tools that provide gateway cluster health, client load, and redundancy information.

Monitoring Gateways in List View

The **List** view for gateways is available from the **Global**, **Groups**, **Sites**, and **Labels** dashboards.

Viewing the Gateways Page

To navigate to the **Gateways** 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 gateway. The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Gateways**. A list of gateways is displayed in the **List** view.

The Gateway List page displays the following second-level tabs:

- **Gateways**—Displays the total number of gateways. When you click the **Gateways** tab, it provides information about all gateways in the **Gateways** table.
- **Online**—Displays the total number of online gateways. When you click the **Online** tab, it provides information about the online gateways in the **Gateways** table.
- **Offline**—Displays the total number of offline gateways. When you click the **Offline** tab, it provides information about the offline gateways in the **Gateways** table.
- **Clusters**—Displays the total number of clusters. For more information on radios in the list view, see [Monitoring Gateway Clusters](#).

The Gateways Table

The **Gateways** table in the second-level tab for **Gateways**, **Online** and **Offline** displays the following information:

- **Device Name**—Displays the gateway name.
- **Model**—Displays the model of the gateway.
- **Firmware Version**—Displays the firmware version of the gateway.

- **Uptime**—Displays the time period for which the gateway has been functioning.
- **IP Address**—Displays the IP address of the gateway.
- **Site**—Displays the site information.
- **MAC**—Displays the MAC address of the gateway.
- **Group**—Displays the gateway group name.
- **Labels**—Displays the labels assigned to the gateway.
- **Serial**—Displays the gateway serial number.

Click the download icon to download the gateways details as a .csv file.

Click the ellipsis icon to perform the following additional operations:

- Select the columns that you want to display in the table.
- Adjust the column width of the table to fit the page evenly.
- Reset the table view to the default columns.

Monitoring Gateways in Summary View

The **Summary** view for gateways is available from the **Global**, **Groups**, **Sites**, and **Labels** dashboards. In all applicable dashboards, the **Summary** view is under **Manage > Devices > Gateways**. Displays a graphical representation of the gateway operations.

Viewing the Gateway Summary Page

To view the summary of gateways, 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 selected option has at least one gateway configured. The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Gateways**. A list of gateways is displayed in the **List** view.
3. Click the **Summary** icon. A graphical representation of the gateway operations is displayed.

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**, and **3 months**.



NOTE

If you have just set up a gateway, you may not see relevant data immediately.

Summary View

The **Summary** view displays a graphical representation for the following:

- **Usage**—Displays the overall usage metrics for the gateways provisioned in your Aruba Central account. Displays the incoming and outgoing traffic for the gateways with time plotted on the x-axis. You can hover over the chart to see the incoming and outgoing traffic for a particular time frame.
- **WAN Compression**—Displays the data packet compression statistics for the WAN network. You can view the compressed, uncompressed, and saved bandwidth. By default, traffic between the Branch Gateway and VPN Concentrator is subject to compression. You can hover over the chart to see the compressed and uncompressed statistics for a particular time frame.
- **WAN Tag Provider Distribution**—Displays the number of online and offline uplinks per WAN provider.

- **WAN Transport Health**—Displays the Mean Opinion Score (MOS) score trends for each uplink for the selected time range. The uplink health trend is plotted using health indicators such as Good, Fair, and Poor. You can hover over the chart to see the uplink scores for a particular time frame. Click an uplink name to show or hide MOS score trends for that uplink.
- **WAN Type Provider Distribution**—Displays the number of online and offline uplinks per WAN circuit type.
- **Model Distribution**—Displays the total percentage of gateways distributed per hardware platform. You can hover over a donut slice to display the percentage for a specific hardware model. Click a hardware platform number to show or hide the distribution percentage for that platform.
- **Firmware Distribution**—Displays the total percentage of gateways distributed by software versions. Click a firmware number to show or hide the distribution percentage for that firmware.

Monitoring Gateway Clusters

The Gateway Cluster dashboard displays a list of Gateway clusters provisioned and managed using Aruba Central.

To view a list of Gateway clusters:

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 Gateway cluster. The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Gateways**. A list of gateways is displayed in the **List** view.
3. Click **Clusters**.

The Gateway Clusters table is displayed that contains the following information:

Table 120: *Gateway Clusters Table*

Table Content	Description
Name	Name of the cluster. On clicking the name, the cluster dashboard is displayed. A green dot indicates that the nodes in the cluster are up and running. A small red circle indicates that one or more of the nodes in the cluster are down.
Group	Name of the group to which the gateways in the cluster belongs.
AP Tunnel	Number of tunnels established between the APs and Gateway cluster.
Clients	Number of WLAN clients connected to the Gateways in the cluster.
Model	The hardware model of the Gateway.
Site	Name of the site in which the cluster is deployed.
Version	The ArubaOS software version running on Gateways in the cluster.
Hitless Failover	Indicator to show if the cluster can support a hitless failover; that is, that ability to provide uninterrupted services in the event of a failover. In a Gateway cluster, if the User Designated Gateway (UDG) fails, another member in the cluster takes over to provide uninterrupted service to APs and clients. If the failover does not impact the AP or client connectivity, it is referred to as a hitless failover.

Table 120: *Gateway Clusters Table*

Table Content	Description
Max Gateway Failover	Maximum failover events supported.

Viewing Gateway Members in a Cluster

To view the members of a cluster, in the **Gateway Cluster** table, click the expand icon. On expanding a Gateway cluster list, the following details are displayed:

- **Gateway Name**—Name of the Gateway. On clicking the Gateway name, the Gateway dashboard is displayed.
- **AP Tunnel**—Number of tunnels established between the Gateway and APs.
- **Clients**—Number of clients connected to the Gateway.
- **Model**—The hardware model of the Gateway.
- **Site**—Name of the site in which the cluster is deployed.
- **Version**—The ArubaOS Software version of the Gateway.
- **MAC Address**—The MAC address of the device.
- **IP Address**—The IP address of the device.

Viewing Details of a Cluster

To view information about the Gateway peers and tunnels, click the name of the cluster in the **Gateway Clusters** table. A Gateway cluster dashboard with the following tabs is displayed:

- [Gateway Cluster > Overview > Summary](#)
- [Gateways Cluster > Overview > Gateways](#)
- [Gateway Cluster > Overview > Tunnels](#)

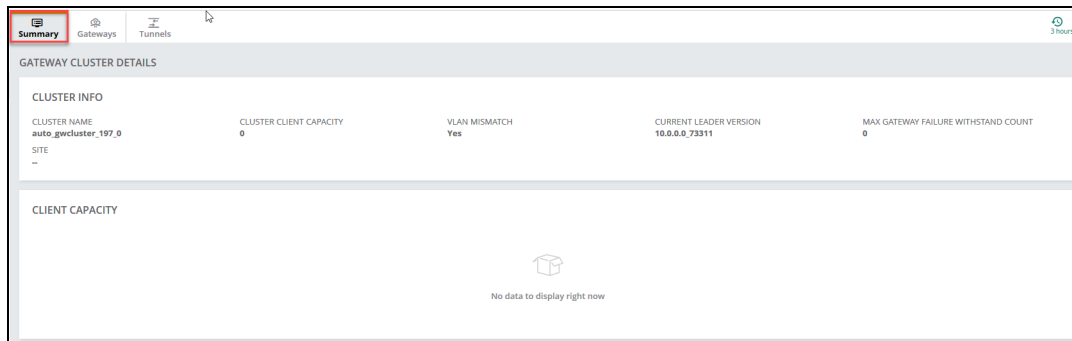
Gateway Cluster > Overview > Summary

To view the **Summary** 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 Gateway cluster. The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Gateways**. A list of gateways is displayed in the **List** view.
3. Click **Clusters**.

The Gateway Clusters table is displayed. Click the name of the gateway cluster to open the **Summary** tab.

Figure 46 Gateway Clusters - Summary tab



The **Summary** tab in the Gateway Cluster dashboard displays the following information:

Table 121: Gateway Cluster Details Page—Overview Tab

Tab Content	Description
Cluster Info	<p>The Cluster Info panel displays the following information:</p> <ul style="list-style-type: none"> ■ Cluster Name—Name of the cluster. ■ Cluster Client Capacity—Number of clients supported by the cluster. ■ VLAN Mismatch—VLAN mismatch in the Gateway cluster if any. ■ Current Leader Version—The ArubaOS software version that is currently running on the Gateway elected as a leader in the cluster. ■ Max Gateway Failure Withstand Count—The maximum number of failures that the Gateways in the cluster can withstand. ■ Max Cluster Gateway Size—The maximum number of Gateways allowed in the cluster.
Client Capacity	<p>The Client Capacity panel displays the percentage of the total client capacity of the cluster that is in use and the percentage of the client capacity used by each Gateway in the cluster. The bullet icons indicate the various client capacity utilization (in percentage) used by the controller.</p>

Gateways Cluster > Overview > Gateways

To view the **Gateways** 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 Gateway cluster. The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Gateways**. A list of gateways is displayed in the **List** view.
3. Click **Clusters**. The Gateway Clusters table is displayed.
4. Click the name of the cluster and click the **Gateways** tab.

The **Gateways** tab in the Gateway Cluster dashboard displays the following information:

Figure 47 Gateway Clusters - Gateway tab

GATEWAYS (3)						
Gateway Name	IP Address	Status	Client Capacity (Active Standby)	Model	Role	Version
7210-US-001A1E:02:65:D0	10.16.136.4	Down	0 (0 0)	A7210	Isoleader	10.0.0.2_75827
7240	10.15.13.71	Down	0 (0 0)	A7240	Isoleader	10.0.0.0_73311
dot9_c2x_7008	10.16.136.9	Down	0 (0 0)	A7008	Member	10.0.0.0_73311

GATEWAY PEER DETAIL (2)				
Type	IP Address	Status	Role	VLAN Mismatch
SELF	10.16.136.4	-	Isoleader	-
PEER	10.16.136.9	Disconnected	Member	-

Table 122: Gateway Cluster Details Page—Gateways Tab

Tab Content	Description
Gateways	<p>Displays the total number of Gateways and the following information for each controller component in the cluster:</p> <ul style="list-style-type: none"> ■ Gateway Name—Name of the Gateway. ■ IP Address—IP address of the Gateway. ■ Status—Operational status of the Gateway. ■ Client Capacity(Active Standby)—Client capacity indicator for active and standby members in a cluster. ■ Model—The hardware model of the Gateway. ■ Role—The role of the Gateway. The value can be Leader or Member. ■ Version—The ArubaOS software version running on the Gateway.
Gateway Peer Detail	<p>Displays a list of the peer Gateways in a cluster.</p> <ul style="list-style-type: none"> ■ Type—Type of peer. Value can be Self or Peer. ■ IPv4 Address—IPv4 address of the Gateway. ■ Status—Operational status of the Gateway. ■ Connection Type—Type of connection; for example L2 connected. ■ Role—Role of the Gateway. The value can be Leader or Member. ■ VLAN Mismatch—Conveys if there is a mismatch in the VLAN configurations between the Gateway and the peer.

Gateway Cluster > Overview > Tunnels

To view the **Tunnels** 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 Gateway cluster. The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Gateways**. A list of gateways is displayed in the **List** view.
3. Click **Clusters**. The Gateway Clusters table is displayed.
4. Click the name of the cluster and click the **Tunnels** tab.

The **Tunnels** tab in the Gateway Cluster dashboard displays the following information:

Figure 48 Gateway Clusters - Tunnels tab

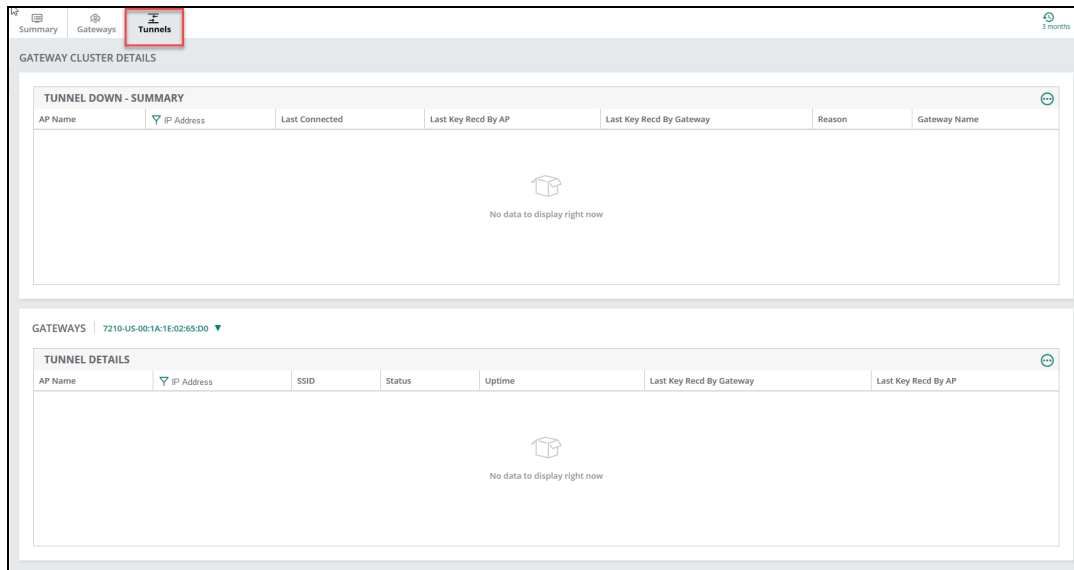


Table 123: Gateway Cluster Details Page—Tunnels Tab

Table Content	Description
Tunnel Down - Summary	<p>Displays a list of overlay tunnels that are currently down. The table displays the following information:</p> <ul style="list-style-type: none"> ■ AP Name—Name of the AP that initiated a tunnel to the Gateway cluster. ■ IP address—IP address of the Gateway cluster. ■ Last connected—The timestamp of the last connection. ■ Last Key Recd by AP—The last key received by the AP. ■ Last Key Recd by Gateway—The last key received by the Gateway. ■ Reason—Possible reason for the failed connection. ■ Gateway Name—Name of the Gateway in the cluster to which the APs initiated a tunnel.
Tunnel Details	<p>The Tunnel Details panel displays the following information:</p> <ul style="list-style-type: none"> ■ AP Name—Name of the AP. ■ IP Address—IP address of the AP. ■ SSID—SSID configured on the AP. ■ Status—The current Status of the tunnel. ■ Uptime—The duration for which the tunnel is active. ■ Last Key Recd By Gateway—Details of the last key recd by Gateway. ■ Last Key Recd By AP—Details of the last key received by the AP.

Monitoring APs in Summary View	400
Monitoring APs in List View	401
Access Point > Overview > Summary	407
Viewing the Overview > Summary Tab	407
Actions	412
Go Live	412
Access Point > Overview > AI Insights	412
Access Point > Overview > Floor Plan	413
Access Point > Overview > Performance	414
Access Point > Overview > RF	415
Access Point > Security > VPN	416
Rebooting an AP	417
Tech Support for an AP	417
Opening a Remote Console	418
Enabling Live AP Monitoring	418
AP Live Events	419

The Network Operations app provides detailed access points (APs) monitoring pages and tools that provide health, client load, and other information.

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.

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 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 APs in List View

The access point (AP) List page provides information associated with the APs provisioned and managed in Aruba Central.

The AP List page is available for Foundation and Advanced licenses for APs.

The AP List page displays the following sections:

- [Access Points Table](#)
- [Deleting an Offline AP](#)
- [Rebooting an AP](#)

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. For more information on radios in the list view, see [Monitoring Radios in List View](#).



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 AP](#).
- **Virtual Controller**—Name of the Virtual Controller.
- **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.
- **Gateway Cluster**—The name of the gateway cluster associated with the AP. Click the gateway cluster name to go to the **Overview > Summary** page for that gateway cluster.
- **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.
- **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.
- **LLDP Port**—Displays the port number of LLDP neighbor.
- **AI Insights**—The number of AI 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.

Important Information

- A search filter is provided only for the **Device Name**, **IP Address**, **Virtual Controller**, **Model**, **Serial**, **MAC Address**, **Group**, **Labels**, **Site**, **LLDP Neighbor**, **Note**, and **Zone** columns. The  and  icons allow you to sort the **Device Name**, **IP Address**, **Serial**, **MAC Address**, 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, Gateway Cluster, Config Status, Group, Labels, Site, Uptime, Last Seen, Public IP, LLDP Neighbor, LLDP Port, 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.
13. Click **Finish** to import the data into Microsoft Excel 2007.



Importing one or more columns is optional.

Deleting an Offline AP

To delete an offline AP, see [Deleting an Offline AP](#).


Rebooting an AP

To reboot an AP, see [Rebooting an AP](#).


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.
5. Click **Delete** in the confirmation dialog box.




To delete multiple offline APs, select the offline APs that you want to delete and click the  delete icon.

Rebooting an AP

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**. 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 online AP that you want to reboot.
4. Click the  reboot icon.
5. Click **Reboot** in the confirmation dialog box.



To reboot multiple online APs, select the online APs that you want to reboot and click the  reboot icon.

Thermal Shutdown Support in AP

ArubaAP-555 and AP-535 access point (AP) devices are equipped with an internal thermal sensor. The sensor initiates a shutdown when the operating temperature crosses the temperature threshold recommended for an AP. In standalone mode, when the AP operates beyond the recommended temperature threshold, the Virtual AP profile is disabled. Once the AP 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 AP 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**.
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.

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 AP, 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 AP. For example, **Thermal management enabled** or **Thermal management disabled**.

About Tri-Radio Mode

Aruba Central offers tri-radio mode support in Aruba AP-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.

The split 5 GHz radio can operate in the following modes:

- Access
- Monitor
- Spectrum

Enabling Tri-Radio Mode

To enable tri-radio, complete the following steps:

1. In the **Network Operations** app, select an AP-555 access point.
2. Under **Manage**, click **Device > Access Point**.
3. Click the **Edit** icon.
4. Click **Radio**.
5. Select the **Split Radio** check box.
6. Click **Save Settings**.

Enabling Second 5 GHz Radio

To enable tri-radio, complete the following steps:

1. In the **Network Operations** app, select an AP-555 access point.
2. Under **Manage**, click **Device > Access Point**.
3. Click the **Edit** icon.
4. Click **Radio**.
5. Under **Second 5 GHz Radio**, select the **Enable Radio** check box.
6. Click **Save Settings**.

Configuring Second 5 GHz Radio

To enable tri-radio, complete the following steps:

1. In the **Network Operations** app, select an AP-555 access point.
2. Under **Manage**, click **Device > Access Point**.
3. Click the **Edit** icon.
4. Click **Radio**.
5. Select **Access**, **Monitor**, or **Spectrum** from the **Mode** drop-down list.
6. Select **Automatic** or **Manual** radio button for **Channel Assignment**. If **Manual** is selected, select a value from the drop-down list. The second 5 GHz radio supports the following channels:
 - 100
 - 104
 - 108
 - 112
 - 116
 - 120
 - 124
 - 128
 - 132
 - 136
 - 140
 - 144
 - 149
 - 153
 - 157
 - 161
 - 165
 - 100+
 - 108+
 - 116+
 - 124+
 - 132+
 - 140+
 - 149+
 - 157+
 - 100E
 - 116E
 - 132E
 - 149E
 - 100S
7. Select **Automatic** or **Manual** radio button for **Transmit Power Assignment**. If **Manual** is selected, enter a value in dBm.
8. 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**.
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.
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.



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 AP Details page is available for Foundation and Advanced licenses for APs.

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 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.
 - **Group**—The group to which the AP belongs. Click the group name to go to the **Overview > Summary** page for that group.



NOTE

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**—Click **Blink LED** to enable the blinking of LEDs on the AP to identify the location. The default blinking time is set to 5 minutes and it stops automatically after 5 minutes. To stop the blinking of the AP, 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.
- **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.
- **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.

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 AP](#).
 - **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.



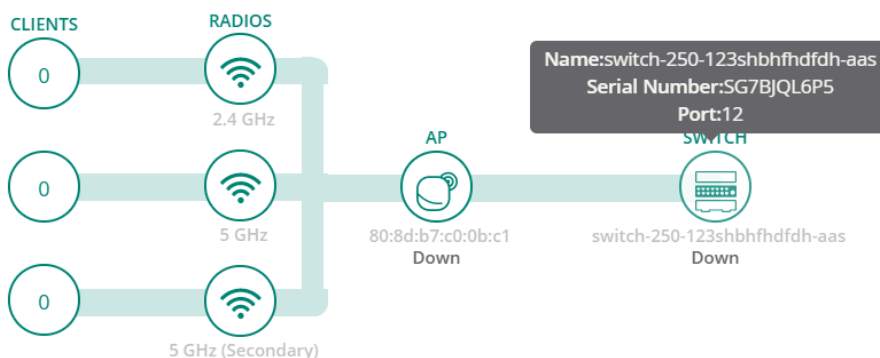
- When the AP radios are set to spectrum scan mode, the **Channel** and **Power** values are empty.
- The tri-radio feature is available only for AP-555. In the **Radios** section, the **Radio 5 GHz (Secondary)** data is available only if the tri-radio mode is enabled. For more information, see [About Tri-Radio Mode](#).

Data Path

The **Data Path** section displays the topology of 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.

Figure 49 *Data Path*

DATA PATH



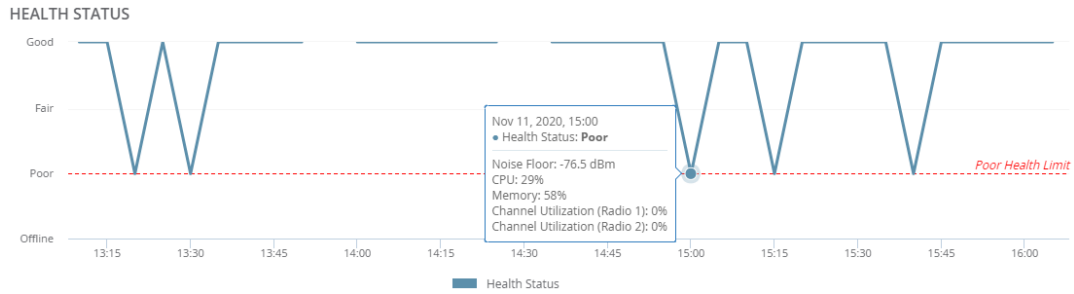
The tri-radio feature is available only for AP-555. In the **Data Path** section, the **5 GHz (Secondary)** data is available only if the tri-radio mode is enabled. For more information, see [About Tri-Radio Mode](#).

Health Status

The **Health Status** trend graph indicates the health status of the device in the network for the time specified in the time range filter. When you 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 50 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 51 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%;">2.4 GHz</td> <td style="width: 50%;">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.
- **Type**—Displays the type of the SSID.
- **VLANs**—Displays the VLAN number.
- **Security**—Displays the type of security.

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.



-
- In the **.csv** file of the **WLANS** table, the **5 GHz (Secondary)** columns are available only if the tri-radio mode is enabled.
 - 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](#).
-

Actions

The **Actions** drop-down list contains the following options:

- **Reboot AP**—Reboots the AP. For more information, see [Rebooting an AP](#).
- **Tech Support**—Enables the administrator to generate a tech support dump required for troubleshooting the AP. For more information, see [Tech Support for an AP](#).
- **Console**—Opens the remote console for a CLI session through SSH for an AP. For more information, see [Opening a Remote Console](#).

Go Live

Aruba Central allows you to monitor live data of an AP updated at every 5 seconds. For more information, see [Enabling Live AP 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.

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](#).

Access Point > Overview > Floor Plan

In the access point (AP) dashboard, the **Floor Plan** tab provides information regarding the current location of the AP.

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 AP. The sitemap is derived from the Visual RF application, if Visual RF service is enabled for the Aruba Central account. You can also edit the location of the AP 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](#).
- **Tech Support**—Enables the administrator to generate a tech support dump required for troubleshooting the AP. For more information, see [Tech Support for an AP](#).
- **Console**—Opens the remote console for a CLI session through SSH for an AP. For more information, see [Opening a Remote Console](#).

Go Live

Aruba Central allows you to monitor live data of an AP updated at every 5 seconds. For more information, see [Enabling Live AP 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 a selected time range in the time range filter. You can select a specific SSID or all SSIDs, Eth 0, or Eth 1 from the drop-down list provided in the **Clients** section.



When you hover over the **Throughput** and **Quality** 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](#).
- **Tech Support**—Enables the administrator to generate a tech support dump required for troubleshooting the AP. For more information, see [Tech Support for an AP](#).
- **Console**—Opens the remote console for a CLI session through SSH for an AP. For more information, see [Opening a Remote Console](#).

Go Live

Aruba Central allows you to monitor live data of an AP updated at every 5 seconds. For more information, see [Enabling Live AP 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**.

The **RF** tab provides the following details:

Channel Utilization

The **Channel Utilization** graph indicates the percentage of channel utilization for the selected time range from the time range filter.

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.

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](#).
- **Tech Support**—Enables the administrator to generate a tech support dump required for troubleshooting the AP. For more information, see [Tech Support for an AP](#).
- **Console**—Opens the remote console for a CLI session through SSH for an AP. For more information, see [Opening a Remote Console](#).

Go Live

Aruba Central allows you to monitor live data of an AP updated at every 5 seconds. For more information, see [Enabling Live AP 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.

Rebooting an AP

You can reboot an access point (AP) using the Aruba Central UI.

To reboot an 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. 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 less than a minute to update the interface status, after the AP is rebooted and reconnected to Aruba Central.

Tech Support for an AP

In Aruba Central UI, the administrators can generate a tech support dump required for troubleshooting the access point (AP).

To generate a tech support dump for an 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. 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.

Opening a Remote Console

In the Aruba Central UI, you can open the remote console for a CLI session through SSH for an access point (AP). You can reset the system configuration of an AP by erasing the existing configuration on the AP.

Resetting an AP through the Console

To reset an AP through the **Console**, 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 **Console**.
A CLI session dialog box is displayed.
5. Execute the `write erase all` command in the command prompt.
6. Reboot the AP.

In this procedure, the complete configuration including the **Per AP Settings** on the AP is reset. After the reboot, the 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 AP to factory default configuration by using the reset button on the device, see *Aruba Instant User Guide*.

Enabling Live AP Monitoring

Aruba Central allows you to monitor live data of an access point (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:

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. Click the **Go Live** button to start live monitoring of the AP.
5. Click the **Stop Live** button to exit live monitoring of the AP.

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.

AP Live Events

Aruba Central allows you to troubleshoot issues related to access points. 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 ArubaOS 10.0.0.0 or later versions to support this feature.

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 troubleshooting 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.

All Clients Monitoring in List View	421
All Clients Monitoring in Summary View	427
Dashboard for Wireless Clients	430
Dashboard for Wired Clients	440
Viewing Applications Monitored by AirSlice	445

Aruba Central provides a separate dashboard to monitor the clients.

In the **Network Operations** app, under **Manage > Clients** page, the details of clients connected to the devices in AOS 10.x and their connectivity status are displayed. It also shows the total number of clients, bandwidth usage, and the application usage by the clients connected to the wired and wireless networks.

- [All Clients Monitoring in Summary View](#)
- [Dashboard for Wireless Clients](#)
- [Dashboard for Wired Clients](#)
- [Viewing Applications Monitored by AirSlice](#)

All Clients Monitoring in List View

The **List** view displays a unified list of all clients for the selected group. By default, the **Clients** page appears in the **List** view.

The following topics are discussed in this section:

- [Navigating to the List View](#)
- [Monitoring in List View](#)
- [Reading the Client Details Table](#)

Navigating to the List View

To monitor the clients in a list or summary view:

1. In the **Network Operations** app, set the filter to **Global**.
The global dashboard is displayed.
2. Under **Manage**, click **Clients**.
The **Clients** page is displayed in the **List** view. This is the default view.
3. Click **Summary** to monitor clients in the **Summary** view.

For information about the **Summary** view, see [All Clients Monitoring in Summary View](#).

Monitoring in List View

You can monitor the clients in the list view as follows:

Figure 52 Clients Monitoring in List View

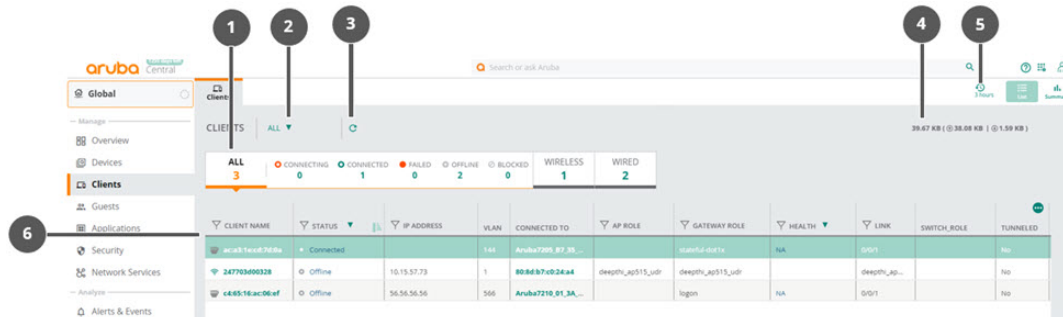





Table 124: User Interface Elements

Number	UI Element	Description
1	Client summary bar	<p>Displays the number of clients based on its status or mode as follows:</p> <ul style="list-style-type: none"> ■ All—Number of clients present in the selected branch. ■ Connecting—Number of clients present in the connecting status. ■ Connected—Number of clients present in the connected status. ■ Failed—Number of clients present in the failed status. ■ Offline—Number of clients present in the offline status. ■ Blocked—Number of clients present in the blocked status. ■ Wireless—Number of clients present in the wireless mode. ■ Wired—Number of clients present in the wired mode. <p>NOTE:</p> <ul style="list-style-type: none"> ■ Click the number to view corresponding details in the clients table. ■ The wired client will show up in the All 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.
2	Client filter	<p>Click Clients to filter the clients based on the device to which the clients are connected. The available options are as follows:</p> <ul style="list-style-type: none"> ■ All—Displays a list of all the clients connected to the network. ■ AP—Displays a list of clients connected to the AP. ■ Switch—Displays a list of clients connected to the switch. ■ Gateway—Displays a list of clients connected to the Aruba Gateway.
3	Refresh icon	Click  to load the latest details about clients in the summary bar and clients table.
4	Data usage details	Displays the total data usage for the selected time period.
5	Time range filter	<p>By default, the list of clients is populated for 3 hours. Click the Time Range Filter icon  and select the required time period to view the list of clients for a different time range. The available options are:</p> <ul style="list-style-type: none"> ■ 3 Hours ■ 1 Day

Number	UI Element	Description
		<ul style="list-style-type: none"> ■ 1 Week ■ 1 Month ■ 3 Months
6	Client details table	<p>Displays the details of each client. By default, the table displays the following columns: Client Name, Status, IP Address, Connected To, VLAN, Connected To, Link, AP Role, Gateway Role, and Health. Click the Ellipsis icon  to perform additional operations as follows:</p> <ul style="list-style-type: none"> ■ Download CSV—Downloads the client details in the .csv file format. ■ Select All—Selects all columns. ■ Reset Columns—Resets the table view to the default columns. <p>For more details, see Reading the Client Details Table.</p>



The wired client will show up in the **All 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.

Reading the Client Details Table

If a filter icon appears next to the column header, click it and enter the filter criteria or select a filter criteria. For example, in the **Client Name** column, enter the name of the client and in the **Status** column, select from one of the predefined filter criteria: **Connecting**, **Connected**, **Offline**, or **Failed**.

Table 125: All Client Details

Column Name	Applicability	Description
Client Name	<ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Gateway 	Username, hostname, or MAC address of the client. Click the client name to view the Summary page.
Status	<ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Gateway 	<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 the cursor over the status column to view a pop-up summary based on the connection status. The status summary is populated based on the status type. Each status type and the summary is described below:</p> <p>Connecting:</p> <ul style="list-style-type: none"> ■ Client name—Name of the client. ■ Last Seen Time—Date and time the client was last connected. <p>Connected:</p> <ul style="list-style-type: none"> ■ Client name—Name of the client. ■ IP address—Client IP address

Table 125: All Client Details

Column Name	Applicability	Description
		<ul style="list-style-type: none"> ■ Connected Since—Date and time at which the client was connected. ■ Health Score—Device health. <p>Offline:</p> <ul style="list-style-type: none"> ■ Client name—Name of the client. ■ IP address—Client IP address ■ Connected Since—Date and time at which the client was connected. ■ Last Seen Time—Date and time the client was last connected. <p>Failed:</p> <ul style="list-style-type: none"> ■ Client name—Name of the client. ■ Authentication—Authentication type of the client. ■ Last Seen Time—Date and time the client was last connected. ■ Failure Stage—Status of the client that failed to connect. ■ Failure Reason—Reason for the client failure. <p>Blocked:</p> <ul style="list-style-type: none"> ■ The values available for clients that are blocked when in failed status, offline status, dynamically blocked, or if a new client is blocked is as follows: <ul style="list-style-type: none"> • Client name—Name of the client. • Last Seen Time—Date and time the client was last connected. ■ The values available for clients that are blocked when in connected status is as follows: <ul style="list-style-type: none"> • Client name—Name of the client. • Authentication—Type of authentication. Displays the authentication label only for authenticated clients. • IP address—Client IP address • Connected Since—Date and time at which the client was connected. • Last Seen Time—Date and time the client was last connected.
IP Address	<ul style="list-style-type: none"> ■ All ■ AP ■ Switch 	IP address of the client.
VLAN	<ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Gateway 	VLAN of the device to which the client is connected.
Connected To	<ul style="list-style-type: none"> ■ All 	AP name, Switch name, or Gateway 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 ■ Gateway 	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 gateway, the column title displays Port.
AI Insights	<ul style="list-style-type: none"> ■ All 	The total number of AI insights generated for the client.

Table 125: All Client Details

Column Name	Applicability	Description
	<ul style="list-style-type: none"> ■ AP 	
AP Role	<ul style="list-style-type: none"> ■ All ■ AP 	Role assigned by the AP.
Gateway Role	<ul style="list-style-type: none"> ■ All ■ Gateway 	Role assigned by the Aruba Gateway.
Switch Role	<ul style="list-style-type: none"> ■ All ■ Switch 	Role assigned by the Aruba switch.
Health	<ul style="list-style-type: none"> ■ All ■ AP ■ Gateway 	Client health. The value can be one of the following: <ul style="list-style-type: none"> ■ Poor–0-25 ■ Fair–26-50 ■ Good–51-100
Failure Stage	<ul style="list-style-type: none"> ■ All ■ AP 	Failure status of the client that failed to connect. The failure reasons could be: <ul style="list-style-type: none"> ■ Association error ■ MAC authentication error ■ 802.1X authentication error ■ Key exchange error ■ DHCP error ■ Captive Portal error
Group Name	<ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Gateway 	Group name of the device managed by Aruba Central.
Site Name	<ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Gateway 	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 ■ Gateway 	MAC address of the client.
Hostname	<ul style="list-style-type: none"> ■ All ■ AP ■ Gateway 	Host name of the client.
User Name	<ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Gateway 	Username of the client.

Table 125: All Client Details

Column Name	Applicability	Description
Key Management	<ul style="list-style-type: none"> ■ All ■ AP 	Security mode used by the client.
Authentication	<ul style="list-style-type: none"> ■ All ■ AP 	Authentication type.
Global Unicast IPv6 Address	<ul style="list-style-type: none"> ■ All ■ AP ■ Gateway 	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 ■ Gateway 	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	<ul style="list-style-type: none"> ■ All ■ AP 	Client capabilities.
Usage	<ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Gateway 	Total data usage for the selected time period.
Client OS	<ul style="list-style-type: none"> ■ All ■ AP ■ Gateway 	Operating system of the client.
Last Seen Time	<ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Gateway 	Date and time when the client was last seen.
Connected Since	<ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Gateway 	Date and time since when the client was connected.
AP Name	<ul style="list-style-type: none"> ■ All ■ AP 	Name of the AP.
AP Mac Address	<ul style="list-style-type: none"> ■ All ■ AP 	MAC address of the AP.
Channel/Band	<ul style="list-style-type: none"> ■ All ■ AP 	Last connected channel and band.
Switch Name	<ul style="list-style-type: none"> ■ All ■ Switch 	Name of the switch.

Table 125: All Client Details

Column Name	Applicability	Description
Port	<ul style="list-style-type: none"> ■ All ■ Switch ■ Gateway 	Port number of the switch.
Gateway Name	<ul style="list-style-type: none"> ■ All ■ Gateway 	Name of the Aruba Gateway.
Tunneled	<ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Gateway 	Specifies if the client is present in tunneled network. The value can be one of the following: <ul style="list-style-type: none"> ■ Yes ■ No
Segmentation	<ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Gateway 	If the client is in tunneled network, the segmentation type of the client. The value can be one of the following: <ul style="list-style-type: none"> ■ None ■ UBT ■ PBT ■ Underlay ■ Overlay

All Clients Monitoring in Summary View

The **Summary** view displays details of bandwidth usage in graphical representation, distribution, and enlists top clients based on the duration of connectivity (minimum of two hours).

The following topics are discussed in this section:

- [Navigating to the Summary View](#)
- [Monitoring in the Summary View](#)
- [Viewing the Top Clients](#)

Navigating to the Summary View

To monitor the clients in a list or summary view:

1. In the **Network Operations** app, set the filter to **Global**.
The global dashboard is displayed.
2. Under **Manage**, click **Clients**.
The **Clients** page is displayed in the **List** view. This is the default view.
3. Click **Summary** to monitor clients in the **Summary** view.

For information about the **List** view, see [All Clients Monitoring in List View](#)

Monitoring in the Summary View


The **Summary** view consists of the following:


Figure 53 Clients Monitoring in Summary View





The following table describes the information displayed:

Table 126: Clients Monitoring in Summary View

Data Pane Content	Description
<p>Time Range Filter</p>	<p>By default, the graphs on the Clients page are plotted for a time range of 3 hours. Click the Time Range Filter icon  and select the required time period to view the list of clients for a different time range.</p> <p>The available options are as follows:</p> <ul style="list-style-type: none"> ■ 3 Hours ■ 1 Day ■ 1 Week ■ 1 Month ■ 3 Months <p>NOTE: The Distribution data (Client OS) under the Distribution tab does not honor the time range you selected in the time range filter.</p>
<p>Total</p>	<p>Displays the total number of clients.</p>
<p>Wireless</p>	<p>Displays the total number of clients connected to wireless network.</p>
<p>Wired</p>	<p>Displays the total number of clients connected to the wired network.</p>

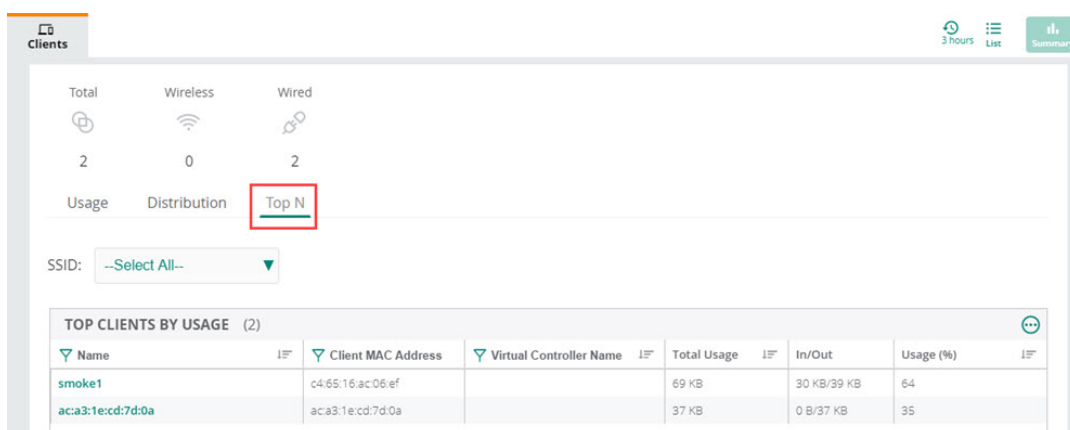
Data Pane Content	Description
<p>Usage tab</p>	<p>Displays the Bandwidth Usage of the incoming and outgoing throughput traffic for all the clients for a specific time range. The graph does not show data for clients that are connected to the network for lesser than two hours.</p>
<p>Distribution tab</p>	<p>Displays the type of client device connected to the wireless network.</p>
<p>Top N tab</p>	<p>Displays a list of clients connected to the currently available SSIDs that utilize the maximum bandwidth in the network. Click the SSID drop-down to filter and view the clients by SSID.</p> <p>The Top Clients by Usage table displays data for the clients that are connected to the network for more than two hours.</p> <p>The columns present in the table are:</p> <ul style="list-style-type: none"> ■ Name—Username, hostname, or MAC address of the client. Click the client name to navigate to the client-specific Summary page. ■ Client MAC Address—MAC address of the client. ■ Virtual Controller Name—Name of the virtual controller. ■ Total Usage—Bandwidth used by the client. ■ In/Out—Incoming and outgoing throughput traffic for the client. ■ Usage (%)—Bandwidth usage in percentage. <p>Search Options:</p> <ul style="list-style-type: none"> ■ The  icon allows

Data Pane Content	Description
	<p>you to search a particular item in the column.</p> <ul style="list-style-type: none"> ■ The  and  icons allow you to sort the data in the column in ascending or descending order. See <i>Viewing the Top Clients</i> section for more details.

Viewing the Top Clients

In the summary view of the **Clients** page, click the **Top N** tab to view the top clients that are connected to the network for more than two hours.

Figure 54 *Monitoring Top Clients By Usage*



The screenshot shows the 'Clients' dashboard with a 'Summary' tab selected. The 'Usage' section is active, and the 'Top N' tab is highlighted with a red box. Below this, there is a table titled 'TOP CLIENTS BY USAGE (2)' with the following data:

Name	Client MAC Address	Virtual Controller Name	Total Usage	In/Out	Usage (%)
smoke1	c4:65:16:ac:06:ef		69 KB	30 KB/39 KB	64
aca3:1eccd:7d:0a	aca3:1e:cd:7d:0a		37 KB	0 B/37 KB	35

Dashboard for Wireless Clients

The **Summary** dashboard displays the client summary details and client sessions details for the selected wireless client.

The following topics are discussed in this section:

- [Viewing Clients Connected to Wireless Networks](#)
- [Wireless Client Details](#)
- [Applications](#)
- [Live Events](#)
- [Events](#)
- [Tools](#)
- [Dashboard for Wireless Clients](#)
- [Sessions](#)

Viewing Clients Connected to Wireless Networks

To view the details of a client connected to the wireless or wired network:

1. In the **Network Operations** app, set the filter to **Groups** or **Devices**. Ensure that the filter selection contains at least one client. 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. By default, the **Clients** table displays a unified list of clients for the selected group.

You can monitor the client details in the following views:

- [All Clients Monitoring in List View](#)
- [All Clients Monitoring in Summary View](#)

3. In the **List** view, click the client name to navigate and view the client details in the **Summary** dashboard for the selected client.

4. Additionally, click the **Sessions** tab to view the client sessions details.

You can use the following search options:

- If there are multiple clients connected to the network, click **Wireless** or **Wired** to filter the corresponding clients.
- Enter the client name in the **Client Name** column and then click the client name. The **Summary** page for the selected client is displayed.

The wireless client **Summary** page displays the wireless client details.

Wireless Client Details

The wireless **Client Details** page displays the client overview details, connectivity summary, location, and sessions information for the selected client.

The client details page consists of the following:

- [Actions](#)
- [Go Live](#)
- [Health Bar](#)
- [Overview](#)
- [Applications](#)
- [Live Events](#)
- [Events](#)
- [Tools](#)

Disconnecting a Client

Click **Actions** and select **Disconnect from AP**. For more details, see [Disconnecting a Wireless Client](#).

Live Monitoring

Click **Go Live** to do live monitoring of the client. For more details, see [Live Client Monitoring](#).

Overview

The **Overview** tab consists of the following:

- [Wireless Client Health Bar](#)
- [Client Details](#)
- [Location](#)
- [Sessions](#)

Wireless Client Health Bar

The client health bar displays the client connection, device health, and transmission rate along with name of the device the client is connected to.

Table 127: *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	Displays the signal strength of the client device. The signal strength value is displayed in percentage: <ul style="list-style-type: none"> ■ Poor—0-30 ■ Fair—31-70 ■ Good—71-100
SNR	Displays the SNR for the client as measured by the AP. The SNR value is displayed in decibels: <ul style="list-style-type: none"> ■ Poor—0-20 ■ Fair—21-35 ■ Good—greater than 35
Tx/Rx Rate	Displays the data transmission or reception rate.
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.
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 Client Monitoring .

Client Details

The following table describes the information displayed in each section:

Table 128: *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: <ul style="list-style-type: none"> ■ Client > SSID > AP ■ Client > SSID > AP > Switch ■ Client > SSID > AP > Switch > Gateway

Table 128: Client Details

Section	Description
	<ul style="list-style-type: none"> ■ Client > SSID > AP > Gateway
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. ■ Global Unicast IPv6 Address—Global unicast IPv6 address of the client. ■ Link Local IPv6 Address—Link local IPv6 address of the client. ■ Client OS—Operating system running on the client. ■ Last Seen—Specific to offline client, the time stamp of the last connectivity. ■ Manufacturer—Manufacturer of the client device. ■ Encryption—Type of client encryption. ■ Connected Since—Specific to a connected client, the date and time since when the client is connected. ■ AI Insights—The total number of AI insights seen on the client device.
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. ■ VLAN Derivation—Displays the VLAN derivation method used for assigning an IP address to the client. Aruba devices can assign a static or dynamically derived IP address from a DHCP pool to the clients. ■ AP Role—Displays the role assigned to the client by the AP. ■ AP Derivation—Displays the role derivation method used for assigning a role to a client. For example, clients that authenticate successfully can be assigned a default role as per the AAA profile. ■ Gateway Role—Displays the role assigned to the client by the gateway. ■ Switch Role—Displays the role assigned to the client by the switch. ■ Segmentation—Displays the type of dynamic segmentation configured for the client. The 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 if the client is tunneled or not. ■ Tunneled ID—Displays the tunnel ID that 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 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.

Table 128: Client Details



Section	Description
Throughput	<p>Displays the received and sent throughput traffic for the client during a specific time range. The overall usage shows the total and the individual values for received and sent throughput. 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. Hover over the graph line to view the time stamp and the received or sent throughput details.</p>
Health	<p>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. Hover over the graph line at a low or at a high point to view the time stamp, health score and status. The value is displayed in percentage:</p> <ul style="list-style-type: none"> ■ Poor–0-30 ■ Fair–31-70 ■ Good–71-100
Signal Quality	<p>Displays the signal quality and the signal to noise ratio (SNR) for the wireless client as measured by the AP. Hover over the graph line to view the time stamp, SNR, and the signal quality. The SNR value is displayed in decibels:</p> <ul style="list-style-type: none"> ■ Poor–0-20 ■ Fair–21-35 ■ Good–greater than 35
Retry Frames	<p>Displays the percentage of data transmission (Tx) and data reception (Rx) retries by a wireless client. Hover over the graph line to view the time stamp, Tx retry, and Rx retry values. Click –Tx Retry or –Rx Retry to view individual values on the graph.</p>
Tx/Rx Rate	<p>Displays the data transmission and reception rate for the wireless client. Hover over the graph line to view the time stamp, Tx rate, and Rx rate values. Click –Tx Rate or –Rx Rate to view individual values on the graph.</p>
Roaming Experience	<p>Displays the details of a roaming event and the latency of the client. When a wireless client roams between two APs, the destination AP creates an event. Hover over the graph line to view the time stamp, total roaming events, high latency roaming events, and percentage-wise high latency roaming events values.</p> <p>Click the graph line to view the following:</p> <ul style="list-style-type: none"> ■ High Latency Roaming Events ■ Roaming Events & Latency <p>Click the graph line to see the High Latency Roaming Events table or click  to swap to Roaming Events & Latency table. By default, the tables display data for the last three hours. To view the table for a different time range, click the Time Range Filter link. You can choose to view the data for a time period of 3 hours, 1 day, 1 week, 1 month, or 3 months. The Roaming Events & Latency displays two views; grid view and trend view.</p> <p>The following columns are present in the table:</p> <ul style="list-style-type: none"> ■ Date/Time–Displays the time of occurrence of the client roaming/ association events. ■ Latency(ms)–Displays the roaming latency in milliseconds between the source and destination APs. ■ To BSSID–Displays the BSSID of the destination AP. ■ Source AP–Displays the AP from which the client is connected. ■ Destination AP–Displays the AP to which the client is connected. ■ Roaming Type–Displays the type of roam.

Table 128: Client Details

Section	Description
	<ul style="list-style-type: none"> ■ Band—Displays the radio band on which the client is connected. ■ RSSI(dBm)—Displays the Received Signal Strength Indicator (RSSI) on the client, estimated measure of power level that the client is receiving from the AP. <p>Click  to view the trend view as a chart that shows the percentage of high latency roaming events, total roaming events, and the number of high latency roaming events at a particular instance based on the value selected in the Time Range Filter.</p> <p>Click Total Roaming Events or High Latency Roaming Events to view individual values on the graph.</p>

Location

The **Location** tab displays the current physical location of the client device on the map.

Sessions

The wireless client **Sessions** tab consists of the firewall session details for the client connected to an Access Point or a Branch Gateway. The information displayed is based on 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** table lists the details of each session. By default, the table displays the following columns: **Application, Source IP, Destination IP, Source Port, Destination Port, Action, Flags, Packets, Bytes, and State**. 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.
- **Add columns**—Select the required columns from the available options.

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 129: 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.
Action	Displays the application specific action.
Flags	Displays the active flags

Table 129: Sessions Tab

Section	Description
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.
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.



Client **Sessions** is supported only if the AP is running ArubaOS 10.0.0.0 firmware version.

For details on the AP client sessions refer, [Access Point > Overview > Summary](#). For details on the Branch Gateway client sessions refer, [Monitoring Gateway Clusters](#).

Applications

The **Applications** page provides you the client details for passive motoring of the client connected to a wireless network.

It consists of the following:

- [Visibility](#)
- [UCC](#)

Visibility

The **Visibility** tab provides a summary of client traffic and their data usage for applications and websites. You can analyze the client traffic flow using the **Visibility** dashboard. It displays metrics and graphs related to client traffic flow. For more details, see [Manage > Applications > 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. It displays call quality, call health, and sessions related to the client traffic flow. For more details, see [Unified Communications](#).

Live Events

Aruba Central allows you to troubleshoot issues related to a client or a site in real time for detailed analysis. You can live troubleshoot clients connected to a wireless network. For more details, see [Client Live Troubleshooting](#).



Live troubleshooting can be performed for wireless clients only.

Events

The **Events** tab 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 130: *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. For more details, see [Alerts & Events](#).

Tools

The **Tools** tab 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 details, see [Using Troubleshooting Tools](#).

Live Client Monitoring

Click **Go Live** to start live monitoring of the client. Live monitoring is supported only if the AP is running ArubaOS 10.0.0.0 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

The **Actions** drop-down is disabled if the AP is offline.

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 multiple 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 client is disconnected from the AP.

Client Live Troubleshooting

Aruba Central allows you to troubleshoot issues related to a wireless client connected to an access point or a wired client connected to a switch.

Troubleshooting a Client

Aruba Central allows you to troubleshoot issues related to a client or a site in real time for detailed analysis.

To troubleshoot a client 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 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 click the client name.
6. Under **Analyze**, click **Live Events**. The **Live Events** page is displayed.
7. 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** 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.

Packet Capture

Aruba Central allows you to interact and launch a targeted packet capture on a client connected to a specific access point or a switch. 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.

Packet capture is only supported for wireless clients connected to APs running on ArubaOS 10.1.0.0 or a later version.



Packet capture for stack switches works only if the client is connected to the commander of the stack.

For packet capture, for a wired client connected to an Aruba 5400R Switch Series (V3 mode), ensure that “no-allow v2 modules” is set for the switch.

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 does not support packet capture for a wired client connected to a switch.

4. Aruba Central does not support packet capture for a wired client connected to a switch.
5. Enable the **Packet Capture** toggle button to start live packet capture for the selected client.
6. 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.
7. The client live troubleshooting starts automatically for the selected client.
8. Click **Stop Troubleshooting** to stop live troubleshooting.
9. Enable the **Packet Capture** toggle button to start live packet capture for the selected client.
10. 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.

Dashboard for Wired Clients

The overview page displays the client summary details and client sessions details for the selected wired client.

The following topics are discussed in this section:

- [Viewing Clients Connected to Wired Networks](#)
- [Wired Client Details](#)
- [Applications](#)
- [Events](#)
- [Tools](#)
- [Dashboard for Wired Clients](#)

Viewing Clients Connected to Wired Networks

To view the details of a client connected to the wireless or wired network:

1. In the **Network Operations** app, set the filter to **Groups** or **Devices**. Ensure that the filter selection contains at least one client. 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. By default, the **Clients** table displays a unified list of clients for the selected group.

You can monitor the client details in the following views:

- [All Clients Monitoring in List View](#)
- [All Clients Monitoring in Summary View](#)

3. In the **List** view, click the client name to navigate and view the client details in the **Summary** dashboard for the selected client.

4. Additionally, click the **Sessions** tab to view the client sessions details.

You can use the following search options:

- If there are multiple clients connected to the network, click **Wireless** or **Wired** to filter the corresponding clients.
- Enter the client name in the **Client Name** column and then click the client name. The **Summary** page for the selected client is displayed.

The wired client **Summary** dashboard displays the wired client details.

Wired Client Details

The wired **Client Details** page displays the client overview details, network summary, and throughput information for the selected client.

The client details page consists of the following:

- [Overview](#)
- [Applications](#)
- [Events](#)
- [Tools](#)

Overview

The **Overview** tab consists of the following:

- [Health Bar](#)
- [Client Details](#)
- [Sessions](#)

Wired Client Health Bar

The wired client summary page displays the client summary bar and the client details. The **Health Bar** displays the following information:

Table 131: Wired Client Health Bar

Field	Description
Connection status icon	<p>Displays the icons with the connection status of the client. Connection status is updated immediately on state change. The available statuses are:</p> <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	Displays the name of the port through which the client is connected.
Connected To	Displays the name of the Gateway to which the client is connected. Click the name of the Gateway to view the device details page.

Client Details

The following table describes the information displayed in each section:

Table 132: Client Details

Section	Description
Data Path	<p>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:</p> <ul style="list-style-type: none"> ■ Client > Wired Profile > AP ■ Client > Wired Profile > AP > Switch ■ Client > Wired Profile > AP > Switch > Gateway ■ Client > Wired Profile > AP > Gateway ■ Client > Switch ■ Client > Switch > Gateway ■ Client > Gateway
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. ■ Global Unicast IPv6 Address—Global unicast IPv6 address of the client. ■ Link Local IPv6 Address—Link local IPv6 address of the client. ■ MAC Address—MAC address of the client. ■ Client OS—Operating system running on the client device.

Table 132: Client Details

Section	Description
	<ul style="list-style-type: none"> ■ Connected Since—Date and time since when the client is connected. ■ Manufacturer—Manufacturer of the client device.
Network	<p>Displays the following information:</p> <ul style="list-style-type: none"> ■ VLAN—VLAN ID on which the client is connected to the AP. ■ Gateway Role—Gateway role associated to the client. ■ Switch Role—Displays the role assigned to the client by the switch. ■ Segmentation—Displays the type of dynamic segmentation configured for the client. The supported values are UBT, PBT, Underlay, or Overlay. ■ Tunneled—Displays if the client is tunneled or not. ■ Tunneled ID—Displays the tunnel ID that the client is connected to. ■ Port—Gateway port to which the client is connected.
Throughput	<p>Displays the received and sent throughput traffic for the client during a specific time range. The overall usage shows the total and the individual values for received and sent throughput. 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. Hover over the graph line to view the time stamp and received or sent throughput values.</p>

Sessions

The wired client **Sessions** tab 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** table lists the details of each session. By default, the table displays the following columns: **Application**, **Source IP**, **Destination IP**, **Source Port**, **Destination Port**, **Action**, **Flags**, **Packets**, **Bytes**, and **State**. 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 133: 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.

Table 133: Sessions Tab

Section	Description
Source Port	Displays the source port number.
Dest Port	Displays the destination port number.
Action	Displays the application specific action.
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.
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.



Client **Sessions** is supported only if the AP is running ArubaOS 10.0.0.0 firmware version.

For details on the Branch Gateway client sessions refer, [Monitoring Gateway Clusters](#).

Applications

The **Applications** page provides you the client details for passive motoring of the client connected to a wired network.

It consists of the following tabs:

- [Visibility](#)
- [UCC](#)

Visibility

The **Visibility** tab provides a summary of client traffic and their data usage for applications and websites. You can analyze the client traffic flow using the **Visibility** dashboard. It displays metrics and graphs related to client traffic flow. For more details, see [Manage > Applications > 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. It displays call quality, call health, and sessions related to the client traffic flow. For more details, see [Unified Communications](#).

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 134: *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. For more information on Events, see [Alerts & Events](#).

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 on Tools, see [Using Troubleshooting Tools](#).

Viewing Applications Monitored by AirSlice

To view the applications monitored by AirSlice, ensure to enable AirSlice. For more information, see [Enabling AirSlice on Access Points](#).

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 55 AirSlice–Applications

APPLICATIONS
Real-time Monitoring

Total Transferred: 176.1 MB

APPLICATION	CATEGORY	USAGE	SENT	RECEIVED
TCP	Network Service	11.8 MB (6.72%)	65 KB	11.7 MB
Dropbox	Dropbox SAAS	2.5 MB (1.44%)	1.5 MB	1.0 MB
Apple Message Mail	Network Service	2.04 KB (0.001%)	1.04 KB	1.04 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%)	4 KB	36 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%)	504 B	9 KB
UDP	Network Service	9 KB (0.01%)	4 KB	6 KB

Monitoring Network Health	448
Monitoring WAN Health	449
Monitoring Network Summary	451
About Floorplans	452
Manage > Applications > Visibility	458
RAPIDS	460
Monitoring Sites in the Topology Tab	465

The AOS 10.x uses the **Network Operations** app to manage the network, the devices, clients, applications and even security.

In the global dashboard, under **Manage > Overview**, the following options are available:

- The **Network Health** page under **All Devices > Overview** provides detailed information on network health for the sites configured in your setup. See [Monitoring Network Health](#)
- The **WAN Health** page under **All Devices > Overview** provides detailed information of the network health status and usage for sites that include gateways. See [Monitoring WAN Health](#)
- The **Summary** page under **All Devices > Overview** displays a summary of the bandwidth usage, client count, top APs by usage, top clients, application usage, and WLAN network details of the selected group. See [Monitoring Network Summary](#)

Monitoring Network Health

The **Network Health** page in the **Overview** context menu at the global level provides detailed information on network health for the sites configured in your setup. The network health page is available when the **All Devices** filter is selected.

In the **Network Operations** app, perform the following steps to access the **Network Health** page:

1. Set the filter to **All Devices**. The Global dashboard is displayed.
2. Under **Manage > Overview**, the network summary page displays the following tabs:
 - **Network Health**
 - **WAN Health**
 - **Summary**
 - **VisualRF**
3. Click the **Network Health** tab.

The **Network Health** page offers the following views. The views can be toggled using the icons on the right in the first level tab:

- **Map**— The map view provides a pictorial view of the sites in the network. The sites are color coded; a red pin indicates potential issues and green pin indicates that there are no issues. Clicking on a site displays the network overview details for that site. Sites can be filtered using the filters available in the column label.

- **List**— The list view provides the network health details of different sites of the network in a table format. Filters for sites are available in the column labels. The columns can be customized by selecting the required ones in the hamburger menu of the column header.
- The **Network Health** page displays the following information:

Table 135: Network Health in MapView and List View

Header	Description
Site Name	Name of the site. Clicking on the site name opens the Overview > Site Health page of the Site.
Number of Devices	<p>Displays the following details for devices:</p> <ul style="list-style-type: none"> ■ Status—Number of devices that are in Up or Down state in a site. In the Down column, hover your mouse on the number displayed to view the following details: <ul style="list-style-type: none"> ●WLAN Devices Down ●Wired Devices Down ●Branch Devices Down ■ High Memory Usage—Number of devices with high memory utilization per site. Hover your mouse on the number displayed to view the following details: <ul style="list-style-type: none"> ●WLAN Memory High ●Wired Memory High ●Branch Memory High ■ High CPU Usage—Number of devices with high CPU usage per site. Hover your mouse on the number displayed to view the following details: <ul style="list-style-type: none"> ●WLAN CPU High ●Wired CPU High ●Branch CPU High ■ High Channel Utilization—Number of APs with a higher channel utilization per radio band. ■ AI Insights—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. ■ High Noise—Number of 2.4 GHz and 5 GHz radios of APs with a high RF noise. <p>NOTE: In the list View, use the filter to select the column that is required to be displayed in the table. By default, the table displays all the above mentioned details.</p>
WAN	<p>Displays the following details for the WAN:</p> <ul style="list-style-type: none"> ■ Uplinks Status—Indicates the uplink status as Down or No Issues. ■ Tunnels Status—Indicates the status of tunnels as Down or No Issues.

Monitoring WAN Health

The **WAN Health** page under **All Devices > Overview**, provides detailed information of the network health status and usage for sites that include gateways.

In the **Network Operations** app, perform the following steps to access the **WAN** page:

1. Set the filter to **All Devices**. The Global dashboard is displayed.
2. Under **Manage > Overview**, the page displays the following tabs:
 - **Summary**
 - **Network Health**
 - **WAN Health**
 - **VisualRF**

- Click the **WAN Health** tab.

Page Views

The **WAN Health** page offers the following views:

- **Summary**—The map provides a pictorial view of the network across various sites. The sites are color coded; **Red** indicates potential issues and **Green** indicates that there are no issues. To change the zoom level, click the **+** or **-** icon on the map. You can click the site on the map to view details.
- **List**—The list view provides a numerical representation of the data. The table displays the following details:

WAN Health

Table 136: Gateways Network Health Page

Header	Totals	Description
Site Name	Displays the total number of sites.	Name of the site. Use the column filter bar to search for a particular site. Click the site name to open the Site Health page. For more information, see the <i>Site Health</i> section in the <i>Aruba Central Help Center</i> .
Site Type	Displays the total number of sites for each site type.	Displays whether the device is deployed as a hub or spoke. <ul style="list-style-type: none"> ■ To filter gateways provisioned as a hub, click Hub. ■ To filter gateways provisioned as a spoke, click Spoke. ■ To filter gateways deployed as cloud instances, click Cloud. Only hubs can be deployed as cloud instances, so if a hub is deployed as a cloud instance, the site type is Cloud.
Device Status	Displays the total number of devices in Up and Down state.	Displays the total count of devices in the UP and DOWN states. <ul style="list-style-type: none"> ■ To filter devices in UP state, click Up. ■ To filter devices in DOWN state, click Down.
Connectivity	Displays the total number of links and the average bandwidth consumed.	Displays the following information: <ul style="list-style-type: none"> ■ Status—Displays the overall connectivity status. One of the following statuses is displayed: <ul style="list-style-type: none"> ■ Up ■ Partial ■ Down Hover over the column to view the circuit status, tunnel status, overlay status, and underlay status separately. <ul style="list-style-type: none"> ■ Bandwidth—Displays bandwidth details. ■ Configured—Displays the bandwidth that is configured on the gateway. ■ Estimated—Displays the estimated bandwidth availability for the uplinks. The Bandwidth Estimation feature must be enabled to display this data. ■ Consumed—Displays the bandwidth consumed by the clients. The consumed bandwidth is split into transmitted and received, and displayed at site level.
Performance	Displays the average value for site availability and policy compliance.	Displays the following metrics: <ul style="list-style-type: none"> ■ Site Availability—Displays the site availability. The range is from 0 to 100 percent. To filter site availability, click the column filter bar and enter values in the Min and Max text boxes. Hover your mouse over the column to view site availability on a per provider basis. ■ Policy Compliance—Displays the policy compliance. The range is from 0 to 100 percent. To filter policy compliance, click the column filter bar and enter values in the Min and Max text boxes. Hover your mouse over the column to view policy compliance on a per policy basis.

This page uses the following indicators to present information on status of the network health:

- Small Grey bullet icon—Indicates no issues.
- Big red bullet icon—Indicates potential issues.

Monitoring Network Summary

The **Overview > Summary** pane displays a summary of the bandwidth usage, client count, top APs by usage, top clients, top AP clusters by usage, top AP clusters by clients, application usage, and WLAN network details of the selected group. By default, the graphs are plotted for a time range of 3 hours. To view the graphs for a different time range, click the **Temporal Filter** link.

In the **Network Operations** app, perform the following steps to access the overall network summary page:

1. Set the filter to **All Devices**. The Global dashboard is displayed.
2. Under **Manage > Overview**, the network summary page displays the following tabs:
 - **Network Health**
 - **WAN Health**
 - **Summary**
 - **VisualRF**

Note that AP clusters are not supported in AOS 10.x.

Table 137: Summary Pane

Data Pane Item	Description
Temporal Filter	Allows you to select a time range for the graphs displayed on the Summary pane. You can choose to view graphs for a time period of 3 hours, 1 day, 1 week, 1 month and 3 months.
Usage	Displays the aggregate incoming and outgoing data traffic of all clients in the selected group.
Clients count	Displays the total number of clients connected to an AP over a specific duration.
Top APs By Usage	Displays the list of top APs that utilize the maximum bandwidth in the network.
Top Clients By Usage	Displays the list of top clients 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. This information is displayed for devices that operate in a cluster deployment mode and not for devices that operate in standalone mode. The section does not display data for APs in AOS 10.x.
Top IAP Clusters by Clients	Displays the list of top AP clusters connected to the client that utilize the maximum bandwidth in the network. This information is displayed for devices that operate in a cluster deployment mode and not for devices that operate in standalone mode. The section does not display data for APs in AOS 10.x.
WLANs	Displays the list of SSIDs configured. The WLANs table displays the SSID details such the name, type, security settings, and the clients connected on the network. To expand or collapse the column view, click the column settings icon next to the last column in the table.

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 APs running 6.5.2.0 or later.
 - 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

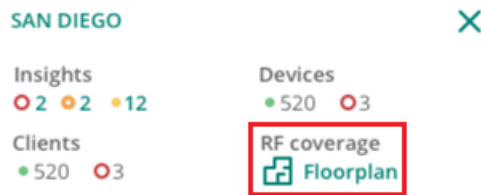
- [Floorplans Dashboard](#)
- [Planning and Provisioning Devices](#)
- [Customizing the Floorplans View](#)

Floorplans Dashboard

The **Floorplans** dashboard can be accessed from a site context or an access point context. 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 **Floorplans** 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 dashboard context for the **Global** filter is displayed.
2. Under **Manage > Overview**, the network summary page is displayed.
3. Hover over a site to view the following details:



4. Click **Floorplan** under **RF Coverage**. The **Floorplans** dashboard for the selected site is displayed.

To view the **Floorplans** dashboard from a site context, 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.
The **Floorplans** dashboard allows you to customize the view by selecting various properties and also allows you to select multiple floors in the same site.

To view the **Floorplans** dashboard from an access point context, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
The dashboard context for the **Global** filter is displayed.
2. Under **Manage**, click **Devices > Access Point**.
A list of APs 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 **Access Point Details** 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.



The floor plan details for an AP is only accessible for the devices that are assigned with license.

Customizing the Floorplans 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 **Floorplans** 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 138: Floorplan Menu Options

Tabs	Options
<p>Properties</p>	<p>Displays the following menu options: 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.
<p>View</p>	<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. Floorplans 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.
<p>Edits</p>	<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 Floorplans Dashboard

The **Floorplans** dashboard provides various options to customize your view. The customizable parameters include:

Table 139: User Interface Elements

UI Element	Description
	Click the drop-down to select a specific floor from the site.
	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.
	Click Heatmaps to view the strength of RF coverage in each location. You can view heatmaps in monochrome also. Click the monochrome checkbox in the Floorplans dashboard to select either the monochrome display or the colored display of heatmaps.
	Click Walls and Regions to view the segregation of regions and walls in the selected floor.
	Click the Refresh icon to refresh the floor plan details.
	Click the + or - icon to zoom in or zoom out of a floor plan. You can also scroll to increase or decrease the floor plan view. Additionally, click the box icon to view the floor plan in full screen mode.

Planning and Provisioning Devices

Floorplans provide the capability to plan buildings, floors, and location for device provisioning before the actual deployment. Using **Floorplans**, 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](#)

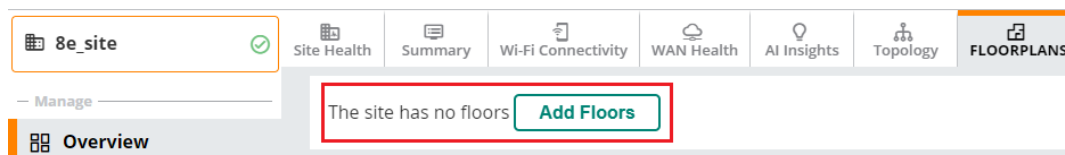
- [Modifying Floor Plan Properties](#)
- [Adding Devices to the Floor Plan](#)

Creating a Floor Plan

Floorplans 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 a **Site**.
The dashboard context for the selected site is displayed.
2. Under **Manage** > **Overview**, click **Floorplans**. The **Floorplans** dashboard is displayed.
3. Click **Add Floors**. The **Floor Plan** tab is displayed.



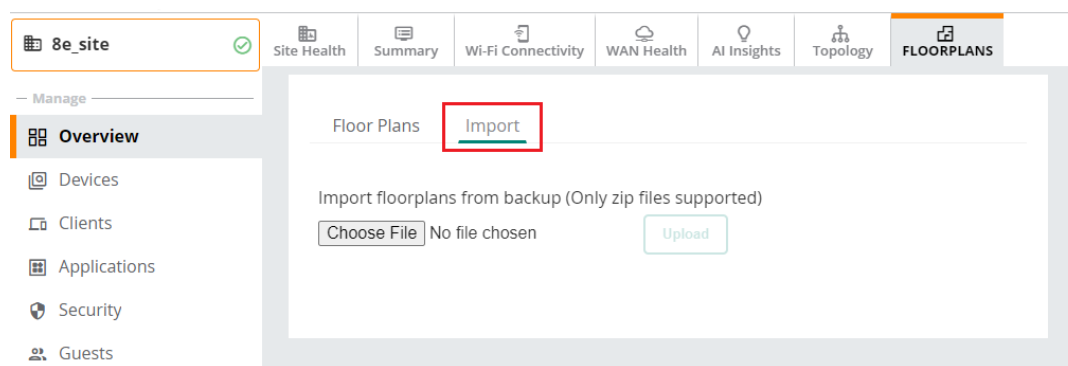
4. Click **Edit** the slide out pane on the right.
5. Click **New Floorplan**. You can also add the floor plan by right clicking on the center gray area and click **New Floorplan**. The **New Floorplan** pop-up window is displayed:
6. Click **Choose File** and locate a floor plan image file from your 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**.
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 a **Site**.
The dashboard context for the selected site is displayed.
2. Under **Manage > Overview**, click **Floorplans**. The **Floorplans** 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. In case of multiple floors, select the floor from the drop-down list and click **Edit**. For more information on edit, see [Customizing the Floorplans View](#).
4. Click **Save**.

Adding Devices to the Floor Plan

You can add the planned devices or the already deployed devices to floor plan.

To add the already deployed devices to the 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**. 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 **Floorplans** 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 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**. 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 Auto-match the planned devices, click **Auto-Match Planned Devices** from the **Action** tab.
7. To remove a planned device from the floor plan, right-click on that device and then click **Remove**.

Manage > Applications > 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:

1. In the **Network Operations** app, set the filter to one of the options under **Groups** or **Sites**. For all devices, set the filter to **Global**. The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Applications**. The visibility dashboard is displayed.

The **Visibility** dashboard displays metrics and graphs related to client traffic flow in the following sections:

- **Applications**
- **Websites**
- **Blocked Traffic**



The **Blocked Traffic** tab is only displayed in **Global** level in the **Network Operations > Manage > Applications** page.



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 Visibility > Applications Tab

The **Applications** section includes a table view and a graph view related to the client traffic flow to and from various applications.

Table View in Application Section

The **Applications** section displays a table with details on the client traffic flow to and from various applications. The table in the **Applications** section displays the following columns:

- **Application**—Name of the application.
- **Category**—The 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.

Graph View in Applications Section

Click the **Graph** icon in the Applications section to display bar graphs indicating the traffic flow in the following two tabs:

- **Applications**—The stacked bar graph 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 beside the bar graphs displays the list of applications to which the traffic flow is detected. By hovering the mouse on the bar graph, you can view the size of data flowing to and from the application same as displayed in legend section,
- **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. By hovering the mouse on the bar graph, you can view the size of data flowing to and from the application categories same as displayed in legend section.

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 the last three hours.

The Visibility > Websites Tab

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.

Table View in Websites Section

The **Websites** section displays tables with 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.

Clicking the **Graph** icon corresponding to the **Websites** section displays bar graphs for the following two tabs:

- **Reputation**—The stacked bar graph in the **Reputation** tab displays details of client traffic flow for the top five reputations listed in the **Websites** table.
- **Web Categories**—The stacked bar graph in the **Web Categories** tab displays details of client traffic flow for the top five web categories listed in the **Websites** table. You can view the size of data flowing to and from each of the web categories by hovering the mouse on the bar graph. The legend beside the bar graphs displays the list of websites based on its reputation, to which the traffic flow is detected.

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 the last three hours.



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, APs, and Gateways levels.



The Applications (Apps) and Web Categories charts are also displayed in the **Applications** pages for the Group, Global, APs, and Gateways levels.

The Visibility > Blocked Traffic Tab

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 one of the options under **Groups**. For all devices, set the filter to **Global**. The dashboard context for the selected filter 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.

RAPIDS

AOS 10.x 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 a rogue or interfering devices that can be later considered for investigation, restrictive action, or both. Once the interfering devices are discovered, AOS 10.x sends alerts to your network administrators about the possible threat and provides essential information needed to locate and manage the threat.

AOS 10.x 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.

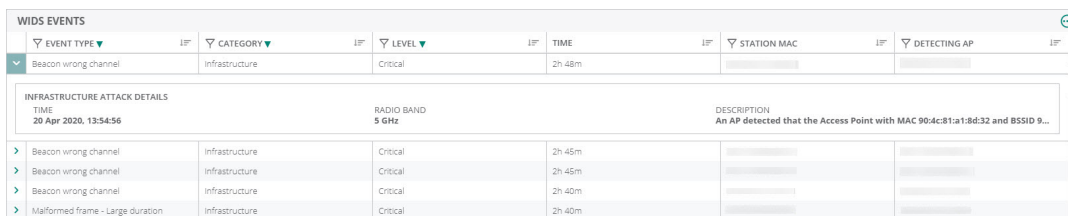
Table 140: *WIDS Events*

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.

Field	Description
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.



The screenshot shows a table titled 'WIDS EVENTS' with columns for Event Type, Category, Level, Time, Station MAC, and Detecting AP. A row for 'Beacon wrong channel' is selected, and its details are expanded below. The expanded view shows 'INFRASTRUCTURE ATTACK DETAILS' with a time of '20 Apr 2020, 13:54:56', a radio band of '5 GHz', and a description: 'An AP detected that the Access Point with MAC 904c:81:a1:8d:32 and BSSID 9...'. Below this, a list of events is shown with columns for Event Type, Category, Level, Time, Station MAC, and Detecting AP.

- 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 AOS 10.x are classified as one of the following:

Table 141: AP Classification in AOS 10.x

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.

Classification	Description
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 142: *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	
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:

- 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 **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	sig...																																																																																					
Aruba, a Hew-0F9C48	Suspect Rogue	TMM-cp-bandi-internal	29 Jan 2021, 13:14:42	f42e7fc07618	-41																																																																																					
<table border="1"> <thead> <tr> <th colspan="2">OVERVIEW</th> <th colspan="5">LOCATION</th> </tr> <tr> <th>SSID</th> <th>LOCATION</th> <th>ACCESS POINT NAME</th> <th>SNR (DB)</th> <th>BAND</th> <th>BSSID</th> <th>RF CHANNEL</th> </tr> </thead> <tbody> <tr> <td>TMM-cp-bandi-internal</td> <td></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>BSSID</td> <td></td> <td>00:4e:35:c2:82:1e</td> <td>-37</td> <td>2.4 GHz</td> <td>00:4e:35:a8:21:00</td> <td>1</td> </tr> <tr> <td>FIRST SEEN</td> <td></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>FIRST SEEN BY</td> <td></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>00:4e:35:c2:89:9c</td> <td></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>LAST SEEN</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>29 Jan 2021, 13:14:42</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>LAST SEEN BY</td> <td></td> <td>00:4e:35:c2:89:9c</td> <td>-41</td> <td>5 GHz</td> <td>00:4e:35:a9:99:00</td> <td>149</td> </tr> <tr> <td>f42e7fc07618</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>SWITCH PORT</td> <td></td> <td>f42e7fc062b2</td> <td>-33</td> <td>2.4 GHz</td> <td>F42E:7F:86:2B:20</td> <td>6</td> </tr> </tbody> </table>							OVERVIEW		LOCATION					SSID	LOCATION	ACCESS POINT NAME	SNR (DB)	BAND	BSSID	RF CHANNEL	TMM-cp-bandi-internal		00:4e:35:c2:97:34	-14	2.4 GHz	00:4e:35:a9:73:40	1	BSSID		00:4e:35:c2:82:1e	-37	2.4 GHz	00:4e:35:a8:21:00	1	FIRST SEEN		00:4e:35:c2:7c:9e	-37	2.4 GHz	00:4e:35:a7:c9:e0	1	FIRST SEEN BY		00:4e:35:c2:7c:9a	-50	2.4 GHz	00:4e:35:a7:c9:a0	1	00:4e:35:c2:89:9c		00:4e:35:c2:84:88	-49	2.4 GHz	00:4e:35:a8:48:80	6	LAST SEEN		00:4e:35:c2:80:ae	-35	2.4 GHz	00:4e:35:a8:0a:e0	6	29 Jan 2021, 13:14:42		00:4e:35:c2:7e:78	-6	2.4 GHz	00:4e:35:a7:e7:80	1	LAST SEEN BY		00:4e:35:c2:89:9c	-41	5 GHz	00:4e:35:a9:99:00	149	f42e7fc07618		00:4e:35:c2:9e:06	-13	2.4 GHz	00:4e:35:a9:e0:60	1	SWITCH PORT		f42e7fc062b2	-33	2.4 GHz	F42E:7F:86:2B:20	6
OVERVIEW		LOCATION																																																																																								
SSID	LOCATION	ACCESS POINT NAME	SNR (DB)	BAND	BSSID	RF CHANNEL																																																																																				
TMM-cp-bandi-internal		00:4e:35:c2:97:34	-14	2.4 GHz	00:4e:35:a9:73:40	1																																																																																				
BSSID		00:4e:35:c2:82:1e	-37	2.4 GHz	00:4e:35:a8:21:00	1																																																																																				
FIRST SEEN		00:4e:35:c2:7c:9e	-37	2.4 GHz	00:4e:35:a7:c9:e0	1																																																																																				
FIRST SEEN BY		00:4e:35:c2:7c:9a	-50	2.4 GHz	00:4e:35:a7:c9:a0	1																																																																																				
00:4e:35:c2:89:9c		00:4e:35:c2:84:88	-49	2.4 GHz	00:4e:35:a8:48:80	6																																																																																				
LAST SEEN		00:4e:35:c2:80:ae	-35	2.4 GHz	00:4e:35:a8:0a:e0	6																																																																																				
29 Jan 2021, 13:14:42		00:4e:35:c2:7e:78	-6	2.4 GHz	00:4e:35:a7:e7:80	1																																																																																				
LAST SEEN BY		00:4e:35:c2:89:9c	-41	5 GHz	00:4e:35:a9:99:00	149																																																																																				
f42e7fc07618		00:4e:35:c2:9e:06	-13	2.4 GHz	00:4e:35:a9:e0:60	1																																																																																				
SWITCH PORT		f42e7fc062b2	-33	2.4 GHz	F42E:7F:86:2B:20	6																																																																																				
Aruba, a Hew-0F9C48	Interfering	aruba-ap	29 Jan 2021, 14:14:43	f42e7fc062b2	-55																																																																																					
Aruba, a Hew-8065:30	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**. For more information on how to configure IDS Parameters, see Aruba Central Help Center.

Generating Alerts for Security Events

AOS 10.x 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. AOS 10.x 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

AOS 10.x 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**. AOS 10.x supports **RAPIDS** to display the report of all wireless intrusions.

Monitoring Sites in the Topology Tab

In Aruba Central, the **Topology** tab in the site dashboard 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.

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 Tab](#)
- [Parts of the Topology Tab User Interface](#)
- [Pop-Up 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)
- Gateway
- Switch—AOS Switch, AOS-CX switch

- Stack—AOS Switch stack, AOS-CX switch stack
- AOS-CX VSX Switch

In the topology map, Aruba Central only supports third-party routers, switches, gateways, 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

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) and gateways in the topology map is ArubaOS version 8.1.0.0-1.0.1.1.
- To view the topology map, ensure that LLDP is enabled. On switches, LLDP is enabled by default. On Branch Gateways, if the port type is LAN, LLDP is enabled by default.
- To view Aruba CX switches in the topology map, you must create a template configuration for the switch with the password in plaintext.

The guidelines for grouping VPNCs are:

- If the tunnels in the overlay are orchestrated, the VPNCs are grouped according to their hub groups. You can also see the group preference order marked as primary, secondary, or tertiary.
- If the tunnels are configured manually, the VPNCs are grouped according to their sites. If the VPNCs are not associated with any site, they are grouped based on their hub groups. For manual tunnels, the Data Center group preference is not displayed.

- If you have a combination of gateways in a single site, with one gateway configured as a manual tunnel and the other gateway configured as an orchestrated tunnel, both the tunnels are treated as manual and the VPNCs are grouped based on their sites. If there are no associated sites, they are grouped according to their hub groups.



Do not install VPNCs with orchestrated tunnels and VPNCs with manual tunnels together in a single site.

Viewing the Topology Tab

To view the topology tab, 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 pop-up details. For more information, see [Pop-Up Details](#).
4. In the device or the link pop-up, click the **Show Details** link to view the corresponding **Details** pane. For more information, see [Details Pane](#).

Parts of the Topology Tab User Interface

In the topology tab, the icons provides the following functionality:

Figure 56 *Parts of the Topology Tab*

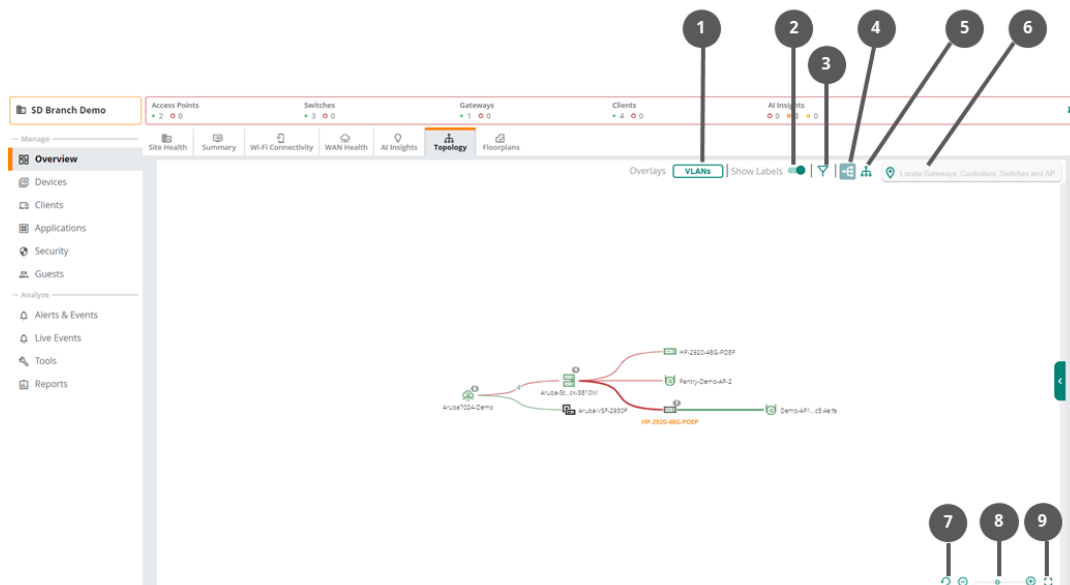


Table 143: Icon Details




Callout Number	Description
1	Click the icon to show or hide the VLANs pane.
2	Set the toggle icon to show or hide the labels.
3	Click the 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.
5	Click the icon to view the topology map in a top to 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 search.
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 pop-up 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 144: Icon Types

Icon	Type
	AP
	Branch Gateway
	Switch
	Switch Stack

Icon	Type
	Unmanaged Device
	Uplink
	VPNC

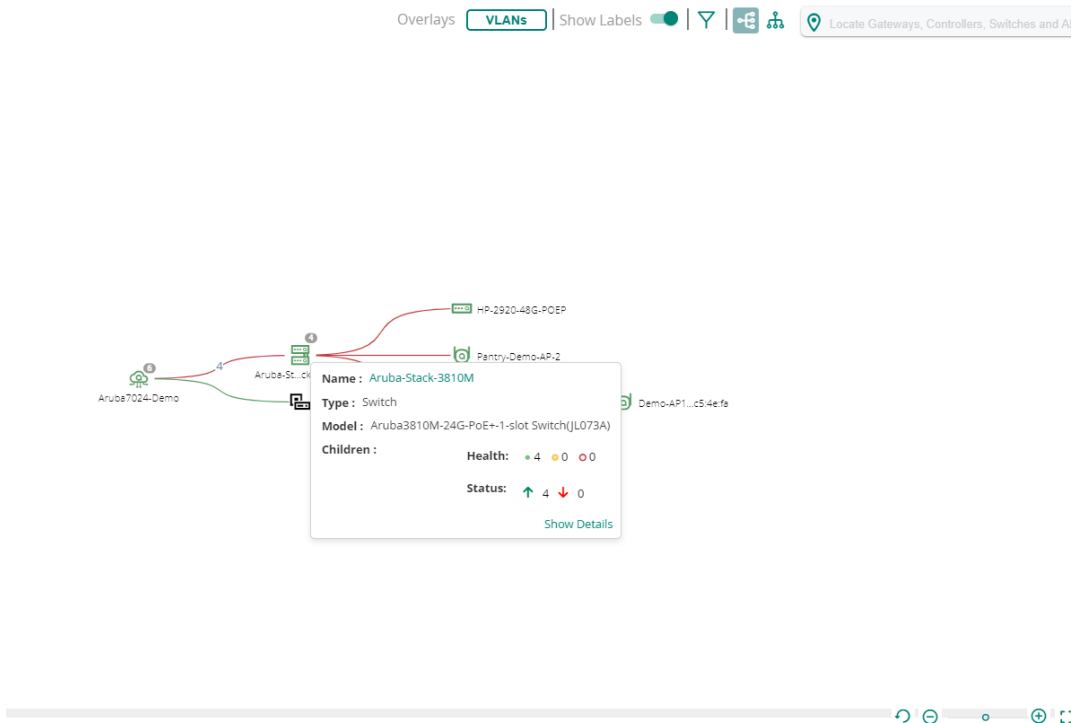
Icon Status

-  –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.

Pop-Up Details

When you hover over a device or link, a pop-up displays the following details:

Figure 57 *Pop-Up Details*



- Access Point—Displays the following details:
 - **Name**—Hostname of the AP.
 - **Type**—Type of the device.
 - **Model**—Hardware model of the AP.
 - **Health Reason**—The health status of the AP. This parameter is only available when the AP is offline.
 - **Show Details**—Click the link to view the **Details** pane.
 - Branch Gateway—Displays the following details:
 - **Name**—Hostname of the Branch Gateway.
 - **Type**—Type of device deployment.
 - **Model**—Hardware model of the device.
 - **Children**—Number of devices connected to the Branch Gateway categorized based on the health and status of the devices. The **Children** field displays the following details:
 - **Health**—Count of devices connected to the Branch Gateway based on the health of the device. 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%.
 - **Status**—Count of devices connected to the Branch Gateway 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.
 - **Show Details**—Click the link to view the **Details** pane.
 - VPNC—Displays the following details:
 - **Name**—Hostname of the VPNC.
 - **Type**—Type of device deployment.
 - **Model**—Hardware model of the device.
 - **Show Details**—Click the link to view the **Details** pane.
 - Unmanaged—Displays the following details:
 - **Name**—Name of the unmanaged device.
 - **IP Address**—IP address of the unmanaged device.
 - **Show Details**—Click the link to view the **Details** pane.



The value of the **IP Address** parameter is empty if LLDP does not provide the neighbor information.

- Switch—Displays the following details:
 - **Name**—Hostname of the switch.
 - **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:
 - **Health**—Count of devices connected to the switch based on the health of the device. 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%.

- **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—Displays the following details:
 - **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:
- **Health**—Count of devices connected to the switch based on the health of the device. 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%.
- **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—Displays the following details:
 - **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**. However, in the map, this name is displayed in the **VSX_<first four characters of device name>...<last eight characters of device name>** format. For example, **VSX_8320...-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:
- **Health**—Count of devices connected to the switch based on the health of the device. 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%.
- **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.
 - Tunnel—Displays the alias map name of the tunnel configured on the Branch Gateway.
In the topology map, the tunnels are shown as dotted lines. The tunnel in green color indicates that the tunnel is up. The tunnel in red color indicates that the tunnel is down.

Click the tunnel link to view the **Details** pane.

- Uplink—Displays the following information about uplinks configured on the Branch Gateway:
- **<Name of the Branch Gateway>**—Displays the name of the Branch Gateway.
- **Uplink**—Type of the uplink.
- **VLAN**—VLAN ID of the uplink.
- **Health Reason**—Displays the health status of the uplink. This parameter is only available when the uplink is down. The uplink in green color indicates that the uplink is up. The uplink in red color indicates that the uplink is down.

Click the uplink to view the **Details** pane.



In case of High Availability, the redundant gateway tunnel details are also displayed in the **Details** tab under **Virtual Tunnels** when you select the uplink.

- Edge—Displays the following information about the link:
- **<Name of the connected device>**—Name of the device connected with the edge link.
- **<Interface number>**—Interface number of the device.
- **Health Reason**—Displays the health status of the edge link. This parameter is only available when the edge link is down.
- **Alternative links**—Number of the alternative links.

The edge in green color indicates that the edge is up. The edge in red color indicates that the edge is down.

Click the uplink to view the **Details** pane.

- Unmanaged edge—Displays the following information about the link:
- **<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 edge link. This parameter is only available when the edge link is down.
- **Alternative links**—Number of the alternative links.

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.

- ISL edge in AOS-CX VSX topology map—Displays the following information about the link:
- **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.
- **<Name of the connected device>**—Name of the device connected with the edge link.
- **<Interface name>**—Interface name where the switches are connected to the devices.



Active tunnels are green in color and inactive tunnels are red in color. If there are multiple tunnels connecting to a VPNCs, and even if one of those tunnels is down, the tunnel mapping is displayed in red dotted lines.

Details Pane

In the topology map, the **Details** pane provides a summary of the devices, uplinks, and tunnel details.

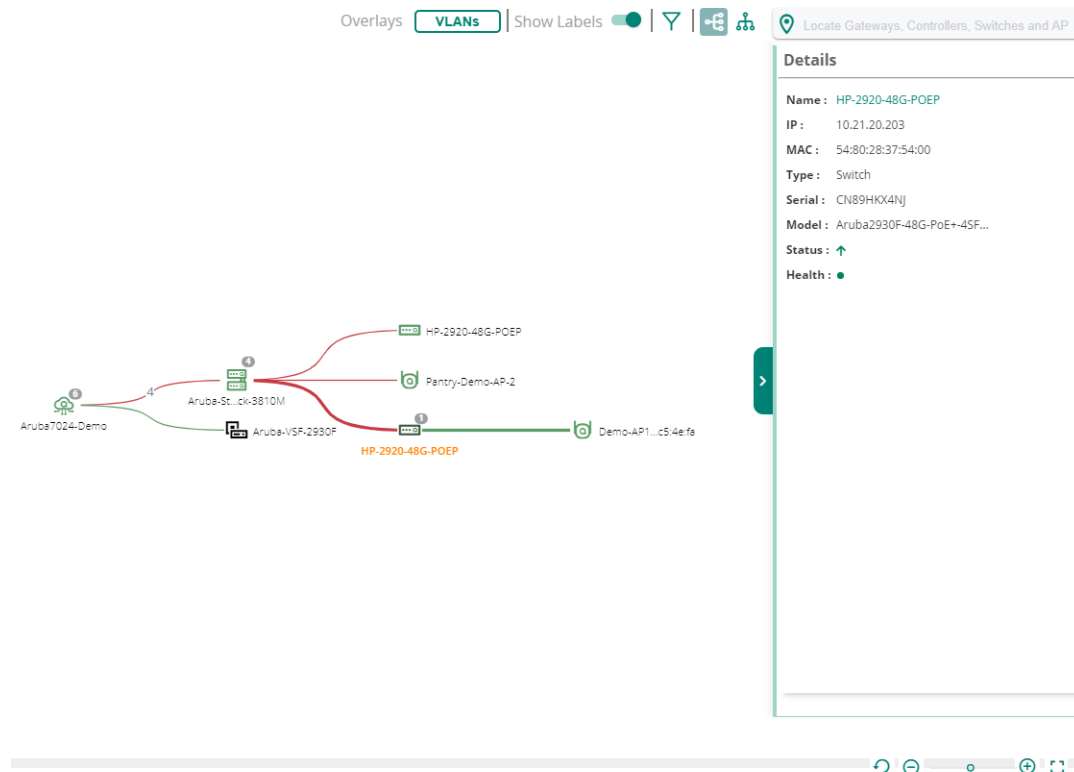
A green bullet icon indicates that the device health is good when the CPU usage is lower than or equal to 75% and the memory usage is lower than or equal to 75%. A yellow bullet icon indicates that the device health is fair when

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 58 *Details Pane*



- Access Point—Displays the following details:

- **Name**—Hostname of the AP. Click the AP name to view the **Access Point Details** page.
- **IP**—IP address of the AP.
- **MAC**—MAC address of the AP.
- **Type**—Type of the device.
- **Serial**—Serial number of the AP.
- **Model**—Hardware model of the AP.
- **Status**—Operational status of the AP.
- **Health**—Operational health of the AP.

- Branch Gateway—Displays the following details:

- **Name**—Hostname of the Branch Gateway. Click the Branch Gateway name to view the **Gateway Details** page.
- **IP**—IP address of the Branch Gateway.
- **MAC**—MAC address of the device.
- **Type**—Type of device deployment.
- **Serial**—Serial number of the Branch Gateway.

- **Model**—Hardware model of the device.
- **Status**—Operational status of the device.
- **Health**—Operational health of the device.
 - **VPNC**—Displays the following details:
- **Name**—Hostname of the VPNC. Click the VPNC name to view the **Gateway Details** page.
- **IP**—IP address of the VPNC.
- **MAC**—MAC address of the device.
- **Type**—Type of device deployment.
- **Serial**—Serial number of the VPNC.
- **Model**—Hardware model of the device.
- **Status**—Operational status of the device.
- **Health**—Operational health of the device.
 - **Unmanaged**—Displays the following details:
- **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.



The value of the parameters are empty if LLDP does not provide the neighbor information.

- **Switch**—Displays the following details:
 - **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**—Displays the following details:
 - **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.
 - **Health**—Operational health of the switch.

- **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—Displays the following details:
- **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.

The **VSX** section displays the following details:

- **ISL State**—State of the ISL connection with the peer AOS-CX switch. Following are the supported values:
 - **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.
 - **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:
 - **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:
 - **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.
 - **Tunnel**—Displays the following information about tunnels configured on the Branch Gateway:
 - **Map Name**—Name of the tunnel interface.
 - **Peer MAC**—MAC address of the peer device with which the tunnel was established.
 - **Local MAC**—MAC address of the Branch Gateway.
 - **Source IP**—Source IP address from where the traffic originates.
 - **Destination IP**—IP address to which the traffic is sent.
 - **Established Time**—Timestamp showing when the tunnel was established.
 - **VLAN**—VLAN ID of the tunnel.
 - **Source Serial**—Source Serial of the tunnel.
 - The tunnel in green color indicates that the tunnel is up. The tunnel in red color indicates that the tunnel is down.
 - **Uplink**—Displays the following information about uplinks configured on the Branch Gateway:
 - **Uplink Type**—Type of the uplink.
 - **VLAN**—VLAN ID of the uplink.
 - **Link Status**—Uplink status.
 - **Description**—Description of the uplink.
 - **WAN Status**—WAN status.
 - **IP Address**—IP address of the WAN interface.
 - **Public IP Address**—Public IP address.
 - **Device MAC**—MAC address of the device.
 - **Serial**—Serial number of the device.
 - **Port Number**—Port number of the device.
 - **Tunnels**—Displays a list of tunnels mapped to the uplink. Click the drop-down on each tunnel to view the tunnel details.
 - The uplink in green color indicates that the uplink is up. The uplink in red color indicates that the uplink is down.
 - **Edge**—Displays the following information about the link:
 - **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.



In case of Branch Office Controller (BOC) to Switch link, if a peer Branch Gateway link is configured for redundancy, link details are displayed for the peer Branch Gateway to switch link as well.

- Unmanaged edge—Displays the following information about all the links:
 - **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—Displays the following information about the ISL edge:
 - **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. This section also displays the details of the devices connected to these interfaces. It displays the following details:
 - **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:
 - **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**

| | |
|--|------------|
| Alerts & Events | 479 |
| Viewing Audit Trail | 504 |
| Using Troubleshooting Tools | 504 |
| Reports | 528 |
| Managing Software Upgrades | 539 |

The AOS 10.x uses the Network Operations app to analyze the network by using different types of alerts and events, tools and reports.

Alerts & Events

The **Alerts & Events** pane displays all types of alerts and events generated for events pertaining to device provisioning, configuration, and user management.

- To view alerts and events: [Alerts & Events Dashboard](#)
- Types of view:
 - [Viewing Alerts in List View](#)
 - [Viewing Events in List View](#)
 - [Viewing Alerts & Events in Summary View](#)
 - To collect event logs: [Dynamic Logs](#)
 - To configure alerts: [Configuring Alerts](#)
 - To add default recipients: [Adding Default Recipients](#)
 - To suppress alert notifications: [Suppressing Alerts](#)
 - Types of Alerts:
 - [User Alerts](#)
 - [Switch Alerts](#)
 - [Gateway Alerts](#)
 - [AP Alerts](#)
 - [Connectivity Alerts](#)
 - [Configuration Change Alerts](#)
 - [Site Alerts](#)
 - To view enabled alerts: [Viewing Enabled Alerts](#)

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 Events in List View](#)
- [Dynamic Logs](#)
- [Viewing Alerts & Events in Summary 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 > Access Points**.
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 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**.



The **Gateway Emergency Mode** and **VPN Peer Failover** alerts can be configured and enabled for all gateways. However, these alerts will not be generated for gateways on versions other than ArubaOS 8.0.x.

3. 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.
4. Optionally, enable the **Show Acknowledged Alerts** button to display the list of acknowledged alerts.

Table 145: *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. |

Filtering Events at an Advanced Level


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. Under **Alerts & Events > 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 **Alerts** table:

Table 146: 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 in List View

To view a summary of 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 > Access Points**. 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** dashboard 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.

Filtering Events at an Advanced Level

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. Under **Alerts & Events > 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 147: *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, Gateway, and 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. |
| Group | Displays the group name of the event. |
| Description | Displays the description of the event. Use the column filter to filter an event based on the description. |

For events related to IAPs running ArubaOS version 10.x or later, Aruba Central offers additional details regarding the selected event. Click the expand arrow in the events row for the IAP, to see the additional details.

If you have an IAP running ArubaOS version 10.2 or later, the expanded text box for an event displays more data compared to a similar event generated for an IAP running an earlier version of ArubaOS.

The additional details expansion box is not available for events related to gateways, switches, and IAPs running an ArubaOS version which is earlier than 10.x.

Figure 59 Additional Details for an Event Related to an IAP running ArubaOS version 10.2

| Occurred On | Device Type | Event Type | Description |
|-----------------------|-------------|--------------------------|--|
| Dec 8, 2020, 12:45:03 | CLIENT | Client Roaming Success | Client a4:83:e7:97:3d:c5 roamed successfully to SSID 555-cap on channel 52 of AP host... |
| Dec 8, 2020, 12:44:13 | CLIENT | Client Roaming Success | Client a4:83:e7:97:3d:c5 associated to BSSID 48:4a:e9:7ca7:92 on channel 36E of AP ho... |
| Dec 8, 2020, 12:44:13 | CLIENT | Client DHCP Acknowledged | DHCP acknowledgement received from DHCP server 10.29.6.162 for client a4:83:e7:97:... |


| Client IP | Client Hostname | DHCP Server IP | Lease Time |
|-------------|-----------------|----------------|------------|
| 10.29.6.179 | arubas-Mac-mini | 10.29.6.162 | 1 day |


| Latency (ms) | Gateway | DNS Server IP |
|--------------|-------------|---------------|
| 3 | 10.29.6.162 | 10.44.17.241 |

Figure 60 Additional Details for an Event Related to an IAP running ArubaOS version 10.1

| Occurred On | Device Hostname | Device MAC | Client MAC | BSSID | Event Type | Loading... | Site |
|------------------------|-----------------|---------------|---------------|---------------|--------------------------|------------|------|
| Nov 17, 2020, 19:09:52 | c2c-324-1 | b45d50c682a4 | 2cf0a2f1de:fc | b45d50e82a55 | Client DHCP Acknowledged | | test |
| Nov 17, 2020, 19:09:52 | c2c-324-1 | b45d50c682a4 | 2cf0a2f1de:fc | b45d50e82a55 | Client DHCP Acknowledged | | test |
| Nov 17, 2020, 19:09:52 | c2c-324-1 | b45d50c682a4 | 2cf0a2f1de:fc | b45d50e82a55 | Client DHCP Acknowledged | | test |
| Nov 17, 2020, 19:06:53 | f05c19c9f7:12 | f05c19c9f7:12 | 2cf0a2f1de:90 | f05c191f71:35 | Client DHCP Acknowledged | | test |

| DHCP Server IP |
|----------------|
| 192.168.2.4 |

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. You can also use the **Events > Dynamic Logs** tab to dynamically troubleshoot and collect debugging logs when events are generated in the network. For more information, see [Dynamic Logs](#).

Dynamic Logs

The Dynamic Logs feature enables Aruba Central to dynamically run CLI commands on APs and gateways and collect the output as logs. You can use the logs to troubleshoot the APs and gateways. Dynamic Logs also sends notifications to Aruba Support team for the same, when events listed in [Table 2](#) are generated in the network.

The Dynamic Logs feature is a limited availability feature in Aruba Central. If you wish to enable the feature, contact your Aruba Representative. If Dynamic Logs is not enabled for the Aruba Central account, the tab is not displayed.

The Dynamic Logs workflow is as follows:


- In an Aruba Central managed network, events generated from APs or gateways trigger Dynamic Logs.
- When such an event is generated, Dynamic Logs automatically initiates the troubleshooting services associated with the specific type of event. The troubleshooting service has a defined troubleshooting recipe for each type of event.
- Based on the event type, the recipe executes the pre-defined CLI commands on the devices, collects all the debugging logs, uploads to a secure location, and sends a notification to the Aruba Support team.
- The Aruba Support team downloads and analyzes the debugging logs. Upon analyzing, it registers a TAC Case and notifies the corrective actions to the user.

To configure the **Dynamic Logs**, complete the following procedure:

1. In the **Network Operations** app, set the filter to **Global**.
The dashboard context for the filter is displayed.
2. Under **Analyze**, click **Alerts & Events**.
The **Alerts & Events** pane is displayed in the **List** view.
3. In the **Alerts & Events** page, click the **Config** icon.
By default, the **Alert Severities & Notifications** page is displayed.
4. Click the **Dynamic Logs** tab.
The **Dynamic Logs** page is displayed.
5. Enable the **Dynamic logs collection** toggle button in order collect logs when applicable events occur.
6. Optionally, select the **Notify Aruba Support** check box, if you want to notify the Aruba Support team.
7. Click **Save**.

Dynamic Logs is supported for both APs and Gateways. For a device with a Foundation license, Dynamic Logs only collects the logs and does not notify Aruba support, even if the option is enabled. The Aruba support notification option is only supported for an AP or gateway with an Advanced license.

To view the **Dynamic Logs** notifications, complete the following procedure:





1. In the **Network Operations** app, click the  notification icon.
The **Notifications** window is displayed.
2. Click the **Dynamic Logs** tab.
A list of **Dynamic Logs** events are displayed.
3. Click **View all**.
The **Alerts & Events** pane is displayed in the **List** view.
4. In the **Alerts & Events** page, click the **Config** icon.
By default, the **Alert Severities & Notifications** page is displayed.
5. Click the **Dynamic Logs** tab.
The **Dynamic Logs** page is displayed.


To filter Dynamic Logs events based on event types, complete the following procedure:



1. In the **Alerts & Events > Events** page, click **Click here for advanced filtering** to filter the dynamic logs based on event types.
2. Select the event type and click **Filter**. You can select multiple event types from the advanced filtering option.
3. Click **Clear All** to clear the selected event types from the advanced filtering option.

The following table describes the information displayed in each column of the **Events** table:

Table 148: *Dynamic Logs Table Parameters*

| 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, Client, Gateway, Switch . Use the filter option to filter events by device type. |
| Device Hostname | Displays the host name of the device where the event is generated. Use the filter option to filter events by device hostname. |
| Device MAC | Displays the MAC address of the device. Use the filter option to filter events by device MAC address. |
| Client MAC | Displays the MAC address of the device to which the client is connected. Use the filter option to filter events by client MAC address. |
| BSSID | Displays the BSSID of the device. Use the filter option to filter events by device BSSID. |
| Event Type | Displays the type of the event. |
| Label | Labels associated with the device. |
| Site | The site to which the device belongs. |
| Group | The group to which the device belongs. |
| Description | Displays the description of the event. |
| Dynamic Logs | <p>Use the filter option to filter events by All or CLI data.</p> <ul style="list-style-type: none"> ■ Hover over the  icon to view the event type and the list of CLI commands associated with the event. ■ Hover over the  icon and click Download from the drop-down to download the dynamic logs. ■ Hover over the  icon and click Email from the drop-down to e-mail the dynamic logs. The content of the e-mail includes the metadata associated with the event, the list of CLI commands, the url link for the users to view the troubleshooting command output, and the url link for the Aruba Support team to access the troubleshooting data. |
| Aruba Support | <p>Provides the following information:</p> <p>The  icon indicates that the notification has been sent to the Aruba Support team.</p> |

| Data Pane Content | Description |
|-------------------|--|
| | Click the  icon to view the TAC Notes. The TAC Notes includes the analysis of the debugging logs and the corrective actions for the TAC Case, registered by the Aruba Support team. |

To customize the **Events** table, click the  eclipses icon to select the required columns, or click **Reset to default** to set the table to the default columns. To autofit the columns, click the  eclipses icon and select **Autofit columns**.

Click the  icon to download the dynamic log events list in a CSV format.

Table 149: *Dynamic Logs Events List*

| Device | Event Name | Description |
|---------|--|---|
| Gateway | Tunnel State Change | This event is received when an IPSec tunnel goes down. |
| AP | Client 802.11 Association Reject | This event is received when 802.11 association is rejected for a client. |
| | Client 802.11 Authentication Failure | This event is received when 802.11 authentication failure occurs for a client. |
| | Client MAC Authentication Reject | This event is received when MAC authentication for a client fails from the radius server. |
| | Client 802.1x Radius Timeout | This event is received when a client does 802.11 authentication and the request to radius server times out. |
| | Client Captive Portal Authentication Failure | This event is received when captive portal authentication fails for a client. |

Table 150: Dynamic Logs CLI List

| Device | CLI Name | Description |
|---------|--|--|
| Gateway | <code>show aruba-central control-channel</code> | The output of the command displays the list of all the gRPC call counters. |
| | <code>show crypto oto</code> | The output of the command displays the current state of the overlay tunnel connection between Aruba Central and the device. |
| | <u>show crypto-local ipsec-map</u> | The output of the command displays the current IPsec configuration on the controller. |
| | <u>show datapath session table</u> | The output of the command displays the datapath session table entries of the managed device. |
| | <u>show crypto ipsec sa</u> | The output of the command displays the IPsec security associations (SAs). |
| | <u>show datapath frame counters</u> | The output of the command displays frame statistics that are received and transmitted from the datapath of the controller. |
| | <u>show datapath error counters</u> | The output of the command displays error statistics in the datapath of the controller. |
| | <u>show datapath tunnel</u> | The output of the command displays a list of tunnels. |
| | <u>show log security all</u> | The output of the command displays all security related logs on a Mobility Conductor or on a managed device. |
| AP | <u>show ap debug client-stats</u> | The output of the command displays the detailed statistics about a client from an AP. |
| | <u>show log security 50 <client mac></u> | The output of the command displays the most 50 recent security log entries for a specific client MAC address. |
| | <u>show ap debug auth-trace-buf mac <client mac></u> | The output of the command displays the authentication trace information for a specific client MAC address. |
| | <u>show running-config</u> | The output of the command displays the current and pending configuration on the Mobility Conductor. |
| | <u>show log user 50 <client-mac></u> | The output of the command displays the last 50 log output entries of the controller. |
| | <u>show ap debug mgmt-frames mac <client-mac></u> | The output of the command displays the trace information for the 802.11 management frames for an AP. The <code><client mac></code> parameter displays the AP associations for a specific client MAC address. |
| | <u>show log driver-log <client-mac></u> | The output of the command displays the status of drivers configured on the AP. |

Viewing Alerts & Events in Summary View

To view a summary of alerts and events and acknowledge alerts, 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 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 list view, summary view, and a configuration view.



Configuration view is only available at the Global context.

3. To view graphs displaying alerts and events, click the **Summary** icon. By default, **All** tab is selected. Select each tab **Access Points**, **Switches**, or **Gateways** 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, set the filter to **Global**.
The dashboard context for the 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** page is displayed.
4. Use the tabs to navigate between the alert categories. 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.
 - **Sites**—Select a site to limit the alert to a specific site.
- d. **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.
 - **Webhook**—Select the **Webhook** check box and select the Webhook from the drop-down list.
 - **Syslog**—Select the **Syslog** checkbox to receive the syslog notifications when an alert is generated.
- e. Click **Save**.
- f. **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 network administrators and users with admin permissions to configure alerts. For more information, see [Configuring Alerts](#).

Following are the user management alerts that you can configure:

- **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.

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:

- **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 and MAS switches:

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.

MAS switches

- Fan failure.
- High temperature.
- **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** 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.

Gateway Alerts

Aruba Central allows network administrators and users with admin permissions to configure alerts. For more information, see [Configuring Alerts](#).

Following are the SD-WAN and Gateway appliance-related alerts that you can configure:

- **SLA DPS Compliance Violations**—Generates an alert when the WAN policy does not meet the compliance criteria.
- **New Gateway Connected**—Generates an alert when a new Branch Gateway is connected.
- **Gateway Disconnected**—Generates an alert when a Branch Gateway is disconnected.
- **Blocked Session Detected**—Generates an alert when a blocked session is detected.

- **Gateway CPU Utilization**—Generates an alert when the Branch Gateway CPU utilization exceeds the threshold value. You can add additional rule(s) for this alert.
- **Gateway Memory Utilization**—Generates an alert when the Branch Gateway memory utilization exceeds the threshold value. You can add additional rule(s) for this alert.
- **Gateway Emergency Mode**—Generates an alert when a gateway enters the emergency mode, where all the uplinks are down and the backup uplink is activated.
- **OSPF Session Error**—Generates an alert when an OSPF session fails.
- **BGP Session Error**—Generates an alert when a BGP session fails.
- **Gateway Base License Capacity Limit Exceeded**—Generates an alert when a Gateway with Foundation-Base Capacity subscription exceed the client capacity threshold.
- **WAN Health-Check Failure**—Generates an alert when WAN health check fails.
- **WAN VPN-Peer Unreachable**—Generates an alert when the WAN VPN peer is unreachable.
- **VPN Peer Failover**—Generates an alert when the VPN peer fails over.
- **WAN Uplink Status Change**—Generates an alert when the WAN uplink status changes.
- **WAN Uplink Autonegotiation State Change**—Generates an alert when the WAN uplink automatic negotiation status changes.
- **WAN Uplink Input Errors**—Generates an alert when the WAN uplink input errors exceed the threshold value. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **WAN Uplink Output Errors**—Generates an alert when the WAN uplink output errors exceed the threshold value. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **WAN Uplink PHY Errors**—Generates an alert when the WAN uplink PHY errors exceed the threshold value. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **DHCP Pool Consumption Alert**—Generates an alert when the DHCP pool consumption exceeds the threshold value. In the **Subnet** field, enter the subnet address to filter the alert based on subnet.
- **IPSec Establishment Failure**—Generates an alert when the IPsec tunnel fails to establish.
- **IPSec SA Down**—Generates an alert when the IPsec SA is down.
- **All IPSec SAs Down**—Generates an alert when all the IPsec SAs are down.
- **CFG-SET Advertisement Failure**—Generates an alert when the CFG-SET advertisement fails.
- **Uplink Flapping**—Generates an alert when the uplink state changes frequently. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **Tunnel Flapping**—Generates an alert when the tunnel state changes frequently. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **Uplink Speed Flapping**—Generates an alert when the uplink speed changes. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **EST Enrollment Failure**—Generates an alert when the Virtual Gateway fails to enroll with the EST server.
- **VGW VM Down**—Generates an alert when an Aruba Virtual Gateway deployed as a Virtual Machine is down.
- **Gateway Cluster VLAN Mismatch**—Generates an alert when one or more gateway(s) in a cluster have a mismatch in the VLAN.
- **Gateway Joining Cluster**—Generates an alert when a gateway joins the cluster.
- **Gateway Leaving Cluster**—Generates an alert when a gateway leaves the cluster.
- **Gateway Cluster Leader Change**—Generates an alert when there is cluster leader change.
- **Gateway Cluster Client Capacity**—Generates an alert when the cluster client capacity exceeds the configured threshold.
- **Gateway Firmware Upgrade Failed**—Generates an alert when there is a firmware upgrade failure.



Alerts that fall under WAN/ Tunnels/ DPS/ Routing/ Firewall are not applicable to AOS 10.x deployments.

AP Alerts

Aruba Central allows network administrators and users with admin permissions to configure alerts. For more information, see [Configuring Alerts](#).

Following are the access point (AP) alerts that you can configure:

- **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.
- **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 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.
- **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.
- **IAP Firmware Upgrade Failed**—Generates an alert when there is any AP 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.

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 failuresSet 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 failuresSet 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.

Configuration Change 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. For more information on how to configure alerts, see [Configuring Alerts](#). 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 151: *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 |

| User Action | Group Name | Device Type | User ID | Config Change | Device Serial/ MAC |
|--|--|----------------------|---------|------------------------------|--------------------|
| 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 |

Site Alerts

Aruba Central allows you to configure and enable this alert for aggregated device disconnects. For more information on how to configure alerts, see [Configuring Alerts](#).

The Aggregated Device Disconnections alert is under **Site** tab. It 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 Notifications** screen 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**.

Suppressing Alerts

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.
The **Suppress Alerts** dialog box is displayed for confirmation.
5. Click **Suppress Alerts**.
6. Click **Save**.

Configuring Alert Notifications at the Site Level

Aruba Central 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 in the site dashboard, 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 in the site dashboard, 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 steps:

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 **Enabled**.
Use the tabs to navigate between the alert categories. The alerts enabled for each category are displayed in the respective tabs.

Dynamic Logs

The Dynamic Logs feature enables Aruba Central to dynamically run CLI commands on APs and gateways and collect the output as logs. You can use the logs to troubleshoot the APs and gateways. Dynamic Logs also sends notifications to Aruba Support team for the same, when events listed in [Table 2](#) are generated in the network.

The Dynamic Logs feature is a limited availability feature in Aruba Central. If you wish to enable the feature, contact your Aruba Representative. If Dynamic Logs is not enabled for the Aruba Central account, the tab is not displayed.

The Dynamic Logs workflow is as follows:

- In an Aruba Central managed network, events generated from APs or gateways trigger Dynamic Logs.
- When such an event is generated, Dynamic Logs automatically initiates the troubleshooting services associated with the specific type of event. The troubleshooting service has a defined troubleshooting recipe for each type of event.
- Based on the event type, the recipe executes the pre-defined CLI commands on the devices, collects all the debugging logs, uploads to a secure location, and sends a notification to the Aruba Support team.
- The Aruba Support team downloads and analyzes the debugging logs. Upon analyzing, it registers a TAC Case and notifies the corrective actions to the user.

Configuring Dynamic Logs

To configure the **Dynamic Logs**, complete the following procedure:

1. In the **Network Operations** app, set the filter to **Global**.
The dashboard context for the filter is displayed.
2. Under **Analyze**, click **Alerts & Events**.
The **Alerts & Events** pane is displayed in the **List** view.
3. In the **Alerts & Events** page, click the **Config** icon.
By default, the **Alert Severities & Notifications** page is displayed.


4. Click the **Dynamic Logs** tab.
The **Dynamic Logs** page is displayed.
5. Enable the **Dynamic logs collection** toggle button in order collect logs when applicable events occur.
6. Optionally, select the **Notify Aruba Support** check box, if you want to notify the Aruba Support team.
7. Click **Save**.

Device Licensing for Dynamic Logs

Dynamic Logs is supported for both APs and Gateways. For a device with a Foundation license, Dynamic Logs only collects the logs and does not notify Aruba support, even if the option is enabled. The Aruba support notification option is only supported for an AP or gateway with an Advanced license.

Viewing the Dynamic Logs Notifications

To view the **Dynamic Logs** notifications, complete the following procedure:

1. In the **Network Operations** app, click the  notification icon.
The **Notifications** window is displayed.
2. Click the **Dynamic Logs** tab.
A list of **Dynamic Logs** events are displayed.
3. Click **View all**.
The **Alerts & Events** pane is displayed in the **List** view.
4. In the **Alerts & Events** page, click the **Config** icon.
By default, the **Alert Severities & Notifications** page is displayed.
5. Click the **Dynamic Logs** tab.
The **Dynamic Logs** page is displayed.

Filtering Events at an Advanced Level






To filter Dynamic Logs events based on event types, complete the following procedure:



1. In the **Alerts & Events > Events** page, click **Click here for advanced filtering** to filter the dynamic logs based on event types.
2. Select the event type and click **Filter**. You can select multiple event types from the advanced filtering option.
3. Click **Clear All** to clear the selected event types from the advanced filtering option.

The following table describes the information displayed in each column of the **Events** table:

Table 152: *Dynamic Logs Table Parameters*

| 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 , Client , Gateway , Switch . Use the filter option to filter events by device type. |

| Data Pane Content | Description |
|------------------------|---|
| Device Hostname | Displays the host name of the device where the event is generated. Use the filter option to filter events by device hostname. |
| Device MAC | Displays the MAC address of the device. Use the filter option to filter events by device MAC address. |
| Client MAC | Displays the MAC address of the device to which the client is connected. Use the filter option to filter events by client MAC address. |
| BSSID | Displays the BSSID of the device. Use the filter option to filter events by device BSSID. |
| Event Type | Displays the type of the event. |
| Label | Labels associated with the device. |
| Site | The site to which the device belongs. |
| Group | The group to which the device belongs. |
| Description | Displays the description of the event. |
| Dynamic Logs | <p>Use the filter option to filter events by All or CLI data.</p> <ul style="list-style-type: none"> ■ Hover over the  icon to view the event type and the list of CLI commands associated with the event. ■ Hover over the  icon and click Download from the drop-down to download the dynamic logs. ■ Hover over the  icon and click Email from the drop-down to e-mail the dynamic logs. The content of the e-mail includes the metadata associated with the event, the list of CLI commands, the url link for the users to view the troubleshooting command output, and the url link for the Aruba Support team to access the troubleshooting data. |
| Aruba Support | <p>Provides the following information:</p> <p>The  icon indicates that the notification has been sent to the Aruba Support team.</p> <p>Click the  icon to view the TAC Notes. The TAC Notes includes the analysis of the debugging logs and the corrective actions for the TAC Case, registered by the Aruba Support team.</p> |

To customize the **Events** table, click the  icon to select the required columns, or click **Reset to default** to set the table to the default columns. To autofit the columns, click the  icon and select **Autofit columns**.

Click the  icon to download the dynamic log events list in a CSV format.

Table 153: *Dynamic Logs Events List*

| Device | Event Name | Description |
|---------|--|---|
| Gateway | Tunnel State Change | This event is received when an IPSec tunnel goes down. |
| AP | Client 802.11 Association Reject | This event is received when 802.11 association is rejected for a client. |
| | Client 802.11 Authentication Failure | This event is received when 802.11 authentication failure occurs for a client. |
| | Client MAC Authentication Reject | This event is received when MAC authentication for a client fails from the radius server. |
| | Client 802.1x Radius Timeout | This event is received when a client does 802.11 authentication and the request to radius server times out. |
| | Client Captive Portal Authentication Failure | This event is received when captive portal authentication fails for a client. |


Table 154: Dynamic Logs CLI List

| Device | CLI Name | Description |
|---------|--|--|
| Gateway | <code>show aruba-central control-channel</code> | The output of the command displays the list of all the gRPC call counters. |
| | <code>show crypto oto</code> | The output of the command displays the current state of the overlay tunnel connection between Aruba Central and the device. |
| | <u>show crypto-local ipsec-map</u> | The output of the command displays the current IPsec configuration on the controller. |
| | <u>show datapath session table</u> | The output of the command displays the datapath session table entries of the managed device. |
| | <u>show crypto ipsec sa</u> | The output of the command displays the IPsec security associations (SAs). |
| | <u>show datapath frame counters</u> | The output of the command displays frame statistics that are received and transmitted from the datapath of the controller. |
| | <u>show datapath error counters</u> | The output of the command displays error statistics in the datapath of the controller. |
| | <u>show datapath tunnel</u> | The output of the command displays a list of tunnels. |
| | <u>show log security all</u> | The output of the command displays all security related logs on a Mobility Conductor or on a managed device. |
| AP | <u>show ap debug client-stats</u> | The output of the command displays the detailed statistics about a client from an AP. |
| | <u>show log security 50 <client mac></u> | The output of the command displays the most 50 recent security log entries for a specific client MAC address. |
| | <u>show ap debug auth-trace-buf mac <client mac></u> | The output of the command displays the authentication trace information for a specific client MAC address. |
| | <u>show running-config</u> | The output of the command displays the current and pending configuration on the Mobility Conductor. |
| | <u>show log user 50 <client-mac></u> | The output of the command displays the last 50 log output entries of the controller. |
| | <u>show ap debug mgmt-frames mac <client-mac></u> | The output of the command displays the trace information for the 802.11 management frames for an AP. The <code><client mac></code> parameter displays the AP associations for a specific client MAC address. |
| | <u>show log driver-log <client-mac></u> | The output of the command displays the status of drivers configured on the AP. |


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.

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.
 - **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.

Using Troubleshooting Tools

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.



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.

This section includes the following topics:

- -
- -
- [Advanced Device Troubleshooting](#)

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 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 > Access Points**. 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** and 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:
 - [Important Points to Note](#)
 - [Troubleshooting Gateway Connectivity Issues](#)
 - [Troubleshooting Switch Connectivity Issues](#)

[Table 155](#) lists the tests available for each device type:

Table 155: Tests and Devices

| Test | Access Point | Switch | Gateway |
|---------------------------|---------------|---------------|---------------|
| Ping Test | Available | Available | Available |
| Ping Sweep Test | Not Available | Not Available | Available |
| Traceroute | Available | Available | Available |
| HTTP Test | Available | Not Available | Available |
| HTTPS Test | Available | Not Available | Available |
| TCP Test | Available | Not Available | Not Available |
| Speed Test (iPerf) | Available | Not Available | Available |

Devices which are already running commands shall not execute newly added commands.



This section includes the following topics:

- [Important Points to Note](#)
- [Troubleshooting Gateway Connectivity Issues](#)
- [Troubleshooting Switch 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:

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. 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.
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 APs:

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, the issue could be isolated to the client device.

To perform an HTTP test on APs:

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.

- 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, the issue could be isolated to the client device. HTTPS is a performance test to identify the time taken to load a web page.

To perform an HTTPS URL test on APs:

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.

- 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:

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.

- 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. The speed test diagnostic tool is available only for Instant AP. 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:

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**.
 - c. A list of access points is displayed in the **List** view.

- d. 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 more information about viewing and downloading the output, see [Viewing the Device Output](#).

Troubleshooting Gateway Connectivity Issues

The following tests are available to diagnose issues pertaining to WAN or SD-WAN 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 Gateways:

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 > Gateways**.
A list of gateways is displayed in the **List** view.
 - c. Click a gateway listed under **Device Name** for which you want to perform diagnostic test.
The dashboard context for the gateway is displayed.
2. Under **Analyze > Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Gateway**.
4. From the **Test** drop-down list, select **Ping Test**.

5. From the **Sources** drop-down list, select source(s). You can select multiple Gateways.
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 gateway.
 - 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 Gateways:

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 > Gateways**.
A list of gateways is displayed in the **List** view.
 - c. Click a gateway listed under **Device Name** for which you want to perform diagnostic test.
The dashboard context for the gateway is displayed.
2. Under **Analyze > Tools**, click **Network Check**.

3. From the **Device Type** drop-down list, select **Gateway**.
4. From the **Test** drop-down list, select **Traceroute**.
5. From the **Sources** drop-down list, select source(s). You can select multiple Gateways.
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.

Ping Sweep Test

Performs a more advanced check on host reachability and network connectivity. Sends different sizes of ICMP echo packets to the IP addresses of selected devices based on start packet size, end packet size and sweep interval field values.

To perform a ping sweep test on Gateways:

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 > Gateways**.
A list of gateways is displayed in the **List** view.
 - c. Click a gateway listed under **Device Name** for which you want to perform diagnostic test.
The dashboard context for the gateway is displayed.
2. Under **Analyze > Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Gateway**.
4. From the **Test** drop-down list, select **Ping Sweep Test**.
5. From the **Sources** drop-down list, select source(s). You can select multiple Gateways.
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. In the **Start Packet Size** field, enter the start packet size to capture and store the range of data packet to analyze network issues at a later stage. The range is from 10 to 1999 bytes.
8. In the **End Packet Size** field, enter the end packet size. The range is from 11 to 2000 bytes.
9. In the **Sweep Interval** field, enter the sweep interval size to set the sweep threshold for the transactions. The range is from 1 to 1990 bytes.
10. In the **Count** field, enter the count. The value should be between 1 to 1000.
11. Click **Run**. The test output is displayed in the **Device Output** section.

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 Gateways:

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 > Gateways**.
 - c. A list of access points is displayed in the **List** view.
 - d. 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 **Gateway**.
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 Gateways.
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.

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 Gateways:

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 > Gateways**.
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 **Gateway**.
4. From the **Test** drop-down list, select **HTTP Test**.
5. From the **Sources** drop-down list, select source(s). You can select multiple Gateways.
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. Click **Run**. The test output is displayed in the **Device Output** section.



NOTE

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 Gateways:

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 > Gateways**.
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 **Gateway**.
4. From the **Test** drop-down list, select **HTTPS Test**.
5. From the **Sources** drop-down list, select source(s). You can select multiple Gateways.
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. Click **Run**. The test output is displayed in the **Device Output** section.



NOTE

The test supports only IPv4 address or domain name in the **URL** field.

For more 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.

- a. In the **Repetitions** field, enter the repetition value. The value should be between 1 to 500.
- b. 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.

Traceroute

Tracks the packets routed from a network host.

To perform a traceroute 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 **Group**, **Label**, or **Site**. 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, Network Check**.
3. From the **Device Type** drop-down, select **Switch**.
4. From the **Test** drop-down list, select **Traceroute**.
5. From the **Sources** drop-down, select source(s). You can select multiple switches.
6. Enter the hostname or IP address in the **Hostname/IP Address** field.
7. To use additional parameters, click **Show Additional Test Settings** and select the **Use Management Interface** option, if you want to use the VRF Management interface. To use the VRF Default interface, clear this option.



Show Additional Test Settings is disabled when no Test type is selected.

Use Management Interface option is available only for AOS-CX switches

8. 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.

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 7.4.x CLI Reference Guide* for Mobility Access Switches 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**.

The dashboard context for the switch is displayed.

2. Under **Analyze > Tools** and click the **Device Check** tab. The **Device Check** page is displayed.
3. Select a device. You can run diagnostic checks on the following types of devices managed by Aruba Central:
 - [Troubleshooting Switch Issues](#)
 - [Troubleshooting Gateway Issues](#)

Troubleshooting Gateway Issues

To perform a device check on gateways, 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 > Gateways**.
A list of gateways is displayed in the **List** view.
 - c. Click a gateway under **Device Name** for which you want to perform diagnostic test.
The dashboard context for the gateway is displayed.
- 2. Under **Analyze > Tools**, click the **Device Check** tab.
The **Device Check** page is displayed.
- 3. From the **Sources** drop-down, select a gateway.
- 4. From the **Test** drop-down, select one of the following tests to perform diagnostic checks on the selected switch:
 - **Interface Bounce**—Restarts the port interface and forces a client to re-initiate a DHCP request.
 - **PoE Bounce**—Restarts the PoE port and the device that is either connected to the PoE port or powered by it.



If you select **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.

5. 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 Switch Issues

To perform a device check 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 the **Device Check** tab.
The **Device Check** page is displayed.
3. From the **Sources** drop-down, select a switch.
4. From the **Test** drop-down, 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 Aruba Switches only from version 16.05.000 or above.
Cable Test is not supported in Aruba CX switches.

- **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.

Important Point to Note



Interface Bounce, PoE Bounce, and Chassis Locate tests are supported only from the following versions in switches:

- Aruba Switches: 16.04.0000 or above
 - Aruba CX: See [Supported AOS-CX Platforms](#)
-

5. Click **Run**. The output is displayed in the **Device Output** section.

For information about viewing and downloading the output, see [Viewing the Device Output](#).

Unlike the other tests, for Cable Test, the output is displayed in a tabular format, and you cannot download, email, or export the 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 7.4.x CLI Reference Guide* for Mobility Access Switches CLI command output
- *ArubaOS CLI Reference Guide* for SD-WAN Gateway 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.

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 > Access Points**. 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 Gateways](#)
 - [Troubleshooting Switches](#)



Devices which are already running shall not execute newly added commands.

Troubleshooting APs

To troubleshoot APs at an advanced level:

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 device 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. (Optional) Enter the client MAC or IP address of the selected command and click **Apply**. If you do not want to apply any filter, click **Apply** without entering any value in the client MAC or IP address field.
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.



To perform advanced troubleshooting on Mobility Access Switches, the minimum version support is 7.4.0.6.

Troubleshooting Switches

To troubleshoot switches at an advanced level:

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**. A list of switches is displayed in the **List** view.
 - c. Click a switch listed under **Device Name** for which you want to perform diagnostic test. The dashboard context for the device is displayed.
2. Under **Analyze > Tools**, click **Commands**.
3. In the **Commands** tab, select the device type as **Switch**.
4. From the **Available Devices** drop-down list, select the switch. You can select multiple switches.
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. (Optional) Enter the client MAC or IP address of the selected command and click **Apply**. If you do not want to apply any filter, click **Apply** without entering any value in the client MAC or IP address field.

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.

Troubleshooting Gateways

To troubleshoot Gateways at an advanced level:

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 > Gateways**.
 - c. A list of switches is displayed in the **List** view.
 - d. Click a gateway listed under **Device Name** for which you want to perform diagnostic test.
 - e. The dashboard context for the device is displayed.
1. Under **Analyze > Tools**, click **Commands**.
2. In the **Commands** tab, select the device type as **Gateway**.
3. From the **Available Devices** drop-down list, select the Gateway. You can select multiple Gateways.
4. Select any command category and the **Commands** pane displays the associated commands.
5. Click **Add>** to add the selected commands to the **Selected Commands** pane.
6. (Optional) Select command(s) and click **<Remove** to remove selected command(s) or click **<Remove All** to clear the **Selected Commands** pane.
7. (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.
8. Click **Run**. The output is displayed in the **Device Output** section.

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. There are two types of filtration available:

- Mandatory filters— Commands marked with '*'
 1. Based on your device perform the task till step 4.

2. Select the command marked with '*' and click **Add**.
The **Additional Filters** dialog box appears.
3. Enter the Client MAC address/ IP Address/ Port number as required.
4. 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.

5. (Optional) Click **Edit All** to reset the filtration parameters for all the commands added in the selected command pane.

- Optional filters— Commands marked with '+'

1. Based on your device perform the task till step 4.
2. Select the command marked with '*' and click **Add**. The **Additional Filters** dialog box appears.
3. Enter the Client MAC address/ IP Address/ Port number as required.
4. 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.

5. (Optional) Click **Edit All** to reset the filtration parameters for all the commands added in the selected command pane.

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 is automatically cleared.

You can perform the following tasks from the **Device Output** section:

1. 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.
2. Click the **Search** icon to search for text in the output.
3. Click the **Email** icon and click **Send** to send the output as an email. You can also add email recipients in the **CC** field.
4. Click the **Export** to export the command output as a zip file.
5. 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:

- *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 Access Points

To troubleshoot APs at an advanced level:

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:
 - 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.

To perform advanced troubleshooting on APs, the minimum software version required on Instant APs is 6.4.3.1-4.2.0.3.

To perform advanced troubleshooting on Mobility Access Switches, the minimum version support is 7.4.0.6.

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.



For information about viewing and downloading the output, see [Viewing the Device Output](#).

Troubleshooting Gateways

To troubleshoot Gateways at an advanced level:

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 > Gateways**.
A list of gateways is displayed in the **List** view.
 - c. Click a gateway listed under **Device Name** for which you want to perform diagnostic test.
The dashboard context for the gateway is displayed.
- 2. Under **Analyze > Tools**, click **Commands**.
- 3. In the **Commands** tab, select the device type as **Gateway**.
- 4. From the **Available Devices** drop-down list, select the gateway. You can select multiple gateways.
- 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** 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 Switches

To troubleshoot switches at an advanced level:

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 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:
 - 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](#).

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.

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 **Gateways**.
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 **Gateway** 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 '*'

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 '+'

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.

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 7.4.x CLI Reference Guide* for Mobility Access Switches CLI command output
- *ArubaOS CLI Reference Guide* for SD-WAN Gateway CLI command output

Reports

The Aruba Central 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 for Foundation and Advanced licenses for APs, switches, and gateways. The **Network Summary** report is available for 1 year and all other reports are available for 90 days.

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:

- [Previewing the Report](#)
- [Creating a Report](#)
- [Editing a Report](#)
- [Viewing the Scheduled Report](#)
- [Viewing the Generated Report](#)
- [Downloading a Report](#)
- [Deleting a Report](#)
- [Report Categories](#)

Previewing the 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 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, or for a custom range.
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**. 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](#).

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, or for a custom range.

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 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.



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**—Time when the report was last run.
- **Group/Device**—The group or device for which the report was run.
- **Label/Site**—The label or site for which the report was run.

- **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.

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 table is displayed in the **List** view.
4. In the **Generated Reports** table, hover over the report you want to delete.
5. Click the **Delete Report** icon.
6. Click **Yes** in the **Delete Report** pop-up window to delete the report.

Deleting Multiple Reports

To 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. In the **Generated Reports** table, select multiple reports that you want to delete.
A pop-up window displays the number of selected items.
5. Click the  icon.
6. Click **Yes** in the **Delete Report** pop-up window to delete the reports.

Report Categories

Aruba Central allows you to create various types of reports based on your network requirements.

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.

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.
- **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.

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.

The following list provides information about the types of report under each category of report:

- **Clients**
 - **Client Inventory**—The Client Inventory report provides information about the total number of clients and the type of connected networks that assists the administrators in planning for scalability and to evaluate the deviations from the baseline. You can select the context of the report from the available options:
 - **Groups**
 - **Labels**
 - **Sites**
- **Groups**
- **Labels**
- **Sites**
 - **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. In the Central 2.5.3 release, the report also projects the WLAN user experience to assist the user in measuring the efficiency of the deployed networks. You can select the context of the report from the available options:
 - **Groups**
 - **Labels**
 - **Sites**
 - **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. You can select the context of the report from the available options:
 - **Groups**
 - **Labels**
 - **Sites**

- **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**. You can choose to generate a report from **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. You can select the context of the report from the available options:

- **Groups**
- **Label**
- **Site**



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. You can select the context of the report from the available options:

- **Groups**
- **Label**
- **Site**

- **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**.

- **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. You can select the context of the report from the available options:

- **Groups**
- **Label**
- **Site**

- **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. You can select the context of the report from the available options:

- **Groups**
- **Label**
- **Site**
 - **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. You can select the context of the report from the available options:
- **Groups**
- **Label**
- **Site**
 - **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. You can select the context of the report from the available options:
- **Groups**
- **Label**
- **Site**
 - **RF Health**—The RF Health report provides detail of the radios of an access point with poor health indicators and assists the administrator in evaluating the deviation from the network baselines. You can select the context of the report from the available options:
- **Groups**
- **Label**
- **Site**
 - **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. You can select the context of the report from the available options:
- **Groups**
- **Label**
- **Site**



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. You can select the transport type for the report from the available options:
- **Overlay**
- **Underlay**
 - **WAN Inventory**—Displays a list of Branch Gateways onboarded. The report is segregated by ArubaOS software version.
 - **WAN Compliance**—Displays the worst performing or best performing links according to the SLA compliance violations.
 - **WAN Transport Health**—Displays the top N links with probed values. You can select the transport type for the report from the available options:
- **Overlay**
- **Underlay**

- **WAN Utilization**—Displays WAN bandwidth utilization information for Underlay, Overlay, and overall network. You can select the transport type for the report from the available options:
 - **Overlay**
 - **Underlay**
 - **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. You can select the transport type for the report from the available options:
 - **Internet**
 - **VPN**
 - **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 context available for this report is only **Groups**.
 - **RAPIDS**—Displays the details of all the rogue devices in the network that assists the administrator about the possible threat and provides essential information needed to locate and manage the threat. You can select the context of the report from the available options:
 - **Groups**
 - **Label**
 - **Site**
 - **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. You can select the context of the report from the available options:
 - **Groups**
 - **Label**
 - **Site**
 - **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 context available for this report is only **Groups**.

Important Point 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.

Managing Software Upgrades

Software upgrades on devices is a time-consuming task that might require rebooting of devices leading to service disruption. Due to this, upgrades are performed during a maintenance window. The **Firmware** page provides an overview of the latest supported version of firmware for the device, details of the device, and the option to upgrade the device. You can also upgrade your devices using any one of the following upgrade types:

- **Standard Upgrade**—This upgrade type is common for all devices and happens simultaneously. During the upgrade, all the services goes down and comes back up after the upgrade is complete. This upgrade is recommended for operations during maintenance windows.
- **Live Upgrade**—This upgrade type is available only for APs and Gateways with clusters. This upgrade happens sequentially without any service disruption and is recommended for operations during working hours.



-
- Live upgrade requires all the devices in the site or group to be assigned with Advanced license. Make sure that you assign the devices with Advanced license before performing live upgrade.
 - Make sure that the Rapids is allow-listed for live upgrade operation.
-

Viewing Firmware Details

To view the firmware details for devices provisioned in Aruba Central:

1. In the **Network Operations** app, select one of the following options:
 - To select a group or site in the filter, set the filter to one of the options under **Groups** 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 **Gateways**. A list of devices is displayed.
 - c. Click a device listed under **Device Name**. The dashboard context for the device is displayed.

- Under **Maintain**, click **Firmware**. The **Firmware** dashboard displays the following information:

Figure 61 The following image displays the **Firmware** dashboard at the global level:

| Name | Site | Firmware Version | Recommended Version | Upgrade Status | Compliance Status |
|-----------------|----------------|------------------|---------------------|--------------------------|-------------------|
| dx15a6caca154 | C2C Site | 10.1.0.1_77499 | 8.6.0.4_74969 | Firmware up to date | Not Set |
| f42e7fcb6d98 | C2C Site | 10.1.0.1_77499 | 8.6.0.4_74969 | Firmware up to date | Not Set |
| instant-C6f786 | Site3_252 | 6.5.4.5_63174 | 6.5.4.15_73677 | Newer firmware available | Not Set |
| instant-C9AA34 | Site3_252 | 6.5.3.8_67000 | 8.6.0.4_74969 | Newer firmware available | Not Set |
| SetMeUp-C050CA | CI-151783 | 8.6.0.4_74969 | 8.6.0.4_74969 | Firmware up to date | Not Set |
| SetMeUp-C3AFEE6 | CI-151783 | 8.6.0.5_73491 | 8.6.0.4_74969 | Newer firmware available | Not Set |
| SetMeUp-C427D4 | new_vrf_test | 8.6.0.4_74969 | 8.6.0.4_74969 | Firmware up to date | Not Set |
| SetMeUp-C9AA2C | Site_253_oct23 | 8.6.0.4_74969 | 8.6.0.4_74969 | Firmware up to date | Not Set |
| SetMeUp-C9AA2C | vrf_sanity | 8.6.0.4_74969 | 8.6.0.4_74969 | Firmware up to date | Not Set |

Firmware Maintenance Window

The following are the data pane items and description:

- Access Points**—Displays the following information:
 - **Name**—Name of the AP. 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 [Dashboard for Wireless Clients](#).
 - **Site**—Displays the site information only on global context.
 - **Firmware Version**—The current firmware version running on the device.
 - **Latest Firmware Version**—The latest firmware version available on the public firmware server.
 - **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. The value displayed in this column is either **Set**, **Not Set**, and **Compliance scheduled on**. The **Compliance scheduled on** displays the date and time that is set in the Firmware Compliance Setting page.



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 [Dashboard for Wireless Clients](#). Click any site name from the **Site** column to view the site associated APs with their firmware details page.

2. **Switches**—Displays the following details about Aruba switches managed through Aruba Central:

- **Name**—Host name of the switch.
- **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.
- **MAC Address**—MAC address of the switch.
- **Model**—Hardware model of the switch.
- **Firmware Version**—The current firmware version running on the switch.
- **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. The value displayed in this column is either **Set**, **Not Set**, and **Compliance scheduled on**. The **Compliance scheduled on** displays the date and time that is set in the Firmware Compliance Setting page.



-
- The **Switch-MAS** tab is only available for accounts with MAS-switches.
 - The **Switches** tab displays details of both Aruba Switch and Aruba CX switches.
-

3. **Gateways**—Displays the following details about the gateways managed through Aruba Central in **Standalone** mode and in **Cluster** mode:

- a. **Standalone** mode:
 - **Name**—Host name of the gateways.
 - **Site**—Displays the site information only on global context.
 - **MAC Address**—MAC address of the gateways.
 - **Model**—Hardware model of the gateways.
 - **Firmware Version**—The current firmware version running on the gateways.

- **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. The value displayed in this column is either **Set**, **Not Set**, and **Compliance scheduled on**. The **Compliance scheduled on** displays the date and time that is set in the Firmware Compliance Setting page.
- b. **Cluster mode:**
 - **Name**—Host name of the gateways.
 - **Group**—Group name of the gateways.
 - **Firmware Version**—The current firmware version running on the gateways.
 - **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. The value displayed in this column is either **Set**, **Not Set**, and **Compliance scheduled on**. The **Compliance scheduled on** displays the date and time that is set in the Firmware Compliance Setting page.
4. **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.
 - **Upgrade Type**—This option is available only at the group context. Select any one of the following upgrade type:
 - **Standard**—Recommended for operations during maintenance windows.
 - **Live**—Recommended for operations during working hours.
 - **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**—To set the compliance to be carried out immediately.
 - **Later Date**—To set at the later date and time.
 - Click **Save and Upgrade** 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.
- **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**—To set the compliance to be carried out immediately.
 - **Later Date**—To set at the later date and time.
 - Click **Save and Upgrade** 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 Gateways 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.
 - **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**—To set the compliance to be carried out immediately.
 - **Later Date**—To set at the later date and time.
 - Click **Save and Upgrade** button to save the firmware compliance with the above settings. To clear the compliance, turn off the toggle switch.
- d. **Set Compliance for Gateways 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.
 - **Upgrade Type**—This option is available only at the group context. Select any one of the following upgrade type:
 - **Standard**—Recommended for operations during maintenance windows.
 - **Live**—Recommended for operations during working hours.
 - **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.



On live upgrade selection, auto reboot option is selected by default.

- **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**—To set the compliance to be carried out immediately.
 - **Later Date**—To set at the later date and time.
 - Click **Save and Upgrade** button to save the firmware compliance with the above settings. To clear the compliance, turn off the toggle switch.
5. **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.
 - **Upgrade Type**—This option is available only at the group and site context. Select any one of the following upgrade type:
 - **Standard**—Recommended for operations during maintenance windows.
 - **Live**—Recommended for operations during working hours.



Make sure that there are no APs in unprovided group when initiating live upgrade for all devices.

- **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**—To set the compliance to be carried out immediately.
- **Later Date**—To set at the later date and time.
 - **Upgrade**—Click this button to start 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 compliance must be carried out immediately or at a later date and time:

- **Now**—To set the compliance to be carried out immediately.
 - **Later Date**—To set at the later date and time.
 - **Upgrade**—Click this button to start the upgrade with the above settings.
 - **Cancel**—Click this button to cancel the upgrade.
- c. **To Upgrade all Gateways in Standalone Mode**—click **Upgrade All** and complete the following parameters in the **Upgrade Gateway 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 compliance must be carried out immediately or at a later date and time.
- **Now**—To set the compliance to be carried out immediately.
 - **Later Date**—To set at the later date and time.
 - **Upgrade**—Click this button to start the upgrade with the above settings.
 - **Cancel**—Click this button to cancel the upgrade.
- d. **To Upgrade all Gateways in Cluster Mode**—click **Upgrade All** and complete the following parameters in the **Upgrade Gateway Firmware** page:
- **Firmware Version**—Select the firmware version number from the drop-down list to which the compliance is required to be set.
 - **Upgrade Type**—This option is available only at the group context. Select any one of the following upgrade type:
 - **Standard**—Recommended for operations during maintenance windows.
 - **Live**—Recommended for operations during working hours.
 - **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.



On live upgrade selection, auto reboot option is selected by default.

- **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**—To set the compliance to be carried out immediately.
 - **Later Date**—To set at the later date and time.
 - **Upgrade**—Click this button to start the upgrade with the above settings.
 - **Cancel**—Click this button to cancel the upgrade.
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 gateways—MAC address and Model.
7. **Column Filter**—Clicking  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 or live upgrade.
10. **Cancel All**—Cancels a scheduled or live upgrade for all devices.

This section also includes the following topics:

- [Managing Software Upgrades](#)
- [Setting Firmware Compliance For Access Points](#)
- [Setting Firmware Compliance For Switches](#)
- [Setting Firmware Compliance For Gateways](#)

Upgrading a Single Device or Multiple Devices

To check a new version for a single device or multiple devices, complete the following steps:

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 **Gateways**. 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.

3. Select **Auto Reboot** if you want Aruba Central to automatically reboot after device upgrade.



The **Auto Reboot** option is available for Mobility Access Switches, Aruba Switch, Aruba CX switches, and Branch Gateways.

4. Specify if the upgrade must be carried out immediately or at a later date and time.
5. 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.
6. 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 Gateways) and AOS-S firmware version and CX firmware version (for Mobility Access Switches, Aruba Switch and Aruba CX 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.

6. In the **Upgrade Type**, select any one of the following:
 - Standard
 - Live



-
- The **Upgrade Type** option is available only at the group or site context.
 - Live upgrade operation requires the devices to be assigned with Advanced license. On the group dashboard, live upgrade is not initiated for the group if any of the device within the group is assigned with Foundation license. Aruba Central recommends that you create a group with devices that are assigned with Advanced license for seamless operation.
-

7. Select **Auto Reboot** if you want Aruba Central to automatically reboot after device upgrade.



The **Auto Reboot** option is available for Mobility Access Switches, Aruba Switch, Aruba CX switches, and Branch Gateways.

8. Specify if the upgrade must be carried out immediately or at a later date and time.
9. 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.
10. If the upgrade fails, retry upgrading your device.



After upgrading a switch, click **Reboot**.

Figure 62 The following is an example image of the **Upgrade Switch Firmware** window:

UPGRADE SWITCH FIRMWARE

Sites ▼

All devices will be upgraded

AOS-S Firmware Version ▼

CX Firmware Version ▼

Auto Reboot

When

Specify when to validate compliance and upgrade the non-compliant devices for the first time.

Now Later Date

Cancel **Upgrade**

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 gateways.
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. In the **Upgrade Type**, select one of the following options:
 - **Standard**
 - **Live**



The **Upgrade Type** option is available only at the group context.

7. Select one of the following as required:

- Select **Now** to set the compliance to be carried out immediately.
 - Select **Later Date** to set the compliance at the later date and time.
8. Click **Save and Upgrade**.
- 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.

The following image displays the **Manage Firmware Compliance** window for Access Points:

MANAGE FIRMWARE COMPLIANCE

Set firmware compliance so when a new device is added to the group, it will immediately install this firmware.

Set firmware compliance

Groups

All Groups ▼

Firmware Version ▼

Upgrade Type

Standard
Recommended operation during maintenance windows.

Live
Recommended operation during working hours.

When

Specify when to validate compliance and upgrade the non-compliant devices for the first time.

Now Later Date

Cancel Save

Setting Firmware Compliance For Switches

To force a specific firmware version for all MAS switches in a group, complete the following steps:

1. In the **Global** dashboard, under **Maintain**, click **Firmware** > **Switch-MAS** tab.
2. Verify the firmware upgrade status for all MAS 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 firmware version from the **Firmware Version** drop-down list.
6. Select **Auto Reboot** if you want Aruba Central to automatically reboot the device after a successful device upgrade.
7. Select one of the following as required:
 - Select **Now** to set the compliance to be carried out immediately.
 - Select **Later Date** to set the compliance at the later date and time.
8. Click **Save and Upgrade**.
 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.

The following image displays the **Manage Firmware Compliance** window for MAS switches:

MANAGE FIRMWARE COMPLIANCE

Set firmware compliance

Groups
All Groups

Firmware Version

Auto Reboot

When
Specify when to validate compliance and upgrade the non-compliant devices for the first time.

Now Later Date

Cancel Save and Upgrade

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 AOS-S firmware version from the **AOS-S Firmware Version** drop-down list.
6. Select CX firmware version from the **CX Firmware Version** drop-down list.
7. Select **Auto Reboot** if you want Aruba Central to automatically reboot the device after a successful device upgrade.

8. Select one of the following as required:
 - Select **Now** to set the compliance to be carried out immediately.
 - Select **Later Date** to set the compliance at the later date and time.
9. Click **Save and Upgrade**.

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.

The following image displays the **Manage Firmware Compliance** window for Aruba switches:

MANAGE FIRMWARE COMPLIANCE

Set firmware compliance

Groups
All Groups

AOS-S Firmware Version

CX Firmware Version

Auto Reboot

When
Specify when to validate compliance and upgrade the non-compliant devices for the first time.

Now Later Date

Cancel Save and Upgrade

Setting Firmware Compliance For Gateways

To force a specific firmware version for all gateways in standalone mode, complete the following steps:

1. In the **Global** dashboard, under **Maintain**, click **Firmware > Gateways** tab. All the gateways with standalone mode is displayed.
2. Verify the firmware upgrade status for all gateways.
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 **Auto Reboot** if you want Aruba Central to automatically reboot the device after a successful device upgrade.
7. Select one of the following as required:
 - Select **Now** to set the compliance to be carried out immediately.
 - Select **Later Date** to set the compliance at the later date and time.
8. Click **Save and Upgrade**.
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.

The following image displays the **Manage Firmware Compliance** window for gateways in standalone mode:

MANAGE FIRMWARE COMPLIANCE

Set firmware compliance so when a new device is added to the group, it will immediately install this firmware.

Set firmware compliance

Groups
All Groups

Firmware Version

Auto Reboot

When
Specify when to validate compliance and upgrade the non-compliant devices for the first time.

Now Later Date

Cancel Save

To force a specific firmware version for all gateways in cluster mode, complete the following steps:

1. In the **Global** dashboard, under **Maintain**, click **Firmware** > **Gateways** tab. All the gateways with cluster mode is displayed.
2. Verify the firmware upgrade status for all gateways.
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. In the **Upgrade Type**, select one of the following options:

- **Standard**
- **Live**



The **Upgrade Type** option is available only at the group context.

7. Select **Auto Reboot** if you want Aruba Central to automatically reboot the device after a successful device upgrade.

8. Select one of the following as required:

- Select **Now** to set the compliance to be carried out immediately.
- Select **Later Date** to set the compliance at the later date and time.

9. Click **Save and Upgrade**.

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.

The following image displays the **Manage Firmware Compliance** window for gateways in cluster mode:

MANAGE FIRMWARE COMPLIANCE

Set firmware compliance so when a new device is added to the group, it will immediately install this firmware.

Set firmware compliance

Groups

All Groups



Firmware Version



Upgrade Type

- Standard**
Recommended operation during maintenance windows.
- Live**
Recommended operation during working hours.

When

Specify when to validate compliance and upgrade the non-compliant devices for the first time.

- Now**
- Later Date**

Cancel

Save

AOS 10.x allows you to provision devices using UI-based or template-based configuration method. If you have a Gateway or AP group with template-based configuration enabled, you can create a template with a set of CLI commands and variables. Using templates, you can apply the CLI-based configuration parameters in bulk 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, complete the following steps:

1. In the **Network Operations** app, filter **All Devices**.
2. Under **Maintain**, click **Organization**.
By default, the **Groups** page is displayed.
3. Click **(+) New Group**.
The **Create New Group** pop-up window opens.
4. Enter the name of the group.
5. Select **IAP and Gateway** to create a template group.
6. Enter the password and confirm the same.
7. Click **Add Group**.



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 on page 556](#)
- [Provisioning Gateways Using Configuration Templates on page 563](#)

Forming Tunnels Manually

In a template configuration, the tunnels need to be formed manually between APs and gateways. To trigger the tunnel, run the following command using a JSON file:

```
{  
  
"address-family": [  

```

```
"openconfig-bgp-types:IPV4_UNICAST"
```

```
],
```

```
"ssid_cluster": [
```

```
{
```

```
"profile": "ethersphere",
```

```
"gw_cluster_list": [
```

```
{
```

```
"cluster": "blr-cluster",
```

```
"cluster_group_name": "blr-group",
```

```
"tunnel_type": "GRE",
```

```
"cluster_type": "PRIMARY"
```

```
}
```

```
],
```

```
"profile_type": "WIRELESS_PROFILE"
```

```
}
```

```
]
```

```
}
```

Editing a Template

To edit or delete a template, select the template row and click the edit or delete icon, respectively.

Configuring APs Using Templates

Templates in AOS 10.x 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 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 APs.

Creating a Group for Template-Based Configuration

For template-based provisioning, APs must be assigned to a group with template-based configuration method enabled.

For more information, see [Creating a Group on page 28](#) and [Assigning APs to a Group on page 29](#).

Creating a Configuration Template

To create a template for the devices 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**. The dashboard context for the selected group is displayed.
2. Under Manage, click **Devices > Access Points**.
3. Click the **Config** icon.
The tabs to configure APs are displayed.
4. Click **Templates**.
The **Templates** page is displayed.
5. Click **+** to add a new template.
The **Add Template** window opens.
6. Under **Basic Info** page, enter following information:
 - **Template Name**—Enter the template name.
 - **Model**—Set the model parameter to ALL.
 - **Version**—Set the model parameter to ALL.
7. Click **Next**.
8. Under **Template**, add the CLI script content.
9. 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 only one **per-ap settings** block. It must include the **per-ap-settings %_sys_lan_mac%** variable. The **per-ap-settings** block uses the variables for the individual APs. The general VC configuration uses variables for master 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.
 - 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 10.10.0.0 255.255.255.0 10.10.0.255
%if condition2=true%
routing-profile 10.20.0.0 255.255.255.0 10.20.0.255
%else%
routing-profile 10.30.0.0 255.255.255.0 10.30.0.255
%endif%
%else%
routing-profile 10.40.0.0 255.255.255.0 10.40.0.255
%if condition3=true%
routing-profile 10.50.0.0 255.255.255.0 10.50.0.255
%else%
routing-profile 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 whitespace. 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 AP 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.

10. Click **OK**.

The variables configured for the AP devices functioning as the VCs are replaced with the values configured at the template level.

If any device in the cluster has any missing variables, the configuration push to those AP devices in the cluster fails. The audit trail for such instances shows the missing variables.



Sample Template

The following example shows the typical contents allowed in a template file for APs:

```
organization %org%
virtual-controller-ip 1.1.1.1
syslog-level debug
syslog-level warn ap-debug
per-ap-settings %_sys_lan_mac%
hostname %hostname%
zonename %zonename%

virtual-controller-country us
virtual-controller-key %vckey%
terminal-access
clock timezone none 00 00
rf-band all
allowed-ap 70:3a:0e:cd:5f:e8

syslog-level debug ap-debug
syslog-level debug network
syslog-level debug security
syslog-level debug system
syslog-level debug user
syslog-level debug user-debug
syslog-level debug wireless

extended-ssid

hash-mgmt-password
hash-mgmt-user admin password hash
1c6be52d022e18a69f04b658b7a96d07bcb3d676586c85a32ca0081356463e4d34f3fbc5f7

wlan access-rule deepthi_c2c_cluster_wpa2
index 0
rule any any match any any any permit

wlan access-rule default_wired_port_profile
index 1
rule any any match any any any permit

wlan access-rule wired-SetMeUp
index 2
rule masterip 0.0.0.0 match tcp 80 80 permit
rule masterip 0.0.0.0 match tcp 4343 4343 permit
rule any any match udp 67 68 permit
rule any any match udp 53 53 permit
```



```

wlan access-rule role_from_cppm
index 3
rule any any match any any any permit

wlan access-rule deepthi_c2c_cluster_wpa3
index 4
rule any any match any any any permit

wlan access-rule cp_logon
index 5
captive-portal external profile cp-prof-iap1
rule 10.15.56.145 255.255.255.255 match tcp 443 443 permit
rule 10.15.56.145 255.255.255.255 match tcp 80 80 permit
rule any any match icmp any any permit
rule any any match igmp any any permit

wlan access-rule guest
index 6
rule any any match any any any permit

wlan access-rule deepthi_c2c_cluster_cp
index 7
rule any any match any any any permit

wlan external-captive-portal cp-prof-iap
server 10.15.56.145
port 80
url /guest/C2C.php
switch-ip

wlan external-captive-portal cp-prof-iap1
server 10.15.56.145
port 80
url /guest/C2C.php
switch-ip
auto-allowlist-disable

wlan ssid-profile deepthi_mixed_cp_#1574239188575_77#_
enable
gw-profile deepthi_mixed_cp_#1574239188575_77#_
gw-auth-server default
index 6
type guest
ssid deepthi_mixed_cp
utf8
opmode enhanced-open
max-authentication-failures 0
set-role-pre-auth extcp_145_#1572196976655_77#_
set-vlan mac-address contains 98 567
rf-band all
captive-portal external profile extcp_145_#1572196976655_77#_
mac-authentication
dtim-period 1
broadcast-filter arp
radius-accounting
radius-interim-accounting-interval 1
denylist
dmo-channel-utilization-threshold 90
local-probe-req-thresh 0
max-clients-threshold 64

```

```
okc

wlan gw-auth-server default
key admins
rfc3576

wlan ssid-profile deepthi_c2c_cluster_wpa2
enable
gw-profile deepthi_c2c_cluster_wpa2
gw-auth-server default
index 0
type employee
ssid deepthi_c2c_cluster_wpa2
opmode wpa2-aes
max-authentication-failures 0
rf-band all
captive-portal disable
dtim-period 1
broadcast-filter none
external-server
radius-reauth-interval 2
radius-accounting
radius-interim-accounting-interval 1
dmo-channel-utilization-threshold 6
dmo-client-threshold 6
local-probe-req-thresh 0
max-clients-threshold 64
wlan ssid-profile deepthi_c2c_cluster_wpa3
enable
gw-profile deepthi_c2c_cluster_wpa3
gw-auth-server default
index 1
type employee
ssid deepthi_c2c_cluster_wpa3
wpa-passphrase aruba123
opmode wpa3-cnsa
max-authentication-failures 0
auth-server deepthi_c2c_cluster_wpa3
rf-band all
captive-portal disable
dtim-period 1
broadcast-filter none
external-server
radius-accounting
radius-interim-accounting-interval 1
dmo-channel-utilization-threshold 6
dmo-client-threshold 6
local-probe-req-thresh 0
max-clients-threshold 64

wlan ssid-profile deepthi_c2c_cluster_cp
enable
gw-profile deepthi_c2c_cluster_cp
gw-auth-server default
index 2
type employee
ssid deepthi_c2c_cluster_cp
opmode opensystem
max-authentication-failures 0
auth-server deepthi_c2c_cluster_cp
```

```
rf-band all
captive-portal external profile cp-prof-iap
set-role-pre-auth cp_logon
mac-authentication
dtim-period 1
broadcast-filter none
external-server
radius-reauth-interval 2
radius-accounting
radius-interim-accounting-interval 1
dmo-channel-utilization-threshold 6
dmo-client-threshold 6
local-probe-req-thresh 0
max-clients-threshold 64
auth-survivability cache-time-out 24

wlan auth-server deepthi_c2c_cluster_wpa3
ip 1.1.1.12
port 1812
acctport 1813
key admins
rfc3576

wlan auth-server deepthi_c2c_cluster_cp
ip 1.1.1.12
port 1812
acctport 1813
key admins
rfc3576

wlan gw-auth-server default
key admins
rfc3576

wired-port-profile wired-SetMeUp
switchport-mode access
allowed-vlan all
native-vlan guest
no shutdown
access-rule-name wired-SetMeUp
speed auto
duplex auto
no poe
type guest
captive-portal disable
no dot1x

wired-port-profile default_wired_port_profile
switchport-mode trunk
allowed-vlan all
native-vlan 1
shutdown
access-rule-name default_wired_port_profile
speed auto
duplex full
no poe
type employee
captive-portal disable
no dot1x
```

```

enet0-port-profile default_wired_port_profile

uplink
preemption
enforce none
failover-internet-pkt-lost-cnt 10
failover-internet-pkt-send-freq 30
failover-vpn-timeout 180

ip dhcp vlan400
server-type Local
server-vlan 400
subnet 40.0.0.1
subnet-mask 255.255.255.0

default-router 40.0.0.1
dns-server 8.8.8.8

airgroup
disable

airgroupservice airplay
disable
description AirPlay

airgroupservice airprint
disable
description AirPrint

```

Password Management in Configuration Templates for AP

In AOS 10.x, the AP management user passwords are stored and displayed as hash instead of plain text. Password for AP can be set using the following commands:

```
mgmt-user <user-name> <password>
```

```
mgmt-user <user-name> <password> read-only
```

```
mgmt-user <user-name> <password> guest-mgmt
```

The **hash-mgmt-user** command is enabled by default on the APs provisioned in the template and UI groups. If a pre-configured AP joins AOS 10.x and is moved to a new group, AOS 10.x uses the **hash-mgmt-user** configuration settings and discards **mgmt-user** configuration settings, if any, on the AP. In other words, AOS 10.x hashes management user passwords irrespective of the management user configuration settings running on an AP.

Password for AP can be set using the following **hash-mgmt-user** commands:

```
hash-mgmt-user <user-name> password hash <hash-password>
```

```
hash-mgmt-user <user-name> password cleartext <cleartext-password>
```

```
hash-mgmt-user <user-name> password hash <hash-password> usertype read-only
```

```
hash-mgmt-user <user-name> password cleartext <cleartext-password> usertype read-only
```

```
hash-mgmt-user <user-name> password hash <hash-password> usertype guest-mgmt
```

```
hash-mgmt-user <user-name> password cleartext <cleartext-password> usertype guest-mgmt
```

```
hash-mgmt-user <user-name> password hash <hash-password> usertype local
```

```
hash-mgmt-user <user-name> password cleartext <cleartext-password> usertype local
```



AOS 10.x supports the use of hash commands with clear text, however, Aruba recommends you to use hash passwords instead of clear text passwords to avoid password disclosures.
AOS 10.x allows you to re-use the hash from one AP on another AP.

Provisioning Gateways Using Configuration Templates

If your deployment has a large number of Aruba Gateways and requires bulk configuration, you can use the configuration template feature in Aruba Central to quickly provision Gateways. The configuration template feature is available for the Gateway devices provisioned in template groups in Aruba Central.

The template groups in Aruba Central allow network administrators to create a common configuration output by using a combination of CLI commands and variables, and apply this configuration to the other Gateway devices provisioned in that group.

Important Points to Note

Before you begin the provisioning procedure, note the following important points and recommendations:

- Aruba recommends that the administrators who are provisioning Gateways using templates familiarize themselves with the Gateway CLI commands. A prior understanding of the Gateway CLI commands helps in determining the service impact and avoiding errors that may occur due to incorrect configuration.
- Before assigning devices to groups, identify the devices that have a common set of CLI commands and configuration requirements.

- The configuration requirements for a Branch Gateway and VPN Concentrator are different, so Aruba recommends that you create separate template groups for Branch Gateways and VPN Concentrators.
- If you are provisioning Gateways with factory-default configuration, you can build a template based on the current configuration of the first device that joins a template group.
- If you want to create a template based on the current configuration of an existing Gateway device, access the CLI console of the device and copy the configuration. Use this configuration as the template text when building a new template. You can enhance this template for multi-device use by adding variable definitions.
- While Aruba Central allows you to move a Gateway device from a UI group to a template group, you must ensure that the current configuration running on the device is backed up and is included in the configuration template created for that template group. However, Aruba recommends that you exercise caution when moving a device from a UI group to a template group as incorrect configuration may lead to service disruption.

Configuring Gateways Using a Template

To provision Gateways in a template group, complete the following steps:

1. [Creating a Template Group on page 564](#)
2. [Assigning a Gateway to a Template Group on page 565](#)
3. [Creating a Configuration Template for Gateways on page 565](#)
4. [Customizing a Template Using Variable Definitions on page 567](#)
5. [on page 572](#)

Creating a Template Group

To create a template group, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Go to **Maintain > Organization > Groups**. The **Groups** page is displayed.
3. Click **(+) New Group**.
The **Create a New Group** pop-up window is displayed.
4. Enter a name for the group.

5. Select the **IAP and Gateway** check box to create a template group for Gateways.

Figure 63 *Template Group Creation*

CREATE NEW GROUP ✕

GROUP NAME
BG-group-1

Use the group as Template group by selecting the device ⓘ

IAP AND GATEWAY SWITCH

Cancel Add Group

6. Click **Add Group**.

Assigning a Gateway to a Template Group

To assign a Gateway to a group:

1. In the **Network Operations** app, set the filter to **Global**.
2. Go to **Maintain > Organization > Groups**.
The **Groups** page is displayed.
3. From the **Devices > Gateways** table, select the Gateway that you want to assign to a template group.
4. Drag and drop the device to the template group that you just created.

Creating a Configuration Template for Gateways

A Gateway configuration template includes a set of common configuration commands that you can apply to multiple Gateway devices provisioned in a group.

Before you Begin

Before generating a configuration template:

- Familiarize with the CLI commands available on the device.
- Identify the commands that you want to use at the group level and the overrides required at the device level.
- Ensure that the Gateways are assigned to a template group.
- Run the **show configuration setup-dialog** command to get the default configuration of the gateway. You can copy this output in the beginning of your template text.

Best Practices and Recommendations

Note the following recommendations when adding configuration text to a template:

- Verify the CLI syntax on the Gateway device before adding it to the template text.
- Ensure that the command text indentation matches the indentation in the running configuration.
- As the command text and definitions are case-sensitive, ensure that there are no errors or discrepancies in the CLI definitions.

Configuration Steps

To create a template for the Gateways provisioned in a template group:

1. In the **Network Operations** app, set the filter to one of the template group under **Groups**. The dashboard context for the selected group is displayed.
2. Under **Manage**, click **Devices > Gateways**.
3. Click the **Config** icon.
The tabs to configure gateways are displayed.
4. Click **Templates**. The **Templates** page is displayed.
5. Click **+** to add a new template. The **Add Template** page opens.
6. Under **Basic Info** page, enter following information:
 - **Template Name**—Enter the template name.
 - **Model**—Set the model parameter to ALL.
 - **Version**—Set the model parameter to ALL.
7. Click **Next**.



In a heterogeneous setup where the gateway models are different, add a template group separately for each gateway model.

8. Under **Template**, add the template text.

Figure 64 *Creating a Configuration Template*

```
1 vlan 4094
2 !
3 interface gigabitethernet 0/0/0
4     swichport access vlan 4094
5     trusted
6     trusted vlan 1-4094
7 !
8 interface gigabitethernet 0/0/1
9 !
10 interface gigabitethernet 0/0/2
11 !
12 interface gigabitethernet 0/0/3
13 !
14 interface gigabitethernet 0/0/4
15 !
16 interface gigabitethernet 0/0/5
17 !
18 interface gigabitethernet 0/0/6
19 !
20 interface gigabitethernet 0/0/7
21 !
```

9. Click **Save**. After you apply the configuration template, Gateways reboot and reconnect to Aruba Central with the new configuration.

See Also: [Sample Template and Variables Files](#)

Customizing a Template Using Variable Definitions

Variables in Aruba Central refer to the data set in the configuration template that can vary per device.

Aruba Central supports composing the variables in JSON and CSV formats. To add variable definitions, you can download a sample variable file from Aruba Central, add the definitions, and then upload it to Aruba Central.

To view a list of variables in a template, select the template row and click the edit or delete icon, respectively.

Downloading a Sample Variables File

To download a sample variables file:

1. In the **Network Operations** app, set the filter to one of the template group under **Groups**. The dashboard context for the selected group is displayed.
2. Under **Manage**, click **Devices > Gateways**.
3. Click the **Config** icon.
The tabs to configure gateways are displayed.
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 Variables File

Note the following conditions when modifying variable definitions:

- The **_sys_serial** and **_sys_lan_mac** are mandatory variables for specifying the serial number and MAC address of each device.
- 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 a correct notation as opposed to `%if 100=var%`
- 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 a variable definition includes **%**, add a space before and after the **%** instance.
- The first character of the variable name must be an alphabet. Numeric values are not supported.
- If quotes are required, they must be included as part of the variable value.
- If you are using a CSV file for modifying variable definitions, the **modified** column must be set to **Y** to allow Aruba Central to parse the modified definition.

Uploading a Variables File

To upload a variables 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 > Gateway**.

4. Click the **Config** icon.
The tabs to configure gateways are displayed.
5. Click **Variables** tab and click **Upload Variables File** and select the variables file to upload.
6. To verify if the variables are added in the template, go to **Gateway Management > Templates**.
7. Click the edit icon in the template. Verify the list of variables displayed in the **Edit Template** screen.

Sample Template and Variables Files

The following example shows the contents of a Gateway configuration template:

```
masterip %bmasterip% web-socket-acp
!
controller-ip vlan %bmgmt_vlan%
!
vlan %bmgmt_vlan%
!
interface gigabitethernet 0/0/0
trusted vlan 1-4094
trusted
!
interface gigabitethernet 0/0/1
!
interface gigabitethernet 0/0/2
!
interface gigabitethernet 0/0/3
!
interface gigabitethernet 0/0/4
!
interface gigabitethernet 0/0/5
!
interface gigabitethernet 0/0/6
!
interface gigabitethernet 0/0/7
!
interface gigabitethernet 0/0/8
!
interface gigabitethernet 0/0/9
!
interface gigabitethernet 0/0/10
!
interface gigabitethernet 0/0/11
!
interface gigabitethernet 0/0/12
!
interface gigabitethernet 0/0/13
!
interface gigabitethernet 0/0/14
!
interface gigabitethernet 0/0/15
!
interface gigabitethernet 0/0/16
switchport access vlan %_vlan_id3_%
!
interface gigabitethernet 0/0/17
switchport access vlan %_vlan_id1_%
!
interface vlan 4094
    ip address dhcp-client
!
```

```

interface port-channel 0
!
interface port-channel 1
!
interface port-channel 2
!
interface port-channel 3
!
interface port-channel 4
!
interface port-channel 5
!
interface port-channel 6
!
interface port-channel 7
!
interface vlan %bmgmt_vlan%
ip address %badmin_ip% %bmask%
!
ip default-gateway %dgate%
!
ip name-server %bdns_ip%
no adp discovery
!
mgmt-server primary-server internal profile default-acp
!
mgmt-user admin root %adpwd%
firewall
  dpi
    cp-bandwidth-contract trusted-ucast 65535
    cp-bandwidth-contract trusted-mcast 3906
    cp-bandwidth-contract untrusted-ucast 9765
    cp-bandwidth-contract untrusted-mcast 3906
    cp-bandwidth-contract route 976
    cp-bandwidth-contract sessmirr 976
    cp-bandwidth-contract vrrp 512
    cp-bandwidth-contract auth 976
    cp-bandwidth-contract arp-traffic 3906
    cp-bandwidth-contract l2-other 1953
  !
clock timezone America/Los_Angeles -08 00
!
mgmt-user admin root itsabug
interface vlan 4094
  ip address dhcp-client
!
vlan %VLAN%
vlan %VLAN100%
interface gigabitethernet 0/0/0
trusted
trusted vlan 1-4094
switchport mode trunk
switchport trunk native vlan 56
!
interface vlan %VLAN%
ip address %VLAN132IP% 255.255.255.0
!
interface vlan %VLAN100%
ip address %VLAN100IP% 255.255.255.0
!

```

```

controller-ip vlan %VLAN%

ip default-gateway %DEFAULTGATEWAY%
ip name-server %DNSIP%
login-session timeout 0
vlan 566
!
hostname %_hostname_%
vlan %_vlan_id_%
interface vlan %_vlan_id_%
ip address %_ip_addr_% %_net_mask_%
!
controller-ip vlan %_vlan_id_%
!
wlan virtual-ap %_vap1_%
aaa-profile %_prof_name7_%
vlan %_vlan_id3_%
!
aaa server-group %_svr_grp1_%
auth-server %_svr1_%
!
aaa server-group %_svr_grp2_%
auth-server %_svr1_%
!
aaa server-group %_svr_grp3_%
auth-server %_svr1_%
!
aaa server-group %_svr_grp4_%
auth-server %_svr1_%
!
aaa server-group %_svr_grp5_%
auth-server %_svr1_%
!
aaa server-group %_svr_grp6_%
auth-server %_svr1_%
!
crypto-local pki ServerCert new_svr1_ocsp new_svr1_ocsp
crypto-local pki ServerCert SERVER-CERT SERVER-CERT
crypto-local pki TrustedCA pata_ca pata_ca
crypto-local pki rcp pata_ca
aaa authentication dot1x %_pdot1x_%
server-cert %_svr_cert_%
ca-cert %_ca_cert_%
!
aaa authentication-server radius %_svr1_%
!
vlan %_vlan_id1_%
wired aaa-profile %_prof_name7_%
!
aaa profile %_prof_name7_%
initial-role %_role1_%
dot1x-default-role %_role1_%
dot1x-server-group %_svr_grp1_%
!
aaa profile %_prof_name5_%
initial-role %_role1_%
dot1x-default-role %_role1_%
!
vlan %_vlan_id2_%
wired aaa-profile %_prof_name5_%

```

```

!
user-role %_role1_%
!
vlan %_vlan_id3_%
!
interface vlan %_vlan_id2_%
ip address %_ip_vlan2_% %_net_mask_%
!
ip access-list session %_acl1_%
!
aaa server-group %_svr_grp1_%
auth-server %_svr1_%
!
aaa authentication-server radius %_svr1_%
!
vlan 3434
!
netdestination peds-devices
    %if local_network_ip%
        range %local_network_ip%.91 %local_network_ip%.100
        range %local_network_ip%.101 %local_network_ip%.110
    %endif%
!
aaa profile %_prof_name8_%
%if role_group%
%role_group%
%endif%
!
aaa authentication captive-portal %_cap1_%
redirect-url "https://abc%xyz"
!
lc-cluster group-profile <profile_name>
controller <GW1_mac_addr>
controller <GW2_mac_addr>
!
user

```

Sample Variables File

The following example shows the contents of a sample variables file in the JSON format:

```

"CG0011297": {
  "_sys_lan_mac": "00:0B:86:dd:67:80",
  "_sys_serial": "CG0011297",
  "_hostname_": "Aruba7010_DD_67_80",
  "_vlan_id_" : "700",
  "_ip_addr_" : "1.70.70.10",
  "_net_mask_" : "255.255.255.0",
  "_vlan_id1_" : "225",
  "_vlan_id2_" : "226",
  "_vlan_id3_" : "227",
  "_prof_name5_" : "prof5",
  "_prof_name6_" : "prof6",
  "_prof_name7_" : "prof7",
  "_prof_name9_" : "prof9",
  "_role1_" : "role1",
  "_ip_vlan2_" : "1.27.26.10",
  "_vap1_" : "vap1",
  "_svr_grp1_" : "svr_grp1",
  "_svr_grp2_" : "svr_grp2",
  "_svr_grp3_" : "svr_grp3",

```

```

"_svr_grp4_" : "svr_grp4",
"_svr_grp5_" : "svr_grp5",
"_svr_grp6_" : "svr_grp6",
"_svr1_" : "svr1",
"_svr_cert_" : "new_svr1_ocsp",
"_ca_cert_" : "pata_ca",
"_pdot1x_" : "pdot1x",
"_server_ocsp3_" : "server_ocsp3",
"_acl1_" : "acl1",
"local_network_ip" : "34.34.54",
"_prof_name8_" : "prof8",
"role_group" : "initial-role role1\n dot1x-default-role role1",
"_cap1_" : "cap1",
"_url_" : "https://abc/%xyz",
"_role2_" : "\"test%role2\""
},
"CG0007810": {
  "_sys_lan_mac": "00:0B:86:dB:B0:C0",
  "_sys_serial": "CG0007810",
  "_hostname_" : "Aruba7010_DB_B0_C0",
  "_vlan_id_" : "166",
  "_ip_addr_" : "166.10.10.10",
  "_net_mask_" : "255.255.255.0",
  "_vlan_id1_" : "225",
  "_vlan_id2_" : "226",
  "_vlan_id3_" : "227",
  "_prof_name5_" : "prof5",
  "_prof_name6_" : "prof6",
  "_prof_name7_" : "prof7",
  "_prof_name9_" : "prof9",
  "_role1_" : "role1",
  "_ip_vlan2_" : "1.27.26.11",
  "_vap1_" : "vap1",
  "_svr_grp1_" : "svr_grp1",
  "_svr_grp2_" : "svr_grp2",
  "_svr_grp3_" : "svr_grp3",
  "_svr_grp4_" : "svr_grp4",
  "_svr_grp5_" : "svr_grp5",
  "_svr_grp6_" : "svr_grp6",
  "_svr1_" : "svr1",
  "_svr_cert_" : "new_svr1_ocsp",
  "_ca_cert_" : "pata_ca",
  "_pdot1x_" : "pdot1x",
  "_server_ocsp3_" : "server_ocsp3",
  "_acl1_" : "acl1",
  "local_network_ip" : "34.34.54",
  "_prof_name8_" : "prof8",
  "role_group" : "initial-role role1\n dot1x-default-role role1",
  "_cap1_" : "cap1",
  "_url_" : "https://abc/%xyz",
  "_role2_" : "\"test%role2\""
}

```

Verifying Configuration Status

- To verify that Gateways are assigned to the template group and the configuration is pushed from Aruba Central, go to **Analyze > Audit Trail**.

- To view the configuration sync errors and overrides, use the **Configuration Audit** for Gateways. For more information, see [Viewing Audit Trail on page 504](#).

Backing up and Restoring Templates

Aruba Central supports backing up and restoring configuration templates. The **Configuration Audit** page for Gateways allows you to back up the configuration templates and variables and restore these when required.

| | |
|----------------------------------|-----|
| Supported Aruba APs | 574 |
| Supported Aruba Gateways | 574 |
| Supported Switch Platforms | 575 |

Supported Aruba APs

The following table shows the list of AP models and supported software required for deploying the AOS 10.x:

Table 156: *Supported APs*

| Platform | Minimum Software Version | Recommended Software Version | Latest Software Version Available for Upgrade |
|--|--------------------------|------------------------------|---|
| <ul style="list-style-type: none"> ■ AP-505H ■ AP-518 ■ 570 Series—AP-574 and AP-575 ■ AP-575EX ■ AP-577 ■ AP-577EX | ArubaOS 10.2.0.0 | ArubaOS 10.2.0.0 | ArubaOS 10.2.0.0 |
| <ul style="list-style-type: none"> ■ 500 Series—AP-504 and AP-505 | ArubaOS 10.1.0.0 | ArubaOS 10.2.0.0 | ArubaOS 10.2.0.0 |
| <ul style="list-style-type: none"> ■ 510 Series—AP-514 and AP-515 ■ 530 Series—AP-534 and AP-535 ■ 550 Series—AP-555 | ArubaOS 10.0.0.0 | ArubaOS 10.2.0.0 | ArubaOS 10.2.0.0 |
| <ul style="list-style-type: none"> ■ AP-303, AP-303H, and AP-303P ■ 300 Series—AP-304 and AP-305 ■ 310 Series—AP-314 and AP-315 ■ AP-318 ■ 320 Series—AP-324 and AP-325 ■ 330 Series—AP-334 and AP-335 ■ 340 Series— AP-344 and AP-345 ■ 360 Series—AP-365 and AP-367 ■ 370 Series— AP-374, AP-375, and AP-377 ■ AP-387 <p>NOTE: The older AP-325 models which are configured with 256 MB of SDRAM are not supported with the Aruba AOS 10.x.</p> | ArubaOS 10.0.0.0 | ArubaOS 10.2.0.0 | ArubaOS 10.2.0.0 |

Supported Aruba Gateways

The following table shows a list of Aruba Gateway models and supported software versions required for deploying the AOS 10.x:

Table 157: Supported Aruba Gateways

| Platform | Minimum Software Version | Recommended Software Version | Latest Software Version Available for Upgrade |
|----------------------------------|--------------------------|------------------------------|---|
| Aruba 9004-LTE Controller | ArubaOS 10.2.0.0 | ArubaOS 10.2.0.0 | ArubaOS 10.2.0.0 |
| Aruba 9004 Controller | ArubaOS 10.1.0.0 | ArubaOS 10.2.0.0 | ArubaOS 10.2.0.0 |
| Aruba 9012 Controller | ArubaOS 10.1.0.0 | ArubaOS 10.2.0.0 | ArubaOS 10.2.0.0 |
| Aruba 7005 Mobility Controller | ArubaOS 10.0.0.0 | ArubaOS 10.2.0.0 | ArubaOS 10.2.0.0 |
| Aruba 7008 Mobility Controller | ArubaOS 10.0.0.0 | ArubaOS 10.2.0.0 | ArubaOS 10.2.0.0 |
| Aruba 7010 Mobility Controller | ArubaOS 10.0.0.0 | ArubaOS 10.2.0.0 | ArubaOS 10.2.0.0 |
| Aruba 7024 Mobility Controller | ArubaOS 10.0.0.0 | ArubaOS 10.2.0.0 | ArubaOS 10.2.0.0 |
| Aruba 7030 Mobility Controller | ArubaOS 10.0.0.0 | ArubaOS 10.2.0.0 | ArubaOS 10.2.0.0 |
| Aruba 7210 Mobility Controller | ArubaOS 10.0.0.0 | ArubaOS 10.2.0.0 | ArubaOS 10.2.0.0 |
| Aruba 7220 Mobility Controller | ArubaOS 10.0.0.0 | ArubaOS 10.2.0.0 | ArubaOS 10.2.0.0 |
| Aruba 7240XM Mobility Controller | ArubaOS 10.0.0.0 | ArubaOS 10.2.0.0 | ArubaOS 10.2.0.0 |
| Aruba 7280 Mobility Controller | ArubaOS 10.0.0.0 | ArubaOS 10.2.0.0 | ArubaOS 10.2.0.0 |

For a complete list of Aruba switches supported in Aruba Central, see the [Supported Switch Platforms on page 575](#).

Supported Switch Platforms



To manage your Aruba switches using Aruba Central, ensure that the switch software is upgraded to 16.05.0007 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.

The following tables list the switch platforms, corresponding software versions supported in Aruba Central, and switch stacking details.

Table 158: Supported Aruba Switch Series, Software Versions, and Switch Stacking

| Switch Platform | Supported Software Versions | Recommended Software Versions | Switch Stacking Support |
|--------------------------|-----------------------------|-------------------------------|-------------------------|
| Aruba 2540 Switch Series | YC.16.03.0004 or later | YC.16.10.0003 | N/A |
| Aruba 2920 Switch Series | WB.16.03.0004 or later | WB.16.10.0003 | Yes |

| Switch Platform | Supported Software Versions | Recommended Software Versions | Switch Stacking Support |
|---------------------------|-----------------------------|-------------------------------|--|
| | | | Switch Software Dependency:
WB.16.04.0008 or later |
| Aruba 2930F Switch Series | WC.16.03.0004 or later | WC.16.10.0003 | Yes
Switch Software Dependency:
WC.16.07.0002 |
| Aruba 2930M Switch Series | WC.16.04.0008 or later | WC.16.10.0003 | Yes
Switch Software Dependency:
WC.16.06.0006 |
| Aruba 3810 Switch Series | KB.16.03.0004 or later | KB.16.10.0003 | Yes
Switch Software Dependency:
KB.16.07.0002 |
| Aruba 5400R Switch Series | KB.16.04.0008 or later | KB.16.10.0003 | Yes
Switch Software Dependency:
KB.16.06.0008 |



Provisioning and configuration of Aruba 5400R Switch Series and switch stacks 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/>

This topic provides information about the AOS 10.x commands.

Navigating to the Commands page

1. In the **Network Operations** app, set the filter to **Global**.
The global dashboard is displayed.
2. Under **Analyze**, select **Tools** and click **Commands** tab.
The **Commands** page is displayed. For more details, see [Advanced Device Troubleshooting](#).

Filtering Information

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. There are two types of filtration available:

Commands marked with '*' or '+'

1. Select the command marked with '*' or '+' and click **Add**.
The **Additional Filters** dialog box appears.
2. Enter the Client MAC address/IP Address/Port number as required.
3. Click **Apply**.
4. Click **Edit All** to reset the filtration parameters for all the commands added in the selected command pane.

The following table contains the AOS 10.x command-line interface (CLIs).

Table 159: *Commands in AOS 10.x*

| Command | Description | Applies To |
|---|---|------------|
| aaa test-server | Displays the configured RADIUS authentication server or the internal database. Run this command to check for an out of service RADIUS server. | AP |
| show 1xcert | Displays the details about the external server certificate, which is used by the AP for client authentication. | AP |
| show aaa authentication all | Displays the authentication statistics for your managed device, including authentication methods, successes and failures. This command displays a general overview of authentication statistics. To view authentication information for specific profiles such as a captive portal, MAC or 801.X authentication profile, issue the commands specific to those features. | GW |

| Command | Description | Applies To |
|--|---|------------|
| show aaa authentication captive-portal customization | Displays the customization settings for a captive portal profile. This command shows how a captive portal profile has been customized with non-default configuration settings. If you do not yet have any captive portal authentication profiles defined, use the command <code>aaa authentication captive-portal</code> to configure your captive portal profiles. | GW |
| show aaa authentication dot1x | Displays the information for 802.1X authentication profiles. Issue this command without the <code><profile-name></code> or <code>countermeasures</code> options to display the entire 802.1X Authentication profile list, including profile status and the number of references to each profile. Include a profile name to display detailed dot1x authentication configuration information for that profile. The <code>countermeasures</code> option indicates whether the 802.1X profiles have been configured for WPA/WPS2 countermeasures. If countermeasures have not been configured, the output for this command will be blank. | GW |
| show aaa authentication vpn | Displays the VPN authentication settings, including authentication roles and servers. Run this command to identify the default role assigned to VPN users, the name of the group of servers used to authenticate the VPN users, and the maximum number of authentication failures allowed before the user is blacklisted. | GW |
| show aaa authentication vpn default | Displays the VPN authentication settings, including authentication roles and servers, for the VPN authentication profile of default. Run this command to identify the default role assigned to VPN users, the name of the group of servers used to authenticate the VPN users, and the maximum number of authentication failures allowed before the user is blacklisted. | GW |
| show aaa authentication vpn default-cap | Displays the VPN authentication settings, including authentication roles and servers, for the VPN authentication profile of default-cap. Run this command to identify the default role assigned to VPN users, the name of the group of servers used to authenticate the VPN users, and the maximum number of authentication failures allowed before the user is blacklisted. | GW |
| show aaa authentication vpn default-rap | Displays the VPN authentication settings, including authentication roles and servers, for the VPN authentication profile of default-rap. Run this command to identify the default role assigned to VPN users, the name of the group of servers used to authenticate the VPN users, and the maximum number of authentication failures allowed before the user is blacklisted. | GW |
| show aaa authentication-server all | Displays the authentication server settings for both external authentication servers and the internal controller database. The output of this command displays statistics for the Authentication Server Table, including the name and address of each server, server type and configured authorization and accounting ports. | GW |

| Command | Description | Applies To |
|---|---|------------|
| <u>show aaa authentication-server internal statistics</u> | Displays the authentication server settings and statistics for the internal controller database. | GW |
| <u>show aaa authentication-server ldap statistics</u> | Displays the configuration settings and statistics of LDAP servers. | GW |
| <u>show aaa authentication-server radius statistics</u> | Displays the configuration settings and statistics of RADIUS servers. | GW |
| <u>show aaa authentication-server tacacs statistics</u> | Displays accounting, authorization, and authentication request and response statistics for the TACACS server. | GW |
| <u>show aaa auth-survivability</u> | Displays the authentication survivability configuration on a stand-alone controller. | GW |
| <u>show aaa auth-survivability-cache</u> | Displays the authentication survivability cached data on a stand-alone controller. | GW |
| <u>show aaa bandwidth-contracts</u> | Displays the contract names, ID numbers, Rate limits, and Note for your bandwidth contracts. | GW |
| <u>show aaa cluster bucketmap</u> | Displays the information on essid counters, bucketmap details for a specified bucket, dormant keycache, mac address, and dormant user entries for a particular ESSID. | GW |
| <u>show aaa derivation-rules server-group</u> | Displays derivation rules based on user information or for the configured server groups. | GW |
| <u>show aaa derivation-rules user</u> | Displays derivation rules based on user information. | GW |
| <u>show aaa fqdn-server-names</u> | Displays the IP addresses that are mapped to fully qualified domain names (FQDNs). If you define a RADIUS server using the FQDN of the server rather than its IP address, the controller will periodically generate a DNS request and cache the IP address returned in the DNS response. Issue this command to view the IP address that currently correlates to each RADIUS server FQDN. | GW |
| <u>show aaa radius-attributes</u> | Displays RADIUS attributes recognized by the controller. | GW |
| <u>show aaa server-group summary</u> | Displays configuration details for your AAA server groups. Run this command without the group-name or summary options to display the entire server group list, including profile status and the number of references to each profile. The References column lists the number of other profiles that reference a server group, and the Profile Status column indicates whether the server group is predefined. User-defined server groups will not have an entry in the Profile Status column. | GW |
| <u>show aaa state ap-group</u> | Displays the names and ID numbers of your AP groups | GW |
| <u>show aaa state configuration</u> | Displays the authentication state configuration information, including the numbers of successful and failed authentications. | GW |

| Command | Description | Applies To |
|---|--|------------|
| show aaa state debug-statistics | Displays the debug statistics for controller authentication, authorization and accounting. | GW |
| show aaa state messages | Displays the numbers of authentication messages sent and received. This command displays a general overview of authentication statistics. To view authentication information for specific profiles such as a captive portalA captive portal is a web page that allows the users to authenticate and sign in before connecting to a public-access network. Captive portals are typically used by business centers, airports, hotel lobbies, coffee shops, and other venues that offer free Wi-Fi hotspots for the guest users., MAC or 801.x authentication profile, issue the commands specific to those features. | GW |
| show about | Displays the information about version, build time and AP model. | AP |
| show access-rule | Displays the details of access rules configured for the wired or wireless clients associated with an AP. | AP |
| show access-rule-all | Displays the details of the access rules configured for all wired and wireless profiles on the AP. | AP |
| show acl ace-table acl 4 | Displays an access list entry (ACE) table for a particular access control list (ACL). | GW |
| show acl acl-table | Displays the information for a specified ACL. | GW |
| show acl hits | Displays the internal ACL hit counters. Run this command to see the number of times an ACL defined a user's role, or traffic and firewall policies for a user session. | GW |
| show airgroup debug statistics | Displays the AirGroup configuration details for an AP client. | AP |
| show airgroup status | Displays the current status of the AirGroup configuration and configured AirGroup services. This command is node specific. | AP |
| show airgroupservice | Displays the information about AirGroup services. | AP, GW |
| show airgroupservice verbose | Displays the additional information about AirGroup services for verbose. | GW |
| show alert global | Displays the list of client alerts for an AP. The client alerts occur when clients are connected to the network. Alerts are generated when a client encounters problems while accessing or connecting to the AP network. | AP |
| show allowed-aps | Displays the list of APs that are allowed to join the AP cluster. | AP |
| show ap active | Displays the APs registered to a Mobility Master. | GW |

| Command | Description | Applies To |
|---|---|------------|
| <u>show ap allowed-channels</u> | Displays the allowed channels on a specific AP name, country code, or IP address. Specify the country code for your controller during initial setup. Changing the country code causes the valid channel lists to be reset to the defaults for that country. | AP |
| <u>show ap allowed-max-EIRP</u> | Displays the regulatory power limits per channel for a specified AP. The values showed in the output of this command include the antenna gain for that device, regardless of whether the AP antenna is internal or external. MIMO gain (if applicable) is also accounted for in the maximum EIRP limits. | AP |
| <u>show ap arm bandwidth-management</u> | Displays the bandwidth management information for clients associated to an AP. The client match feature must be enabled. | AP |
| <u>show ap arm history</u> | Displays the history of the channel and power changes due to Adaptive Radio Management (ARM) for each interface on an AP. | AP |
| <u>show ap arm neighbors</u> | Displays the ARM settings for an AP's neighbor. | AP |
| <u>show ap arm rf-summary</u> | Displays the state and statistics for all the channels being monitored by an individual AP. | AP |
| <u>show ap arm scan-times</u> | Displays the channel scan times for an individual AP and also the information on the channel being scanned. | AP |
| <u>show ap arm state</u> | Displays the Adaptive Radio Management (ARM) information for an individual AP's neighbor, or show all available data for any neighboring AP using an 802.11a or 802.11g radio type. Include an AP name or IP address to show data for just a single AP, or use the <i>dot11a</i> or <i>dot11g</i> keywords to show data for all APs using that radio type. | GW |
| <u>show ap association</u> | Displays the AP association table. Run this command to check if user is connected to an AP. This command validates whether the client is associated and indicates the last AP to which it was connected. If the flags column shows an 'A', the client is currently associated with that AP. Alternately, if the client is not currently associated, the AP with the smallest value of association time is the last AP used by the client. | AP, GW |
| <u>show ap blacklist-clients</u> | Displays a list of clients that have been denied the access. | GW |
| <u>show ap bss-table</u> | Displays the Basic Service Set (BSS) table of an AP. To filter this information and view BSS table data for an individual AP or a specific port and slot number, include the <i>ap-name</i> , <i>bssid</i> , <i>essid</i> , <i>ip-addr</i> or <i>port</i> keywords. | AP, GW |
| <u>show ap client-match-history</u> | Displays the historical record of the client match events and actions for the clients associated with an AP. | AP |
| <u>show ap client-match-live</u> | Displays the current client match events and actions for clients associated with an AP. | AP |

| Command | Description | Applies To |
|---|--|------------|
| show ap client-probe-report 0 | Displays the client probe report for an AP. You can filter the output based on the radio ID number (for example, 0). | AP |
| show ap client-probe-report 1 | Displays the client probe report for an AP. You can filter the output based on the radio ID number (for example, 1). | AP |
| show ap client-view | Displays the information about the clients in an AP's neighborhood. | AP |
| show ap debug auth-trace-buf+ | Displays the trace buffer for authentication events associated with the AP. Use the output of this command to troubleshoot authentication errors. Include the <MAC> parameter to filter data by the MAC address of the client to view specific details. | AP |
| show ap debug c2c-nodes | Displays the c2c nodes settings for authentication events associate with the AP. | AP |
| show ap debug client-mgmt-counters | Displays the message counters. This command shows the numbers for each type of message sent from a client to an AP. Use this information to troubleshoot problems of an AP. | AP, GW |
| show ap debug client-stats* | Displays the detailed statistics about a client from an AP. | AP |
| show ap debug client-table | Displays the clients associated with an AP. The <i>Tx_Rate</i> , <i>Rx_Rate</i> , <i>Last_ACK_SNR</i> , and <i>Last_Rx_SNR</i> columns shown in the output of this command show valuable troubleshooting information for clients trying to connect to a specific AP. Use this command to verify that the transmit (<i>Tx_Rate</i>) and receive (<i>Rx_Rate</i>) rates are not too low, and that the SNR is acceptable. | AP |
| show ap debug cloud-config-received | Displays the configuration information received by the AP from the Central server. | AP |
| show ap debug cloud-data-sent | Displays the information about data exchange between the Central server and the AP. | AP |
| show ap debug cloud-events-pending | Displays the pending Central server events. | AP |
| show ap debug cloud-server | Displays the AP management details, either local or cloud server. If the AP is managed by a cloud server, the server details are displayed. | AP |
| show ap debug cloud-signon-key | Displays the Central sign on key information that is used by the administrator to manually authorize the first Virtual Controller for an organization. | AP |
| show ap debug cloud-state | Displays the configuration details and status of the Central events associated with an AP. | AP |
| show ap debug cloud-stats | Displays the configuration statistics associated with an AP managed by the Central server. | AP |

| Command | Description | Applies To |
|--|--|------------|
| <u>show ap debug counters</u> | Displays the AP reboot/bootstrap counters and crash information for an individual AP or AP group, or all APs referenced on the controller. | GW |
| <u>show ap debug crash-info</u> | Displays the crash log information (if any) for an individual AP. The stored information is cleared from the flash after the AP reboots. | AP |
| <u>show ap debug dot1x-statistics</u> | Displays the aggregate 802.11X debug statistics for an AP. | AP |
| <u>show ap debug driver-config</u> | Displays the AP driver configuration. Run this command to review configuration changes made since the AP driver was last reset. | AP |
| <u>show ap debug lldp neighbor</u> | Displays the LLDP information for a specific AP, or all APs sending or receiving LLDP PDUs. The LLDP protocol allows switches, routers, and WLAN APs to advertise information such as identity, capabilities, and neighbors to other nodes on the network. Run this command to view information about LLDP peers and APs. By default, this command displays LLDP neighbors for the entire list of LLDP interfaces. Include the IP address of a device to display neighbor information only of that device. | AP |
| <u>show ap debug mgmt-frames+</u> | Displays the trace information for the 802.11 management frames. | AP |
| <u>show ap debug persistent-clients</u> | Displays the information about the persistent AP clients. Use the output of this command to view information about the clients that are persistently connected to an AP. | AP |
| <u>show ap debug pmk-sync-statistics</u> | Displays the PMK synchronization statistics for the authentication servers configured on an AP. | AP |
| <u>show ap debug radio-stats 0</u> | Displays the aggregate radio debug statistics of an AP. Specify the ID number of the radio to view its specific statistics (for example, 0). | AP |
| <u>show ap debug radio-stats 1</u> | Displays the aggregate radio debug statistics of an AP. Specify the ID number of the radio to view its specific statistics (for example, 0). | AP |
| <u>show ap debug radius-statistics</u> | Displays the RADIUS statistics for the authentication servers configured on an AP. Use the output of this command to view the authentication server details. | AP |
| <u>show ap debug shaping-table</u> | Displays the shaping information for the clients associated to an AP. | AP |
| <u>show ap debug sta-msg-stats</u> | Displays the AP-STM to STM message statistics. | GW |
| <u>show ap debug stm-bucketmap</u> | Displays the AP STM configuration information. | AP |
| <u>show ap debug stm-config</u> | Displays the AP STM configuration information. | AP |

| Command | Description | Applies To |
|---|---|------------|
| show ap debug stm-role | Displays the STM user roles configured for the SSIDs in an AP. Use the output of this command to view the user roles configured for the AP STM. This includes details of the VLANs assigned to each SSID and also shows if the Calea feature is enabled or disabled. | AP |
| show ap debug system-status | Displays the detailed system status information for an AP. | AP |
| show ap dot11k-beacon-report* | Displays the beacon report details for the 802.11k clients of an AP. | AP |
| show ap dtls allowed-aps | Displays the active APs, AP scanning, and AP synchronization status for DTLS allowed devices. | AP |
| show ap dtls ephemeral-neighborlist | Displays the active APs, AP scanning, and AP synchronization status for DTLS ephemeral neighborlist devices. | AP |
| show ap dtls provisioned-neighborlist | Displays the active APs, AP scanning, and AP synchronization status for DTLS provisioned neighborlist devices. | AP |
| show ap essid | Displays the ESSID summary for the controller, including the number of APs and clients associated with each ESSID. | GW |
| show ap global acl-table | Displays the ACL table of STM. | GW |
| show ap image version | Displays an AP's image version information. By default, this command displays image version information for all APs associated with the controller. To view image version information for a single AP, specify an AP using the <i>ap-name</i> or <i>ip-addr</i> parameters. | GW |
| show ap image-preload status all | Displays the list of APs that preloads a new version of software from a controller with the AP preload feature activated. Run this command to display a list of APs in the AP image preload list, and monitor the download status of each AP. | GW |
| show ap license-usage | Displays the AP license usage information. | GW |
| show ap machine-authcache | Displays the active APs, AP scanning, and AP synchronization status for authentication cache. | AP |
| show ap mesh active | Displays the active mesh cluster APs currently registered on this Mobility Master. | GW |
| show ap mesh counters | Displays the mesh counters for an AP. Use the output of this command to view a list of mesh counters available for an AP. | AP |
| show ap mesh link | Displays the mesh link of the AP. | AP |
| show ap mesh neighbours | Displays the mesh neighbors of an AP. | AP |
| show ap mesh topology long | Displays the mesh topology tree with names of mesh portal's children in the output of this command. | GW |

| Command | Description | Applies To |
|--|---|------------|
| show ap monitor active-laser beams | Displays the information for active laser beam generators of Aruba Air Monitors. The output of this command shows a list of all APs that are actively performing policy enforcement containment such as rogue containment. This command can tell us which AP is sending out deauthorization frames, although it does not specify which AP is being contained. | AP |
| show ap monitor ap-list | Displays the list of APs being monitored for Aruba Air Monitors. | AP |
| show ap monitor arp-cache | Displays the ARP cache of learned IP to MAC binding for Aruba Air Monitors. | AP |
| show ap monitor containment-info | Displays the containment events and counters triggered by the wired containment and wireless containment features configured in the Intrusion Detection System (IDS) general-profile. The output of this command shows device and target data for wired containment activity. | AP |
| show ap monitor pot-ap-list | Displays the potential AP table for Aruba Air Monitors. The table shows the following data: <ul style="list-style-type: none"> ■ bssid—The AP's Basic Service Set Identifier. ■ channel—The AP's current radio channel. ■ phy type—The radio's PHY type. Possible values are 802.11a, 802.11a-HT-40, 802.11b/g, 802.11b/g-HT-20. ■ num-beacons—Number of beacons seen during a 10-second scan. ■ tot-beacons—Total number of beacons seen since the last reset. ■ num-frames—Total number of frames seen since the last reset. ■ mt—Monitor time; the number of timer ticks elapsed since the controller first recognized the AP. ■ at—Active time, in timer ticks. ■ ibss—Shows if adhoc BSS is enabled or disabled. It will be enabled if the bssid has detected an adhoc BSS (an ibss bit in an 802.11 frame). ■ rsi—The Receive Signal Strength Indicator (RSSI) value displayed in the output of this command represents signal strength as a signal to noise ratio. For example, a value of 30 would indicate that the power of the received signal is 30 dBm above the signal noise threshold. | AP |
| show ap monitor pot-sta-list | Displays the potential client table. It shows the following values: <ul style="list-style-type: none"> ■ last-bssid—The last BSSID to which the client associated. ■ from—BSSID. ■ to—BSSID. ■ mt—Monitor time; the number of timer ticks elapsed since the first client is recognized. ■ it—Client idle time, expressed as a number of timer ticks. | AP |

| Command | Description | Applies To |
|--|--|------------|
| <u>show ap monitor routers</u> | Displays the router MAC addresses learned. The output of this command includes the router's MAC address, IP address, and uptime for Aruba Air Monitors. | AP |
| <u>show ap monitor scan-info</u> | Displays the AP scanning information for Aruba Air Monitors. | AP |
| <u>show ap monitor sta-list</u> | Displays the configuration and status of monitor information of the AP. | AP |
| <u>show ap monitor status</u> | Displays the general AP status information and the maximum classification delay that was observed in monitored APs and clients for the WLAN Interface. The unclass_sta_update parameter must be enabled to view the maximum delay for clients. | AP |
| <u>show ap mpskcache</u> | Displays the multiple PSK local cache table for clients associated with the AP. | AP |
| <u>show ap pmkcache</u> | Displays the PMK cache table for clients associated with the AP. | AP |
| <u>show ap radio-summary</u> | Displays the AP radios registered to the controller. | GW |
| <u>show ap regulatory</u> | Displays the currently active regulatory certificate. | GW |
| <u>show ap spectrum monitors</u> | Displays the list of APs terminating on the controller that are currently configured as spectrum monitors or hybrid APs. | GW |
| <u>show ap virtual-beacon-report</u> | Displays the virtual beacon report for an AP or a client with a specific IP or MAC address. The client match feature must be enabled. Run this command to view the client RSSI from the APs in its RF neighborhood, the channel used by each AP radio, and the number of clients associated to each radio. | AP |
| <u>show ap vlan-usage</u> | Displays the number of clients on each VLAN. | GW |
| <u>show ap wmm-flow</u> | Displays the Wireless Multimedia (WMM) flow table. The WMM or Wireless Multimedia Extensions are a subset of the 802.11e standard. WMM provides four different types of traffic classification: voice, video, best effort, and background, with voice having the highest priority and background the lowest. Run the show ap wmm-flow command to view WMM flow data for all APs. | GW |
| <u>show ap-alert</u> | Displays all the alerts received for the specified APs. | AP |
| <u>show ap-env</u> | Displays the provisioned AP parameters such as the type of antenna used by an AP. The output of this command indicates if the AP is configured to use an external or integrated antenna and if the AP is configured as a master AP. | AP |
| <u>show app-services</u> | Displays the list of application services available on an AP. | AP |
| <u>show aps</u> | Displays the active APs, AP scanning, and AP synchronization status. | AP |

| Command | Description | Applies To |
|---|---|------------|
| show aps scanning | Displays the AP scanning details. | AP |
| show arm config | Displays the ARM configuration details for an AP. | AP |
| show arm-channels | Displays the ARM channel details configured on an AP. | AP |
| show arp | Displays the Address Resolution Protocol (ARP) entries for the controller. | AP, GW |
| show aruba-central control-channel | Displays the number of control channel references to Aruba-Central. | GW |
| show aruba-central details | Displays the references to Aruba-Central. | GW |
| show ata counters | Displays the counters for the AP Tunnel Agent (ATA). | AP |
| show ata current-cfg | Displays the configuration of the tunnels. | AP |
| show ata endpoint | <p>Displays the status of the tunnel endpoints. The information includes the following parameters:</p> <ul style="list-style-type: none"> ■ UUID– Assigned by the Overlay Tunnel Orchestrator (OTO. Unique for each tunnel. ■ IP ADDR– IP address of a gateway. ■ STATE– State of the tunnel as defined by the AP Tunnel Agent (ATA). ■ TUN DEV– Tunnel device name. ■ TUN SPIOut/In– In and Out Tunnel SPI. ■ PORT (SRC/DST)– UDP ports which are used to encapsulate packets to the IPsec tunnel. ■ VALID TIME– Time in seconds for the tunnel key usage. ■ GRE TYPE– Values are: <ul style="list-style-type: none"> • GRE. • GRE over IPSEC. ■ GRE VLANs– VLANs to which GRE tunnel belongs. ■ HBT– Displays the following 4 counters: <ul style="list-style-type: none"> • Jiffies of the latest received heartbeat response. • Missed heartbeat count. • Sequence number of the last heartbeat that the AP sent. • Sequence number of the latest heartbeat that the AP received. | AP |
| show audit-trail | Displays the controller's audit trail log. | GW |
| show audit-trail history | Displays the audit trail history log. | GW |
| show auth-survivability cached-info | Displays the authentication credentials cached by the AP. | AP |

| Command | Description | Applies To |
|---|--|------------|
| show auth-tracebuf+ | Displays the trace buffer for authentication events. Use the output of this command to troubleshoot 802.1X authentication errors. Include the <address> parameter to filter data by the MAC address of the client which is experiencing errors. | GW |
| show boot | Displays the boot parameters, including the boot partition and the configuration file to use when booting the controller. | GW |
| show boot history | Displays the controller's reloads and upgrade history. | GW |
| show captive-portal auto-white-list | Displays the external and internal captive portal parameters configured for a network profile. Use the output of this command to view information about the contents displayed on the internal and external captive portal pages for guest users. | AP |
| show captive-portal-domains | Displays the internal and external captive portal server domains. Use this command to view information about the internal and external captive portal domains. | AP |
| show cellular config | Displays the status and cellular configuration of the AP. | AP |
| show cellular status | Displays the status and cellular configuration of the AP. | AP |
| show client status* | Displays the current status for a client based on the specified MAC address. | AP |
| show clients | Displays the details about the AP clients. Use this command to view information about the AP clients. The AP client table provides basic information about the clients. For detailed information of each client, use the required parameter and specify the MAC address of the client. | AP |
| show clients debug | Displays the AP client configuration details, which can be used for debugging purpose. | AP |
| show clients wired | Displays the list of clients connected to wired or Ethernet interface. | AP |
| show clients wired debug | Displays the list of clients connected to wired or Ethernet interface. The debug parameter is used to view the end-to-end information of the wired clients for debugging purpose. | AP |
| show clock | Displays the configuration for the system clock, summer daylight savings configuration, timezone configuration, and gives details if the CLI-timestamp is enabled or disabled. | AP |
| show clock summer-time | Displays the configuration for the system clock, summer daylight savings configuration, timezone configuration, and gives details if the CLI-timestamp is enabled or disabled. The summer-time parameter shows the configured daylight savings time settings. | AP |

| Command | Description | Applies To |
|---|---|------------|
| show clock timezone | Displays the configuration for the system clock, summer daylight savings configuration, timezone configuration, and gives details if the CLI-timestamp is enabled or disabled. The timezone parameter shows the current timezone, with its time offset from Greenwich Mean Time. | AP |
| show clock timezone all | Displays the configuration for the system clock, summer daylight savings configuration, timezone configuration, and gives details if the CLI-timestamp is enabled or disabled. Include the optional summer-time parameter to display configured daylight savings time settings. The timezone parameter shows the current timezone, with its time offset from Greenwich Mean Time. The timezone parameter shows the current timezone, with its time offset from Greenwich Mean Time. | AP |
| show cluster | Displays the cluster configuration for the control plane security feature. | AP |
| show cluster bss-table | Displays the Basic Service Set (BSS) table of a cluster. | AP |
| show cluster-config | Displays the cluster configuration for the control plane security feature.
When you run this command from the cluster root, the output of this command shows the cluster role of the managed device, and the IP address of each member node in the cluster.
When you issue this command from a cluster member, the output of this command shows the cluster role of the managed device, and the IP address of the cluster root. | GW |
| show cluster-security | Displays the cluster security configuration details for all the APs in the cluster. | AP |
| show cluster-security connections | Displays the total number of connections monitored in the swarm by cluster security DTLS. | AP |
| show cluster-security counter | Displays the cluster security configuration details for all the APs in the cluster for a counter. | AP |
| show cluster-security peers | Displays the details and status of the peers monitored by cluster security DTLS. | AP |
| show cluster-switches | Displays the IP address of the VLAN used by the cluster member to connect to the cluster root when this command is run at cluster root. When the command is run from a cluster member, the output of this command displays the IP address of the VLAN used by the cluster root to connect to the cluster member. | GW |
| show cluster-tech-support | Displays the cluster-related information in relation to the managed device. | GW |
| show configuration | Displays the saved configuration on the controller. Execute this command to view the entire configuration saved on the controller, including all profiles, ACLs, and interface settings. | AP |

| Command | Description | Applies To |
|--|---|------------|
| show configuration effective | Displays the effective configuration of devices connected to the node. | GW |
| show control-plane-security | Displays the current configuration of the control plane security profile. The control plane security profile enables and disables the control plane security feature and identifies campus APs to receive security certificates. Run this command to view current control plane security settings. | GW |
| show country | Displays the country and domain upgrade trail of the controller. A controller's country code sets the regulatory domain for the radio frequencies that the APs use. This value is typically set during the controller's initial setup procedure. Run this command to determine the country code specified during setup. | GW |
| show country trail | Displays the record showing how the switch was reconfigured for its current country domain when the controller hardware was upgraded. | GW |
| show country-codes | Displays the list of supported country codes for the AP. | AP |
| show cp-bwcontracts | Displays the list of Control Processor (CP) bandwidth contracts for whitelist ACLs. | GW |
| show cp-stats | Displays the control plane (CP) queue statistics. | GW |
| show cpu | Displays the CPU details. Run this command to view CPU load for application and system processes. | AP |
| show cpu details | Displays the CPU troubleshooting statistics. | AP |
| show cpuload | Displays the controller CPU load for application and system processes. The CPU load stats for a controller can be viewed by using the current parameter, or displayed per-processor by using the <i>per-cpu</i> command. | GW |
| show cpuload current | Displays the CPU troubleshooting statistics. | GW |
| show crypto dp | Displays crypto data packets. Run this command to send crypto data packet information to the controller log files, or to clear a crypto ISAKMP state associated with a specific IP address. | GW |
| show crypto dynamic-map | Displays the IPsec dynamic map configurations. Dynamic maps enable IPsec SA negotiations from dynamically addressed IPsec peers. Once you have defined a dynamic map, you can associate that map with the default global map using the command <i>crypto map global-map</i> . | GW |
| show crypto ipsec ipsec-map-id | Displays the IPsec MAP to ID mapping of current IPsec configuration on the managed device. Run this command to view the Maximum Transmission Unit (MTU) size allowed for network transmissions using IPsec security. It also displays the transform sets that define a specific encryption and authentication type. | GW |

| Command | Description | Applies To |
|---|--|------------|
| show crypto ipsec sa | Displays the security associations (SAs) of current IPsec configuration on the managed device. | GW |
| show crypto ipsec transform-set | Displays the IPsec transform sets on the managed device. | GW |
| show crypto isakmp groupname | Displays the Internet Key Exchange (IKE) aggressive groupname for the Internet Security Association and Key Management Protocol (ISAKMP). Run this command to view ISAKMP settings, statistics and policies. | GW |
| show crypto isakmp key | Displays the IKE pre-shared keys. | GW |
| show crypto isakmp policy | Displays the following information for predefined and manually configured IKE policies: <ul style="list-style-type: none"> ■ IKE version ■ Encryption and hash algorithms ■ Authentication method ■ PRF methods ■ DH group ■ Lifetime settings | GW |
| show crypto isakmp sa | Displays the security associations. | GW |
| show crypto isakmp stats | Displays the detailed IKE statistics. This information can be very useful for troubleshooting problems with ISAKMP. | GW |
| show crypto isakmp uplink-vlan | Displays the Internet Key Exchange (IKE) parameters for the Internet Security Association and Key Management Protocol (ISAKMP) for uplink VLANs. Use the show crypto isakmp command to view ISAKMP settings, statistics and policies. | GW |
| show crypto map | Displays the IPsec map configurations. Use the show crypto map command to view configuration for global, dynamic, and default map configurations. | GW |
| show crypto oto | Displays the Internet Key Exchange (IKE) parameters for the Internet Security Association and Key Management Protocol (ISAKMP) for overlay tunnel orchestration. | GW |
| show crypto-local ipsec-map | Displays the current IPsec map configuration on the controller. | GW |
| show crypto-local isakmp ca-certificate | Displays the Certificate Authority (CA) certificates associated with VPN clients. | GW |
| show crypto-local isakmp certificate-group | Displays the existing certificate groups by server certificate name and CA certificate. | GW |
| show crypto-local isakmp dpd | Displays the IKE Dead Peer Detection (DPD) configuration on the managed device. | GW |
| show crypto-local isakmp server-certificate | Displays the IKE server certificates used to authenticate the managed device for VPN clients. | GW |

| Command | Description | Applies To |
|--|---|------------|
| show crypto-local pki CRL | Displays the name, original filename, reference count and expiration status of all CRLs on this controller. | GW |
| show crypto-local pki ocsp-client-stats | Displays the OCSP client statistics. | GW |
| show crypto-local pki OCSPResponderCert | Displays the name, original filename, reference count and expiration status of all OCSPResponderCert certificates on this controller. | GW |
| show crypto-local pki OCSPSignerCert | Displays the OCSP signer certificate. | GW |
| show crypto-local pki PublicCert | Displays the public key of the certificate. | GW |
| show crypto-local pki rcp | Displays the revocation check point. | GW |
| show crypto-local pki ServerCert | Displays the server certificate. | GW |
| show crypto-local pki service-ocsp-responder | Displays the OCSP responder service availability and the corresponding statistics. | GW |
| show crypto-local pki TrustedCA | Displays the trusted CA certificate information. This certificate can be either a root CA or intermediate CA. | GW |
| show database synchronize | Displays the Multiple Master Switches redundancy status (Master-Master communication). | GW |
| show datapath acl id 2700 | Displays the system statistics for the managed device. Run the command with a specific ACL ID to display its datapath statistics for debugging purposes. | GW |
| show datapath acl id 2701 | Displays the system statistics for the managed device. Run the command with the specific ID of the ACL to display its datapath statistics for debugging purposes. | GW |
| show datapath acl id 2702 | Displays the system statistics for the managed device. Run the command with the specific ID of the ACL to display its datapath statistics for debugging purposes. | GW |
| show datapath acl id 4 | Displays the system statistics for the managed device. Run the command with the specific ID of the ACL to display its datapath statistics for debugging purposes. | GW |
| show datapath acl-all | Displays the datapath statistics associated with all ACLs. | AP |
| show datapath acl-allocation | Displays the ACL table allocation details. | AP |
| show datapath application counters | Displays the various counters maintained in the datapath. This parameter is useful in debugging if any datapath issue is encountered. | GW |
| show datapath bridge | Displays the bridge table entry statistics including MAC address, VLAN, assigned VLAN, Destination and flag information for an AP. | AP |

| Command | Description | Applies To |
|---|--|------------|
| show datapath bridge counters | Displays the bridge counter statistics including MAC address, VLAN, assigned VLAN, Destination and flag information for an AP. | GW |
| show datapath bridge table | Displays the bridge table entry statistics including MAC address, VLAN, assigned VLAN, Destination and flag information for an AP. | GW |
| show datapath bwm table | Displays the configured bandwidth contracts and the allocated bandwidth contracts. | GW |
| show datapath cp-bwm table | Displays the configured bandwidth contracts and the allocated bandwidth contracts. | GW |
| show datapath crypto counters | Displays the datapath station crypto counters or statistics. | GW |
| show datapath debug dma counters | Displays the low-level datapath details of DMA counters. | GW |
| show datapath debug eap counters | Displays the low-level datapath details of EAP counters. | GW |
| show datapath debug opcode | Displays the datapath debug details. | GW |
| show datapath debug trace-buffer | Displays the datapath route or cache tracing debug details. | GW |
| show datapath dmo-session | Displays the details of a DMO session. | AP |
| show datapath dns-id-map | Displays the IP address of the domain name configured in a domain-based ACL. | AP |
| show datapath exthdr | Displays the datapath default IPv6 Extended Header Map. | GW |
| show datapath frame | Displays the frame statistics that are received and transmitted from the data path of the controller. Several output fields include the following descriptions: <ul style="list-style-type: none"> ■ Descr failures– This is the number of times a packet descriptor was not available and the packet dropped. ■ Dot1QDiscards– The number of packets received on a trunk port where the VLAN presented did not match any configured on the controller and the packet dropped. ■ Dot1d Discards– Spanning tree is disabled and each BPDU frame is counted and dropped. ■ Denied Frames– Frames that are denied by the data path of the ACL for the controller. | GW |
| show datapath frame counters | Displays the frame counter statistics that are received and transmitted from the data path of the controller. | GW |
| show datapath hardware counters | Displays the datapath hardware counters or hardware packet statistics information. | GW |
| show datapath hardware statistics | Displays the datapath hardware packet statistics information. | GW |

| Command | Description | Applies To |
|--|--|------------|
| <u>show datapath internal dir int file pic_regs</u> | Displays the internal details of the hardware directory and the file in the directory. | GW |
| <u>show datapath internal dir nae file rx_free_fifo</u> | Displays the internal details of the file in the directory. | GW |
| <u>show datapath internal dir nae file rx_misc</u> | Displays the internal details of the file in the directory. | GW |
| <u>show datapath internal dir nae file tx_credit</u> | Displays the internal details of the file in the directory. | GW |
| <u>show datapath internal dir nae file tx_misc</u> | Displays the internal details of the file in the directory. | GW |
| <u>show datapath internal dir poe file class_drop_ctrs</u> | Displays the internal details of the file in the directory. | GW |
| <u>show datapath internal dir poe file ecc_1bit_errs</u> | Displays the internal details of the file in the directory. | GW |
| <u>show datapath internal dir poe file enq_msg_ctrs</u> | Displays the internal details of the file in the directory. | GW |
| <u>show datapath internal dir poe file err_regs</u> | Displays the internal details of the file in the directory. | GW |
| <u>show datapath internal dir poe file stats_n_dbg</u> | Displays the internal details of the file in the directory. | GW |
| <u>show datapath internal dir poe file vec_drop_ctrs</u> | Displays the internal details of the file in the directory. | GW |
| <u>show datapath internal dir sae file error_status</u> | Displays the internal details of the file in the directory. | GW |
| <u>show datapath internal dir sae file int_status</u> | Displays the internal details of the file in the directory. | GW |
| <u>show datapath internal dir sae file msg_cnt</u> | Displays the internal details of the file in the directory. | GW |
| <u>show datapath internal dir sae file op_cnt</u> | Displays the internal details of the file in the directory. | GW |
| <u>show datapath ip-mcast destination</u> | Displays the Datapath IP Multicast Entries table statistics. | GW |
| <u>show datapath ip-mcast group</u> | Displays the Datapath IP Multicast Entries table statistics for layer 3 groups. | GW |
| <u>show datapath ip-reassembly counters</u> | Displays the contents of the IP reassembly statistics counters. | GW |
| <u>show datapath ipsec-map</u> | Displays the datapath IPsec map details. | GW |

| Command | Description | Applies To |
|--|--|------------|
| <u>show datapath ipv6-mcast destination</u> | Displays the datapath IP multicast table statistics for the IPv6 tunnel and port membership. | GW |
| <u>show datapath ipv6-mcast group</u> | Displays the datapath IP multicast table statistics for the IPv6 station membership. | GW |
| <u>show datapath ipv6-mcast station</u> | Displays the datapath IP multicast table statistics for the IPv6 station membership. | GW |
| <u>show datapath lag table</u> | Displays the contents of the datapath LAG or port channel table. | GW |
| <u>show datapath maintenance counters</u> | Displays the datapath maintenance counters statistics. | GW |
| <u>show datapath mcast</u> | Displays the multicast table statistics for the AP. | AP |
| <u>show datapath message-queue counters</u> | Displays the statistics of messages received by a CPU from other datapath CPUs (only CPUs that receive messages and non-zero statistics are shown). The datapath SOS message queue statistics by CPU IDs and Opcode is displayed. | GW |
| <u>show datapath mobility home-agent-table</u> | Displays the datapath IP mobility information for the home agent table. | GW |
| <u>show datapath mobility mcast-table</u> | Displays the datapath IP information for the mobility multicast-group table that is used to flood the multicast RA traffic to the roamed clients. | GW |
| <u>show datapath mobility stats</u> | Displays the IP information for the datapath mobility statistics. | GW |
| <u>show datapath nat table</u> | Displays the contents of the datapath NAT entries table. It displays NAT pools as configured in the datapath. Statistics include pool, SITP start, SIP end and DIP. | GW |
| <u>show datapath nat-pool</u> | Displays the contents of the datapath NAT entries table. It displays NAT pools as configured in the datapath. Statistics include pool, SITP start, SIP end and DIP. | AP |
| <u>show datapath network ingress</u> | Displays the network ingress details as follows: <ul style="list-style-type: none"> ■ LIFO Queue ■ Threshold count ■ Empty Count ■ Threshold Recovery ■ Empty Recovery | GW |
| <u>show datapath nexthop-list</u> | Displays the information about the datapath for packets routed to next-hop devices. The output contains the following details: <ul style="list-style-type: none"> ■ Dest ■ Version ■ Nexthop ■ Nexthop Dest ■ Nexthop Index | GW |

| Command | Description | Applies To |
|--|--|------------|
| | <ul style="list-style-type: none"> ■ Nexthop Version ■ Nexthop VLAN ■ Nexthop Priority | |
| show datapath openflow acl | Displays the datapath OpenFlow information for the ACL table and actions. | GW |
| Show datapath openflow session | Displays the datapath OpenFlow information for the session tables and actions. You can filter the sessions based on the IP address. | GW |
| show datapath papi counters | Displays the datapath PAPI statistics including the SUM or CPU, addr, description, and value. | GW |
| show datapath port | Displays the datapath port table information. This consists of the port number, PVID, Ingress ACL, Egress ACL, Session ACL, and the following flags: <ul style="list-style-type: none"> ■ B–Blocked by the Spanning Tree protocol ■ L–LSG ■ M–Tunneled node ■ Q–Trunk ■ T–Trusted ■ X–xSec ■ Z–QinQ | GW |
| show datapath route | Displays datapath route table statistics. | AP, GW |
| show datapath route counters | Displays datapath route table statistics such as current entries, high water mark, maximum entries, total entries, allocation failures, and max link length. | GW |
| show datapath route ipv6 | Displays the statistics for the datapath IPv6 routing table. | GW |
| show datapath route verbose | Displays the statistics for all the route table entries including IP, mask, gateway, cost, VLAN, flags, and Internal VerNum Index. | GW |
| show datapath route-cache counters | Displays the route cache table statistics such as current entries, high water mark, maximum entries, total entries, allocation failures, and max link length. | GW |
| Show datapath route-cache ipv6 | Displays the datapath route cache table statistics for the IPv6. | GW |
| show datapath route-cache verbose | Displays the route cache table entries including IP, mask, gateway, cost, VLAN, flags, and Internal VerNum Index. | GW |
| show datapath sbr | Displays the destination servers that are reachable through a particular IP address. | AP |
| show datapath session | Displays the datapath session statistics. The command output details are as follows: <ul style="list-style-type: none"> ■ Source IP ■ Destination IP ■ SPort | AP |

| Command | Description | Applies To |
|--|---|------------|
| | <ul style="list-style-type: none"> ■ DPort ■ Prio ■ ToS ■ Age ■ Destination ■ TAge ■ Packets ■ Bytes ■ NhIdx ■ NhIdx ■ NhNhVer | |
| show datapath session include O | Displays the datapath session statistics for specific session IDs. | GW |
| show datapath session counters | Displays the counters statistics including current entries, high water mark, maximum entries, total entries, current maximum link length, maximum link length, stale entries, aged entries, and pending delete entries. | GW |
| show datapath session dpi | Displays the Deep Packet Information (DPI) for the current session. The output details are as follows: <ul style="list-style-type: none"> ■ AcVersion—This is used to store the current version number of the ACL that is used at session creation time and is used for troubleshooting purposes. ■ PktsDpi—The number of packets sent to the DPI engine for a given session. ■ AcIdx—The Index of the Access List entry (in a given ACL) that triggered a match during session creation. ■ DpiTIdx—This is an index to the DPI engine Tbl and is only used for troubleshooting purposes. | AP |
| show datapath session dpi include O | Displays the Deep Packet Information (DPI) for the specific session IDs. | GW |
| show datapath session dpi counters | Displays the statistics for DPI counters for the current session. | GW |
| show datapath session dpi table | Displays the datapath session entries and statistics including current entries, high water mark, maximum entries, total entries, allocation failures, duplicate entries, cross linked entries, number of reverse entries, and maximum link length. | GW |
| show datapath session ipv6 include O | Displays the datapath IPv6 session entries and statistics including current entries, high water mark, maximum entries, total entries, allocation failures, duplicate entries, cross linked entries, number of reverse entries, and maximum link length for specific session IDs. | GW |

| Command | Description | Applies To |
|--|--|------------|
| show datapath session ipv6 dpi include O | Displays the datapath IPv6 session entries and DPI statistics including current entries, high water mark, maximum entries, total entries, allocation failures, duplicate entries, cross linked entries, number of reverse entries, and maximum link length for specific session IDs. | GW |
| show datapath session ipv6 verbose | Displays the datapath IPv6 session entries and statistics including current entries, high water mark, maximum entries, total entries, allocation failures, duplicate entries, cross linked entries, number of reverse entries, and maximum link length. | GW |
| show datapath session ucc | Displays the datapath session statistics. | AP |
| show datapath session uplink verbose | Displays the statistics of datapath session with uplink VLAN and additional information that can be used for debugging. The output details are as follows: <ul style="list-style-type: none"> ■ SIDX ■ SRTI ■ SRCI ■ UsrIdx ■ UsrVer ■ AclVer ■ NhIdx ■ NhVer | GW |
| show datapath session verbose | Displays the datapath session statistics with additional information that can be used for debugging. | GW |
| show datapath session web-cc | Displays the web-content category information about the session. The output details are as follows: <ul style="list-style-type: none"> ■ WebCCRep– Reputation score (integer). To see the reputation type associated with that particular score, run the command <code>show web-cc reputation</code>. ■ WebCCID– Web content category ID. To see the name of the category associated with that category ID, run the command <code>show web-cc category</code>. ■ WebCCURL– URL for that session entry. | GW |
| show datapath station table | Displays the datapath station association table statistics. | GW |
| show datapath statistics | Displays the datapath station association table statistics. | AP |
| show datapath tunnel | Displays the contents of the datapath tunnel table for the tunnels that are terminated by the controller, including the GRE tunnels of Aruba AP. The output details are as follows: <ul style="list-style-type: none"> ■ Source ■ Destination ■ Port ■ Type ■ MTY ■ VLAN ■ ACLs | GW |

| Command | Description | Applies To |
|---|--|------------|
| | <ul style="list-style-type: none"> ■ BSSID ■ Decaps ■ Encaps ■ Heartbeats ■ Flags ■ Encap Bytes ■ Decap Bytes | |
| show datapath tunnel counters | Displays the tunnel counters or statistics. | GW |
| show datapath tunnel heartbeat | Displays the datapath heartbeat tunnel details. | GW |
| show datapath tunnel ipv6 | Displays the TCP tunnel table filtered on IPv6 entries. | GW |
| show datapath tunnel ipv6 verbose | Displays the TCP tunnel table filtered on IPv6 entries. The encaps or verbose parameter is optional. | GW |
| show datapath tunnel verbose | Displays the datapath tunnel internal details. | GW |
| show datapath tunnel-group | Displays the tunnel group, active status, and members. | GW |
| show datapath uplink | Displays the statistics of datapath session with uplink VLAN. | GW |
| show datapath uplink verbose | <p>Displays the statistics of datapath session with uplink VLAN and additional information about the session that can be used for debugging. The output details are as follows:</p> <ul style="list-style-type: none"> ■ SIDX ■ SRTI ■ SRCI ■ UsrIdx ■ UsrVer ■ AcIVer ■ NhIdx ■ NhVer | GW |
| show datapath user | Displays the datapath user statistics such as current entries, pending deletes, high water mark, maximum entries, total entries, allocation failures, invalid users, and maximum link length. | AP |
| show datapath user counters | Displays the datapath user counter statistics such as current entries, pending deletes, high water mark, maximum entries, total entries, allocation failures, invalid users, and maximum link length. | GW |
| show datapath user ipv6 | Displays the datapath IPv6 user entries and statistics such as current entries, pending deletes, high water mark, maximum entries, total entries, allocation failures, invalid users, and maximum link length. | GW |
| show datapath user table | Displays the user table statistics. | GW |

| Command | Description | Applies To |
|--|---|------------|
| show datapath utilization | Displays the current CPU utilization of datapath CPUs by the CPU ID. The output includes CPU ID and CPU utilization during the past 1 sec, 4 sec, and 64 sec. | GW |
| show datapath vlan | Displays the VLAN table information such as VLAN memberships inside the datapath including Layer 2 tunnels which tunnel L2 traffic. The output details are as follows: <ul style="list-style-type: none"> ■ VLAN ■ Flags ■ Ingress RACL ■ Ports | AP |
| show datapath vlan table | Displays the VLAN number, flag, port, and datapath VLAN multicast entries. | GW |
| show datapath vlan-mcast table | Displays the datapath VLAN Multicast table entries. | GW |
| show datapath wan counters | Displays the datapath WAN health check counters or statistics. | GW |
| show datapath wan hc | Displays the datapath WAN health check statistics. By default, combined statistics of all CPUs is shown. | GW |
| show datapath wan hits | Displays the datapath WAN statistics. | GW |
| show datapath wan policy | Displays the datapath statistics for WAN policy. | GW |
| show datapath wan probestats | Displays the datapath statistics for WAN probestats. | GW |
| show datapath wan threshold | Displays the datapath statistics for WAN threshold. | GW |
| show datapath web-cc counters | Displays the web content classification table information. The output details are as follows: <ul style="list-style-type: none"> ■ Rep ■ ContentID ■ TTL ■ Age | GW |
| show dds debug peers | Displays the dds debug information for the peers. | GW |
| show dds debug stats | Displays the statistics of the DDS log. | GW |
| show debug | Displays the debug information for the debug logging levels. | GW |
| show derivation-rules | Displays the list of role and VLAN derivation rules configured for the WLAN SSIDs and wired profiles in an AP. Run this command to view the derivation rules configured for a network profile. | AP |
| show dhcp-allocation | Displays the information about the DHCP address allocation. Run this command to view DHCP address allocation for network address translated clients to allow mobility of the clients across APs. | AP |

| Command | Description | Applies To |
|---|---|------------|
| show dhcpc-opts | Displays the DHCP options configured on an AP. Run this command to view the current status of the vendor-specific DHCP options configured on an AP. | AP |
| show dot1x ap-table | Displays the 802.1X AP table. | GW |
| show dot1x counters | Displays the dot1x counters table. | GW |
| show dot1x machine-auth-cache | Displays the machine authentication cache information. | GW |
| show dot1x supplicant-info list-all | Displays the 802.1X supplicants. | GW |
| show dot1x supplicant-info statistics | Displays the 802.1X statistics of the users. | GW |
| show dot1x watermark history | Displays the historical sessions in the 802.1X session queue. This command must be run under the guidance of Aruba support to view information about the table that contains 802.1X sessions being processed. | GW |
| show dot1x watermark table active | Displays the current active sessions in the 802.1X queue and the corresponding user-age. | GW |
| show dot1x watermark table pending | Displays the pending sessions in the 802.1X queue, the duration for which the user is pending in the queue, and the corresponding user-age. | GW |
| show dpi debug status | Displays the DPI status that can be used for debugging. The ssid-table parameter shows the mapping of WLAN index and BSSID in the DPI process. | AP |
| show dpi-stats session | Displays the datapath session details for the DPI. | AP |
| show election statistics | Displays the election statistics of the master AP selected as Virtual Controller. | AP |
| show fault | Displays the list of active faults that occur in the event of a system fault and the faults that were cleared from the system. | AP |
| show fault history | Displays the list of faults that were cleared. | AP |
| Show firewall | Displays the list of global firewall policies and its details. | GW |
| Show firewall-cp | Displays the Control Path firewall policies on the controller. | GW |
| show firewall-cp internal | Displays the Control Path internal firewall policies on the controller. | GW |
| show firewall-visibility debug | Displays the process state information for debugging firewall visibility. | GW |
| show firewall-visibility status | Displays the status of firewall visibility as enabled or disabled. | GW |

| Command | Description | Applies To |
|---|---|------------|
| <u>show firewall-visibility-blk-session status</u> | Displays the policy enforcement firewall visibility process state and status information for bulk sessions. | GW |
| <u>show gap-debug</u> | Displays the troubleshooting information for the global AP database. | GW |
| <u>show gre config</u> | Displays the GRE configuration information for an AP. | AP |
| <u>show gre status</u> | Displays the various parameters indicating the status of GRE. | AP |
| <u>show gsm application all status</u> | Displays the status of the GSM application, for example, stm, auth, and so on. | GW |
| <u>show gsm debug channel all status</u> | Displays the status, event ring channel information, and trace events for channel and assignment related features like cluster, LLDP, tunneled nodes, UCC, and so on. | GW |
| <u>show gsm debug channel bucket_map</u> | Displays the STA Hash Bucket to UAC map for the channel. | GW |
| <u>show gsm debug channel cluster</u> | Displays the controller cluster information for the channel. | GW |
| <u>show gsm debug channel cluster_ddg</u> | Displays the controller cluster information for the channel. | GW |
| <u>show gsm debug channel cluster_device</u> | Displays the controller cluster information for the device. | GW |
| <u>show gsm debug channel cluster_tunneled_node</u> | Displays the controller cluster information for the tunneled node channel. | GW |
| <u>show gsm debug channel cluster_user</u> | Displays the controller cluster information for the cluster user channel. | GW |
| <u>show gsm debug channel dds_peer</u> | Displays the controller cluster information for the DDS peer. | GW |
| <u>show gsm debug channel device_info</u> | Displays the controller cluster information for the channel device. | GW |
| <u>show gsm debug channel tunneled_node</u> | Displays the controller information for the tunneled node channel. | GW |
| <u>show gsm debug channel tunneled_user</u> | Displays the controller information for the tunneled user channel. | GW |
| <u>show ha ap table</u> | Displays the HA AP table to view information about APs configured to use the HA feature. | GW |
| <u>show ha group-membership</u> | Displays the name of the HA group to which the managed device should be a member. | GW |
| <u>show ha group-profile</u> | Displays the list of HA groups. You can include the optional <profile> parameter to display configuration settings for the specific profile. | GW |

| Command | Description | Applies To |
|--|---|------------|
| <u>show ha heartbeat counters</u> | Displays the statistics for the HA extended managed device capacity feature. | GW |
| <u>show iap detailed-table</u> | Displays the details of all the branches terminating at the managed device. | GW |
| <u>show iap table long</u> | Displays the branches connected to the managed device in a detailed view. | GW |
| <u>show iap trusted-branch-db</u> | Displays the details of IAP trusted branch database information. | GW |
| <u>show idps stats</u> | Displays the IDPS statistics. | GW |
| <u>show idps summary</u> | Displays the IDPS summary. | GW |
| <u>show ids aps</u> | Displays the unknown APs detected by the AP. | AP |
| <u>show ids clients</u> | Displays the details of the AP to which the client is connected. | AP |
| <u>show image version</u> | Displays the current system image version on both partition 0 and 1. | AP, GW |
| <u>show inbound-firewall-rules</u> | Displays the details of inbound firewall rules configured on an AP. | AP |
| <u>show interface counters</u> | Displays the table of L2 interfaces counters. | AP, GW |
| <u>show interface loopback</u> | Displays the information about the loopback IP interface. | GW |
| <u>show interface mgmt</u> | Displays the information about management Ethernet IP interfaces. | GW |
| <u>show interface vhost counters</u> | Displays the table of L2 interfaces counters for the vhost. | GW |
| <u>show interface vlan 1</u> | Displays the information about a specified VLAN interface. | GW |
| <u>show inventory</u> | Displays the hardware inventory of Mobility Master or the managed device. | GW |
| <u>show iostat</u> | Displays the Input/Output statistics information. Run this command to view Central Processing Unit (CPU) statistics and Input/Output statistics for devices and partitions. | GW |
| <u>show ip access-list bri</u> | Displays the table with information about all the ACLs. | GW |
| <u>show ip bgp</u> | Displays the BGP statistics. | GW |
| <u>show ip bgp neighbors</u> | Displays the BGP statistics for neighbors. | GW |
| <u>show ip dhcp database</u> | Displays the DHCP server settings. | AP, GW |
| <u>show ip dhcp option-82</u> | Displays the DHCP server binding, database setting, relay, and pool statistics for the option-82 feature. | GW |

| Command | Description | Applies To |
|---|---|------------|
| show ip dhcp statistics | Displays the DHCP pool statistics. | GW |
| show ip health-check | Displays the health-check status of the uplink interfaces of a branch office managed device. This command must be executed from the branch office managed device. | GW |
| show ip igmp | Displays the IGMP timers and counters. | AP |
| show ip igmp config | Displays the current IGMP configuration. | GW |
| show ip igmp counters | Displays the list of counters for the following IGMP queries: <ul style="list-style-type: none"> ■ received-total ■ received-queries ■ received-v1-reports ■ received-v2-reports ■ received-leaves ■ received-unknown-types ■ len-errors ■ checksum-errors ■ not-vlan-dr ■ transmitted-queries ■ forwarded | GW |
| show ip igmp group | Displays the following IGMP group information: <ul style="list-style-type: none"> ■ mac– Specify MAC address of the specific member. ■ source– Specify the source address of the specific SSM group. | GW |
| show ip igmp interface | Displays the IGMP interface information. | GW |
| show ip igmp proxy-group | Displays the IGMP proxy group information for a specific interface. | GW |
| show ip igmp proxy-mobility-group | Displays the IGMP proxy group information stored for mobile clients that are away from the managed device. | GW |
| show ip igmp proxy-mobility-stats | Displays the most important messages exchanged between the mobility process and the IGMP proxy. | GW |
| show ip igmp proxy-stats | Displays the number of messages transmitted and received by the IGMP proxy on the upstream interface | GW |
| show ip interface brief | Displays the IP-related information on all interfaces in summary format. | AP, GW |
| show ip mobile active-domains | Displays the IP mobility domains active on the switch. | GW |
| show ip mobile binding | Displays the list of home agent bindings information for the mobile protocol. | GW |
| show ip mobile domain | Displays the subnet, VLAN, and home agent information for all mobility domains. You can specify a mobility domain name to view data only for that particular domain. | GW |

| Command | Description | Applies To |
|---|--|------------|
| show ip mobile global | Displays the current mobility agents global configuration. | GW |
| show ip mobile hat | Displays the active home agent table. | GW |
| show ip mobile host | Displays the list of mobile IP hosts. | GW |
| show ip mobile multicast-vlan-table | Displays the mobility multicast VLAN table information. | GW |
| show ip mobile traffic | Displays the mobile IP protocol statistics for the following: <ul style="list-style-type: none"> ■ Proxy Mobile IP ■ Home Agent Registrations ■ Foreign Agent Registrations ■ Registration Revocations | GW |
| show ip mobile tunnel | Displays the mobile tunnel table for IPIP tunnels. | GW |
| show ip mobile visitor | Displays the list of mobile nodes visiting a foreign agent. | GW |
| show ip nexthop-list | Displays the next hop list settings for policy-based routing. | GW |
| show ip oap | Displays the IP OAP tunnels information. | GW |
| show ip oap advertise | Displays the advertised IP OAP tunnels information. | GW |
| show ip oap advertise verbose | Displays the advertised IP OAP tunnels information that can be used for debugging. | GW |
| show ip oap hub-mesh nexthops | Displays the IP OAP hub-mesh tunnels next hop information. | GW |
| show ip oap hub-mesh nodes | Displays the IP OAP hub-mesh tunnels node information. | GW |
| show ip oap hub-mesh topology | Displays the IP OAP hub-mesh topology tunnels information. | GW |
| show ip oap route | Displays the IP OAP route information. | GW |
| show ip oap route all verbose | Displays the IP OAP route information that can be used for debugging. | GW |
| show ip oap tunnel | Displays the IP OAP tunnels information. | GW |
| show ip ospf | Displays the statistics and configuration information for the OSPF routing protocol. | GW |
| show ip ospf database | Displays the database information for the OSPF protocol. | GW |
| show ip ospf interface | Displays the status of OSPF on an individual interface by specifying a tunnel or VLAN ID number. | GW |
| show ip ospf neighbor | Displays the data for OSPF neighboring routers. | GW |
| show ip prefix-list | Displays the prefix list for policy-based routing. | GW |

| Command | Description | Applies To |
|--|--|------------|
| show ip probe | Displays the health-check profile settings for measuring WAN reachability and latency on a managed device uplink, and the default probe profile settings for PBR using next-hop lists. | |
| show ip radius source-interface | Displays the global parameters for configured RADIUS servers and the source interface address of outgoing RADIUS requests. | GW |
| show ip rip | Displays the statistics and configuration information for the protocol. | GW |
| show ip rip interfaces | Displays the statistics and configuration information for the interfaces. | GW |
| show ip rip neighbors | Displays the statistics and configuration information for the neighbors. | GW |
| show ip route | Displays the Mobility Master routing table with static routes configured using the ip route command. Use the ip default-gateway command to set the default gateway to the IP address of the interface on the upstream router or switch to which you connect the Mobility Master. | AP, GW |
| show ip route counters | Displays the number of routes present, categorized by type. | GW |
| show ipv6 dhcp database | Displays the DHCPv6 server settings. | GW |
| show ipv6 firewall | Displays the status of all the IPv6 firewall configurations. | GW |
| show ipv6 global | Displays the IPv6 global configuration information. | GW |
| show ipv6 interface | Displays the IPv6-related information on all the interfaces. | GW |
| show ipv6 mld config | Displays the Multicast Listener Discovery (MLD) configuration details. | GW |
| show ipv6 mld counters | Displays the statistics of the MLD. | GW |
| show ipv6 mld group | Displays the MLD group details. | GW |
| show ipv6 mld interface | Displays the MLD status on VLANs | GW |
| show ipv6 mld proxy-group | Displays the MLD proxy-group details. | GW |
| show ipv6 mld proxy-mobility-group | Displays the MLD proxy-mobility-group details. | GW |
| show ipv6 mld proxy-mobility-stats | Displays the details of MLD proxy-mobility statistics. | GW |
| show ipv6 mld proxy-stats | Displays the status of the MLD proxy. | GW |
| show ipv6 neighbors | Displays the neighbors configured for IPv6 on the VLAN interface. | GW |

| Command | Description | Applies To |
|---|--|------------|
| <u>show ipv6 ra proxy</u> | Displays the RA proxy server information and IPv6 RA. | GW |
| <u>show ipv6 ra status</u> | Displays the status of the IPv6 RA. | GW |
| <u>show ipv6 route</u> | Displays the IPv6 routing table details about the static IPv6 routes configured on the managed device. | GW |
| <u>show keys all</u> | Displays the if the keys and features are enabled or disabled on the Mobility Master. | GW |
| <u>show lacp status</u> | Displays the LACP configuration status on an AP. | AP |
| <u>show lc-cluster group-membership</u> | Displays the active cluster member of cluster profile. | GW |
| <u>show lc-cluster group-profile+</u> | Displays the cluster profile information. | GW |
| <u>show lc-cluster load distribution ap</u> | Displays the current load distribution on the AP. | GW |
| <u>show lc-cluster load distribution client</u> | Displays the current load distribution on the client. | GW |
| <u>show lc-cluster vlan probe status</u> | Displays the status of the cluster VLAN probe. | GW |
| <u>show license client-table</u> | Displays the license limits applied to the managed device from its licensing pool. | GW |
| <u>show license debug</u> | Displays the Mobility Master's licensing role and IP address summary. | GW |
| <u>show license heartbeat stats</u> | Displays the license heartbeat statistics between the centralized licensing server and the license client. | GW |
| <u>show license verbose</u> | Displays the license usage for the global configuration pool. You can specify a pool name to view license usage for the specific license pool. The verbose parameter displays aggregated license usage for each configuration node and managed devices in those nodes. | GW |
| <u>show lldp interface</u> | Displays the LLDP interfaces information. | GW |
| <u>show lldp neighbor</u> | Displays the information about LLDP peers. | GW |
| <u>show lldp statistics</u> | Displays the LLDP statistics information. By default, the entire list of LLDP interfaces is present. You can specify a slot/module/port number to view statistics specific to the interface. | GW |
| <u>show log all</u> | Displays the log files on Mobility Master or a managed device. | GW |
| <u>show log gap-debug</u> | Displays the controller's AP debug logs. | AP |
| <u>show log ap-debug all</u> | Displays all the AP debug logs for the controller. | GW |

| Command | Description | Applies To |
|--|--|------------|
| <u>show log apifmgr</u> | Displays the log information for an AP interface manager. | AP |
| <u>show log arm all</u> | Displays all the ARM debug logs for the controller. | GW |
| <u>show log arm-user-debug all</u> | Displays all the ARM user debug logs for the controller. | GW |
| <u>show log convert</u> | Displays the image conversion details for the AP. | AP |
| <u>show log debug</u> | Displays the AP full log. | AP |
| <u>show log driver</u> | Displays the status of drivers configured on the AP. | AP |
| <u>show log errorlog all</u> | Displays all the error logs for the controller. | GW |
| <u>show log kernel</u> | Displays the AP's kernel logs. | AP |
| <u>show log l3-mobility</u> | Displays the logs for Layer-3 mobility domains configured on an AP. | AP |
| <u>show log network</u> | Displays the controller's system network errors. | AP |
| <u>show log network all</u> | Displays all the network logs for the controller. | GW |
| <u>show log openflow</u> | Displays the OpenFlow logs of an AP. | AP |
| <u>show log pppd</u> | Displays the PPPd network connection details. | AP |
| <u>show log rapper</u> | Displays the details of VPN connection logs in detail. | AP |
| <u>show log sapd</u> | Displays the SAPd details. | AP |
| <u>show log security</u> | Displays the controller's security logs. | AP |
| <u>show log system</u> | Displays the controller's system logs. | AP |
| <u>show log system all</u> | Displays all the system logs for the controller. | GW |
| <u>show log upgrade</u> | Displays the image download from URL and upgrade details for both local image file and URL for the AP. | AP |
| <u>show log user</u> | Displays the controller's user logs. | AP |
| <u>show log user all</u> | Displays all the user logs for the controller. | GW |
| <u>show log user-debug</u> | Displays the controller's user debug logs. | AP |
| <u>show log user-debug all</u> | Displays all the user debug logs for the controller. | GW |
| <u>show log vpn-tunnel</u> | Displays the VPN tunnel status for the AP. | AP |
| <u>show log wireless</u> | Displays the controller's wireless logs. | AP |
| <u>show log wireless all</u> | Displays all the wireless logs for the controller. | GW |
| <u>show loginsessions</u> | Displays the current administrator login sessions statistics. | GW |

| Command | Description | Applies To |
|--|--|------------|
| show mac-address-table | Displays the MAC forwarding table. | GW |
| show master-local stats | Displays the statistics for communication between Mobility Master and managed devices. | GW |
| show memory | Displays the used and available memory on Mobility Master. | AP, GW |
| show memory debug | Displays the detailed information to debug the memory errors. | GW |
| show memory ecc | Displays the DRAM ecc counters. | GW |
| Show netstat stats | Displays the network statistics summary. | GW |
| show network | Displays the network configuration details for an AP. | AP |
| show ntp authentication-keys | Displays the information for Network Time Protocol (NTP) authentication key. | GW |
| show ntp debug | Displays the NTP logs of the AP. | AP |
| show ntp servers | Displays the information for NTP servers. | GW |
| show ntp status | Displays the status information for NTP server. | AP, GW |
| show ntp trusted-keys | Displays the list of trusted keys for the NTP server. | GW |
| show opendns support | Displays the information of OpenDNS and the status of the connection. | AP |
| show openflow capabilities | Displays the OpenFlow system capability information. | GW |
| show openflow clickstream-statistics | Displays the configuration information about an OpenFlow controller, flow list, packet capture, syslog, and click-stream statistics. | AP |
| show openflow controller | Displays the OpenFlow Controller configuration information. | AP, GW |
| show openflow controller detail | Displays the information about OpenFlow connection, TLS status, interface list, and OpenFlow ports to the OpenFlow Controller. | AP |
| show openflow debug ap-client state detail | Displays the debug information for the OpenFlow AP client status. | GW |
| show openflow debug event | Displays the the debug information for the OpenFlow AP events. | GW |
| show openflow debug flows | Displays the debug information for the OpenFlow AP flows. | GW |
| show openflow debug ports | Displays the debug information for the OpenFlow AP ports. | GW |
| show openflow flow-table | Displays the flow table information. | AP |
| show openflow ports | Displays all the ports configured for OpenFlow. | GW |

| Command | Description | Applies To |
|---|---|------------|
| show openflow statistics | Displays the OpenFlow statistics information. | GW |
| show openflow-profile | Displays the OpenFlow profile information configured on the managed device. | GW |
| show overlay bucketmap status | Displays the overlay cluster bucketmap, nodelist, and the associated wireless stations. | AP |
| show overlay cluster-info | Displays the overlay cluster with multizone details of overlay VLANs, tunnel MTU, Hearbeat status of the tunnels, and the associated number of wireless stations per UAC. | AP |
| show overlay multicast-vlan | Displays the overlay cluster profile names and the associated multicast VLAN IDs. | AP |
| show overlay ssid-cluster status | Displays the overlay SSIDs configured in an AP with its associated primary and backup Cluster details. | AP |
| show overlay tunnel config | Displays the overlay tunnels in an AP with cluster UAC IPs, tunnel type, MTU, overlay VLANs, and the Heartbeat status of the overlay tunnel. | AP |
| show papi kernel-socket-stats | Displays the the state of UDP PAPI sockets in the kernel. | GW |
| show perf-test reports controller | Displays the results of an Iperf throughput test launched from a controller. This command must be run under the guidance of Aruba technical support. | GW |
| show perf-test reports controller format-json | Displays the results of an Iperf throughput test launched from a controller in JSON format. This command must be run under the guidance of Aruba technical support. | GW |
| show port link-event | Displays the link status on each of the port on the controller. | GW |
| show port stats | Displays the activity statistics on each of the port on the controller. | GW |
| show port status | Displays the status of all ports on the controller. | AP, GW |
| show pppoe debug-logs | Displays the PPPoE debug logs and uplink status. | AP |
| show pppoe status | Displays the uplink status. | AP |
| show process | Displays the list of processes running on an AP. You can use it for debugging. | AP |
| show process monitor statistics | Displays the current status of the processes running under the process monitor watchdog. | GW |
| show processes | Displays the list of all system process running on the managed device. | GW |
| show profile-errors | Displays the list of invalid user-created profiles. | GW |

| Command | Description | Applies To |
|---|---|------------|
| show radio config | Displays the 2.4 GHz and 5 GHz radio configuration details for an AP. | AP |
| show radius status | Displays the status of TLS tunnel between the AP and RadSec proxy. | AP |
| show radius-attributes | Displays the RADIUS server attributes for an AP. | AP |
| show radius-servers support | Displays the RADIUS server configuration details for an AP. | AP |
| show rights+ | Displays the list of user roles in the roles table with high level details of role policies. | GW |
| show roleinfo | Displays the role of the controller. | GW |
| show route-map | Displays the route information. | GW |
| show running-config | Displays the current Mobility Master configuration inclusive of all the pending changes that are yet to be saved. | AP |
| show slots | Displays the list of slots in the managed device, including the status and card type. | GW |
| show snmp inform stats | Displays the length of SNMP inform queue. | GW |
| show snmp-configuration | Displays the SNMP configuration details for a Virtual Controller. | AP |
| show socket | Displays the active internet connections. | AP |
| show spanning-tree | Displays the RSTP and PVST+ configuration. | GW |
| show spantree | Displays the global RSTP and PVST+ topology. | GW |
| show speed-test data | Displays the details obtained from the Virtual Controller speed-test client. | AP |
| show station-table | Displays the internal station table entries and also details of a station table entry. | GW |
| show stats global | Displays the global statistics for an Instant AP cluster and the Instant APs and clients connected to it. | AP |
| show storage | Displays the storage information on the controller. | GW |
| show summary support | Displays the summary support containing the configuration details used by support. | AP |
| show swarm state | Displays the current status of the Instant AP cluster. | AP |
| show switches | Displays the details of managed device connected to the Mobility Master, including the Mobility Master itself. | GW |
| show switches debug | Displays the details of managed switches. | GW |

| Command | Description | Applies To |
|---|--|------------|
| show switches regulatory | Displays the information about the currently active regulatory file. | GW |
| show syslocation | Displays the location details of the controller. | GW |
| show tech-support | Displays the information about the controller that is required for the technical support purpose. | AP, GW |
| show threshold-limits controlpath-memory | Displays the default memory threshold, the current configured threshold, the total memory (in MB), and the currently available memory (in MB). If default threshold is exceeded, an alert is triggered. | GW |
| show threshold-limits no-of-aps | Displays the following values: <ul style="list-style-type: none"> ■ The default threshold for the number of APs, which, when exceeded, will trigger an alert. ■ The current configured threshold. ■ The maximum number of APs supported by the managed device. ■ The number of available licenses for campus and remote APs. ■ The total number of APs, and the current number of campus, remote and virtual APs. | GW |
| show threshold-limits no-of-locals | Displays the default threshold for the number of managed devices and the current configured threshold. If default threshold is exceeded, an alert is triggered. | GW |
| show threshold-limits total-tunnel-capacity | Displays the default tunnel capacity threshold and the current configured tunnel threshold. The output also includes the maximum number of tunnels supported by the managed device, as well as the number of tunnels currently used by the managed device. If default threshold is exceeded, an alert is triggered. | GW |
| show threshold-limits user-capacity | Displays the default user capacity threshold as well as the current configured user threshold. The output also includes the maximum number of users supported by the managed device, as well as the number of users currently associated with the managed device. If default threshold is exceeded, an alert is triggered. | GW |
| show tpm cert-info | Displays the TPM and factory certificate information. | GW |
| show tpm errorlog | Displays the TPM and error log. | GW |
| show trunk | Displays the list of trunk ports on the controller. | GW |
| show tunneled-node config | Displays the wired tunneled node configuration details. | GW |
| show tunneled-node database | Displays the tunneled nodes in the database. | GW |
| show tunneled-node state | Displays the state of the tunneled node. | GW |
| show tunneled-node-mgr cluster-bucket-map | Displays the tunneled node configuration details and cluster bucket map details. | GW |

| Command | Description | Applies To |
|---|--|------------|
| <u>show tunneled-node-mgr cluster-node-list verbose</u> | Displays the cluster node list information. | GW |
| <u>show tunneled-node-mgr gsm-counters</u> | Displays the GSM counters details. | GW |
| <u>show tunneled-node-mgr mcast-tunnel-table</u> | Displays the information about multicast tunnel. | GW |
| <u>show tunneled-node-mgr mcast-vlan-user-map</u> | Displays the information about the user count on each multicast tunnel VLAN pair. | GW |
| <u>show tunneled-node-mgr node-heartbeat-table</u> | Displays the node heartbeat table-related information. | GW |
| <u>show tunneled-node-mgr stats</u> | Displays the tunneled node manager statistics. | GW |
| <u>show tunneled-node-mgr trace-buf</u> | Displays the contents of trace buffer. | GW |
| <u>show tunneled-node-mgr tunneled-nodes</u> | Displays the information about manager tunneled nodes. | GW |
| <u>show tunneled-node-mgr tunneled-users</u> | Displays the information about tunneled users. | GW |
| <u>show tunneled-node-mgr tunnel-vlan-user-map</u> | Displays the information about the user count on each multicast tunnel VLAN pair. | GW |
| <u>show tunneled-node-mgr user-tunnel-table</u> | Displays the information about user tunnel tables. | GW |
| <u>show tunnelmgr counters</u> | Displays the tunnel counters details. | GW |
| <u>show tunnelmgr tunnel-list</u> | Displays the tunnel list details. | GW |
| <u>show ucc call-info cdrs</u> | Displays the Call Detailed Records (CDR) statistics for Unified Communication and Collaboration (UCC). | GW |
| <u>show ucc call-info cdrs detail</u> | Displays the detailed CDR statistics. | GW |
| <u>show ucc client-info</u> | Displays the UCC client status and CDR statistics. | GW |
| <u>show ucc statistics counter cac</u> | Displays the UCC call statistics. | GW |
| <u>show ucc statistics counter call client</u> | Displays the per client call statistics counter. | GW |
| <u>show ucc statistics counter call global</u> | Displays the system-wide call statistics counter. | GW |
| <u>show uplink</u> | Displays the uplink manager configuration details. | GW |
| <u>show uplink cellular config</u> | Displays the uplink manager, the default wired priority and default cellular priority. | GW |

| Command | Description | Applies To |
|---|--|------------|
| <u>show uplink cellular connection-logs</u> | Displays the connection details. | GW |
| <u>show uplink cellular details</u> | Displays the uplink manager details. | GW |
| <u>show uplink cellular signal</u> | Displays the statistical information on the designated uplink. | GW |
| <u>show uplink config</u> | Displays the uplink manager, the default wired priority and default cellular priority. | AP, GW |
| <u>show uplink connection logs all</u> | Displays the connection details. | GW |
| <u>show uplink debug</u> | Displays the uplink details. | GW |
| <u>show uplink load-balance</u> | Displays the uplink details of load balance. | GW |
| <u>show uplink signal</u> | Displays the cellular uplink signal strength. | GW |
| <u>show uplink stats</u> | Displays the statistical information on the designated uplink. | GW |
| <u>show uplink stats all</u> | Displays all the statistical information on the designated uplink. | GW |
| <u>show uplink status</u> | Displays the uplink manager status. | AP |
| <u>show usb</u> | Displays the detailed USB device information on a stand-alone controller or managed device. | GW |
| <u>show user+</u> | Displays the detailed information about user in terms of AP group, authentication method, role and so on. | GW |
| <u>show users</u> | Displays the users configured for an Instant AP. | AP |
| <u>show user-table</u> | Displays the detailed information about the controller's connection to a user device, in regards to mobility state and statistics, authentication statistics, VLAN assignment method, AP datapath tunnel info, radius accounting statistics, user name, user-role derivation method, datapath session flow entries, and 802.11 association state and statistics. | GW |
| <u>show user-table verbose</u> | Displays the information about the user table. | GW |
| <u>show valid-channels</u> | Displays the list of channels that are valid for an Instant AP serving a specific regulatory domain. | AP |
| <u>show version</u> | Displays the system software version. | AP, GW |
| <u>show vlan</u> | Displays the configured VLAN interface number, description and associated ports. Issue this command to show the selected VLAN configuration. | GW |
| <u>show vlan mapping</u> | Displays the configured VLAN name, its pool status, assignment type, and the VLAN IDs assigned to the pool. | GW |


| Command | Description | Applies To |
|--|--|------------|
| show vlan status | Displays the current status of all VLANs on the controller. | GW |
| show vlan-assignment | Displays the number of clients assigned to a VLAN. Issue this command to show the number of clients that are assigned to a VLAN. | GW |
| show vpdn l2tp configuration | Displays the VPN L2TP tunnel configuration. | GW |
| show vpdn l2tp local pool | Displays the VPN L2TP tunnel local pool details. | GW |
| show vpdn pptp configuration | Displays the PPTP configuration on the controller. | GW |
| show vpdn pptp local pool | Displays the IP address pool for VPN users using Point-to-Point Tunneling Protocol. | GW |
| show vpdn tunnel l2tp | Displays the VPN L2TP tunnel details. | GW |
| show vpn status | Displays the status of the VPN connections enabled on an Instant AP. | AP |
| show vpn-dialer | Displays the VPN dialer configuration for users using VPN dialers. | GW |
| show vrrp | Displays the list of all VRRP configuration on the managed device. To view a specific VRRP configuration, specify the VRID number. | GW |
| show vrrp ipv6 | Display VRRP information for IPv6 address. | GW |
| show vrrp ipv6 stats all | Displays the operational statistics of the VRRP. | GW |
| show vrrp stats all | Displays the statistics of the VRRP. | GW |
| show web-cc md stats | Displays the statistics for the specified web-cc category bandwidth contract. | GW |
| show web-cc stats | Display counters for web content traffic and web content classification table statistics | GW |
| show web-cc status | Display information about the current operational status of the web content classification feature. | GW |
| show whitelist-db cpsec | Displays the campus AP whitelist for campus APs using the control plane security feature. | GW |
| show whitelist-db cpsec-local-switch-list | Displays the list of managed devices with APs using the control plane security feature. | GW |
| show whitelist-db cpsec-master-switch-list | Displays the master switch list whitelist on managed devices with APs using the control plane security feature. | GW |
| show whitelist-db cpsec-seq | Displays the current sequence number for the Mobility Master or managed device whitelists. | GW |
| show whitelist-db cpsec-status | Displays the aggregate status information APs in the campus AP whitelist. | GW |

| Command | Description | Applies To |
|---|---|------------|
| <u>show whitelist-db rap</u> | Displays the detailed information for the remote AP whitelist database. | GW |
| <u>show whitelist-db rap long</u> | Displays the additional debugging information about an entry in the RAP whitelist, including when it was last updated, the sequence number for the update, and any flags for the entry. | GW |
| <u>show whitelist-db rap-local-switch-list</u> | Displays the remote AP whitelist local switch list on Mobility Master. | GW |
| <u>show whitelist-db rap-master-switch-list</u> | Displays the remote AP whitelist master switch list on managed devices with remote APs. | GW |
| <u>show whitelist-db rap-status</u> | Displays the aggregate status information APs in the remote AP whitelist. | GW |
| <u>show wired-port-settings</u> | Displays the list of wired profiles configured on an Instant AP. | AP |
| <u>show wispr config</u> | Displays the WISPr authentication parameters configured on an Instant AP. | AP |


Here is a list of FAQs on how to accomplish some common tasks in AOS 10.x.

Navigation


How do I view the details of an AP?

1. In the **Network Operations** app, use the filter bar to select a group or device.
2. Under **Manage**, click **Device(s)** > **Access Points** to view the AP dashboard.
3. Click the list icon  to display the AP list dashboard.
4. Click on any AP name under **Device Name** to view the access points details page.


How do I configure an AP?

1. In the **Network Operations** app, use the filter bar to select a group or device.
2. Under **Manage**, click **Device(s)** > **Access Points** to view the AP dashboard.
3. Click the settings icon  to display the AP configuration dashboard.
4. To edit an AP, click the edit icon for that AP.

How do I view the details of a Gateway?

1. In the **Network Operations** app, use the filter bar to select a Gateway or Aruba Gateway group.
2. Under **Manage**, click **Devices** > **Gateways**.
3. Click the list  icon to display the Gateway configuration dashboard.
4. Click any Gateway name under **Device Name** to view the Gateway details page.

How do I configure a Gateway?

1. In the **Network Operations** app, use the filter bar to select a Gateway or Aruba Gateway group.
2. Under **Manage**, click **Devices** > **Gateways**.
3. Click the settings  icon to display the Gateway configuration page.

How do I access the global dashboard?

To access the Global dashboard, perform the following steps:

1. In the **Network Operations** app, set the filter to **All Devices**.

The global dashboard is displayed.

How do I view the overall network summary?

To view the overall network summary, perform the following steps:

1. In the **Network Operations** app, set the filter to **All Devices**.

The global dashboard is displayed.

2. Under **Manage**, click **Overview** to view the Summary dashboard.

How do I view AI Insights?

To view AI Insights, perform the following steps:

1. In the **Network Operations** app, set the filter to **All Devices**.

The global dashboard is displayed.

2. Under **Manage**, click **Overview** > **AI Insights** to view the dashboard.

How do I view network health?

To view network health, perform the following steps:

1. In the **Network Operations** app, use the filter bar to select a group or device.

2. Under **Manage**, click **Device(s)** > **Network Health** to view the dashboard

How do I access the VisualRF dashboard?

To view the VisualRF dashboard, perform the following steps:

1. In the **Network Operations** app, set the filter to **All Devices**.

The global dashboard is displayed.

2. Under **Manage**, click **Overview** > **VisualRF** to view the dashboard.

How do I view client details?

1. In the **Network Operations** app, use the filter to set the group to **All Devices**.

2. Under **Manage**, click **Clients**.

The clients overview page is displayed.

3. Click the list icon  to view the client table.

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** or **Wired** to filter the clients and enter the client name in the **Client Name** column and then click the client name. The **Client Summary** page is displayed.

How do I create a group?

1. In the **Network Operations** app, filter **All Devices**.
2. Under **Maintain**, click **Organization**.
By default, the **Groups** page is displayed.
3. Click (+) **New Group**.
The **Create New Group** pop-up window is displayed.
4. Enter a name for the group.



By default, Aruba Central enables template-based configuration method for switches and UI-workflow-based configuration method for AP.

5. To enable UI-based configuration method on all device categories:
 - a. For APs, ensure that the **IAP and Gateway** checkbox is cleared.
 - b. For switches, clear the **Switch** checkbox.
6. Assign a password. This password enables administrative access to the device interface.
7. Click **Add Group**.

How do I create a template group?

1. In the **Network Operations** app, filter **All Devices**.
2. Under **Maintain**, click **Organization**.
By default, the **Groups** page is displayed.
3. Click (+) **New Group**.
The **Create New Group** pop-up window opens.
4. Enter the name of the group.
5. Select the device type for which you want to create a template group:
 - IAP and Gateway
 - Switch
6. Enter the password.
7. Click **Save**.



If the group is set as a template group, a configuration template is required for managing device configuration.

How do I view the Visibility dashboard?

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. To view the graphs on the **Visibility** pane, ensure that the **Application Visibility** service is enabled.

To view the **Visibility** dashboard, perform the following steps:

1. In the **Network Operations** app, set the filter to **Global**.

2. Under **Manage**, click **Applications** to view the **Visibility** dashboard.

Network Profile

What is an SSID?

An SSID is the primary name associated with an 802.11 wireless local area network (WLAN). Client devices use this name to identify and join wireless networks.

What are the deployment modes supported?

AOS 10.x supports the following modes of deployment:

- Bridge
- Tunnel
- Mixed
- Micro Branch

What is a Bridge mode deployment ?

In Bridge mode, standalone APs are connected to a switch backbone that is in-turn connected to the Aruba Cloud platform for management and configuration services. When AOS 10.x is deployed in Bridge mode, the network created acts as a physical network. All wireless traffic is terminated locally at the AP and Bridged onto the local Ethernet segment. Saturation issues in the network can be largely avoided if much of the traffic remain local.

What is a Tunnel mode deployment?

The AOS 10.x in Tunnel mode consists of at least one gateway cluster for security and network resiliency. The network created on Tunnel mode acts as a virtual network on top of the physical network that is created on Bridge mode. In the Tunnel mode, VLANs are configured on a gateway cluster and APs tunnel traffic to Gateways. APs function as authenticators and send authentication and accounting requests to the gateway cluster.

What is a Mixed mode deployment?

In the Mixed mode deployment, VLANs are configured either on the gateway cluster or on APs. Traffic is either local or tunneled through a gateway cluster depending based on the optimum traffic route.

How do I create an SSID profile?

To configure WLAN settings, complete the following steps:

3. In the **Network Operations** app, use the filter bar to select a group or a device containing at least one AP.
4. Under **Manage**, click **Devices** > **Access Points**.
5. Click the settings icon to display the AP configuration page.
6. Click **WLANS**.
7. To create a new SSID profile, click **+ Add SSID**. The **Create a New Network** pane is displayed.

How is user authentication performed ?

In a Bridge mode, authentication is performed at the AP level. In a Tunnel mode or Mixed Mode, authentication is performed at the gateway cluster level.

What is the basic requirement to set up Bridge mode?


To set up a Bridge mode in AOS 10.x, the hardware infrastructure must include at least one AP that runs ArubaOS 10.0.0.0 version or later.

What is the basic requirement to set up Tunnel and Mixed mode?

To set up a Tunnel and Mixed mode in AOS 10.x, the hardware infrastructure must include at least one AP and one Gateway that runs ArubaOS 10.0.0.0 version or later.

How do I view the configurations of an already existing network profile?

To view the configurations of an already created network profile, perform the following:

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:
 - c. Under **Manage**, click **Devices > Access Points**.
 - d. Click the Configuration  icon to display the AP configuration page.
3. If you select the device, click **Device** under **Manage**.
4. In the **WLANS** tab,
The **WLANS** page lists the SSIDs created in Bridge, Tunnel, and Mixed mode.
5. Click the SSID for which the configuration summary is required to be displayed.
The Network Summary section appears below the table listing the configurations specific to AP.

What is a Gateway cluster?

A Gateway cluster is a combination of multiple Aruba Gateways operating as a single entity to provide high availability and service continuity to the WLAN clients in a network. Gateway clusters provide full redundancy to APs and WLAN clients in the event of a failover.

What are the types of clusters supported for Gateways?

Following are the two types of Gateway clusters:

- **Homogeneous cluster:** It is a cluster built with all nodes of the same platform type, and consists of the same Aruba Gateway models.
- **Heterogeneous cluster:** It allows you to combine different models of Gateways.


What are the Gateway cluster configuration methods supported in the AOS 10.x?

Aruba Central supports the following Gateway cluster configuration modes:

- Automatic cluster configuration
- Manual cluster configuration

How do I monitor the Gateway clusters?

To monitor Gateway clusters:

1. In the **Network Operations** app, use the filter bar to select a Gateway or Aruba Gateway group.
2. Under **Manage**, click **Devices > Gateways**.
3. Click the list  icon to display the Gateway configuration dashboard.
4. Click **Clusters** to view the cluster details.

What is Dynamic Segmentation?

Dynamic Segmentation is Aruba's security architecture that simplifies and secures the network by unifying policy enforcement across wired and wireless networks. It dynamically assign roles to a wired port based on the access method of a client and enforce application-aware policies to all devices connecting to the infrastructure.

What is User-Based Tunneling ?


User-Based Tunneling (UBT) is a type of tunneling that allows you to redirect specific wired users traffic from the switches to the Gateway to enforce DPI and firewall functionality, application visibility, and bandwidth control offered by Aruba Gateway.

What is Tunnel Orchestrator for LAN Tunnels

The Tunnel Orchestrator for LAN Tunnels service automates routing between AP and the Gateway cluster provisioned in an Aruba Central account. The Tunnel Orchestrator for LAN Tunnels service also computes the cost for route between multiple data centers, so that different data centers preference can be applied for the devices in a branch.

How to enable automatic Gateway cluster configuration ?

To enable automatic Gateway cluster configuration:

1. In the **Network Operations** app, use the filter bar to select a Gateway or Aruba Gateway group.
2. Under **Manage**, click **Devices > Gateways**.
3. Click the settings  icon to display the Gateway configuration page.
4. Click **High Availability**, and then click the **Clusters** tab.
5. Disable **Manual cluster configuration**.
6. Click **Save Settings**.

What is a Micro Branch Deployment ?

AOS 10.x supports deployment of APs in remote sites such as home offices, small branch offices, retail locations, and so on. The AOS 10.x enables the AP to form an IPsec tunnel to the Gateway cluster of the parent WLAN campus. For the network administrator, configuring and managing the remote AP can be done from the same Aruba portal that manages the parent WLAN campus network. For the user at such remote sites, connecting to the WLAN campus network is a seamless experience.

How many APs can you deploy in a Micro Branch deployment?


AOS 10.x currently supports deployment of a single AP as a Micro Branch AP in remote sites.

What are the traffic forwarding modes currently supported for Micro Branch deployments?

The DHCP traffic in Micro Branch deployments is tunneled through three different modes—Centralized Layer-2 full tunnel, Centralized Layer-2 split-tunnel, or Local (NAT Layer-3).

How do I enable the Micro Branch setting on an AP group?

To enable Micro Branch on the AP group:

1. In the **Network Operations** app, select the group with the micro Branch APs from the filter bar.
2. Under **Manage**, click **Device(s) > Access Points**.
3. Click the **Settings** () icon.
4. Under the **Security** tab, expand the **Microbranch** drop-down.
5. Toggle **Enable Microbranch** to **enabled** on the slider menu.
6. After enabling the Micro Branch setting on the AP group, you must configure the Inner IP Pool on the group. The AP group then forms an IPsec tunnel with the Inner IP configured. Under **AP Inner IP Pool**, enter the **Start Address** and **End Address** of the Inner IP Pool. The IP address range for the inner IP pool is 0 to 645160.
7. Click **Save Settings**
8. Verify the status of the Micro Branch and Inner IP configuration before you reboot the AP by using the **show running-config** command.
9. Manually reboot each AP in the Micro Branch group for the Micro Branch configurations to take effect:
 - a. Go to **Access Point Details > Actions**.
 - b. Select **Reboot AP** from the drop-down menu.



At a later point in time, if you choose to add new APs to an existing Micro Branch group, ensure that you reboot each new AP manually as shown in Step 8 for the above configurations to take effect.

How do I verify the Micro Branch configuration on an AP?

After you have enabled the Micro Branch setting and assigned an Inner IP pool on the AP group, run the **show running-config** command to view the status of the Micro Branch configuration and the Inner IP address assigned to the AP.

Security

What is a Rogue AP?

A rogue AP is an unauthorized access point plugged into the wired side of the network that can potentially disrupt network operations.

What is Security?

Security is designed to identify, classify and locate wireless threats by leveraging all the available information from the infrastructure. Security takes the information it collects and feeds it through a customizable set of classification rules, isolating the threat devices based on your security concerns. Security can be configured to alert administrators via email, SNMP traps or syslog messages after a threat is identified.

How does Security determine classification?

Security consists of certain set of customizable rules that give users control over how rogues are identified. These rules work similarly to firewall rules.

- If the first one is a match, use it. If not, go on to the next one.
- Order of these rules are very important.

How do I locate a rogue device to remove it from my network?

The VisualRF app automatically calculates the device location on the Rogues details page. Security indicates which switch ports have seen the rogue MAC Address and if switch ports are being polled. With that information, you can determine the edge switch and port and can trace the wire and find the device.

What is VisualRF?

VisualRF is a tool for monitoring and managing radio frequency (RF) dynamics within your wireless networks. It helps in real time location of users, rogues and interferer. Physically inspect the area where VisualRF has placed the rogues or where you estimate it to be.

What user role is needed to view the Rogue APs and interfering devices?

Users must have an admin role to view all the rogue APs and interfering devices.

What are the available classification for Rogue APs?

- Valid APs
- Rogue AP
- Suspected Rogue AP
- Interfering AP

How can we generate alerts and reports for Security?

After a rogue device meets the conditions/ classifications the trigger send an alert for the customer to identify rogues detected.

Tools

What type of troubleshooting can be performed under Tools?

The **Tools** page offers the following types of troubleshooting categories:

- **Network Check**—Network check aims to identify, diagnose, and debug issues detected in a managed network. It allows you to run commands like Ping and Traceroute from any network devices such as access points, controllersgateways, and switches.
- **Device Check**—Device check aims to identify, diagnose, and debug issues on your device. It slows you to run diagnostic check like Cable Test and Interface/PoE Bouce designed specifically for switches.
- **Commands**—Commands aim to identify, diagnose, and debug issues on your device at an advanced level using CLI commands. You can run these commands on all managed devices and export the output in a required format.




What user role is needed to perform troubleshooting?

Users must have an admin role or custom role to perform network check and device check. Advance check can be performed by a read-only user as well.

Alerts and Events

What does the Alert & Events pane displays?

The **Alerts & Events** pane displays all types of alerts and events generated for events pertaining to device provisioning, configuration, and user management. Click the list view to see a detailed graph pertaining to each device type.

- Summary View  —Allows you to view a detailed graph pertaining to each device type.
- List View  —Allows you to view the list of total alerts and events generated. You can also filter the alerts based on the severity level by clicking the severity level tabs.
- Configuration View  —Allows you to configure different types of alerts.

What are the alert severity levels displayed?

- Critical
- Major
- Minor
- Warning

What does Acknowledged Alerts mean?

Acknowledged alert means that the admin has acknowledged or worked on a specific alert raised against an event. It means that the admin is now ready to start alerting on that event again.

What does the WIDS Events table displays?

Navigate to **Analyze > Alerts & Events > Events** tab to view the total number WIDS events generated. The Wireless Intrusion Detection System (WIDS) monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools. The WIDS Events table displays the total number of wireless

attacks detected on an AP and client devices for a given duration.


AirMatch

What is RF optimization?

RF Optimization is the process of improving the operation of the RF Network for better utilization available infrastructure and network resources to provide customers the best possible quality of service and experience.

How do I optimize the radio frequencies?

To enable RF optimization on APs, complete the following procedure:

1. In the **Network Operations** app, use the filter to select **All Devices**.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the settings  icon.
The **Radios** page is displayed.
4. To enable RF optimization, turn on the **Activate Optimization** toggle switch.
5. Under **Wireless Coverage Tuning**, set one of the following wireless coverage tuning options:
 - a. **Unreactive**—Takes no or very few corrective actions for channel and power adjustments. Allows algorithm to prioritize preserving network settings over optimal RF health.
 - b. **Adaptive**—Allows Aruba Unified Network Architecture to dynamically adjust radio channels and power while keeping a balance between preserving network settings, and finding optimal RF settings. This is the recommended option.
 - c. **Aggressive**—Allows Aruba Unified Network Architecture to prioritize change of radio channels and power, over preserving network settings.



When you apply the RF optimization changes to a live network, it may impact the clients that are currently connected to the network. Therefore, Aruba recommends that you exercise caution when applying RF optimization on all APs in the network.

6. Click **Save**.

How do I monitor my Access Points using the Radio Monitoring Dashboard?

You can monitor your Access Points by using the **Radios** tab in the AP monitoring dashboard. This page displays information on the radios that are currently in operational mode. For more information, see [Monitoring Radios in Summary View](#).

List the uses of Radio Resource Management.



The following are some of the advantages of this feature:

- Clean slate RF optimization service
- Long term network stability and performance
- Holistic view of network
- Different modes of data collection and calculation


- Daily optimization
- Reactive optimization

Applications

How do I enable AirGroup?

1. In the **Network Operations** app, use the filter to select all devices, a group, or a device.
2. Under **Manage**, click **Applications > AirGroup**
3. Click the  icon.
4. On the desired AirGroup service, click  under **Action**.
5. To enable the desired AirGroup service, move the slider to the right.

How do I enable call prioritization?

1. In the **Network Management** app, use the filter bar to select all devices.
2. Under **Manage**, click **Applications > UCC**.
3. Click the  icon.
4. To enable call prioritization, move the slider to the right.

Clients

How do I view wireless clients in my 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 **Client Summary** page is displayed.

How do I live monitor clients?

Navigate to a wireless client and click **Go Live** to start live monitoring of the client. At any point, you can click **Stop Live** to go back to the historical view.

How do I disconnect a wireless client from an AP?

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 wireless client gets disconnected from the AP.

How can I troubleshoot a client in real time?

Aruba Central allows you to troubleshoot issues related to a client or a site in real time for detailed analysis. To troubleshoot a client at a site level:

1. In the **Network Operations** app, use the filter bar to select a site.
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 client:

1. In the **Network Operations** app, use the filter bar to select a group, a label, a site 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 **Client Summary** page is displayed.
6. Under **Analyze**, click **Live Events**. The **Live Events** page is displayed.
7. Enter the MAC address of the client and click **Start Troubleshooting**.

Live troubleshooting starts and 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.