Aruba Central

a Hewlett Packard
Enterprise company

User Guide

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

This user guide describes the features supported by Aruba Central and provides detailed instructions to set up and configure devices such as Instant APs, Aruba Switches, and Aruba SD-WAN Gateways.

Intended Audience

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

Related Documents

In addition to this document, the Aruba Central product documentation includes the following documents:

- *Aruba Central Help Center*
- *Aruba Central Getting Started Guide*
- *Aruba Central Managed Service Provider User Guide*
- *Aruba Central SD Branch Solution Guide*

Conventions

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

Table 1: *Typographical Conventions*

Type Style	Description
Italics	This style is used to emphasize important terms and to mark the titles of books.
`System items`	This fixed-width font depicts the following: ■ Sample screen output ■ System prompts

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	support.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	hpe.com/networking/support
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

Aruba Central provides a cloud platform for managing your networks from anywhere. Using Aruba Central, you can provision, configure, monitor, manage, and troubleshoot devices such as Aruba WLAN Instant APs and Switches in your network.

For more information on Aruba Central, see the following topics:

- Key Features on page 25
- Supported Devices on page 27

Key Features

Aruba Central offers the following key features and benefits:

- Streamlined configuration and deployment of devices— Leverages the ZTP capability of Aruba devices to bring up your network in no time. Aruba Central supports group configuration of devices, which allows you to provision and manage multiple devices with similar configuration requirements with less administrative overhead.
- Integrated wired, WAN, and wireless Infrastructure management— Offers a centralized management interface for managing wireless, WAN, and wired networks in distributed environments, and thus help organizations save time and improve efficiency.
- Secure cloud based platform—Offers a secure cloud platform with HTTPS connection and certificate based authentication.
- Interface for Managed Service Providers—Offers an additional interface for MSPs to provision and manage their respective tenant accounts. Using the MSP mode, service provider organizations can administer network infrastructure for multiple organizations in a single interface.
- SD Branch Management—Offers a simplified solution for managing and monitoring SD Branch devices such as Branch Gateways, VPN Concentrators, Instant APs, and Aruba Switches. It also provides detailed dashboards showing WAN health and pictorial depictions of the branch setup.
- Health and usage monitoring—Provides a comprehensive view of your network, device status and health, and application usage. You can monitor, identify, and address issues by using data-driven dashboards, alerts, reports, and troubleshooting workflows. Aruba Central also utilizes the DPI feature of the devices to monitor, analyze and block traffic based on application categories, application type, web categories and website reputation. Using this data, you can prioritize business critical applications, limit the use of inappropriate content, and enforce access policies on a per user, device or location basis.
- Guest Access—Allows you to manage access for your visitors with a secure guest Wi-Fi experience. You can create guest sponsor roles and social logins for your guest networks. You can also design your guest landing page with custom logos, color, and banner text.
- Presence Analytics—Offers a value added service for Instant AP based networks to get an insight into user presence and loyalty. The Presence Analytics dashboard allows you to view the presence of users at a specific site and the frequency of user visits at a given location or site. Using this data, you can make business decisions to improve customer engagement.
- Analytics for Client Service Assurance—Provides a value added service called Clarity that helps you analyze and monitor client onboarding and connectivity health. Using this data, you can proactively address issues pertaining to client connectivity and enhance user experience.

Operational Modes and Interfaces

Aruba offers the following variants of the Aruba Central web interface:

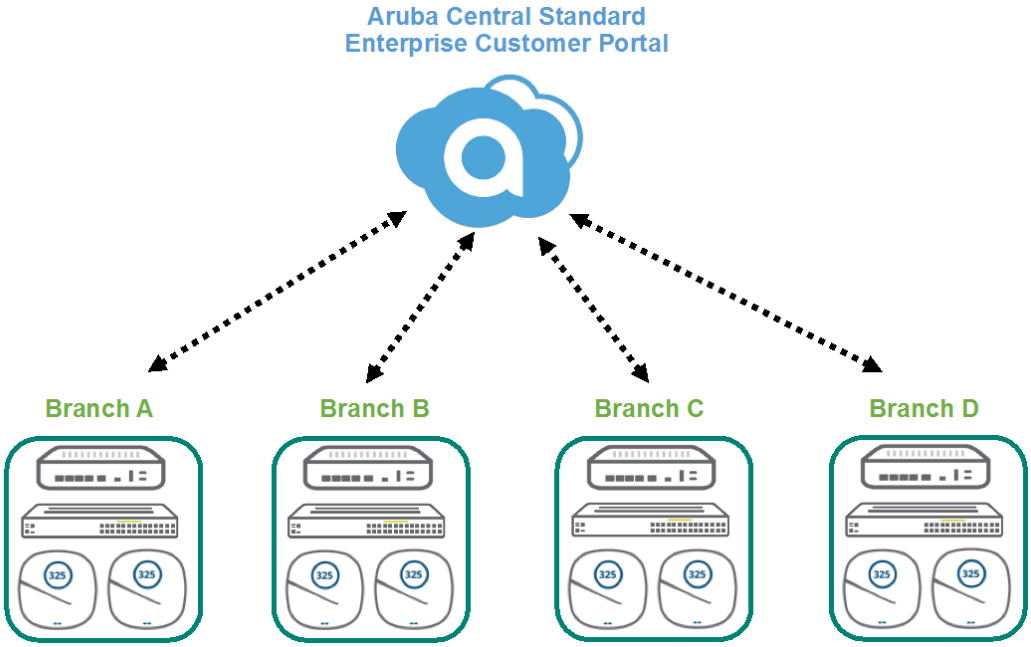
- Standard Enterprise Mode
- Managed Service Provider Mode

Standard Enterprise Mode

The Standard Enterprise interface is intended for users who manage their respective accounts end-to-end. In the Standard Enterprise mode, the customers have complete access to their accounts. They can also provision and manage their respective accounts.

Figure 1 illustrates a typical Standard Enterprise mode deployment.

Figure 1 *Standard Enterprise Mode*

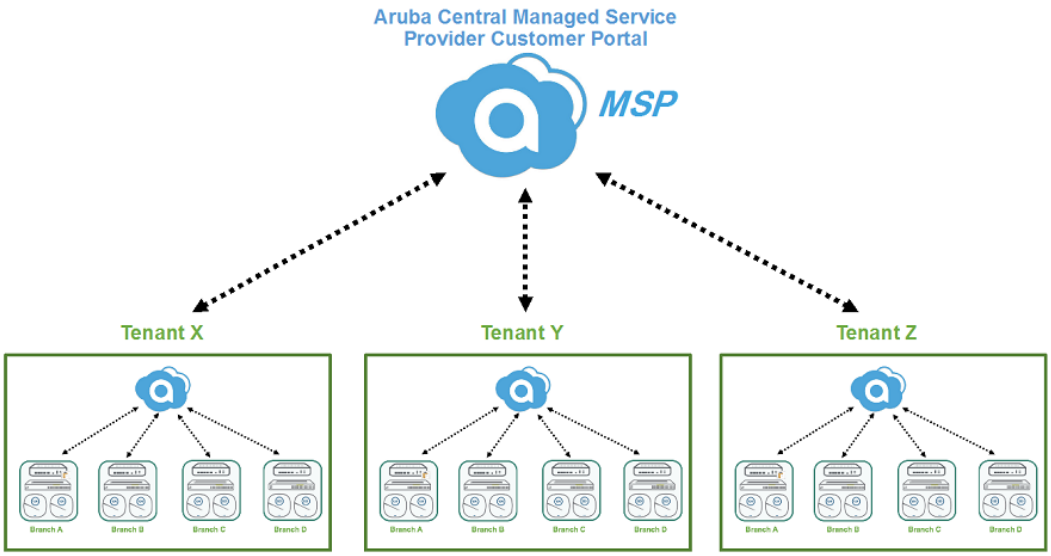


Managed Service Provider Mode

Aruba Central offers the MSP mode for managed service providers who need to manage multiple customer networks. The MSP administrators can provision tenant accounts, allocate devices, assign licenses, and monitor tenant accounts and their networks. The administrators can also drill down to a specific tenant account and perform administration and configuration tasks. Tenants can access only their respective accounts, and only those features and application services to which they have subscribed.

Figure 2 illustrates a typical MSP mode deployment.

Figure 2 *Managed Service Provider Mode*



Supported Web Browsers

NOTE

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

Table 3: *Browser compatibility matrix*

Browser Versions	Operating System
Google Chrome 39.0.2171.65 or later	Windows and Mac OS
Mozilla Firefox 34.0.5 or later	Windows and Mac OS
Internet Explorer 10 or later	Windows
Safari 7 or later	Mac OS

Supported Devices

This section provides the following information:

- Supported Instant APs
- Supported Switch Platforms
- Supported Aruba Gateways

Supported Aruba Gateways

As part of the Aruba SD-WAN solution, Aruba Central supports management, monitoring, and configuration of Aruba Gateways. The SD-WAN solution includes the following types of branch devices:

The SD-WAN Branch Gateways operate at the branch sites to optimize and control WAN, LAN, and cloud security services. Branch Gateways also serve as a policy enforcement point for LAN, WLAN, and WAN setups. Branch Gateways can also route traffic over the most efficient link based on availability, application type, user-role, and link health.

The Headend Gateways act as VPN Concentrator for branch offices. Branch Gateways establish IPSec tunnels to one or more VPN Concentrators over the Internet or other untrusted networks—private WAN or public Internet connections.

The following table lists the SD-WAN Gateway platforms and the supported firmware versions in Aruba Central:

Table 4: *Supported Aruba Gateways*

Platform	Minimum Supported Software Version	Latest Software Version	Recommended Software Version
Aruba 7005 Mobility Controller	ArubaOS_70xx_8.1.0.0-1.0.0.0	ArubaOS_70xx_ 8.4.0.0-1.0.6.0	ArubaOS_70xx_8.4.0.0-1.0.5.1
Aruba 7008 Mobility Controller			
Aruba 7010 Mobility Controller			
Aruba 7024 Mobility Controller			
Aruba 7030 Mobility Controller			
Aruba 7210 Mobility Controller	ArubaOS_72xx_8.1.0.0-1.0.0.0	ArubaOS_72xx_ 8.4.0.0-1.0.6.0	ArubaOS_72xx_8.4.0.0-1.0.5.1
Aruba 7220 Mobility Controller Aruba 7240 Mobility Controller Aruba 7240XM Mobility Controller			
Aruba 7280 Mobility Controller			

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. For Aruba 2530 Switch Series, the recommended software version is 16.05.0008. However, if you already have switches running lower software versions in your account, you can continue to manage these devices from Aruba Central.

Table 5 and Table 6 list the switch platforms, corresponding software versions supported in Aruba Central, and switch stacking details.

Table 5: *Supported Aruba Switch Series, Software Versions, and Switch Stacking*

Switch Platform	Supported Software Versions	Recommended Software Versions	Switch Stacking Support
Aruba 2530 Switch Series	YA/YB.16.05.0008 or later	YA/YB.16.08.0001	N/A
Aruba 2540 Switch Series	YC.16.03.0004 or later	YC.16.08.0001	N/A
Aruba 2920 Switch Series	WB.16.03.0004 or later	WB.16.08.0001	Yes **Switch Software Dependency**: WB.16.04.0008 or later
Aruba 2930F Switch Series	WC.16.03.0004 or later	WC.16.08.0001	Yes **Switch Software Dependency**: WC.16.07.0002
Aruba 2930M Switch Series	WC.16.04.0008 or later	WC.16.08.0001	Yes **Switch Software Dependency**: WC.16.06.0006
Aruba 3810 Switch Series	KB.16.03.0004 or later	KB.16.08.0001	Yes **Switch Software Dependency**: KB.16.07.0002
Aruba 5400R Switch Series	KB.16.04.0008 or later	KB.16.08.0001	Yes **Switch Software Dependency**: KB.16.06.0008

Table 6: *Supported Aruba Mobility Access Switch Series and Software Versions*

Mobility Access Switch Series	Supported Software Versions
■ S1500-12P ■ S1500-24P ■ S2500-24P ■ S3500-24T	ArubaOS 7.3.2.6 ArubaOS 7.4.0.3 ArubaOS 7.4.0.4 ArubaOS 7.4.0.5 ArubaOS 7.4.0.6

Provisioning and configuration of Aruba 5400R Switch Series and switch stacks is supported only through configuration templates.

Supported Instant APs

For the up-to-date list of supported Instant AP platforms and firmware versions, see Supported Instant APs.

Thank you for choosing Aruba Central as your network management solution!

Before you get started with Aruba Central, we recommend that you review the Key capabilities of Aruba Central and the list of Aruba devices supported in Aruba Central.

Key Terms and Concepts

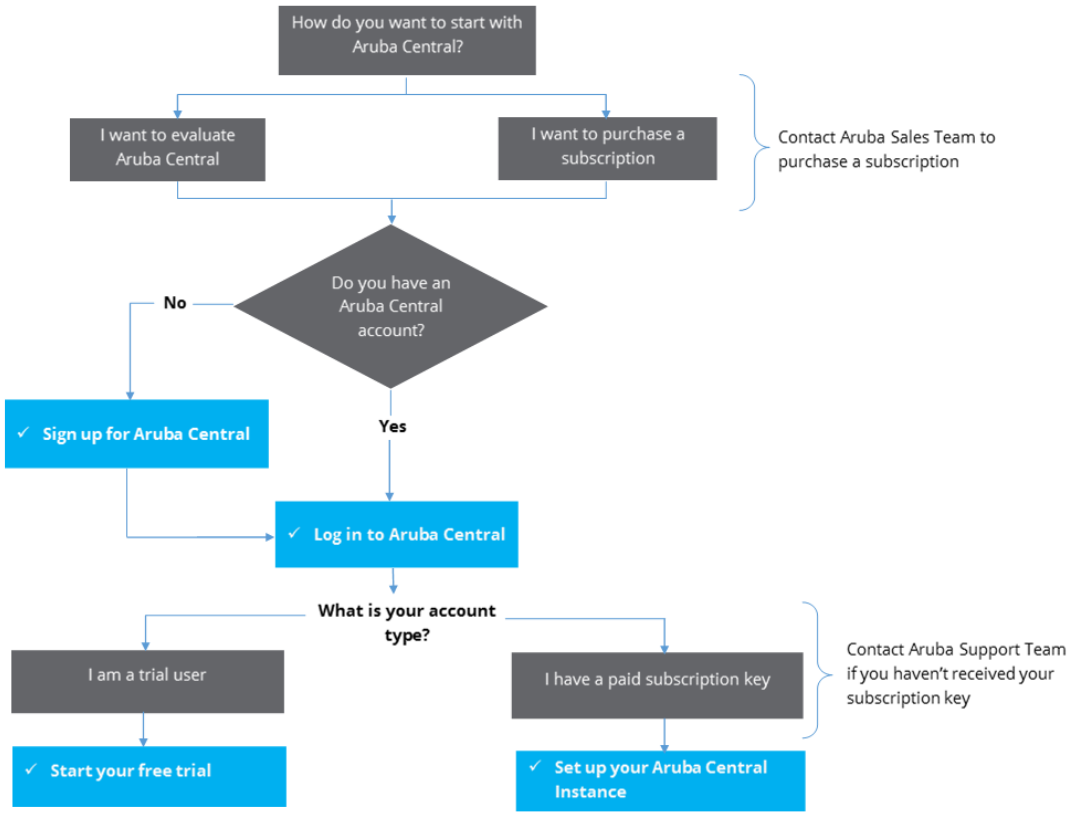
Take a few minutes to familiarize yourself with the key terms and concepts used in the help topics.

Cluster Zone	Refers to an Aruba Central deployment area within a specific region. In other words, cluster zones are regional grouping of one or more container instances on which Aruba Central is deployed. Cluster zones allow your deployments to restrict customer data to a specific region and plan timezone-specific maintenance windows. Each cluster zone has separate URLs for signing up for Aruba Central, accessing Aruba Central portal, and for allowing devices to communicate with Aruba Central. To view the zone in Aruba Central UI, click the **User Settings** menu at the bottom of the left navigation pane.
Enterprise Mode	Refers to the Aruba Central solution deployment mode in which the customers provision, manage, and maintain their networks end-to-end for their respective organizations or businesses.
Managed Services Mode	Refers to the Aruba Central deployment mode in which the service providers, resellers, administrators, and retailers to centrally manage and monitor multiple tenant or end-customer accounts from a single management interface.
Subscription	Refers to the license granted to a customer for using a product or service.
Evaluation Account	Refers to the Aruba Central account created for evaluating Aruba Central solution and its services.
Paid Subscriber	Refers to the customers who have purchased a subscription to obtain access to Aruba Central and its services.
Subscription Key	Refers to the license key. A subscription key is a 14-character alphanumeric string; for example, PQREWD6ADWERAS.
Customer ID **Subscriber ID**	Refers to the identity number of your Aruba Central account. To view your subscriber ID, click the **User Settings** menu at the bottom of the left navigation pane in the Aruba Central UI.
Zero Touch Provisioning	Refers to one of the following: ■ Zero Touch Provisioning of Aruba Central accounts— When you purchase a subscription key and add this subscription key in Aruba Central, Aruba Central queries the Aruba Activate database to retrieve the devices mapped to your purchase order and add these devices to the inventory. This process is referred to as zero touch provisioning in Aruba Central. ■ Zero Touch Provisioning of Devices—Most Aruba devices support self-provisioning; that is, when you connect a device to a provisioning network, it can automatically download provisioning parameters from the Activate server and connect to their management entity.
Onboarding	Refers to the process of importing devices to Aruba Central's device inventory, activating subscriptions, and making devices available for management from Aruba Central.

Device Sync	Refers to the process of synchronizing devices from the Activate database. The device sync operation allows Aruba Central to retrieve devices from Activate and automatically add these devices to the device inventory in Aruba Central.
Provisioning	Refers to the process of setting up a device for deploying networks as per the configuration requirements of your organization.
Group	Refers to the device configuration container in Aruba Central. You can combine devices with common configuration requirements into a single group and apply the same configuration to all the devices in that group.
Site	Refers to the physical locations where devices are installed. Organizing devices per sites allows you to filter your dashboard view per site.
Label	Refers to the tags used for logically grouping devices based on various parameters such as ownership, specific areas within a site, departments, and so on.

Workflow Summary

The following illustration summarizes the steps required for getting started with Aruba Central:



Related Topics

Navigate through the following steps to complete the onboarding and provisioning procedures.

- Creating an Aruba Central Account
- Accessing Aruba Central Portal on page 36
- Starting Your Free Trial on page 46
- Setting up Your Aruba Central Instance

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 7: *Sign Up URLS*

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
APAC-1	https://portal-apac.central.arubanetworks.com/signup
EU-1	https://portal-eu.central.arubanetworks.com/signup
Canada-1	https://portal-ca.central.arubanetworks.com/signup

Signing up for an Aruba Central Account

To sign up for an Aruba Central account:

1. Go to http://www.arubanetworks.com/products/sme/eval/.
2. Click **SIGN UP NOW**. The **Registration** page opens.
3. Select the language.
4. Enter your email address. Based on the email address you entered, the Registration page guides you to the subsequent steps:

Table 8: *Registration Workflow*

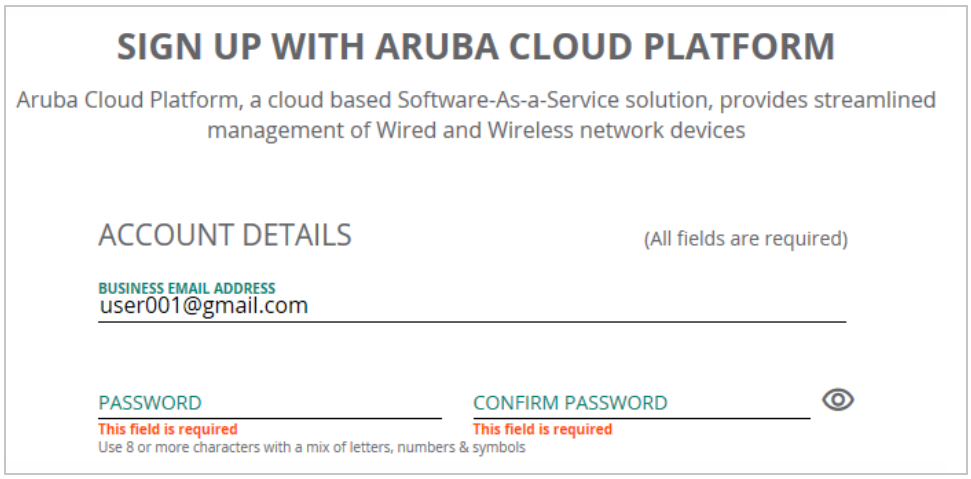
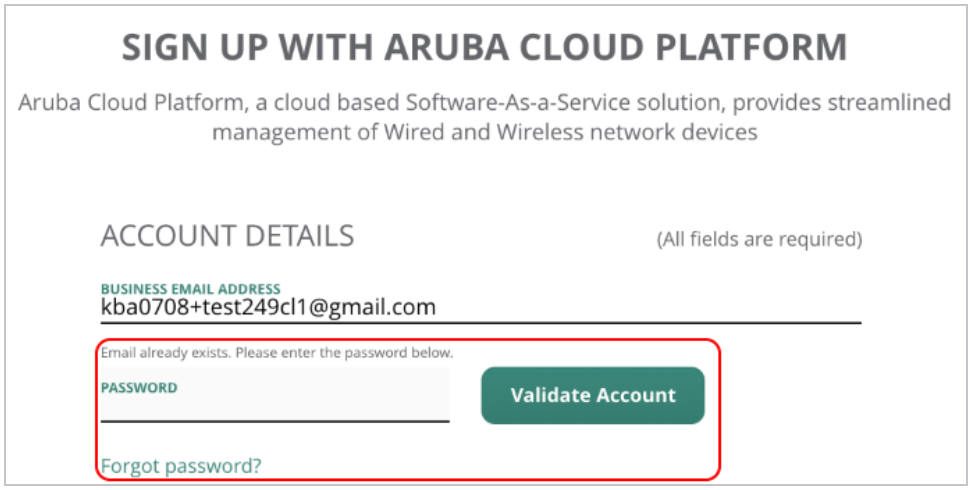
If...	Then...
If you are a new user:	The **Registration** page prompts you to create a password. To continue with the registration, enter a password in the **Password** and **Confirm Password** fields. 
If you are an existing Aruba customer, but you do not have an Aruba Central account: If your email account is already registered with Aruba, but you do not have an Aruba Central account:	The **Registration** page displays the following message: **Email already exists. Please enter the password below**. To continue with registration, validate your account: 1. Enter the password. 2. Click **Validate Account**. **NOTE:** If you do not remember the password, click **Forgot Password** to reset the password. 
If you are invited join as a user in an existing Aruba Central customer account:	The **Registration** page displays the following message: **An invitation email has already been sent to your email ID. Resend**. To continue with the registration: 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 8: *Registration Workflow*

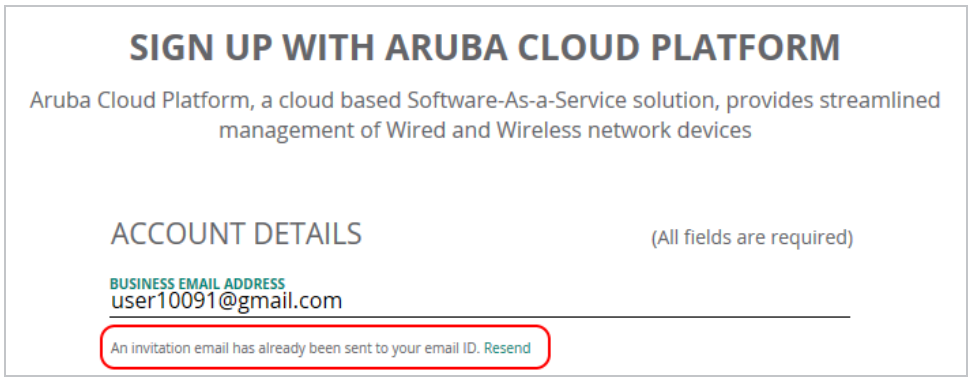
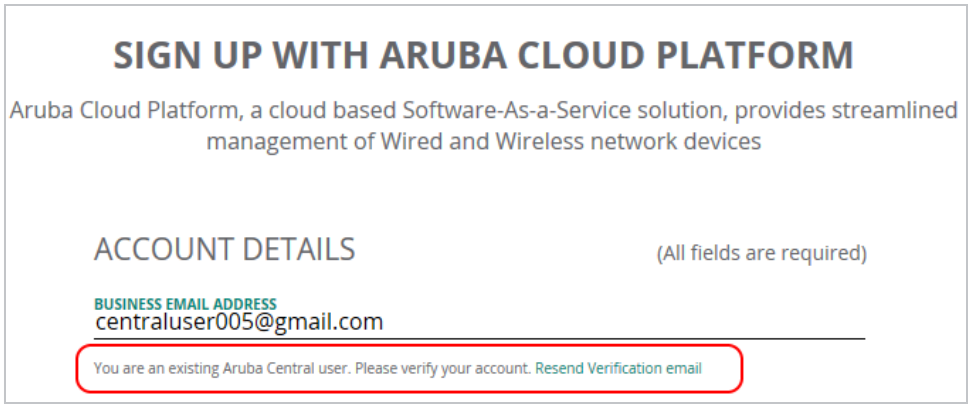
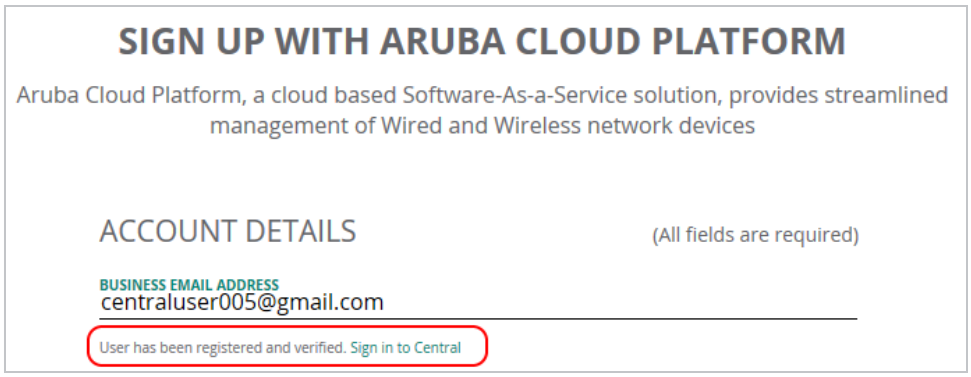
If...	Then...
	
If you are a registered user of Aruba Central and have not verified your email yet:	The **Registration** page displays the following message: **You are an existing Aruba Central user. Please verify your account. Resend Verification email**. To continue: 1. Go to your email box and check 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. 
If you are already a registered user of Aruba Central and have verified your email:	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.

Table 8: *Registration Workflow*

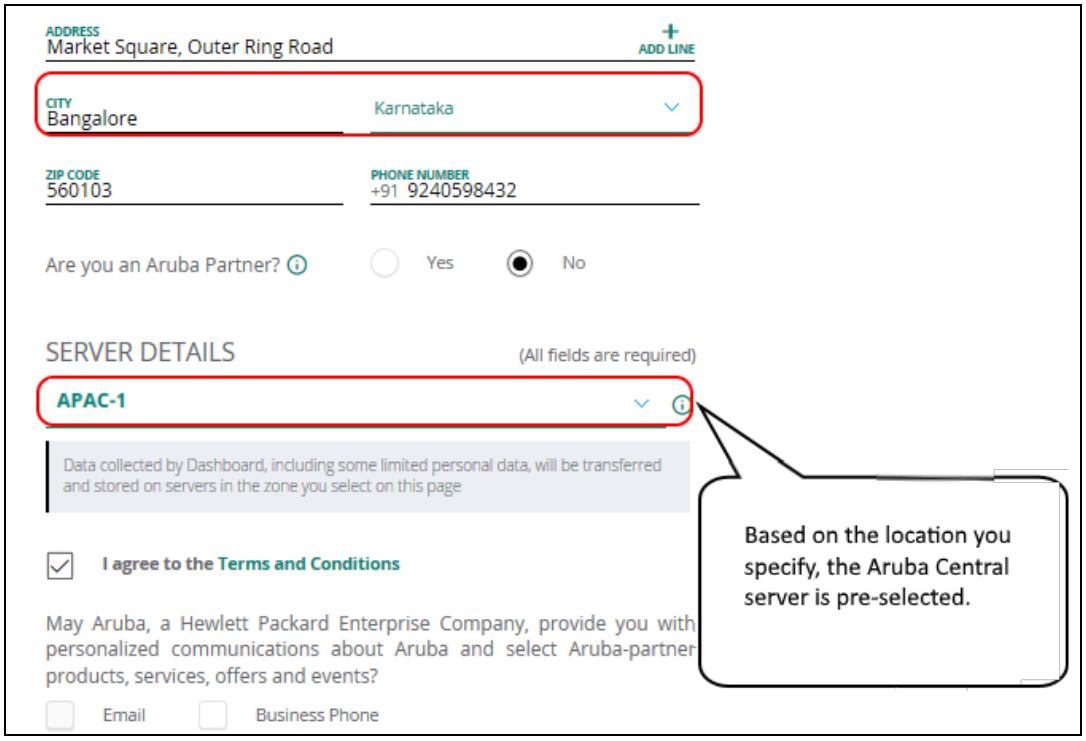
If...	Then...
	
If your email address is in the **arubanetworks.com** or **hpe.com** domain:	The **Single Sign-On** option is enabled. You can use your respective Aruba or HPE credentials to log in to your Aruba Central account after the registration. 

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

6. Specify if you are an Aruba partner.

7. 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 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.

Figure 3 *Account Registration Page*



8. Select the **I agree to the Terms and Conditions** check box.
9. Set a preferred mode of communication for receiving notifications about Aruba products and services.
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.

Accessing Aruba Central Portal

After you create an Aruba Central account, the link to Aruba Central portal will be sent to your registered email address. You can use this link to log in to Aruba Central.

If you are accessing the login URL from the www.arubanetworks.com website, ensure that you select the zone in which your account was created.

Login URLs

When you try to access Aruba Central portal, you are redirected to the Aruba Central URL that is mapped to your cluster zone.

Table 9: *Cluster Zone— Portal URLs*

Cluster Zone	Portal URL
US-1	https://portal.central.arubanetworks.com
US-2	https://portal-prod2.central.arubanetworks.com
China-1	https://portal.central.arubanetworks.com.cn

Cluster Zone	Portal URL
EU-1	https://portal-eu.central.arubanetworks.com
APAC-1	https://portal-apac.central.arubanetworks.com
Canada-1	https://portal-ca.central.arubanetworks.com

Logging in to Aruba Central:

To log in to Aruba Central:

1. Access the Aruba Central login URL for your zone.
2. Notice that the zone is automatically selected based on your geographical location.
3. Enter the email address and click **Continue**.
4. Log in using your credentials.

If your user credentials are stored in your organization's Identity Management server and SAML SSO authentication is enabled for your IdP on Aruba Central, complete the SSO authentication workflow.

5. Enter the password.

If you have forgotten password, you can click the **Forgot Password** and reset your password. The Forgot Password link resets only your Aruba Central account; hence, it is not available to SSO users.

6. If you have forgotten your password,
7. Click **Continue**. The **Initial Setup** wizard opens.

- If you have a paid subscription, click **Get Started** and set up your account.
- If you are a trial user, click **Evaluate Now** and start your trial.

Changing Your Password

To change your Aruba Central account:

1. In the Aruba Central UI, click the user icon ( ) in the header pane.
2. Click **Change Password**.
3. Enter a new password.
4. Log in to Aruba Central using the new password.

The **Change Password** menu option is not available for federated users who sign in to Aruba Central using their SSO credentials.

Logging Out of Aruba Central

To log out of Aruba Central:

1. In the Aruba Central UI, click the user icon ( ) in the header pane.
2. Click **Logout**.

Exploring the User Interface

Aruba offers the following variants of the Aruba Central web interface:

- Standard Enterprise mode—The Standard Enterprise interface is intended for customers who manage their respective accounts end-to- end. In the Standard Enterprise mode, the customers have complete access to their accounts. They can also provision and manage their respective accounts. For more information, see Aruba Central User Interface.
- Managed Service mode—Aruba Central offers the MSP mode for managed service providers who need to manage multiple customer networks. With MSP mode enabled, the MSP administrators can provision customer accounts, allocate devices, assign licenses, and monitor customer accounts and their networks. The administrators can also drill down to a specific tenant account and perform administration and configuration tasks. The tenants can access only their respective accounts, and only those features and application services to which they have subscribed. For more information, see MSP User Interface on page 43.

Aruba Central User Interface

After you log in to the Aruba Central web interface, the Standard Enterprise view opens.

The main window consists of the following elements:

Left Navigation Pane

The left navigation pane shows the company logo at the top. It includes the following UI elements:

App Selector

The app selector lists the apps available for the Aruba Central users.

Most of the apps require service subscriptions to be enabled on the devices. Contact your administrator and the Aruba Central Support team to obtain access to an application service.

Monitoring & Reports

The following menu options are available for the **Monitoring and Reports** app:

- **Network Overview**—This page includes the following tabs:
  - **Network Overview**—Displays a summary of bandwidth usage, client count, top devices in use, top 5 clients in the network, and a list of network profiles configured on the devices in the network.

- **APs**—Displays a dashboard for monitoring APs provisioned in the network. You can also view the usage graphs, top N APs by usage, and a complete list of APs in the network. To view the details of an AP, click MAC address of the AP in the list.
- **Switches**—Displays a dashboard for monitoring switches and switch stacks provisioned in the network. You can also view the usage graphs, top N switches s by usage, and a complete list of list of switches in the network. To view the details of a switch or switch stack, click name of the switch or the switch stack from the list view.
- **Gateways**—Provides an overall summary of the WAN network and the details of the gateways provisioned in the network.
- **Security**—Displays a summary of the rogue devices and intrusion detected in the network. You can view a list of rogue devices, WIDS events, and interferences detected in the network.

- **Network Health**—Displays an overall summary of the health and performance of the network and devices deployed on a site.
- **Label Health**—Displays an overall summary of the health and performance of devices tagged to a label.
- **Client Overview**—Provides a summary of wireless and wired clients associated with the devices provisioned in your Aruba Central account.
- **AppRF**—Provides a summary of application usage by clients and charts that show trends for applications, application categories, websites category, and website reputation score.
- **VisualRF**—Provides a real-time picture of the radio environment of your wireless network and the ability to plan the wireless coverage of new sites.
- **Alerts**—Displays a list of alerts. The **Alerts** page also allows you to acknowledge these alerts.
- **Reports**—Allows you to generate reports such as Network Summary, Security, PCI Compliance, Client Inventory, Infra Inventory, Client Usage, Capacity Planning, New Infra Inventory, and AppRF reports.

Wireless Management

The **Wireless Management** app allows you to configure SSIDs, radio profiles, security and firewall settings, and enable services on Instant APs. It also allows you to configure Instant APs provisioned under template groups through configuration templates.

Wired Management

The **Wired Management** app allows you to configure Aruba Switches and switch stacks. It also allows you to configure switches provisioned in a template group through configuration templates.

Gateway Management

The **Gateway Management** app allow you to configure WAN and LAN interfaces, overlay network, routes, security, routing and path steering policies on SD Branch devices.

Maintenance

The **Maintenance** app allows you to maintain network, view reports and audit trails, and manage APIs:

. The app includes the following menu options:

- **Firmware**—Allows you to view the current firmware version of the devices and provides options to upgrade the devices to the latest firmware version.
- **Troubleshooting**—Allows you to run troubleshooting commands for devices.
- **Audit Trail**—Shows audit trail for the events pertaining to device allocation, configuration, user addition deletion, and firmware upgrade status.
- **API Gateway**—Allows you to view APIs and manage OAuth tokens.

Guest Access

The **Guest Access** app includes the following menu options:

- **Overview**—Displays a dashboard that shows the details of the cloud guest SSIDs, duration for which the guest users are connected, client count, and the type of client devices connected to the cloud guest SSIDs.
- **Splash Page**—Allows you to configure splash page profiles for guest network profiles.
- **Visitors**—Allows you create guest user accounts and assign these users to a guest SSID.

Global Settings

The **Global Settings** tab includes the following menu options:

- **Manage Groups**—Displays menu options for viewing, adding and modifying groups.
- **Device Inventory**—Displays a list of devices added in Aruba Central. The **Device Inventory** page also allows you to add devices and assign devices to groups.
- **Key Management**—Allows you to track the subscription keys in use and the available keys.
- **Subscription Assignment**—Allows you to assign subscription key to devices. You can also enable automatic assignment of subscriptions for devices joining the Aruba Central inventory.
- **Cluster Management**—Allows the administrators to provision and manage the on-premise cluster of nodes.
- **Labels and Sites**—Allows you to create and manage labels and sites. The administrators can create sites to monitor devices installed inn a specific physical location. They can also use labels to tag devices to a specific area in a physical location, specific owners, or departments.
- **Users & Roles**—Allows the MSP administrators create and modify users and roles. The administrators can control user access to applications and network management functions by creating a custom role and assigning to the users.
- **Certificates**—Allows the administrators to upload certificates.

Presence Analytics

The **Presence Analytics** app allows you to analyze client presence patterns in public venues and enterprise environments.

The **Presence Analytics** app includes the following menu options:

- **Activity**—Displays a dashboard with the client presence details and loyalty metrics.
- **Settings**—Allows you to configure RSSI threshold and dwell time settings for the clients .

Clarity

The **Clarity** app view provides an analytical dashboard for real-time monitoring of the client on-boarding, client association and authentication transactions, and DHCP and DNS service request and responses.

The **Clarity** application view includes the following menu options:

- **Activities**— Displays graphs showing connectivity health, latency, performance of the network and the device, and the association and authentication transactions between the client device and the network.
- **Insights**—Displays insights for the onboarding performance of the clients for a time range of 1 day or 1 month.
- **Troubleshooting**—Allows you to view the onboarding details for a specific client device for debugging purpose.
- **Health Checks**—Allows you to configure health check parameters, run periodic health checks, and view reports.

Unified Communications

The **Unified Communications** application manage your enterprise communication ecosystem. The Unified Communications application on Aruba devices provides a seamless user experience when using applications such as Microsoft® Lync/Skype for Business for voice, video calls, and application sharing. The application actively monitors and provides visibility into Lync/Skype for Business traffic and allows you to prioritize sessions. The Unified Communications application also leverages the functions of the Service Engine on the cloud platform and provides rich visual metrics for analytical purpose.

The **Unified Communications** application view includes the following menu options:

- **Activity**—Displays a variety of charts that allow you to assess the quality of voice and video traffic on network.
- **Insights**—Displays a summary of the patterns identified for poor quality sessions for each day in the last month.
- **Troubleshooting**—Provides a summary of the client connection details and displays possible causes for the poor session quality, and lists poor call records.
- **Call Detail Records**—Displays various details about the call.

Install Manager

The Install Manager app allows you to manage and monitor device installations at specific physical locations or sites. The Install Manager app enables third-party installation operations managers to set up installer profiles and monitor device installations at the given sites. This app works in conjunction with the Aruba Installer app.

Icons at the bottom pane

- The mobile icon—Allows you to download the Aruba Central mobile app from the following sites:
  - **App Store**—For Apple devices running iOS 9.0 or later.
  - **Google Play Store**—For mobile devices running Android 5.0 Lollipop or later.
- The bubble icon—Displays the following options:
  - **Documentation**—Opens the Aruba Central user documentation portal.
  - **View / Update Case**—Directs you to the support site to view or update an existing support case.
  - **Open New Case**—Directs you to the support site to open a new support case.
- The Help Icon—Click the **?** icon to view a short description or definition of the selected terms and fields in a pane or dialog box. To view the online help:
  a. Click the **(?)** at the top.
  b. Move your cursor over a data pane item to view the help text.
  c. To disable the help mode, click **(?)** again.

Search Bar

The search bar at the top right corner of the header pane allows users to search for devices, clients, events, or a specific network profile. The search bar is available for the following apps only:

- Monitoring & Reports
- Wireless Management
- Wired Management
- Gateway Management
- Maintenance
- Guest Access

- Install Manager

User Icon

Click the user icon at the top right corner of the header pane to view user account details such as account name, domain, customer ID, and zone details. It also includes the following options for managing your accounts:

- **Change Password**—Allows you to change the password of account.
- **User Settings**—Displays the zone, date, time and timezone. The administrators can also set a language preference and a timeout value for inactive user sessions.

The Aruba Central web interface is available in English, French, Spanish, German, Brazilian Portuguese, and Japanese languages. You can now set your language preference through the **User Settings** menu from the drop-down list on the header pane. Aruba Central saves your language preference and displays the UI in the language set by you.

- **Terms of Service**—Displays the terms and conditions for using Aruba Central services.
- One of the following options:
  - **Managed Service Mode**—Enables MSP mode and switches the interface to the MSP mode.
  - **Disable MSP**—If you have activated **Managed Service Mode**, this option appears. Disables the MSP mode and opens the Aruba Central standard interface. The MSP mode can be disabled only if there are no active tenant accounts. The option is grayed out if there are any active tenant accounts.
- **Logout**—Allows you to log out your account.

Filter bar

The filter bar on the left of data pane includes the following UI elements:

Groups Selection

The groups selection filter bar on the left side of the data pane displays the following:

- Name of group. If no group filter is applied, the data pane view is set to **All Devices**.
- Total number devices provisioned in the network.
- The number of APs and switches that are currently down.

The groups filter supports the following functions:

- Filter the data pane view by group or devices
- Perform configuration tasks at the group or device level
- Perform maintenance tasks at the group or device level
- Run reports at the group level

Label Selection

The filter bar also lists the labels to which the devices are assigned. You can also filter your dashboard view and run reports per label.

Site Selection

The filter bar now allows you to filter your monitoring dashboard contents per sites. The filter bar shows a list of sites created in your setup.

Temporal Filter

The Temporal filter at the top right corner of the data pane is available for **Monitoring & Reports** app. The filter allows you to set a time range for pages showing monitoring and reports data. You can set the filter to any of the following time ranges:

- 3 hours
- 1 day
- 1 week
- 1 month
- 3 months

Data Pane

Displays detailed information of the tabs and data for the selected menu commands.

Notifications Pane

The Notifications pane at the bottom of the UI shows alerts for device addition, provisioning, and country code configuration.

Need Help Bubble

The Need Help? bubble is a new feature that provides contextual information on the UI elements and features available on a page.

MSP User Interface

The MSP mode is intended for the managed service providers who manage multiple distinct tenant accounts. The MSP mode allows MSP customers to provision and manage tenant accounts, assign devices to tenant accounts, manage subscription keys and other functions such as configuring network profiles and viewing alerts.

The MSP UI consists of the following elements:

- Left Navigation Pane on page 43
- Search Bar on page 45
- User Icon on page 45
- Filter bar on page 46
- Data Pane on page 46
- Notifications Pane on page 46

Left Navigation Pane

The left navigation pane shows the company logo at the top. It includes the following UI elements:

App Selector

The app selector lists the apps available for MSP users.

Most of the apps require service subscriptions to be enabled on the devices. Contact your administrator and the Aruba Central Support team to obtain access to any application service.

Monitoring and Reports

The following menu options are available for the **Monitoring and Reports** app:

- **Dashboard**—Provides a summary of hardware and subscriptions owned by the MSP and the tenant accounts managed by the MSP. You can also view graphs representing the devices under management, tenant accounts added, and subscription renewal schedule.
- **Alerts**—Displays a list of alerts. The **Alerts** page also allows you to acknowledge these alerts.

Wireless Configuration

The **Wireless Configuration** app allows you to configure SSIDs, radio profiles, security and firewall settings, and enable services on Instant APs.

Aruba Central allows the percolation of the country code configured in the **Set Country Code For Group** field of the **Wireless Management > System** page in MSP view. The country code at the tenant default group exhibits the following behavior:

- An existing country code that is already set in the tenant default group overrides the country code percolated from the MSP group.
- If no country code is set at the tenant level, the tenant default group inherits the country code configured at the MSP group level.

Wired Configuration

The **Wired Configuration** app allows you to configure Aruba Switches and switch stacks.

Maintenance

The **Maintenance** app allows you to maintain the devices associated with tenant accounts provisioned in the MSP mode. The app includes the following menu options:

- **Firmware**—Allows you to view the current firmware version of the devices and provides options to upgrade the devices to the latest firmware version.
- **Portal Customization**—Allows you to customize the look and feel of the email notifications and the user interface.
- **Audit Trail**—Shows audit trail for the events pertaining to device allocation, configuration, and firmware upgrade status.
- **API Gateway**—Allows you to view APIs and manage OAuth tokens.

Guest Access

The **Guest Access** app displays a list of cloud guest splash page profiles. You can also create new splash page profiles for a device group.

Global Settings

The **Global Settings** tab includes the following menu options:

- **Manage Groups**—Displays menu options for viewing, adding and modifying groups.
- **Device Inventory**—Displays a list of devices and allows you to assign devices to tenant accounts provisioned in the MSP mode.

- **Key Management**—Displays details of the subscription key assigned to tenant accounts provisioned in the MSP mode. The **Key Management** page also allows users to track the subscription keys associated with the tenant accounts.
- **Subscription Assignment**—Allows MSP users to assign device management subscription and enable network service subscriptions for the devices provisioned in the network.
- **Users & Roles**—Allows MSP administrators create and modify users and roles. The administrators can control user access to applications and network management functions by creating a custom role and assigning to the users.
- **Certificates**—Allows MSP administrators to add, edit, and view device certificates.

Icons at the bottom pane

- The bubble icon—Displays the following options:
  - **Documentation**—Opens the Aruba Central user documentation portal.
  - **View / Update Case**—Directs you to the support site to view or update an existing support case.
  - **Open New Case**—Directs you to the support site to open a new support case.
  - **Airheads Community**—Directs you to the Airheads Community page to view existing topics to start a new a new topic.
- The Help Icon—Click the **?** icon to view a short description or definition of the selected terms and fields in a pane or dialog box. To view the online help:

  a. Click the **(?)** at the top.

  b. Move your cursor over a data pane item to view the help text.

  c. To disable the help mode, click **(?)** again.

Search Bar

In the tenant account view, the search bar at the top right corner of the header pane allows MSP users to search for devices, clients, events, or a specific network profile. The search bar is available for the following apps only:

- Monitoring & Reports
- Wireless Management
- Wired Management
- Maintenance
- Guest Access
- Install Manager

User Icon

Click the user icon at the top right corner of the header pane to view user account details such as account name, domain, customer ID, and zone details. It also includes the following options for managing your accounts:

- **Change Password**—Allows you to change the password of account.
- **User Settings**—Displays the zone, date, time and timezone. The administrators can also set a language preference and a timeout value for inactive user sessions.

The Aruba Central web interface is available in English, French, Spanish, German, Brazilian Portuguese, and Japanese

languages. You can now set your language preference through the **User Settings** menu from the drop-down list on the header pane. Aruba Central saves your language preference and displays the UI in the language set by you.

- One of the following options:
  - **Managed Service Mode**—Enables MSP mode and switches the interface to the MSP mode.
  - **Disable MSP**—If you have activated **Managed Service Mode**, this option appears. Disables the MSP mode and opens the Aruba Central standard interface. The MSP mode can be disabled only if there are no active tenant accounts. The option is grayed out if there are any active tenant accounts.
- **Terms of Service**—Displays the terms and conditions for using Aruba Central services.
- **Logout**—Allows you to log out from your account.

Filter bar

The filter bar on the left of data pane includes the following UI elements:

Groups Selection Filter

The groups selection filter bar on the left side of the data pane displays the name of group only. The groups filter is available for the following apps only:

- Wireless Management
- Wired Management
- Guest Access

The groups filter supports the following functions:

- Filter the data pane view by group
- Perform configuration tasks at the group level
- Perform maintenance tasks at the group level

Data Pane

Displays detailed information of the tabs and data for the selected menu commands.

Notifications Pane

The Notifications pane at the bottom of the UI shows alerts for device addition, provisioning, and country code configuration.

Starting Your Free Trial

Aruba Central offers a 90-day evaluation subscription for customers who want to try the Aruba cloud solution for managing their networks.

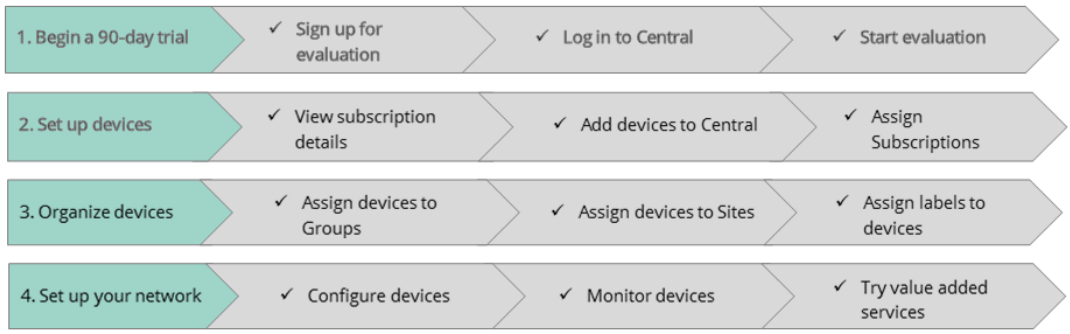
The evaluation subscription allows you use the following functions:

- Device management
  - Manage up to 10 Instant APs and/or switches
  - Manage up to two SD-WAN Gateways
- Monitoring—Monitor your devices, network and client status
- Guest Access app—Set up guest Wi-Fi on your custom portals
- Presence Analytics—Analyze consumer presence data for your stores

- Troubleshooting—Run diagnostic checks and troubleshoot device issues

Figure 4 shows the steps required for getting started with your free trial.

Figure 4 *Getting Started Workflow for Free Trial*



Get Started with the Free Trial

Complete the following steps to evaluate Aruba Central:

Step 1: Getting Started with the Initial Setup

To get started with the trial:

1. Register for evaluating Aruba Central.
2. Log in to Aruba Central. After you log in, the **Initial Setup** wizard opens.
3. Click **Evaluate Now**. The **Initial Setup** wizard guides you through the onboarding steps
4. Click through the steps to set up your account and start using Aruba Central. If you want to exit the wizard and complete the onboarding steps on your own, click **Exit and go to Aruba Central**.

The Initial Setup wizard is displayed only when you log in to Aruba Central for the first time. The wizard is not available for Aruba Central users in the MSP mode.

Step 2: Viewing Subscription Details (Optional)

At your first login, the **Initial Setup** wizard displays the details of the evaluation subscription details. After you exit the wizard, you can view the subscription details on the **Global Settings** > **Key Management** page.

Viewing Subscription Key Details

The following table shows the typical contents of a subscription key:

Table 10: *Subscription Key Details*

Keys	Subscription key number.
Type	Type of the subscription. Aruba Central supports the following types of subscriptions: ■ Device subscriptions—The device subscription allows you to avail services such as device onboarding, configuration, management, monitoring, and reports. The device subscriptions can be assigned only to the devices managed by Aruba Central. ■ Service subscriptions—Aruba Central supports application services that you can run on the devices provisioned in your setup. For example, if you have Instant APs with 6.4.4.4-4.2.3.0 or later, you can assign a service subscription for Presence Analytics. ■ Gateway Subscriptions—Aruba Central supports a separate set of subscriptions for configuring and managing SD-WAN gateways. The Gateway subscriptions are marked as **Foundation-<device>**; for example, Foundation-70XX.
Expiration Date	Expiration date for the subscription key.
Quantity	Number of license tokens available for a subscription. Each Aruba Central subscription holds a specific number of tokens. For example, when a subscription is assigned to a device, Aruba Central binds the device with a token from the existing pool of subscriptions.
Status	Status of the subscription key. For example, if you are a trial user, Aruba Central displays the status of subscription key as **Eval**.

Step 3: Adding Devices

To manage devices from Aruba Central, trial users must manually add the devices to Aruba Central's device inventory.

You can add up to 10 devices. The devices can be 10 Instant APs or 10 Switches, or a total of 10 Instant APs and switches.

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

In 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.

From the Device Inventory Page

1. Go to **Global Settings** > **Device Inventory**.
2. Click **Add by MAC/SN**. The **Add Devices** pop-up window opens.
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.

Step 4: Assigning Subscriptions

By default, Aruba assigns an evaluation subscription key for users who sign up for a free trial of Aruba Central. The evaluation subscription key allows you to manage up to 10 devices from Aruba Central, and avail value added services such as Presence Analytics and Guest Access with Instant APs.

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.
- Service subscription—Allows you to enable value added services on the Instant APs managed from Aruba Central. For example, if you have Instant APs, you can assign a service subscription for Guest Access.
- Gateway subscription—Allows you to manage and monitor SD-WAN Gateways from Aruba Central.

You can either enable automatic assignment of subscription or manually assign subscriptions to your devices. By default, the automatic subscription assignment is disabled.

Enabling Automatic Assignment of Subscriptions

Use one of the following options to enable automatic assignment of subscriptions:

In the Initial Setup Wizard

1. Verify that you have a 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. Go to **Global Settings** > **Subscription Assignment**. The **Subscription Assignment** page opens.
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.

Manually Assigning Subscriptions

In the Initial Setup Wizard

1. In the **Assign Subscription** tab, ensure that the **Auto Subscribe** toggle switch is turned off.
2. Select the devices in the list for which you want to manually assign subscriptions.
3. Click **Update Subscription**.

From the Subscription Assignment Page

1. Go to **Global Settings** > **Subscription Assignment**.
2. On the **Subscription Assignment** page, ensure that the **Auto Subscribe** toggle is turned off.
3. Select the devices to which you want to assign subscriptions.
4. Click **Update Subscription**.

For more information on subscriptions. see Managing Subscriptions on page 63.

Step 5: Organize Your Devices into Groups

A group in Aruba Central functions as a configuration container for devices added in Aruba Central.

Why Should You Use Groups?

Groups allow you to create a logical subset of devices and simplify the configuration and device management

tasks. Groups offer the following functions and benefits:

- Combining different types of devices under a group. For example, a group can have Instant APs and Switches. Aruba Central allows you to manage configuration of these devices in separate containers (wireless and wired management) within the same group. Any new device that is added to a group inherits the current configuration of the group.
- Assigning multiple devices to a single group. For example, a group can consist of multiple Instant AP Virtual Controllers (VCs). These VCs can share common configuration settings and push the configuration updates to slave Instant AP in their respective clusters. For example, you can apply a common security policy for the devices deployed in a specific geographical location.
- Cloning an existing group allows you to create a base configuration for the devices and customize it as per your network requirements.

You can also use groups for filtering your monitoring dashboard content, generating reports, and managing software upgrades.

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

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

For more information on groups and group configuration workflows, see Using Groups for Device Configuration and Management on page 73.

Assigning Devices to Groups

After you successfully complete the onboarding workflow, the **Initial Setup** wizard prompts you to assign your devices to a group. You can click **Assign Group** and assign your devices to a group. You can also use one of the following methods to assign your devices to groups.

To assign a device to a group from the **Global Setting** > **Device Inventory** page:

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

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

1. Click **Global Settings** > **Manage Groups**. The **Groups** page opens.
2. From the devices table on the right, select the device that you want to assign to a new group.
3. Drag and drop the device to the group to which you want to assign the device.

Step 6: Assigning Sites and Labels (Optional)

A site in Aruba Central refers to a physical location where a set of devices are installed; for example, campus, branch, or venue. Aruba Central allows you to use sites as a primary navigation element. For example, if your devices are deployed in a campus, you can create a site called CampusA. You can also tag the devices within CampusA using labels. If your campus consists of multiple buildings, the devices deployed in the campus can be labeled as **Building1** or **Lobby**.

For more information on sites and labels and how to assign devices to sites and labels, see Managing Sites on page 69 and Managing Labels on page 71.

Step 7: Configure Your Network

If you have added Instant APs as part of your evaluation, you can configure an employee and guest wireless

network. If you have Switches or SD-WAN Gateways, configure wired access network or SD-WAN respectively.

Step 8: Monitor Your Network and Devices

Use monitoring dashboards to view the health of the device and network.

You can also run reports, configure alerts, and view client details.

Step 9: Evaluate Value Added Services (Optional)

Enable Presence Analytics and Guest Access services on your Instant APs and review these services.

Step 10: Cancel or Upgrade Your Subscription (Optional)

During the trial period or after you complete your trial, if you want to continue using Aruba Central for managing your devices, contact Aruba Customer Support to upgrade your subscription.

If you do not want to continue, contact Aruba support team to cancel your subscription or wait until the trial expires. When the trial period expires, your devices can no longer be managed from Aruba Central.

Upgrading to a Paid Account

If you have purchased a subscription, upgrade your account by completing the following steps:

1. On left navigation pane, above the product logo, click the link that shows the number of days left for subscription expiry. The **Add a New Subscription** pop-up window opens.
2. Enter the new subscription key that you purchased from Aruba.
3. Click **Add Subscription**.

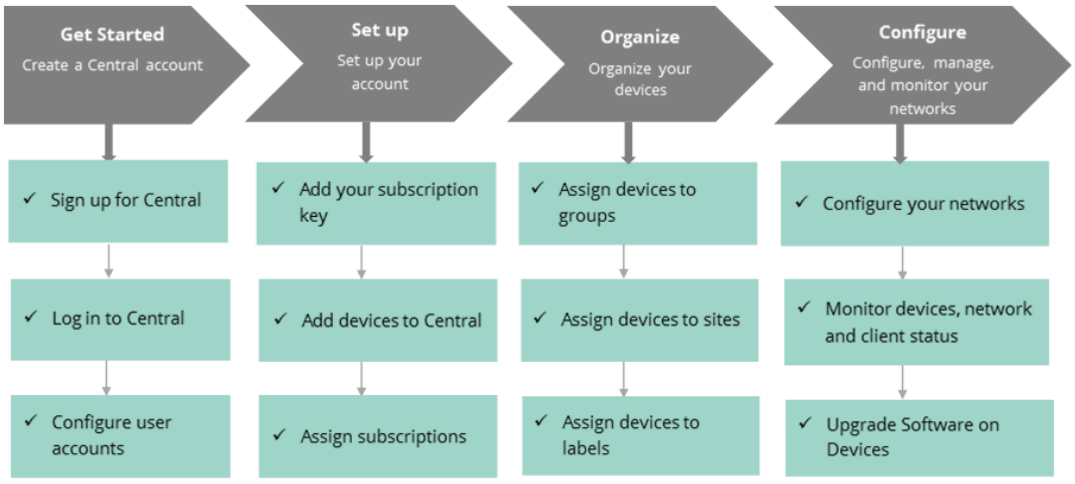
After you upgrade your account, you can add more devices and enable services, and continue using Aruba Central.

Setting up Your Aruba Central Instance

If you have purchased a subscription key to manage your devices and networks from Aruba Central, get started with steps described in this topic.

Figure 5 illustrates the steps required for setting up your Aruba Central instance:

Figure 5 *Getting Started Workflow*



Getting Started with Aruba Central

Complete the following steps to start using Aruba Central for managing your devices and setting your networks.

Step 1: Getting Started

To get started:

1. Sign up to create your Aruba Central account.
2. If you already have an Aruba Central account, log in to Aruba Central with your credentials. When you log in for the first time, the **Initial Setup** wizard opens and guides you through the onboarding workflow.
3. Click **Get Started**.
4. Click through the wizard to complete the onboarding workflow. If you want to exit the wizard and complete the onboarding steps on your own, click **Exit and go to Aruba Central**.

The Initial Setup wizard is displayed only when you log in to Aruba Central for the first time. The wizard is not available for Aruba Central users in the MSP mode.

Step 2: Adding a Subscription Key

At your first login, the **Initial Setup** wizard prompts you add your subscription key. To continue with the onboarding workflow, add your subscription key in the Add Subscription Key tab.

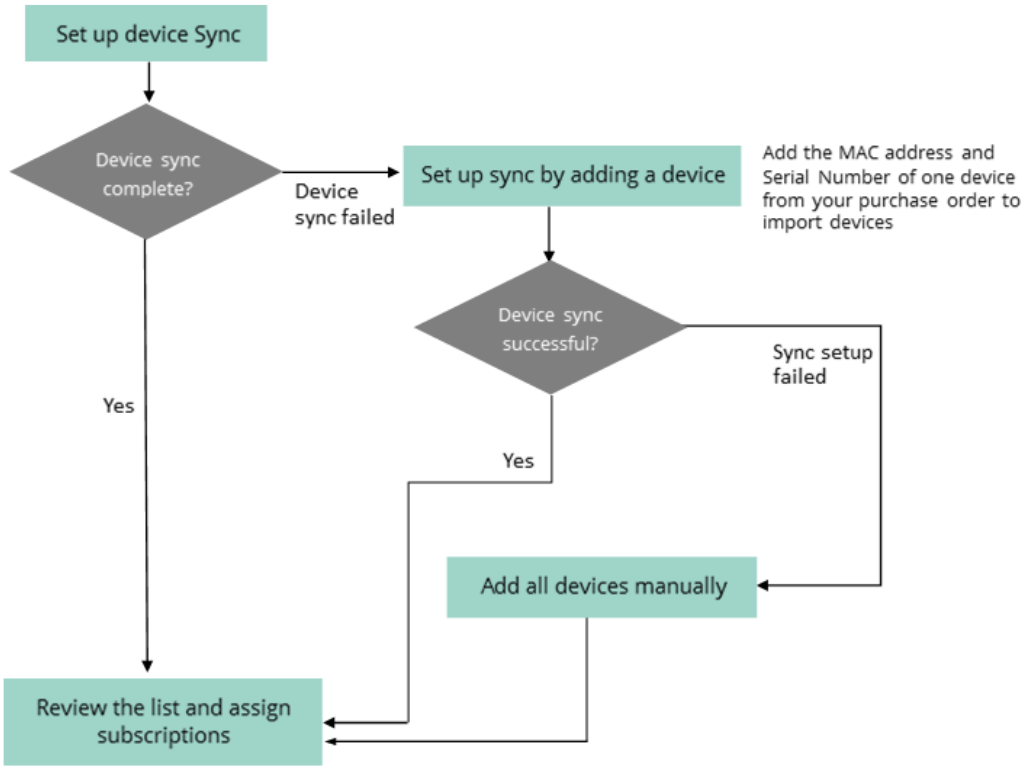
If you are not using the wizard, complete the following steps to add your subscription key.

To add a subscription key:

1. Go to **Global Settings** > **Key Management**. The **Key Management** page opens.
2. Enter your subscription key.
3. Click **Add Subscription**. The subscription key is added to Aruba Central and the contents of the subscription key are displayed in the **Subscription Details** page.
4. Review the subscription details.

Step 3: Adding Devices

If you have a paid subscription, you can automatically import devices from the Activate database to the Aruba Central device inventory.



Setting up Device Sync for Automatic Device Addition

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. If the device sync fails, use any of the following options:

- **Add Devices Manually**—To manually add devices by entering the MAC address and serial number of each device.
- **Add Via Mobile App**—To add devices from the Aruba Central mobile app. You can download the Aruba Central app from Apple AppStore on iOS devices and Google Play Store on Android devices.
- **Contact support**—To contact Aruba Technical Support.

From the Device Inventory Page

1. Go to **Global Settings** > **Device Inventory**.

2. Click **Sync Devices**.
3. Enter the serial number and MAC address of one device from your purchase order. Aruba Central imports all other devices associated with your purchase order from Activate.
4. Review the devices in your inventory.
5. If the device sync fails, use any of the following options:

- **Add Devices Manually**—To manually add devices by entering the MAC address and serial number of each device.
- **Add Via Mobile App**—To add devices from the Aruba Central mobile app. You can download the Aruba Central app from Apple AppStore on iOS devices and Google Play Store on Android devices.
- **Contact support**—To contact Aruba Technical Support.

Manually Adding Devices

Use any of the following options to add devices using MAC address and serial number:

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 of MAC address of your 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 list of devices.

From the Device Inventory Page

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

1. Go to **Global Settings** > **Device Inventory**.
2. Click **Add by MAC/SN**. The **Add Devices** pop-up window opens.
3. Enter the serial number and MAC address of your 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 added to the inventory.

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

For more information on adding devices, see Onboarding Devices on page 59.

Step 4: Assigning 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.
- Service subscription—Allows you to enable value added services on the Instant APs managed from Aruba Central. For example, if you have Instant APs, you can assign a service subscription for Guest Access.
- Gateway subscription—Allows you to manage and monitor SD-WAN Gateways from Aruba Central.

You can either enable automatic assignment of subscription or manually assign subscriptions to your devices. By default, the automatic subscription assignment is disabled.

Enabling Automatic Assignment of Subscriptions

Use one of the following options to enable automatic assignment of subscriptions:

In the Initial Setup Wizard

1. Verify that you have a 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. Go to **Global Settings** > **Subscription Assignment**. The **Subscription Assignment** page opens.
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.

Manually Assigning Subscriptions

In the Initial Setup Wizard

1. In the **Assign Subscription** tab, ensure that the **Auto Subscribe** toggle switch is turned off.
2. Select the devices in the list for which you want to manually assign subscriptions.
3. Click **Update Subscription**.

From the Subscription Assignment Page

1. Go to **Global Settings** > **Subscription Assignment**.
2. On the **Subscription Assignment** page, ensure that the **Auto Subscribe** toggle is turned off.
3. Select the devices to which you want to assign subscriptions.
4. Click **Update Subscription**.

For more information on subscriptions and how to assign network service and SD-WAN Gateway subscriptions. see Managing Subscriptions on page 63.

Step 5: Organize Your Devices into Groups

A group in Aruba Central functions as a configuration container for devices added in Aruba Central.

Why Should You Use Groups?

Groups allow you to create a logical subset of devices and simplify the configuration and device management tasks. Groups offer the following functions and benefits:

- Combining different types of devices under a group. For example, a group can have Instant APs and Switches. Aruba Central allows you to manage configuration of these devices in separate containers (wireless and wired management) within the same group. Any new device that is added to a group inherits the current configuration of the group.
- Assigning multiple devices to a single group. For example, a group can consist of multiple Instant AP Virtual Controllers (VCs). These VCs can share common configuration settings and push the configuration updates to slave Instant AP in their respective clusters. For example, you can apply a common security policy for the devices deployed in a specific geographical location.

- Cloning an existing group allows you to create a base configuration for the devices and customize it as per your network requirements.

You can also use groups for filtering your monitoring dashboard content, generating reports, and managing software upgrades.

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

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

For more information on groups and group configuration workflows, see Using Groups for Device Configuration and Management on page 73.

Assigning Devices to Groups

After you successfully complete the onboarding workflow, the **Initial Setup** wizard prompts you to assign your devices to a group. You can click **Assign Group** and assign your devices to a group. You can also use one of the following methods to assign your devices to groups.

To assign a device to a group from the **Global Setting** > **Device Inventory** page:

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

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

1. Click **Global Settings** > **Manage Groups**. The **Groups** page opens.
2. From the devices table on the right, select the device that you want to assign to a new group.
3. Drag and drop the device to the group to which you want to assign the device.

Step 6: Assigning Sites and Labels (Optional)

A site in Aruba Central refers to a physical location where a set of devices are installed; for example, campus, branch, or venue. Aruba Central allows you to use sites as a primary navigation element. For example, if your devices are deployed in a campus, you could create a site called CampusA. You can also tag the devices within CampusA using labels. If your campus consists of multiple buildings, the devices deployed in the campus can be labeled as **Building1** or **Lobby**.

For more information on sites and labels and how to assign devices to sites and labels, see Managing Sites on page 69 and Managing Labels on page 71.

Step 7: Configuring Users

Add system users, assign user roles, and configure role based access control.

For more information, see Configuring System Users on page 110.

Step 8: Configuring and Managing Networks

To start configuring your network setup:

1. Connect your devices to Aruba Central.
2. Provision Instant APs, Switches, or Gateways to set up your WLAN, wired access and SD-WAN network.

Step 9: Monitoring Your Network and Devices

Use the monitoring dashboards to view the health of the device and network.

You can also run reports, configure alerts, and view client details.

Step 10: Upgrading Software Images on Devices

View software images available for the devices provisioned in your account, run a compliance check for the recommended software version, and upgrade devices.

For more information and step-by-step instructions, see Managing Software Upgrades on page 102.

Step 11: Running Diagnostic Checks and Troubleshooting Issues

Run diagnostic checks and troubleshooting commands to analyze network connectivity and latency issues and debug device issues if any. For more information and step-by-step instructions, see Troubleshooting Devices on page 104.

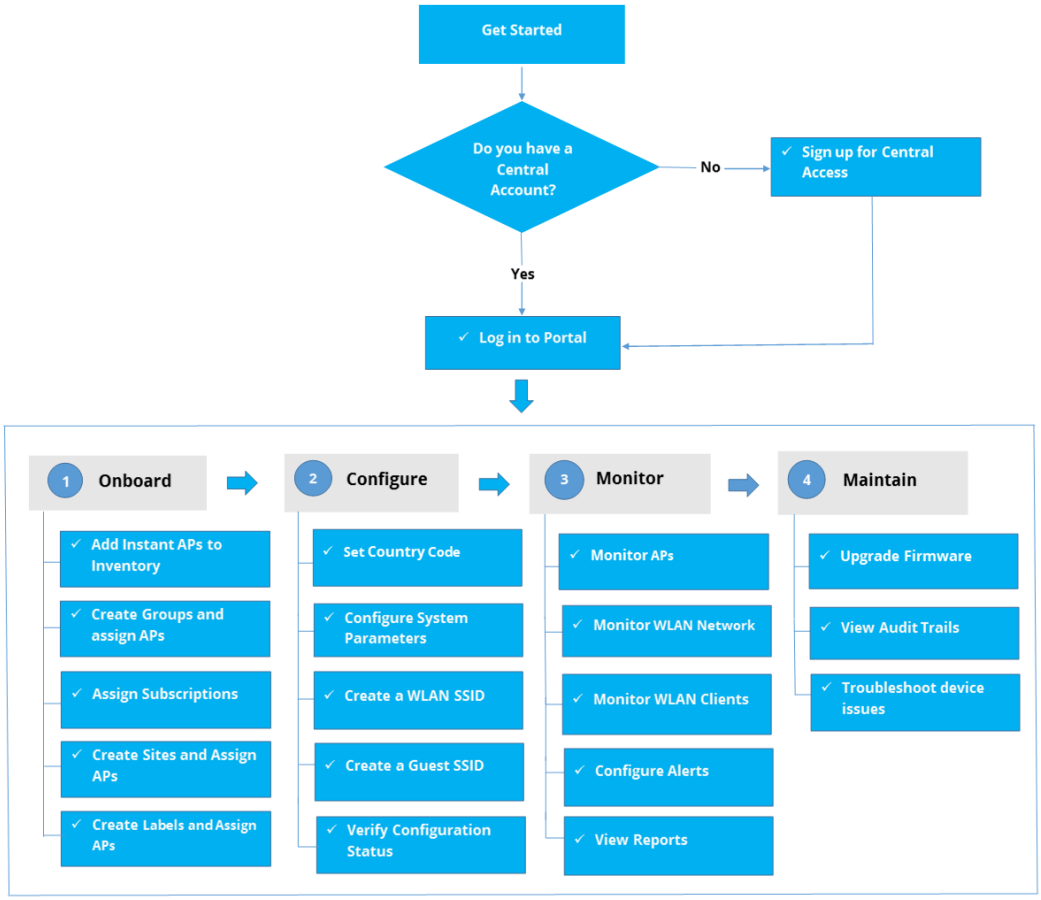
Provisioning Instant APs

The following figure illustrates the procedure for bringing up Instant APs and configuring a basic WLAN setup. To view a detailed description of the tasks, click the task link in the flowchart.

NOTE

When you click a task in the flowchart, the linked topic opens in a pop-up window. After you browse through the topic, click outside the pop-up window to return to this page.

Figure 6 *Getting Started—Instant APs*



In the Aruba Central UI, most of the general administration tasks are grouped under **Global Settings**. The administrators can use the menu options available in the **Global Settings** module to manage groups, devices, subscriptions, sites, labels, certificates, users, and configure role based user access control.

Managing Your Device Inventory

The devices purchased by the customers are automatically added the device inventory in their respective Aruba Central accounts. If the device you purchased does not show up in the inventory, you can manually add it.

Aruba Central allows you to add up to 32 devices manually by entering the valid MAC and serial number combination for each device.

Users having roles with **Modify** permission can add devices. Users having roles with **View Only** permission can only view the Device Inventory module.

Viewing Devices

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

Table 11 shows the contents of the **Device Inventory** page.

Table 11: *Details of Devices*

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

Adding Devices to Inventory

For information on adding devices, see Onboarding Devices.

Onboarding Devices

Aruba Central supports the following options for adding devices.

- If you are a trial user, you must manually add the serial number and MAC address of the devices that you want manage from Aruba Central. For more information, see Adding Devices (Evaluation Account) on page 59.
- If you are paid subscriber, Aruba Central retrieves devices associated with your purchase order from Activate. If the devices are not automatically discovered and added to Central's device inventory, set up a sync to import devices from the Activate database. Adding Devices (Paid Subscription) on page 60.

Adding Devices (Evaluation Account)

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

In 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.

From the Device Inventory Page

1. Go to **Global Settings** > **Device Inventory**.
2. Click **Add by MAC/SN**. The **Add Devices** pop-up window opens.
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 you have a paid subscription, Aruba Central automatically discovers and imports the devices mapped to your purchase order. 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. If the device sync fails, use any of the following options:

- **Add Devices Manually**—To manually add devices by entering the MAC address and serial number of each device.
- **Add Via Mobile App**—To add devices from the Aruba Central mobile app. You can download the Aruba Central app from Apple AppStore on iOS devices and Google Play Store on Android devices.
- **Contact support**—To contact Aruba Technical Support.

From the Device Inventory Page

1. Go to **Global Settings** > **Device Inventory**.
2. Click **Sync Devices**.
3. Enter the serial number and MAC address of one device from your purchase order. Aruba Central imports all other devices associated with your purchase order from Activate.
4. Review the devices in your inventory.
5. If the device sync fails, use any of the following options:

- **Add Devices Manually**—To manually add devices by entering the MAC address and serial number of each device.
- **Add Via Mobile App**—To add devices from the Aruba Central mobile app. You can download the Aruba Central app from Apple AppStore on iOS devices and Google Play Store on Android devices.
- **Contact support**—To contact Aruba Technical Support.

Manually Adding Devices When Device Sync Fails

If you have a paid subscription, you can set a device sync for automatic discovery and importing of devices from the Activate database. However, when the device sync fails, add devices manually by using one of the following methods:

- Adding Devices Using MAC address and Serial Number on page 61
- Adding Devices Using Activate Account
- Adding Devices Using Cloud Activation Key on page 62

Adding Devices Using MAC address and Serial Number

Use any of the following options to add devices using MAC address and serial number:

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 of MAC address of your 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 list of devices.

From the Device Inventory Page

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

1. Go to **Global Settings** > **Device Inventory**.
2. Click **Add by MAC/SN**. The **Add Devices** pop-up window opens.
3. Enter the serial number and MAC address of your 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 added to the inventory.

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

Adding Devices Using Activate Account

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

To add devices from your Activate account:

1. Go to **Global Settings** > **Device Inventory**.

2. On the **Device Inventory** page, click **Advanced** and select **Add Using Activate**.
3. Enter the username and password of your Activate account.
4. Click **Add**.
5. Review the devices added to the inventory.

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 Instant APs:
  1. Log in to the Instant AP UI or CLI.
     - If using the UI, go to the **Maintenance** > **About**.
     - If using the CLI, execute the **show about** command at the Instant AP CLI.
  2. Note the cloud activation key and MAC address.
- For Aruba Switches:
  1. Log in to the switch CLI.
  2. Execute the **show system | in Base** and **show system | in Serial** commands.
  3. Note the cloud activation key and MAC address in the command output.
- For Mobility Access Switches
  1. 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.
  2. 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. Go to **Global Settings** > **Device Inventory**.
2. On the **Device Inventory** page, click **Advanced** and select the **Add with Cloud Activation Key**. The **Cloud Activation Key** pop-up window opens.
3. Enter the cloud activation key and MAC address of a device.
4. Click **Add**.

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

See Also:

- Starting Your Free Trial on page 46
- Setting up Your Aruba Central Instance on page 51

Managing Subscriptions

A subscription key is a 14-character alphanumeric string; for example, PQREWD6ADWERAS. Subscription keys allow your devices to be managed by Aruba Central. To use Aruba Central for managing and monitoring your devices, you must ensure that you have a valid subscription key.

Managing Subscription Keys

Evaluation Subscription Key

The evaluation subscription key is enabled for trial users by default. It allows you to add up to 10 devices, either 10 Instant APs or 10 Switches, or a total of 10 devices. The evaluation subscription also allows you to enable services such as Presence Analytics and Guest Access on your devices.

The **Global Settings** > **Key Management** page displays the subscription expiration date. You will receive subscription expiry notifications through email on the 30th, 15th and 1 day before the subscription expiry and on day 1 after the subscription expires. Aruba Central also the number of days left for subscription expiry above the product logo on the left navigation pane.

Upgrading to a Paid Account

If you have purchased a subscription, upgrade your account by completing the following steps:

1. On left navigation pane, above the product logo, click the link that shows the number of days left for subscription expiry. The **Add a New Subscription** pop-up window opens.
2. Enter the new subscription key that you purchased from Aruba.
3. Click **Add Subscription**.

After you upgrade your account, you can add more devices and enable services, and continue using Aruba Central.

Paid Subscription Key

If you have a purchased a subscription key, you must ensure that your subscription key is added to Aruba Central. If you are logging in to Aruba Central for the first time, Aruba Central prompts you to add your subscription key to activate your account. Ensure that you add the subscription key before onboarding devices to Aruba Central.

The **Global Settings** > **Key Management** page displays the subscription expiration date. You will receive subscription expiry notifications through email 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.

When you upgrade or renew your subscription, or purchase another subscription key, you must add the key details in the **Global Settings** > **Key Management** page to avail the benefits of new subscription.

Adding a Subscription Key

To add a subscription key:

1. Go to **Global Settings** > **Key Management**. The **Key Management** page opens.
2. Enter your subscription key.
3. Click **Add Subscription**. The subscription key is added to Aruba Central and the contents of the subscription key are displayed in the **Subscription Details** page.
4. Review the subscription details.

Viewing Subscription Key Details

To view the subscription key details, complete the following steps:

1. From the app selector, click **Global Settings**.
2. Click **Key Management**. The **Key Management** page opens.

Table 12 describes the contents of the **Manage Keys** table on the **Key Management** page.

Table 12: *Subscription Key Details*

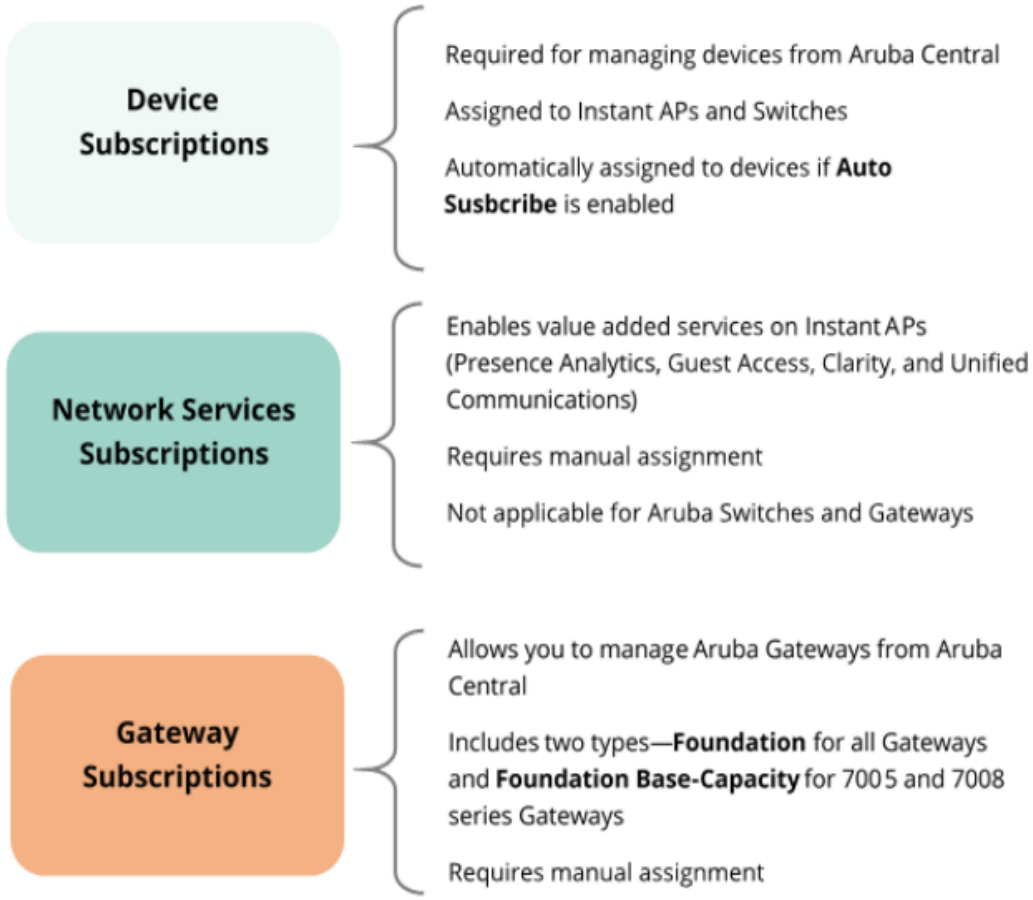
Data Pane Item	Description
Keys	Subscription key number.
Type	Type of the subscription. Aruba Central supports the following types of subscriptions: ■ Device subscriptions—The device subscription allows you to avail services such as device onboarding, configuration, management, monitoring, and reports. The device subscriptions can be assigned only to the devices managed by Aruba Central. ■ Service subscriptions—Aruba Central supports application services that you can run on the devices provisioned in your setup. For example, if you have Instant APs with 6.4.4.4-4.2.3.0 or later, you can assign a service subscription for Presence Analytics. ■ Gateway Subscriptions—Aruba Central supports a separate set of subscriptions for configuring and managing SD-WAN gateways. The Gateway subscriptions are marked as **Foundation-<device>**; for example, Foundation-70XX.
Expiration Date	Expiration date for the subscription key.
Quantity	Number of license tokens available for a subscription. Each Aruba Central subscription holds a specific number of tokens. For example, when a subscription is assigned to a device, Aruba Central binds the device with a token from the existing pool of subscriptions.
Status	Status of the subscription key. For example, if you are a trial user, Aruba Central displays the status of subscription key as **Eval**.

Supported Subscription Types

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.
- Service subscription—Allows you to enable value added services on the Instant APs managed from Aruba Central. For example, if you have Instant 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 Subscriptions

Read through the following sections to understand the subscription assignment procedures:

- Assigning Device Subscriptions on page 65
- Assigning Subscriptions on page 65
- Assigning Gateway Subscriptions on page 67

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. Go to **Global Settings** > **Subscription Assignment**. The **Subscription Assignment** page opens.
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, Aruba Central 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.

Important Notes for MSP Users

If you want to enable automatic assignment of subscriptions to the devices mapped to your tenant accounts, note the following points:

- Aruba Central assigns subscriptions only if the devices are mapped to a tenant account. If your account has devices that are not mapped to any tenant account and if these devices already have a subscription assigned, the existing assignments are preserved.
- When a device is moved from a tenant account to the MSP, Aruba Central removes the subscription assigned to this device.
- When the automatic subscription assignment is enabled, Aruba Central disables the device and tenant-specific overrides. MSP administrators can modify the subscription settings for a specific event only through the API Gateway interface.
- When the automatic subscription assignment is enabled, all the existing tenants and newly created tenants in the MSP view inherit the subscription assignment settings. Subsequently, Aruba Central assigns device subscriptions to the tenants and their respective devices.
- If you migrate from the Standard Enterprise mode to the MSP mode, Aruba Central retains your device and service subscription settings.
- If the devices are no longer mapped to a tenant account, MSP administrators can unassign subscriptions these devices.

Manually Assigning Subscriptions

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

1. Go to **Global Settings** > **Subscription Assignment**.
2. On the **Subscription Assignment** page, ensure that the **Auto Subscribe** toggle is turned off.
3. Select the devices to which you want to assign subscriptions.
4. Click **Update Subscription**.

Important Notes for MSP Users

When you turn off the **Auto Subscribe** toggle:

- Automatic assignment of subscription for all the existing tenants, including the MSP devices, are disabled.
- All device subscriptions assigned to devices are preserved.
- Devices must be assigned to tenant accounts before assigning a subscription to it. If a subscription is assigned to a device that is not mapped to any specific tenant account, Aruba Central displays the following

error message: **Please assign this device to a tenant before subscribing it. Tenant assignment can be performed in the Device Inventory page**.

Assigning Network Service Subscriptions

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

1. Go to **Global Settings** > **Subscription Assignment**. The **Subscription Assignment** page opens.
2. Select the service subscription that you want to enable on a device.
3. Under **Network Service Subscriptions**, select the Instant AP device from the table on the right.
4. Drag and drop the device to the subscription selected in the table on the left.

Important Note for MSP Users

Ensure that the device is assigned to a tenant before assigning a service subscription to it. When a device or network service subscription is assigned to a device that is not mapped to any specific tenant, the following error is displayed: **Please assign this device to a tenant before subscribing it. Tenant assignment can be performed in the Device Inventory page**.

Assigning Gateway Subscriptions

For Aruba Gateways to function as SD-WAN Gateways, you must onboard them to the Aruba Central's device inventory and ensure that a valid subscription is assigned to each Gateway. The Gateway subscription allows Aruba Mobility Controllers to function as SD branch devices.

Gateway Subscriptions

Aruba Central supports the following types of subscriptions for Gateways:

- **Foundation**—This subscription can be assigned to all Mobility Controllers irrespective of the hardware model.
- **Foundation-Base capacity** —This subscription can be assigned only to Aruba 7005 Mobility Controllers. 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 alert to trigger an incident using Webhook. .

Assigning Subscriptions to Gateways

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

1. Go to **Global Settings** > Click **Subscription Assignment**. The **Subscription Assignment** page opens.
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.

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.

Managing Sites

A site in Aruba Central refers to a physical location where a set of devices are installed; for example, campus, branch, or venue.

Overview

Aruba Central allows you to use sites as a primary navigation element. For example, if your devices are deployed in a campus, you could create a site called CampusA. You can also tag the devices within CampusA using labels. For example, if the campus consists of multiple buildings, the devices deployed in the campus can be labeled as **Building1** or **Lobby**. If the devices in a specific location or an area within a specific location must have similar configuration, the devices can be grouped together.

Sites Page

The **Sites** page in the UI allows you to create sites, view the list of sites configured in your setup, and assign devices to sites.

The **Sites** page includes the following functions:

Table 13: *Sites Page*

Name	Contents of the Table
Convert Labels to Sites	Allows you to convert existing labels to sites. To convert labels, download the CSV file with the list of labels configured in your setup, add the site information, and upload the CSV file. For more information, see Creating a Site on page 69.
Sites Table	Displays a list of sites configured in Aruba Central. It provides the following information: ■ **Site Name**—Name of the site. ■ **Address**—Physical address of the site. ■ **Device Count**—Number of devices assigned to a site. The table also includes the following sorting options to reset the table view on the right: ■ **All Devices**—Displays all the devices provisioned in Aruba Central. ■ **Unassigned**—Displays the list of devices that are not assigned to any site. You can also use the filter and sort icons on the **Sites** and **Address** columns to filter and sort sites respectively.
New Site	Allows you to create a new site.
Bulk upload	Allows you to add sites in bulk from a CSV file.
Devices Table	Displays a list of devices provisioned in Aruba Central. It provides the following information: ■ Name—Name of the device ■ Group—Group to which the device is assigned. ■ Type—Type of the device.

Creating a Site

To create a site, complete the following steps:

1. From the app selector, click **Global Settings**.
2. Click **Labels and Sites**. The **Labels and Sites** page opens.
3. Set the toggle switch to **Site(s)**.
4. To add a new site, click **(+) New Site**. The **Create New Site** pop-up window opens.

5. In the **Create New Site** pop-up window, enter the following details for the site:
   a. **Site Name**—Name of the site.
   b. **Street Address**—Address of the site.
   c. **City**—City in which the site is located.
   d. **Country**—Country in which the site is located.
   e. **State/Province**—State or province in which the site is located.
   f. **ZIP/Postal Code**—(Optional) ZIP or postal code of the site.
6. Click **Add**. The new site is added to the **Sites** table.

Adding Multiple Sites in Bulk

To import site information from a CSV file in bulk, complete the following steps:

1. From the app selector, click **Global Settings**.
2. Click **Labels and Sites**. The **Labels and Sites** page opens.
3. Set the toggle switch to **Sites**. The site management options are displayed.
4. Click **(+) Bulk upload**. The **Bulk Upload** pop-up opens.
5. Download a sample file.
6. Fill the site information and save the CSV file in your local directory.

The CSV file for bulk upload of sites must include the mandatory information such as the name, address, city, state, and country details.

7. Go to **Global Settings** > **Labels and Sites** > **Sites** > **(+) Bulk upload** window in Aruba Central UI, click **Browse** and add the file from your local directory.
8. Click **Upload**. The sites from the CSV file are added to the site table.

Assigning a Device to a Site

To assign devices to a site, complete the following steps:

1. On the **Global Settings** > **Labels and Sites** > **Sites** page, locate the site to which you want to assign a device.
2. Select **Unassigned**. The list of devices that are not assigned to any site is displayed.
3. Select one or several devices from the list of devices.
4. Drag and drop the devices to the site on the left. A pop-up window opens and prompts you to confirm the site assignment.
5. Click **Yes**.

Converting Existing Labels to Sites

To convert existing labels to sites, complete the following steps:

1. Go to **Global Settings** > **Labels and Sites**. The **Labels and Sites** page opens.
2. Set the toggle switch to **Sites**. The site management options are displayed.
3. Click **Convert Labels to Sites**. The **Confirm Conversion** pop-up window opens.
4. To download a CSV file with the list of labels configured in your setup, click **Download a File**. A CSV file with a list of all the labels in your setup is downloaded to your local directory.
5. Enter address, city, state, country, and ZIP code details for the labels that you want to convert to sites.

NOTE

In the CSV file, you must mandatorily enter the following details: address, city, state, and country.

6. Save the CSV file.
7. On the **Confirm Conversion** pop-up window, click **Browse** and select the CSV file with the list of labels to convert.
8. Click **Upload**.
9. Click **Convert**. The labels are converted to sites.

If the conversion process fails for some labels, Aruba Central generates and opens an Excel file showing a list of labels that could not be converted to sites. Verify the reason for the errors, update the CSV file, and re-upload the file.

NOTE

Aruba Central does not allow conversion of sites to labels. If the existing labels are converted to sites, you cannot revert these sites to labels.

When the existing labels are converted to sites, Aruba Central retains only the historical data for these labels. Aruba Central displays the historical data for these labels only in reports and on the monitoring dashboard.

Editing a Site

To modify site details, complete the following steps:

1. On the **Global Settings** > **Labels and Sites** > **Sites** page, select the site to edit.
2. Click the edit icon.
3. Modify the site information and click **Update**.

Deleting a Site

To delete a site, complete the following steps:

1. On the **Global Settings** > **Labels and Sites** > **Labels** page, select the site to delete.
2. Click the delete icon.
3. Confirm deletion.

Managing Labels

Labels are tags attached to a device provisioned in the network. Labels determine the ownership, departments, and functions of the devices. You can use labels for creating a logical set of devices and use these labels as filters when monitoring devices and generating reports.

For example, consider an Instant AP labeled as **Building 25** and **Lobby**. These tags identify the location of the Instant AP within the enterprise campus or a building. The Instant APs in other buildings within the same campus can also be tagged as **Lobby**. To filter and monitor Instant APs in the lobbies of all the campus buildings, you can tag all the Instant APs in a lobby with the label **Lobby**.

Device Classification

The devices can also be classified using **Groups** and **Sites**.

- The group classification can be used for role-based access to a device, while labels can be used for tagging a device to a location or a specific area at a physical site. However, if a device is already assigned to a group and has a label associated with it, it is classified based on both groups and labels.

- The site classification is used for logically grouping devices deployed at a given physical location. You can also convert labels to sites.

Labels Page

The **Labels** page in the UI allows you to create labels, view a list of labels, and assign devices to labels. The page includes two tables. The table on the left lists the labels, whereas the table on the right lists the devices. These tables provide the following information:

Table 14: *Labels*

Name	Contents of the Table
Labels	This table displays a list of labels configured in Aruba Central. It provides the following information: ■ Name of the label ■ Number of devices assigned to a label The table also includes the following sorting options to reset the table view on the right: ■ **All Devices**—Displays all the devices provisioned in Aruba Central. ■ **Unassigned**—Displays the list of devices that are not assigned to any label.
Devices	This table displays a list of devices provisioned in Aruba Central. It provides the following information about the devices: ■ Name—Name of the device ■ Group—Group to which the device is assigned ■ Type—Type of the device ■ Labels—Number of labels assigned to a device

Creating a Label

To create a label, complete the following steps:

1. From the app selector, click **Global Settings**.
2. Click **Labels and Sites**. The **Labels and Sites** page opens.
3. Ensure that the **Label** option is enabled.
4. To add a new label, click **(+) Add Label**. The **Create New Label** pop-up window opens.
5. Enter a name for the label.
6. Click **Add**. The new label is added to the **All Labels** table.

Assigning a Device to a Label

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

1. On the **Global Settings** > **Labels and Sites** > **Labels** page, locate the label to which you want to assign a device.
2. 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.
3. Select **Unassigned**. The list of devices that are not assigned to any label is displayed.
4. Select one or several devices from the list of devices.
5. Drag and drop the selected devices to a specific label. A pop-up window asking you to confirm the label assignment opens.
6. Click **Yes**.

NOTE

Aruba Central allows you to assign up to five label tags per device.

Detaching a Device from a Label

To remove a label assigned to a device, complete the following steps:

1. On the **Global Settings** > **Labels and Sites** > **Labels** page, select the device from the table on the right.
2. Click the delete icon.
3. To detach labels from the multiple devices at once, select the devices, and click **Batch Remove Labels**.
4. Confirm deletion.

Editing a Label

To edit a label, complete the following steps:

1. On the **Global Settings** > **Labels and Sites** > **Labels** page, select the label to edit.
2. Click the edit icon.
3. Edit the label and click **Update**.

Deleting a Label

To delete one or several labels, complete the following steps:

1. On the **Global Settings** > **Labels and Sites** > **Labels** page, select the label to delete.
2. Click the delete icon.
3. Confirm deletion.

Using Groups for Device Configuration and Management

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 a primary configuration element that functions as a container for device management, monitoring, and maintenance. Groups enable administrators to manage devices efficiently by using either a UI-based configuration workflow or CLI-based configuration template.

Groups provide the following functions and benefits:

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

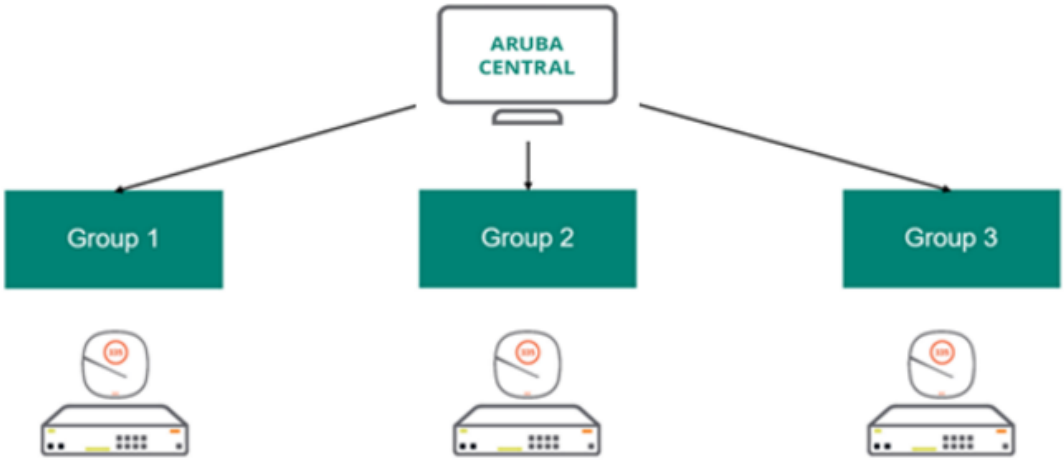
NOTE

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

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

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

Figure 7 *Group Deployment*



Group Operations

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

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

Group Configuration Modes

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

- UI-based configuration method—For device groups that use UI-based workflows, Aruba Central provides a set of UI menu options. You can use these UI menu options to configure devices in a group. You can also secure the UI-based device groups with a password and thus restrict user access.
- Template-based configuration method—For device groups that use a template-based workflow, Aruba Central allows you to manage devices using configuration templates. A device configuration template includes a set of CLI commands and variable definitions that can be applied to all other devices deployed in a group.

If your site or store has different types of devices, such as the Aruba Instant AP, Switch, and Gateways, and you want to manage these devices using different configuration methods, that is, either using the UI or template-based workflows, you can create a single group and define a configuration method to use for each type of device. This allows you to use a single group for both UI and template based configuration and eliminates the need for creating separate groups for each configuration method.

For example, you can create a group with the name **Group1** and within this group, you can enable template-based configuration method for switches and UI-based configuration method for Instant APs and Gateways. Aruba Central identifies both these groups under a single name (**Group1**). If a device type in the group is marked for template-based configuration method, the group name is prefixed with **TG** prefix is added (**TG Group1**. You can use **Group1** as the group ID for workflows such as user management, monitoring, reports, and audit trail.

When you add Instant APs, Gateways, and switches to a group, Aruba Central groups these devices based on the configuration method you chose for the device type, and displays relevant workflows when you try to access any of the following configuration menu containers:

- **Wireless Management** for APs
- **Wired Management** for switches
- **Gateway Management** for Aruba Gateways

For information on how to create a group, see Creating a Group on page 76.

Default Groups and Unprovisioned Devices

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

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

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

Best Practices and Recommendations

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

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

Working with Groups

See the following topics for detailed information and step-by-step instructions on how to manage groups and provision devices assigned to a group:

- Managing Groups
- Provisioning Devices Using UI-based Workflows
- Provisioning Devices Using Configuration Templates

Managing Groups

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

This section describes the following topics:

Creating a Group

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

Aruba Central allows you to create single group with different configuration methods defined for each device type. For example, you can create a group with the name **Group1** and within this group, you can enable template-based configuration method for switches and UI-based configuration method for Instant APs and Gateways. Aruba Central identifies both these groups under a single name (**Group1**). If a device type in the group is marked for template-based configuration method, the group name is prefixed with **TG** prefix is added (**TG Group1**. You can use **Group1** as the group ID for workflows such as user management, monitoring, reports, and audit trail.

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

To create a group:

1. Go to **Global Settings** > **Manage Groups**.
2. Click (+) **New Group**. The **Create New Group** pop-up window opens.
3. Enter a name for the group.

By default, Aruba Central enables template-based configuration method for switches and UI-workflow-based configuration method for Instant AP and Gateway.

4. To enable template-based configuration method for all device categories:
   - For Instant APs or Gateways, select the **IAP and Gateway** check box.
   - For Switches, ensure that **Switch** check box is selected. The **Switch** check box is enabled by default.
5. To enable UI-based configuration method on all device categories:
   a. For Instant APs and Gateways, ensure that the **IAP and Gateway** checkbox is cleared.
   b. For switches, clear the **Switch** checkbox.
   c. Assign a password. This password enables administrative access to the device interface.

d. Click **Add Group**.

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

Assigning Devices to Groups

To assign a device to a group from the **Global Setting** > **Device Inventory** page:

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

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

1. Click **Global Settings** > **Manage Groups**. The **Groups** page opens.
2. From the devices table on the right, select the device that you want to assign to a new group.
3. Drag and drop the device to the group to which you want to assign the device.

Viewing Groups and Associated Devices

To view the groups dashboard, complete the following steps:

1. Go to **Global Settings** > **Manage Groups**. The **Groups** page opens. The groups table on the left side of the page displays the following information:
   - **Group Name**—Name of the group.
   - **Devices**—Number of devices assigned to a group.
   - **All Connected Devices**—Total number of devices provisioned in Aruba Central. The devices table on right side of the page show all the devices provisioned in Aruba Central.
   - **Unassigned Devices**—Total number of devices that are yet to be assigned. The devices table on the right shows the devices are not assigned any group.
2. To view the devices assigned to a group, select the group from the table on the left. The devices table displays the following information:
   - **Name**—Name of the device.
   - **Location**—Physical location of the device.
   - **Type**—Type of the device such as Instant AP or Switch.
   - **Serial**—Serial number of the device.
   - **MAC address**—MAC address of the device.

Creating a New Group by Importing Configuration from a Device

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

1. On the **Groups** page, select the device.
2. Click **Import Configuration to New Group**. The **Import Configuration** pop-up window opens.
3. Enter a name for the group.
4. Configure a password for the group.
5. Click **Import Configuration**.

Cloning a Group

To clone a group, complete the following steps:

1. Click **Global Settings** > **Manage Groups**. The **Groups** page opens.
2. To create a clone of an existing group, select the group from the groups table, and then click the **Clone Selected Group** link.
3. Enter a name for the cloned group.
4. Click **Add Group**.

When you clone a group, Aruba Central also copies the configuration templates applied to the devices in the group.

Moving Devices between Groups

To move a device from one group to another group:

1. Click **Global Settings** > **Manage Groups**. The **Groups** page opens.
2. From the devices table on the right, select the device that you want to move.
3. Drag and drop the device to group to which you want to assign the device.
4. Click **Yes** when the system prompts you to confirm device movement.

The MSP does not support moving devices across different groups.

Configuring Device Groups

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

- Provisioning Devices Using UI-based Workflows on page 78
- Provisioning Devices Using Configuration Templates on page 83

Deleting a Group

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

To delete a group:

1. Click **Global Settings** > **Manage Groups**. The **Groups** page opens.
2. From list of groups, select the group that you want to delete.
3. Click the delete icon.
4. Confirm deletion.

Provisioning Devices Using UI-based Workflows

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

- Provisioning Instant APs using UI-based Configuration Method on page 79
- Provisioning Switches Using UI-based Configuration Method on page 80
- Provisioning Aruba Gateways Using UI-based Configuration Method on page 81

Provisioning Instant APs using UI-based Configuration Method

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

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

Aruba Central allows configuration operations at the following levels for a device group with Instant APs.

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

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

Table 15: *Instant AP Provisioning*

APs with Default Configuration	APs with Non-Default Configuration
If an Instant AP with factory default configuration joins Aruba Central, it is automatically assigned to the **default** group or an existing group with similar configuration settings. The administrators can perform any of the following actions: ■ Manually assign them to an existing group. ■ Create a new group.	If an Instant AP with non-default or custom configuration joins Aruba Central, it is automatically assigned to an **unprovisioned** group. The administrators can perform any of the following actions: ■ Create a new group for the device and preserve device configuration. ■ Move the device to an existing group and override the device configuration.

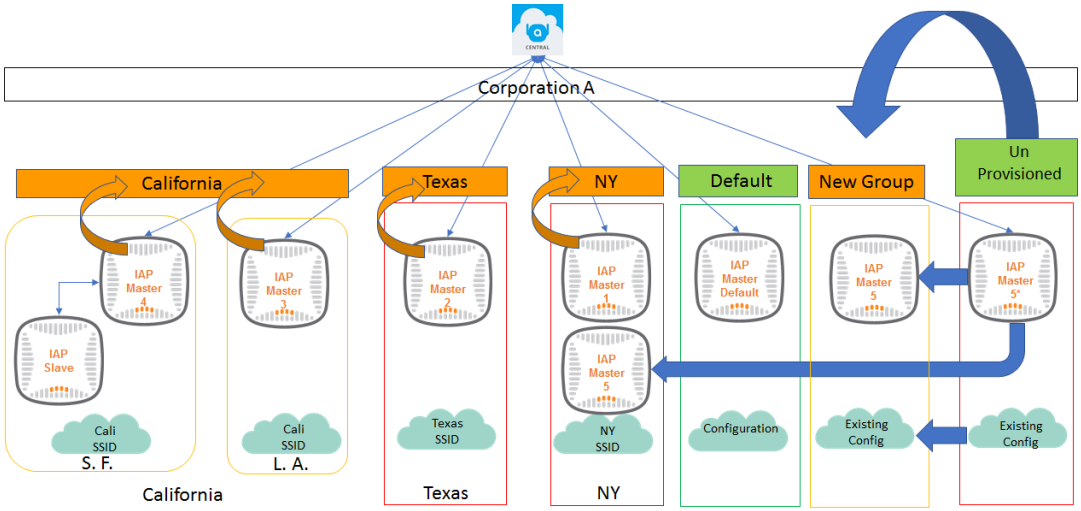
Ensure that the master Instant AP and the slave Instant APs are assigned to the same group. You must convert the slave Instant AP to a standalone AP in order to move the slave Instant AP to another group independently.

In the following illustration, the Instant APs from three different geographical locations are grouped under the California, Texas, and New York states. Each state has unique SSIDs and can support devices from multiple locations in a state. As shown in Figure 8, the California group has devices from different locations and has the same SSID, while devices in the other states/groups have different SSIDs.

When a device with the factory default configuration connects to Aruba Central, it is automatically assigned to the default group. If the device has custom configuration, it is marked as unprovisioned. If you want to

preserve the custom configuration, create a new group for the device. If you want to overwrite the custom configuration, you can assign the device to an existing group.

Figure 8 *Instant AP provisioning*



Configuration Steps

For more information on how to configure Instant APs using UI-based configuration workflows, see Deploying a Wireless Network Using Instant APs.

Configuration Overrides

To view local overrides and configuration errors, navigate to the **Wireless Management** > **Configuration Audit** page.

Provisioning Switches Using UI-based Configuration Method

Aruba Central allows switches to join UI groups only if the switches are running factory default configuration. Aruba Central assigns switches with factory default configuration to the **default** group.

The administrators can either move the switch to an existing group or create a new group.

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

NOTE

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

Aruba Central allows the following configuration operations at the following levels for switches in a UI group:

- **Per group configuration**— Aruba Central allows you to maintain unique configuration settings for each group. However, these settings are applied to all devices within that group. For example, all switches within a group can have common VLAN settings.
- **Per Device Configuration**—Although the Switches inherit group configuration, the users can maintain device-specific configuration, for example, ports or DHCP pools.

Configuration Steps

For more information on how to configure switches using UI-based configuration workflows, see Configuring or Viewing Switch Properties in UI Groups on page 363.

Configuration Overrides

To view local overrides and configuration errors, navigate to the **Wired Management** > **Configuration Audit** page.

Provisioning Aruba Gateways Using UI-based Configuration Method

For SD-Branch deployments with Aruba Gateways, the following recommendations apply:

- Combine Branch Gateways of identical characteristics and configuration requirements under a single group.
- Create groups according to your branch requirements.
  - You can create separate groups for the small, medium, and large sized branches.
  - You can also create separate groups for the branch sites in different geographical locations; for example, East Coast and West Coast branch sites. If these groups have similar characteristics with minor differences, you can create the first group and then clone it.
  - You can use either a single group for all their devices or deploy devices in multiple groups. For example, you can deploy 7008 controllers and Aruba 2930F Switch Series with 24 ports in a single group for every branch.
  - You can also deploy 7005 controller and Aruba 2930F Switch Series with 24 ports in one group and provision 7008 controller with Aruba 2930F Switch Series with 48 ports in another group.

Important Points to Note

- The groups in Aruba Central are not device-specific, however, Aruba recommends that you use the following guidelines for provisioning SD-WAN Gateways.
  - Assign Branch Gateways and VPN Concentrators to separate groups. Because the configuration requirements for Branch Gateways and VPN Concentrators are different, the Branch Gateways and VPN Concentrators must be assigned to different groups.
  - Ensure that the configuration group for SD-WAN Gateways consists of the same type of devices. For example, Branch Gateways assigned to a group must have the same number of ports.
- Before assigning SD-WAN Gateways to groups, you must set the device persona or role as Branch Gateway or VPN Concentrator.

Example

The following figures shows a few sample group deployment scenarios for Aruba Branch Gateways and VPN Concentrators:

Figure 9 *Branch Gateway Groups*

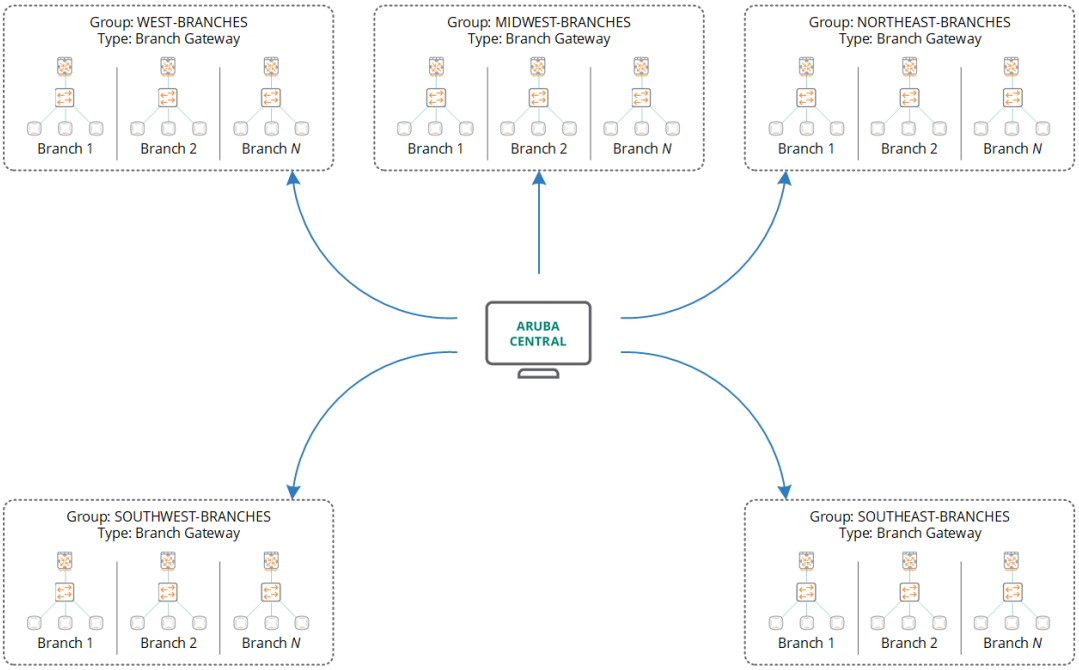
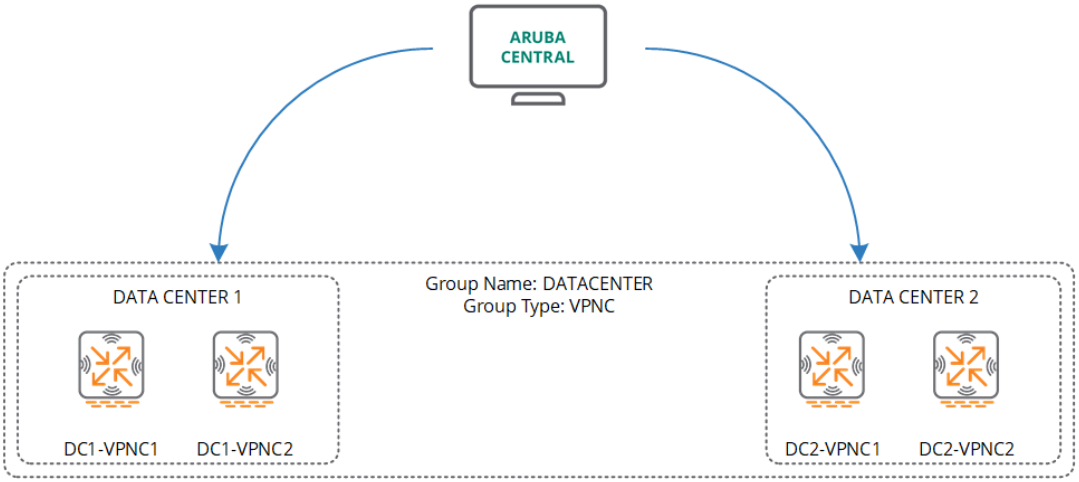


Figure 10 *VPN Concentrator Groups*



Configuration Steps

For more information on how to configure Aruba using UI-based configuration workflows, see the *SD-Branch Configuration* section in *Aruba Central Help Center*.

Configuration Overrides

To view local overrides and configuration errors, navigate to the **Gateway Management** > **Configuration Audit** page.

Provisioning Devices Using Configuration Templates

Aruba Central allows you to provision devices using UI-based or template-based configuration method. If you have groups with template-based configuration enabled, you can create a template with a common set of CLI scripts, configuration commands, and variables. Using templates, you can apply CLI-based configuration parameters to multiple devices in a group.

If the template-based configuration method is enabled for a group, the UI configuration wizards for the devices in that group are disabled.

Creating a Group with Template-Based Configuration Method

To create a template group, complete the following steps:

1. From the app selector, select the **Global Settings** app.
2. Click **Manage Groups**.
3. Click **(+) New Group**. The **Create New Group** pop-up window opens.
4. Select the device type for which you want to create a template group.
5. Click **Save**.

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 Instant APs Using Templates on page 344
- Using Configuration Templates for Switch Management on page 356
- Managing Variable Files on page 358

Editing a Template

To edit or delete a template, select the template row and click the edit or delete icon, respectively.

Managing Variable Files

Aruba Central allows you to configure multiple devices in bulk using templates. However, in some cases, the configuration parameters may vary per device. To address this, Aruba Central identifies some customizable CLI parameters as variables and allows you to modify the definitions for these variables as per your requirements.

You can download a sample file with variables for a template group or for the devices deployed in a template group, update the variable definitions, upload the file with the customized definitions, and apply these configuration changes in bulk.

Downloading Sample Variables File

The sample variables file includes a set of sample variables that the users can customize. You can download the sample variables file in the JSON or CSV format.

To download a sample variables file:

1. Go to **Variables**.

- For switches—Go to **Wired Management** > **Variables**.
- For Instant APs—Go to **Wireless Management** > **Variables**.
- For Gateways—Go to **Gateway Management** > **Variables**.

2. Download the sample variables file.
- To download a sample variables file for the device group, select a template group.
- To download a sample variables file for a device, select the device from the filter bar.

3. Select any of the following format:
- JSON—shows the file JSON format.
- CSV—Shows the variables in different columns.

4. Click **Download Sample Variables File**. The sample variables file is saved to your local directory.

Modifying a Variable File

The CSV file includes the following columns for which the variable definitions are mandatory:

- **_sys_serial**—For serial number of the device
- **_sys_lan_mac**—For MAC address of the device
- **modified**—To indicate the modification status of the device. The value for this column is set to N in the sample variables file. When you edit a variable definition, set the **modified** column to **Y** to allow Aruba Central to parse the modified definition.

Predefined Variables

The system defined variables in the sample variables files are indicated with **_sys** prefix.

Table 16shows a list of predefined variables for switches.

Table 16: *Predefined Variables Example*

Variable Name	Description	Variable Value
_sys_gateway	Populates gateway IP address.	10.22.159.1
_sys_hostname	Maintains unique host name.	HP-2920-48G-POEP
_sys_ip_address	Indicates the IP address of the device.	10.22.159.201
_sys_module_command	Populates module lines	module 1 type j9729a
_sys_netmask	Netmask of the device.	255.255.255.0
_sys_oobm_command	Represents Out of Band Management (OOBM) block.	oobm ip address dhcp-bootp exit
_sys_snmpv3_engineid	Populates engine ID.	00:00:00:0b:00:00:5c:b9:01:22:4c:00
_sys_stack_command	Represents stack block	stacking member 1 type "J9729A" mac-address 5cb901-224c00 exit

Variable Name	Description	Variable Value
_sys_template_header	Represents the first two lines of the configuration file. Ensure that this variable is the first line in the template.	; J9729A Configuration Editor; Created on release #WB.16.03.0003+ ; Ver #0f:3f.f3.b8.ee.34.79.3c.29.eb.9f.fc.f3.ff.37.ef:91
_sys_use_dhcp	Indicates DHCP status (true or false) of VLAN 1	0
_sys_vlan_1_untag_command	Indicates untagged ports of VLAN 1	1-28,A1-A2
_sys_vlan_1_tag_command	Indicates tagged ports of VLAN 1	28-48

The **_sys_template_header_** and **_sys_snmpv3 engineid** are mandatory variables that must have the values populated, irrespective of their use in the template. If there is no value set for these variables, Aruba Central re-imports the values for these mandatory variables when it processes the running configuration of the device.

For Instant APs, the sample variables file includes the **_sys_allowed_ap** variable for which you can specify a value to allow new APs to join the Instant AP cluster.

Important Points to Note

The following conditions apply to the variable files:

- The variable names must be on the left side of condition and its value must be defined on the right side. For example, %if var=100% is supported and %if 100=var% is not supported.
- The < or <= or > or >= operators should have only numeric integer value on the right side. The variables used in these 4 operations are compared as integer after flooring. For example, if any float value is set as %if dpi_value > 2.8%, it is converted as %if dpi_value > 2 for comparison.
- The variable names should not include white space, and the **&** and **%** special characters. The variable names must match regular expression [a-zA-Z0-9_]. If the variables values with **%** are defined, ensure that the variable is surrounded by space. For example, *wlan ssid-profile %ssid_name%*.
- The first character of the variable name must be an alphabet. Numeric values are not accepted.
- The values defined for the variable must not include spaces. If quotes are required, they must be included as part of the variable value. For example, if the intended variable name is *wlan ssid-profile "emp ssid"*, then the recommended format for the syntax is "*wlan ssid-profile %ssid_name%*" and variable as *"ssid_name": "\"emp ssid\""*.
- If the configuration text has the percentage sign **%** in it—for example, **"url "/portal/scope.cust-5001098/Splash%20Profile%201/capture"**—Aruba Central treats it as a variable when you save the template. To allow the use of percentage **%** as an escape character, use **\"** in the variable definition as shown in the following example:

  Template text

  ```
  wlan external-captive-portal "Splash Profile 1_#guest#_"
  server naw1.cloudguest.central.arubanetworks.com
  port 443
  url %url%
  ```

  Variable

  ```
  "url": "\"/portal/scope.cust-5001098/Splash%20Profile%201/capture\""
  ```

- Aruba Central supports adding multiple lines of variables in Instant AP configuration templates. If you want to add multiple lines of variables, you must add the `HAS_MULTILINE_VARIABLE` directive at the beginning of the template.

  Example

  ```
  #define HAS_MULTILINE_VARIABLE 1
  %if allowed_aps%
  %allowed_aps%
  %endif%
  ```

  Variable

  ```
  "allowed_aps": "allowed-ap 24:de:c6:cb:76:4e\n allowed-ap ac:a3:1e:c5:db:d8\n allowed-ap
  84:d4:7e:c4:8f:2c"
  ```

For Instant APs, you can configure a variable file with a set of values defined for a master AP in the network. When the variable file is uploaded, the configuration changes are applied to all Instant AP devices in the cluster.

Examples

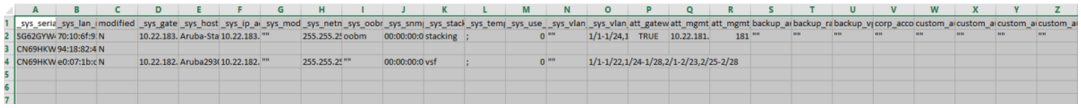
The following example shows the contents of a variable file in the JSON format for Instant APs:

```
{
"CK0036968": {
"_sys_serial": "CK0036968",
"ssid": "s1",
"_sys_lan_mac": "ac:a3:1e:c5:db:7a",
"vc_name": "test_config_CK0036968",
"org": "Uber_org_test",
"vc_dns_ip":"22.22.22.22",
"zonename": "Uber_1",
"uplinkvlan": "0",
"swarmmode": "cluster",
"md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
"hostname": "Uber_1"
},
"CJ0219729": {
"_sys_serial": "CJ0219729",
"ssid": "s1",
"_sys_lan_mac": "ac:a3:1e:cb:04:92",
"vc_name": "test_config_CK0036968",
"org": "Uber_org_test",
"vc_dns_ip":"22.22.22.22",
"zonename": "Uber_1",
"uplinkvlan": "0",
"swarmmode": "cluster",
"md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
"hostname": "Uber_2"
},
"CK0112486": {
"_sys_serial": "CK0112486",
"ssid": "s1",
"_sys_lan_mac": "ac:a3:1e:c8:29:76",
"vc_name": "test_config_CK0036968",
"org": "Uber_org_test",
"vc_dns_ip":"22.22.22.22",
"zonename": "Uber_1",
"uplinkvlan": "0",
"swarmmode": "cluster",
"md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
"hostname": "Uber_3"
},
```

```
"CT0779001": {
"_sys_serial": "CT0779001",
"ssid": "s1",
"_sys_lan_mac": "84:d4:7e:c5:c6:b0",
"vc_name": "test_config_CK0036968",
"org": "Uber_org_test",
"vc_dns_ip":"22.22.22.22",
"zonename": "Uber_1",
"uplinkvlan": "0",
"swarmmode": "cluster",
"md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
"hostname": "Uber_4"
},
"CM0640401": {
"_sys_serial": "CM0640401",
"ssid": "s1",
"_sys_lan_mac": "84:d4:7e:c4:8f:2c",
"vc_name": "test_config_CK0036968",
"org": "Uber_org_test",
"vc_dns_ip":"22.22.22.22",
"zonename": "Uber_1",
"uplinkvlan": "0",
"swarmmode": "cluster",
"md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
"hostname": "Uber_6"
},
"CK0037015": {
"_sys_serial": "CK0037015",
"ssid": "s1",
"_sys_lan_mac": "ac:a3:1e:c5:db:d8",
"vc_name": "test_config_CK0036968",
"org": "Uber_org_test",
"vc_dns_ip":"22.22.22.22",
"zonename": "Uber_1",
"uplinkvlan": "0",
"swarmmode": "cluster",
"md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
"hostname": "Uber_7"
},
"CK0324517": {
"_sys_serial": "CK0324517",
"ssid": "s1",
"_sys_lan_mac": "f0:5c:19:c0:71:24",
"vc_name": "test_config_CK0036968",
"org": "Uber_org_test",
"vc_dns_ip":"22.22.22.22",
"zonename": "Uber_1",
"uplinkvlan": "0",
"swarmmode": "cluster",
"md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
"hostname": "Uber_8"
}
}
```


Figure 11 shows a sample variables file in the CSV format:

Figure 11 *Variables File in the CSV Format*



Uploading Variable Files

To upload a variable file, complete the following steps:

1. Ensure that the **_sys_serial** and **_sys_lan_mac** variables are defined with the serial number and MAC address of the devices, respectively.
2. Navigate to the **Variables** page:
   - For switches—Go to **Wired Management** > **Variables**.
   - For Instant APs—Go to **Wireless Management** > **Variables**.
   - For Gateways—Go to **Gateway Management** > **Variables**.
3. Click **Upload Variables File** and select the variable file to upload.
4. Click **Open**. The content of the variable file is displayed in the **Variables** table.
5. To search for a variable, specify a search term and click the **Search** icon.
6. To download variable file with device-specific definitions, click the download icon in the **Variables** table.

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 template-based configuration method.

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. From the group selector, select a group that uses template-based configuration method.
2. Based on the device type, navigate to the appropriate configuration container:

a. For Instant AP templates, go to **Wireless Management** > **Configuration Audit**.

b. For Switch templates, go to **Wired Management** > **Configuration Audit**.

c. For Aruba Gateway templates, go **to Gateway Management** > **Configuration Audit**.

3. Click **New Configuration Backup** under **Configuration Backup and Restore**. The **Create New Backup** pop-up box opens.
4. Enter a name for **Backup Name**.
5. Select **Do Not Delete** if you do not want the backed up file to be deleted by new backup after a 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** pop-up window opens.
7. Read through the information. 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. Click the **Manage Backup** option.
2. Download the backup and untar the downloaded file. The following example shows the tree structure of a typical backup download.

```
<backup-name_timestamp>
├── templates
│   ├──<hppctemplate1.tmpl>
│   ├──<iaptemplate1.tmpl>
│   ├──template_meta.json
└── variables
    ├──HPPC_variables_1.json
    ├──IAP_variables_1.json
    └──devices_meta.json
```

The variables are stored per device type, that is, 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. From the group selector, select a group that uses template-based configuration method.
2. Go to **Configuration Audit** page. The **Configuration Audit** page can be accessed from the **Wireless Management**, **Wired Management**, or **Gateway Management** menu.
3. Click **Restore Configuration Backup** under **Configuration Backup and Restore**. The **Restore from Backup** pop-up window opens.
4. Select the backup name that you want to restore from **Backup Name** drop-down list.
5. Select a 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, Aruba IAP, 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** pop-up box opens.
7. Read the instructions. Then, 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. From the group selector, select a group that uses template-based configuration method.
2. Go to the **Configuration Audit** page. The **Configuration Audit** page can be accessed from the **Wireless Management**, **Wired Management**, or **Gateway Management** menu.
3. Click **Manage Backup** under **Configuration Backup and Restore.** The **Last <#> Backups** pop-up window opens.
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** pop-up box 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**. To get the error log for a restore error event, click **Last Restore Error Log**.

Backing Up and Restoring Templates and Variables Using APIs

Aruba Central supports the following NB APIs for the backup and restore feature:

- Create new configuration backup for group
  [POST] /configuration/v1/groups/snapshot/{group}
- Create backups for multiple groups associated with a customer account
  [POST]/configuration/v1/groups/snapshot/create_backups

Aruba Central creates a backup of configuration template and variables only for the groups included in the API request payload. You can use the include or exclude parameters to create backups for specific list of groups.

The following table describes the API response based on the inputs provided in the parameters:

Table 17: *API Functionality for Backup Creation*

include_groups	exclude_groups	API Functionality
No groups specified	No groups specified	Raises an exception to either include or exclude groups.
group names	group names	Raises an exception to include or exclude groups.
[]	No groups specified	Raises an exception to provide valid values for the include groups parameter.
group names	No groups specified	Includes selected groups for the backup operation.
No groups specified	ALL_GROUPS	Creates a backup for all groups.
No groups specified	group names	Does not create backup for the excluded groups.

- Restore a backed up version of the configuration template for all devices in a group:
  [POST] /configuration/v1/groups/<group_name>/snapshots/<snapshot_name>/restore
  The API restores a specific version of the backup snapshot for the group specified in the API request.
- Restore a backed up version of the configuration template by device type:
  The **[POST]/configuration/v1/groups/{group}/snapshots/{snapshot}/restore** API provides you an option to restore the configuration by device type. By selecting a specific device type, you can control the order in which the configuration is restored by device type. This minimizes the impact of the configuration restore activity on the network.

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** menu option is available for all types of device configuration containers, such as **Wireless Management** for Aruba WLAN APs, **Wired Management** for Aruba Switches, and **Gateway Management** for Aruba Gateways.

Accessing the Configuration Audit Page

To access the **Configuration Audit** page:

- For Instant APs:

a. Click **Wireless Management**.

b. From the group selection filter, select a group or device.

c. Click **Configuration Audit**.

- For Aruba switches:

a. Click **Wired Management**.

b. From the group selection filter, select a group or device.

c. Click **Configuration Audit**.

- For Aruba Gateways:

a. Click **Gateway Management**.

b. From the group selection filter, select a group or a device.

c. Click **Configuration Audit**.

Applying Configuration Changes

Aruba Central now supports a two-staged configuration commit workflow for Instant AP and switches.

The **Auto Commit State** section in the **Configuration Audit** page allows administrators to switch their preference for committing configuration changes to devices.

- When **Auto Commit State** is set to **ON**, the configuration changes are applied instantly to the device.
- When **Auto Commit State** is set to **OFF**, the administrators can build a candidate configuration, save it on cloud, review it, and then push the configuration changes to the managed devices for activation.

When a device is moved from one group to another, Aruba Central resets the **Auto Commit State** for the device. The device inherits the **Auto Commit State** settings of the group to which the device is moved.

Auto Commit Workflow

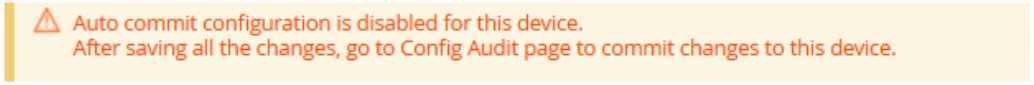
To enable Aruba Central to push configuration changes instantly, complete the following steps:

1. Select a device and navigate to the appropriate configuration app (**Wireless Management** for Instant APs and **Wired Management** for switches).
2. Click **Configuration Audit**.
3. Ensure that the **Auto Commit State** is set to **ON**.
4. 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. Aruba Central automatically pushes the configuration changes to the devices.
5. Go to **Configuration Audit** and click Failed Changes to view configuration errors if any.

Manual Commit Workflow

To build configuration and review it before applying the changes to devices:

1. Select a device and navigate to the appropriate configuration app (**Wireless Management** for Instant APs and **Wired Management** for switches).
2. Click **Configuration Audit**.
3. Ensure that the **Auto Commit State** is set to **OFF**.
4. 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 changes, Aruba Central displays the following message:



5. Go to **Configuration Audit** and click **Failed/PendingChanges**.
6. Click the **Failed Push** tab and review the configuration.
7. Click **Close**.
8. If you want to push the configuration to devices, click **Commit Now**.

Aruba Central does not support the two-staged configuration commit workflow only for 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.

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 page include:

- **Failed/Pending Changes**
  - **Failed Changes**—The devices managed by Aruba Central receive the configuration changes from Aruba Central. Occasionally, a managed device may fail to receive a configuration change from Aruba Central. The **Failed changes** tile allows you to view a list of the configruation push errors.
  - **Pending Changes**—With the Auto Commit feature is disabled, Aruba Central allows you to build your configuration changes, save it, and review it before committing the configuration changes. The **Failed/Pending Changes** tile displays the configuration that is not yet pushed to the devices.
- **Local Overrides**—In Aruba Central, devices are assigned to groups that serve as the primary configuration elements. Occasionally, based on the network provisioning requirements, the administrators may need to modify the configuration of a specific device in a group. As these modifications override the configuration settings that the device has inherited from the group, Aruba Central marks these changes as local overrides.
- **Configuration Conflicts**—For all connected devices in Aruba Central, when a new feature is introduced and applied to the device, one of two subsequent scenarios might ensue. The new feature might not cause any conflict with the existing configuration and no further action is required from the administrator. However, if the new feature causes a conflict with the existing configuration in the device, the feature is disabled automatically and no further configuration is pushed for that device. The **Configuration Audit** page displays a configuration conflict error. For each device under conflict, click the **Manage Configuration Conflict** link. In the subsequent **Configuration Conflict** page, enable the checkbox against each conflict and type REMOVE to remove the conflict. After you resolve all conflicts, you are able to push group configuration to the device.
- **Template Errors**—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 devices fails. Aruba Central records such failed instances as template errors and displays these errors on the **Configuration Audit** page.
- **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)

On selecting a template group from the filter bar, the **Configuration Audit** page displays the options listed in Table 18:

Table 18: *Configuration Audit Status for a Template Group*

Data Pane Content	Description
Template Errors	Displays the number of template errors for the selected template group. 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 To view a complete list of errors, click **View Template Errors**. The **Template Errors** pop-up window allows you to view and resolve the template errors issues if any.
Failed/Pending Changes	Displays the number configuration sync errors for the selected template group. To view and resolve the configuration sync errors, click the **Failed Config Difference** link.
Configuration Backup and Restore	Allows you to create a backup of templates and variables applied to the devices in the template group. For more information, see Viewing Configuration Status.
All Devices	The **All Devices** table provides the following device information for the selected group: ■ **Name**—The name of the device. ■ **Type**—The type of the device. ■ **Auto Commit**—Enabled or disabled status of the **Auto Commit** feature. ■ **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)

On selecting a device that is provisioned in a template group, the **Configuration Audit** page displays the options listed in Table 18:

Table 19: *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**.
Failed Changes	Displays configuration sync errors for the selected device. To view and resolve the configuration sync errors, click the **Failed/Pending Config Changes** link.
Config Comparison Tool	Allows you to view the difference between the current configuration and the configuration that is yet to be pushed to the device (pending configuration). To view the current and pending configuration changes side by side, click **View**.

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

On selecting a UI group, the **Configuration Audit** page displays the options listed in Table 18.

Table 20: *Configuration Audit Status for a UI Group*

Data Pane Content	Description
Failed Changes	Displays the number of devices with configuration sync errors for the selected UI group. To view and resolve the configuration sync errors, click the **Failed Config Difference** link.
Local Overrides	Displays the number of devices with local overrides. To view a complete list of overrides, click the **Manage Local Overrides** link. The **Local Overrides** pop-up window opens. ■ To preserve the overrides, click **Close**. ■ To remove the overrides, select the group name with local override, click **Remove** and click **OK**.
All Devices	The **All Devices** table provides the following device information for the selected group: ■ **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. ■ **Config Sync** / **Config Status**—Indicator showing configuration sync errors. ■ **Local Override**—Indicator showing configuration overrides for the devices deployed in UI groups. **NOTE:** The **MAC Address**, **IP Address**, **Config Status**, **Site**, and **Type** columns are available only for groups in which Aruba Gateways are provisioned (**Gateway Management** > **Configuration Audit**).

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

On selecting a device assigned to a UI group, the **Configuration Audit** page displays the options listed in Table 18.

Table 21: *Configuration Audit Status for a Device Assigned to a UI Group*

Data Pane Content	Description
Failed Changes	Displays the number of devices with configuration sync errors for the selected device. To view and resolve the configuration sync errors, click the **Failed Config Difference** link.
Local Overrides	Displays the number of local overrides. To view a complete list of overrides, click the **Manage Local Overrides** link. The **Local Overrides** pop-up window opens. ■ To preserve the overrides, click **Close**. ■ To remove the overrides, click **Remove**, and click **OK**.

Backing up and Restoring Configuration Templates

Aruba Central allows you to back up configuration templates assigned to the devices deployed in a template group. The **Configuration Audit** pages for Instant AP, Switch, and Gateway configuration containers allow

you to create and manage backed up files and restore these files when required. For more information, see Backing Up and Restoring Configuration Templates.

Connecting Devices to Aruba Central

Aruba devices support automatic provisioning, also known as ZTP. In other words, Aruba devices can download provisioning parameters from Aruba Activate and connect to their management entity once they are powered on and connected to the network.

Although most of the communication between devices on the remote site and Aruba Central server in the cloud is carried out through HTTPS (TCP 443), you may want to open the following ports for devices to communicate over network firewall.

Domain names for Aruba Central Portal Access

Table 22: *Domain Names and URLs for Aruba Central Portal Access*

Region	Domain Name	Protocol
US-West-A (US-1 cluster zone)	portal.central.arubanetworks.com	HTTPS TCP port 443
US-West-B (US-2 cluster zone)	portal-prod2.central.arubanetworks.com	HTTPS TCP port 443
Europe	portal-eu.central.arubanetworks.com	HTTPS TCP port 443
APAC	portal-apac.central.arubanetworks.com	HTTPS TCP port 443
China	portal.central.arubanetworks.com.cn	HTTPS TCP port 443
Canada	portal-ca.central.arubanetworks.com	HTTPS TCP port 443

Domain Names for Device Communication with Aruba Central

Table 23: *Domain Names for Device Communication with Aruba Central*

Region	Aruba Central URL	URL for Device Connectivity	Protocol
US-West-A (US-1 cluster zone)	app.central.arubanetworks.com	app1.central.arubanetworks.com	HTTPS TCP port 443
US-West-B (US-2 cluster zone)	app-prod2.central.arubanetworks.com	device-prod2.central.arubanetworks.com	HTTPS TCP port 443
Europe	app2-eu.central.arubanetworks.com	device-eu.central.arubanetworks.com	HTTPS TCP port 443
APAC	app2-ap.central.arubanetworks.com	app1-ap.central.arubanetworks.com	HTTPS

Region	Aruba Central URL	URL for Device Connectivity	Protocol
			TCP port 443
China	app.central.arubanetworks.com.cn	device.central.arubanetworks.com.cn	HTTPS TCP port 443
Canada	app-ca.central.arubanetworks.com	device-ca.central.arubanetworks.com	HTTPS TCP port 443

Domain Names for Device Communication with Aruba Activate

Table 24: *Domain Names for Device Communication with Aruba Activate*

Domain Name	Protocol
device.arubanetworks.com	HTTPS TCP port 443

Cloud Guest Server Domains for Guest Access Service

Table 25: *Domain Names for Cloud Guest Server Access*

Region	Domain Name	Protocol
US-West-A (US-1 cluster zone)	nae1.cloudguest.central.arubanetworks.com naw1.cloudguest.central.arubanetworks.com	TCP port 443
US-West-B (US-2 cluster zone)	naw2.cloudguest.central.arubanetworks.com	TCP port 443
Europe	euw1.cloudguest.central.arubanetworks.com	TCP port 443
APAC	asw1-m.cloudguest.central.arubanetworks.com	TCP port 443

Domain Names for OpenFlow

Table 26: *Domain Names for OpenFlow*

Region	Domain Name
APAC	https://app2-ap-ofc.central.arubanetworks.com
US-West A	https://app2-ofc.central.arubanetworks.com
US-West B	https://ofc-prod2.central.arubanetworks.com
Canada	https://ofc-ca.central.arubanetworks.com
Europe	https://app2-eu-ofc.central.arubanetworks.com
China	https://ofc.central.arubanetworks.com.cn

Other Domain Names

Table 27: *Other Domain Names*

Domain Name	Protocol	Description
sso.arubanetworks.com	TCP port 443	To allow users to access their accounts on the internal server.
internal.central.arubanetworks.com internal2.central.arubanetworks.com	TCP port 443	To allow users to access the Aruba Central Internal portal.
pool.ntp.org	UDP port 123	To update the internal clock on and configure time zone when a factory default device comes up. By default, the Aruba devices contact **pool.ntp.org** and use NTP to synchronize their system clocks.
activate.arubanetworks.com	TCP port 443	To configure provisioning rules in Activate.
images.arubanetworks.com	TCP port 80	To access the server that hosts software images available for upgrading devices.
http://h30326.www3.hpe.com	TCP port 80	To access the Aruba switch software images. To view the URL for software updates, use the **show activate software-update** command.
d2vxf1j0rhr3p0.cloudfront.net	TCP port 80	To access the CloudFront server for locating Instant AP software images.
rcs-m.central.arubanetworks.com (For all other regions) central-eu-rcs.central.arubanetworks.com (For Europe region)	TCP port 443	To access a device console through SSH.
cloud.arubanetworks.com	TCP port 80	To open the Aruba Central evaluation sign-up page.
aruba.brightcloud.com	TCP port 443	To enable devices to access the Webroot Brightcloud server for application, application categories, and website content classification.
bcap15-dualstack.brightcloud.com	TCP port 443	To allow Aruba devices to look up the Webroot Brightcloud server for Website categories.
api-dualstack.bcti.brightcloud.com	TCP port 443	To allow Aruba devices to access the IP Reputation and IP Geolocation service on the Webroot Brightcloud server.
database-dualstack.brightcloud.com	TCP port 443	To allow Aruba devices to download the website classification database from the Webroot Brightcloud server.

When configuring ACLs to allow traffic over a network firewall, use the domain names instead of the IP addresses.

For Branch Gateways to set up IPsec tunnel with the VPN concentrators, the UDP 4500 port must be open.

Connecting Instant APs to Aruba Central

To bring up Instant APs in Aruba Central:

1. Connect the Instant AP to a provisioning network.
2. Ensure that Instant AP is operational and is connected to the Internet.
3. Ensure that the Instant AP has a valid DNS server address either through DHCP or static IP configuration.
4. Ensure that NTP server is running and Instant AP system clock is configured.

Connecting Aruba Switches to Aruba Central

Note the following points about automatic provisioning of switches:

Pre-configured switches can now join Aruba Central. You can also import configuration from these switches to generate a template. For more information, see Creating a Configuration Template.

If the switches ship with a version lower than the minimum supported firmware version, a factory reset may be required, so that the switch can initiate a connection to Aruba Central. For information, on the minimum firmware versions supported on the switches, see Supported Switch Platforms on page 28.

During Zero Touch Provisioning, the Aruba switches can join Aruba Central only if they are running the factory default configuration, and have a valid IP address and DNS settings from a DHCP server.

The provisioning of the Aruba Mobility Access Switch fails when the provisioning process is interrupted during the initial booting and if the switch has a static IP address with no DNS server configured.

Connecting SD-WAN 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). By default, ZTP is enabled on all ports except for 0/0/1. All these ZTP ports are assigned to VLAN 4094.

To automatically provision the Gateways:

1. Connect your SD-WAN 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.
   - If the device is running a software version that does not have the SD-WAN image, the devices are automatically upgraded to a supported SD-WAN software version.
3. Observe the LED indicators. Table 28 describes the LED behavior.

Table 28: *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*.

Uploading Certificates

By default, Aruba Central includes a self-signed certificate that is available on the **Global Settings** > **Certificates** page. The default certificate is not signed by a root CA. For devices to validate and authorize Aruba Central, administrators must upload a valid certificate signed by the root CAs.

Aruba devices use digital certificates for authenticating a client's access to user-centric network services. Most devices such as controllers and Instant APs include a server certificate by default for captive portal server authentication. However, Aruba recommends that you replace the default certificate with a custom certificate issued for your site or domain by a trusted CA. Certificates can be stored locally on the devices and used for validating device or user identity during authentication.

Aruba Central-managed devices such as Instant AP and switches support the following root CA certificates:

Instant APs	Switches
■ AddTrust ■ GeoTrust ■ VeriSign ■ Go Daddy	■ Comodo ■ GeoTrust

Uploading Certificates

To upload certificates, complete the following steps:

1. Go to **Global Settings** > **Certificates**. The **Certificates** page opens.
2. Click the plus icon to add the certificate to the certificate store.
3. In the **Add Certificate** dialog box, do the following:
   a. In the **Name** text box, specify the certificate name.
   b. Select the type of certificate. You can select any one of the following certificates:

- **CA** —Digital certificates issued by the CA.
- **Server**—Server certificates required for communication between devices and authentication servers.
- **CRL**—Certificate Revocation List that contains the serial numbers of certificates that have been revoked. This certificate is required for performing a certificate revocation check.
- **OCSP Responder Cert**—OCSP responder certificates.
- **OCSP Signer Cert**—OCSP Response Signing Certificate.

The OCSP certificates are required for OCSP server authentication.

c. From the **Format** drop-down list, select a certificate format; for example, PEM, DER, and PKCS12.

d. In the **Passphrase** text box, enter a passphrase.

e. In the **Retype Passphrase** text box, retype the passphrase for confirmation.

The **Passphrase** and **Retype Passphrase** text boxes are displayed only when you select **Server Certificate** from the **Type** drop-down list.

f. In the **Certificate File** field, click **Choose File** and browse to the location where the certificates are stored and select the certificate files.

g. Click **Add**. The certificate is added to the Certificate Store.

Managing Certificates on Instant APs Configured Using Templates

Aruba Central supports uploading multiple certificates to Instant APs configured using templates. You can manage certificates either from the Aruba Central UI or through the API Gateway. For more information about APIs, see API Documentation.

To push certificates to Instant APs configured using templates:

1. Upload certificate(s).
   - From the app selector, go to **Global Settings** > **Certificates** and click the plus icon to upload the certificate to the certificate store. For more information, see Uploading Certificates on page 100.
   - **API**—Use the **[POST] /configuration/v1/certificates** API to upload certificates. .
2. Make a note of the certificate name and MD5 checksum.
   - In the UI, go to **Global Settings** > **Certificates** > **Certificate Store** table to get these details.
   - Use the **[GET] /configuration/v1/certificates** API to get these details.
3. In the template, anywhere before the **per-ap settings** block, depending on your requirement, add one or more of the following commands:

```
ca-cert-checksum <ca_cert_checksum/ca_cert_name>
cp-cert-checksum <captive_portal_cert_checksum/captive_portal_cert_name>
radsec-ca-checksum <radsed_ca_checksum/radsed_ca_name>
radsec-cert-checksum <radsed_cert_checksum/radsed_cert_name>
server-cert-checksum <server_cert_checksum/server_cert_name>
```

You can either use the certificate name or the checksum value in the command. Or, you can set it as a variable and enter the variable value for the Instant AP. Aruba recommends using the certificate name.

Example 1

```
ca-cert-checksum my_default_cert
```

Example 2

```
ca-cert-checksum %ca_cert_name%
variable:
{
```

```
"ca_cert_name": "my_default_cert"
}
```

Managing Software Upgrades

The **Firmware** menu in the **Maintenance** app provides an overview of the latest supported version of firmware for the device, details of the device, and the option to upgrade the device.

Viewing Firmware Details

To view the firmware details for devices provisioned in Aruba Central:

1. From the app selector, click **Maintenance**.
2. Click **Firmware**. The **Firmware** window opens and displays the following information:

Table 29: *Firmware Maintenance*

Data Pane Item	Description
Search Filter	Allows you to define a filter criterion for searching devices based on the host name, MAC address, location, firmware version, and the current upgrade status of the device.
Filter by Upgrade Status	Filters the device list based on any of the following firmware upgrade status: ■ Show All ■ Need upgrade ■ Scheduled ■ In progress ■ Failed ■ Upgrade not required Show All is selected by default.
Virtual Controllers	Displays the following information: ■ **VC Name**—Name of the VC. ■ **APs**—Number of APs associated to VC. ■ **Firmware Version**—The current firmware version running on the device. ■ **Latest Firmware Version**—The latest firmware version available on the public firmware server. ■ **Firmware compliance**—Status of the firmware compliance setting. The value displayed in this column is either **Set**, **Not Set**, or **Set<date and time>**. The **Set<date and time>** displays the date and time that is set in the Firmware Compliance Setting page. ■ **Status**—Firmware upgrade status.
Switch-MAS **Switch-Aruba**	Displays the following details about Aruba switches managed through Aruba Central: ■ **Host name**—Host name of the switch. ■ **MAC Address**—MAC address of the switch. ■ **Model**—Hardware model of the switch. ■ **Firmware Version**—The current firmware version running on the switch. ■ **Latest Available Version**—The latest firmware version available for the switch platform. ■ **Firmware compliance**—Status of the firmware compliance setting. The value displayed in this column is either **Set**, **Not Set**, or **Set<date and time>**. The **Set<date and time>** displays the date and time that is set in the Firmware Compliance Setting page. ■ **Status**—The upgrade status of the switch.
Gateways	Displays the following details about the SD-WAN Gateways managed through Aruba Central: ■ **Host name**—Host name of the SD-WAN Gateway.

Table 29: *Firmware Maintenance*

Data Pane Item	Description
	■ **MAC Address**—MAC address of the SD-WAN Gateway. ■ **Model**—Hardware model of the SD-WAN Gateway. ■ **Firmware Version**—The current firmware version running on the SD-WAN Gateway. ■ **Latest Available Version**—The latest firmware version available for the SD-WAN Gateway. ■ **Firmware Status**—The upgrade status of the SD-WAN Gateway. ■ **Compliance Status**—Status of the firmware compliance setting. The value displayed in this column is either **Set**, **Not Set**, or **Set<date and time>**. The **Set<date and time>** displays the date and time that is set in the Firmware Compliance Setting page.
Continue	Allows you to continue with firmware upgrade.
Firmware Compliance Setting	Allows to set firmware compliance for devices within a group. Clicking the gear icon in the **Virtual Controllers**, **Switch - MAS**, **Switch - Aruba** and **Controllers** tabs displays the **Firmware Compliance Setting** page. It also allows you to view a list of supported firmware versions for each device in a group.
Update All	Allows you to simultaneously upgrade firmware for multiple devices.
Cancel Upgrade	Cancels a scheduled upgrade.
Cancel All	Cancels a scheduled upgrade for all devices.

Upgrading a Device

To check for a new version on the image server in the cloud, complete the following steps:

1. From the app selector, click **Maintenance** app.
2. Click **Firmware**.
3. To upgrade firmware for devices in a specific group, select a group from the group selection filter bar.
4. Select one or several devices to upgrade.
5. Click **Continue**. The **Upgrade <Device> Firmware** pop-up window opens.
6. Select a firmware version. You can either select a recommended version or manually choose a specific firmware version.

NOTE

To obtain custom build details, contact Aruba Central Technical Support.

7. Select **Auto Reboot** if you want Aruba Central to automatically reboot after device upgrade.

NOTE

The **Auto Reboot** option is available for Mobility Access Switches and Aruba Switches.

The **Auto Reboot** option is available for Mobility Access Switches, Aruba 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**.

Setting Firmware Compliance

Aruba Central now allows you to run a firmware compliance check and force firmware upgrade for devices in a group. To force a specific firmware version for all AP devices or Switches in a group, complete the following steps:

1. From the app selector, click the **Maintenance** app.
2. Click **Firmware**.
3. Verify the firmware upgrade status for the device.
4. Click the settings icon at the top right corner. The **Firmware Compliance Setting** window opens.
5. Select the groups, and device type for upgrade.
6. Select **Auto Reboot** if you want Aruba Central to automatically reboot the device after a successful device upgrade.
7. In the **When** section, perform the following
   - Select **Now** to set the compliance to be carried out immediately.
   - Select **Later** 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.

Troubleshooting Devices

The **Troubleshooting** menu in the **Maintenance** module allows your network administrators to run troubleshooting or diagnostics commands on the devices managed from Aruba Central. When a troubleshooting operation is initiated, Aruba Central establishes a session with the devices, retrieves the output of the commands, and displays the output in the UI.

Aruba Central supports running troubleshooting operations on one or several devices. You can select up to 10 devices for a troubleshooting operation. If the user access is restricted to certain groups within a network, Aruba Central allows running troubleshooting commands only for the devices provisioned in the allowed groups.

For running a troubleshooting operation, the minimum software version required on the Instant APs is 6.4.3.1-4.2.0.3.

Troubleshooting a Device

To run troubleshooting commands on the devices, complete the following steps:

1. From the app selector, click **Maintenance** > **Troubleshooting**. The **Troubleshooting** page opens.
2. Select a device category.
   - To troubleshoot an AP, click the **Access Points** tab.
   - To troubleshoot a Switch, click the **Switch- MAS** or **Switch - Aruba** tab.
   - To troubleshoot an SD-WAN Gateway, click the **Gateways** tab.

3. Select the devices for which you want to run diagnostic checks or troubleshooting operations. Table 30 describes the fields and filtering parameters available on the **Troubleshooting** page:

Table 30: *Contents of the Troubleshooting Page*

Data Pane Item	Description
Access Points	Allows you to run troubleshooting commands on Instant APs. To run diagnostic checks, select the Instant APs from the **AP Name** drop-down.
Switch-MAS **Switch-Aruba**	Allows you to run the troubleshooting commands on a Switch. To run diagnostic checks, select the Switches from the **Switch Name** drop-down.
Gateways	Allows you to run troubleshooting commands on SD-WAN Gateways. To run diagnostic checks, select the SD-WAN Gateway devices from the **Gateway Name** drop-down.

Table 30: *Contents of the Troubleshooting Page*

Data Pane Item	Description
Troubleshooting	Allows you to select one of the following options: ■ **Tools**—Provides a list of basic troubleshooting tools to verify network connectivity and latency issues. ■ **Commands**—Allows you to select a specific set of CLI commands to run on the selected devices for diagnostics and troubleshooting purposes.
Tools	Allows you to run the following diagnostic tools on the selected devices: ■ **Ping**—Sends ICMP echo packets to the IP addresses of the selected devices to check for latency issues. ■ **Traceroute**—Tracks the packets routed from a network host. ■ **Speed-Test**—Runs a speed test to measure network speed and bandwidth. The speed-test diagnostic tool is available only for Instant APs. For speed-test diagnosis, you must provide the **Iperf server address**, the protocol type, and speed-test options such as bandwidth. ■ **LED Chassislocate**—Activates the Switch locator LED. The locator LED indicates the physical location where an Aruba Switch is currently installed. This option is not available for the Mobility Access 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 the Aruba switches. ■ **Interface Bounce**—Restarts the port interface and forces a client to re-initiate a DHCP request. This option is available only for the Aruba switches.
Commands	Category—Allows you to select a category. The troubleshooting commands are segregated under the following categories: **Access Points** ■ Wireless ■ Security ■ Network ■ Airgroup ■ System ■ ARM ■ Datapath ■ Logs ■ Aruba Central ■ Cluster Security ■ Speed Test ■ OFC **Switch- MAS** ■ Physical Connection ■ Traffic ■ Configuration ■ Media Access ■ Network **Switch - Aruba** ■ Physical Connection ■ PoE and Media Access ■ L2 Loop Prevention ■ Link Aggregation ■ Loop Detection ■ Network ■ Management ■ Security and Traffic ■ Show Tech ■ Modules ■ Stacking **Gateways** ■ System

Table 30: *Contents of the Troubleshooting Page*

Data Pane Item	Description
	■ License ■ Datapath ■ Crypto ■ Security ■ Services ■ Network ■ Mobility ■ Wireless ■ HA ■ Speed Test ■ Config

4. If you have selected the **Tools** option, enter the required input parameters such as the host name, IP address, protocol details, and other required options to perform a diagnostic health check.
5. If you want to run the troubleshooting commands on the devices:
   a. Select a command category and select the commands.
   b. Click **Run**. The command output is displayed in the output pane.
6. To set a frequency for automatically running the troubleshooting commands:
   a. Click **Auto Run**.
   b. Specify an interval for running the troubleshooting commands. You can also specify how frequently the commands must be run during a given interval.
   c. Click **Start**.
7. To clear the command output, click **Clear All**.
8. To export the command output as a zip file, click **Export All**.
9. To send the output as an email, click **Email** and add email recipient details.

Viewing Command Output

After you run troubleshooting commands on devices, Aruba Central displays the command output in the output pane of the **Troubleshooting** page.

The output pane shows a list of devices on which the troubleshooting commands were executed, the CLI commands that were executed on the devices, and time stamp of command execution.

The output pane also allows you to filter a command output. For example, if you enter DPI in the **Filter** text box, only the command output with the DPI text is displayed.

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

Viewing Audit Trails

The **Audit Trail** page shows the logs for all the device management, configuration, and user management events triggered in Aruba Central.

To view the details of a particular event, click the details icon under the **Details** column

You can search or filter the audit trail records based on any of the following columns:

- Time (All, Today, Last 3 months, Custom Range)
- Username
- IP Address
- Classification
- Target
- Details

To view the audit trail log details in Aruba Central:

1. From the app selector, click **Maintenance**.
2. Click **Audit Trail**. By default, audit trails are displayed for all devices. Perform any of the following actions:
   - To view audit trails for a specific group, select a group from the group selection filter bar.
   - To view audit trails for a specific device, select the device from the group selection filter.
   - To view audit trails for a device from another group, switch to the group in which the device is available, and select the device from the list of devices in the group selection filter bar.

Viewing Audit Trails in the Standard Enterprise Portal

The **Audit Trail** logs are displayed for the following types of operations in the Standard Enterprise Portal:

- Device status and configuration
- Firmware upgrade
- Device assignment to subscriptions and groups
- Label assignment to devices
- User addition and deletion
- License reconciliation

The **Audit Trail** page in the Standard Enterprise portal displays the following details:

Table 31: *Audit Trail Pane in the Standard Enterprise View*

Data Pane Content	Description
Time	Time stamp of the events for which the audit trails are shown.
Username	The username of the admin user who applied the changes.
IP Address	IP address of the client device.
Classification	Type of modification and the affected device management category. For more information, see Classification of Audit Trails on page 109.
Target	The group or device to which the changes were applied.
Details	A short description of the changes such as subscription assignment, firmware upgrade, and configuration updates. **NOTE:** Complete details of the event can be seen by clicking the ellipsis. For example, if an event was not successful, clicking the ellipsis displays the reason for the failure.

Classification of Audit Trails

The audit trail is classified according to the type of modification and the affected device management category. The category can be one of the following:

- Configuration
- Firmware Management
- Reboot
- Device Management
- Templates
- User Management
- Variables
- Label Management
- MSP
- Guest
- Groups
- Subscription Management
- API Gateway
- RBAC
- Sites Management
- SAML Profile
- User Activity
- Federated User Activity
- Alert Configuration
- Install Manager
- Gateway Management
- Tools

Removing Devices

The device monitoring dashboards allow you to remove an offline device. However, you will not be able to remove a device completely from Aruba Central database, because the device entry remains in the **Device Inventory** page. The devices appearing in the **Device Inventory** page shows the hardware devices that belong to your account or purchase order.

For information on removing an offline device, see the following topics:

- Deleting an Offline AP
- Deleting an Offline Switch
- Deleting an Offline Gateway

Removing a Device from the Device Inventory Page

You cannot remove a device completely from Aruba Central, but you can unsubscribe the device. After you unsubscribe, the device status changes to **Unsubscribed** in the **Device Inventory** page. If you have more than one Aruba Central account and if another Aruba Central user adds this unsubscribed device to another Aruba Central account, the device entry is removed from the **Device Inventory** page in your Aruba Central account.

Aruba Central users are broadly categorized as follows:

- Network Administrators—Network administrators manage, configure, and monitor devices in their respective network or organization using the Standard Enterprise Aruba Central interface.
- Service Provider Administrators—Service Provider administrators are referred to as the MSP administrators who create, manage, and monitor accounts for multiple organizations (tenants). For MSP accounts, Aruba Central provides a separate interface called MSP View, using which MSP administrators can provision and manage their respective tenant accounts. The tenant account users access is limited to their respective organization or network setup. For more information on creating tenant accounts, see the*Aruba CentralMSP User Guide*.

Within each Aruba Central account, the admin users of the respective accounts can configure and manage the following types of users :

- System users—Refer to the Aruba Central users who authenticate to the Aruba SSO server (public cloud deployments) or LocalDB servers (private cloud deployments). System users can access both the UI and API interface with their Aruba Central login credentials. Access for the system users is determined by the role to which they are mapped. For more information on configuring system users, see Configuring System Users on page 110
- External users—Refer to the Aruba Central users who log in to Aruba Central using an external authentication source. External user accounts are maintained by IT administrators of the respective organizations. External users are also referred to as federated users. To provide a secure and seamless sign-on experience for external users, Aruba Central supports a federation configuration module based on the SAML SSO framework. For more information on configuring the SAML SSO framework for federated users, see the Aruba Central SAML SSO Solution Guide.

Configuring System Users

The **Users & Roles** menu option in the **Global Settings** application allows you to create, modify, and delete users.

Adding a System User

To add a user in Aruba Central, complete the following steps:

1. Go to **Global Settings** > **Users & Roles**.
2. Click the **Users** tab.
3. To add a new user, click **+**. The **New User** window is displayed.
4. Configure the parameters described in Table 32:

Table 32: *User Configuration Attributes*

Parameters	Description
Username	Name of the user. Enter a valid email address.
Description	Description of the user role. You can enter up to a maximum of 32 characters including alphabets, numbers, and special characters in the text field.
Role	Enter the user role. For more information on user roles, see Configuring User Roles.
Allowed Groups	Select the groups to which want to allow access to the user.
Language	Specify a language.

5. Click **Save**. An email invite is sent to the user with a registration link. Users can use this link to access Aruba Central.
6. If the user has not received an email invite, click **Actions** > **Resend Invite Email** to resend the invitation.

Editing a User

To edit a user account, complete the following steps:

1. Go to **Global Settings** > **Users & Roles**.
2. In the **Users** tab, select the user and click the edit icon.
3. In the **Edit User <"Username">** window, edit **Role** and **Allowed Groups**.
4. Click **Save**.

Deleting a User

To delete a user account:

1. Go to **Global Settings** >**Users & Roles**.
2. In the **Users** tab, select the user and click the delete icon.
3. Confirm user deletion in the **Confirm Action** dialog box.

Viewing Audit Logs

Aruba Central creates audit logs when a new user is added to or deleted from an Aruba Central account. It also records the login and logout activities of Aruba Central users.

To view audit logs for Aruba Central users:

1. Go to **Maintenance** > **Audit Trail**. The **Audit Trail** page opens.
2. To view audit logs for user addition and deletion, click the filter in the **Classification** column, and select **User Management**.
3. To filter audit logs about user activity, click the filter in the **Classification** column, and select **User Activity**.

The **User & Roles** page also includes the **Support Access** and **Two-factor Authentication (2FA)** options under **Actions**. When **Support Access** is enabled, the Aruba support team can access your Aruba Central account remotely. For more information, see Support Access on page 115.

For more information on two-factor authentication, see Two-Factor Authentication on page 113.

Configuring User Roles

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

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

Predefined User Roles

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

User Role	Standard Enterprise Mode
admin	■ Has full access to all devices. ■ Can provision devices and enable access to application services. ■ Can create or update users, groups, and labels.
readwrite	■ Has access to the groups and devices assigned in the account. ■ Can add, modify, configure, and delete a device in the account.
readonly	■ Can view the groups and devices. ■ Can view generated reports.
guestoperator	■ Can access and modify cloud guest splash page profiles. ■ Can configure visitor accounts for the cloud guest splash page profiles.

Custom Roles

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

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

Adding a Custom Role

To add a custom role, complete the following steps:

1. From the app selector, click **Global Settings** and then click **Users & Roles**.
2. Click the **Roles** tab.
3. To add a new role, click **+**. The **New Role** window is displayed.
4. Specify a name for the role.
5. Set permissions at the application level.
6. For Network Management, you can set access rights at the module level.

   To set view or edit permissions or block the users from accessing a specific module, complete the following steps:

   a. Click **Customize**.

   b. Select one of the following options for each module as required:

- **View Only**
- **Modify**
- **Block**

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

User roles with **Modify** permission can perform add, edit, or delete actions within the specific module.

User roles with **View Only** permission can only view the specific module.

User roles with **Block** permission cannot view that particular module.

Application Permissions

Aruba Central allows you to define user roles with **view** or **modify** permissions. You can also block user access to some applications. For example, if the Guest Access application is blocked for a specific user role, the app selector will not display this application.

Aruba Central supports setting permissions for the following application categories:

- **Group management**—Allows users to create, view, modify, and delete groups and assign devices to groups.
- **Devices and Subscription**—Allows users to add devices and assign subscriptions to devices.
- **Network management**—Allows users to configure, troubleshoot, and monitor Aruba Central-managed networks.
- **Guest management**—Allows users to configure cloud guest splash page profiles.
- **Clarity**—Allows user to access the Clarity application for client connectivity health checks.
- **Presence Analytics**—Allows users to access the Presence Analytics app and analyze user presence data.
- **VisualRF**—Allows user to access VisualRF and RF heatmaps.
- **Unified Communications**—Allows users to access the Unified Communications application.
- **Install Manager**—Allows users to manage installer profiles and site installations.
- **Reports**—Allows users to view and create reports.
- **Other Applications**—Allows users to access other applications modules such as notifications and Virtual Gateway deployment service.

Viewing User Role Details

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

1. From the app selector, click **Global Settings** and then click **Users & Roles**.
2. Click the **Roles** tab. The Roles tab displays the following information:
   - **Role Name**—Name of the user role.
   - **Allowed Applications**—The applications to which the users have access.
   - **Assigned Users**—Number of users assigned to a role.

Two-Factor Authentication

Aruba Central now supports two-factor authentication for both computers and mobile phones to offer a second layer of security to your login, in addition to password. When two-factor authentication is enabled on a user account, the users can sign in to their Aruba Central account either through the mobile app or the web application, only after providing their password and the six-digit verification code displayed on their trusted devices.

When two-factor authentication is enabled at the customer account level, all the users belonging to the customer account are required to complete the authentication procedure when logging in to Aruba Central. If a user account is associated with multiple customer accounts and if two-factor authentication is enabled on one of these accounts, the user must complete the two-factor authentication during the login procedure.

If two-factor authentication is enabled on your accounts, you must install the Google Authenticator app on your devices such as mobile phones to access the Aruba Central application. When the users attempt to log in to Aruba Central with their credentials, the Google Authenticator app provides a six-digit verification code to complete the login procedure.

Installing Google Authenticator App

For two-factor authentication, ensure that the Google Authenticator app is installed on your mobile device.

During the registration process, the Aruba Central application shares a secret key with the mobile device of the user over a secure channel when the user logs in to Aruba Central. The key is stored in the Google Authenticator app and used for future logins to the application. This prevents unauthorized access to a user account as this authentication procedure involves two-levels for secure transaction.

When you register your mobile device successfully, the Google Authenticator app generates a six-digit token for the second level authentication. The token is generated every thirty seconds.

Enabling Two-factor Authentication for User Accounts

To enable two-factor authentication, complete the following steps:

1. Click **Global Settings** > **User& Roles**. The **User & Roles** page opens.
2. From the **Actions** menu, set **Two-Factor Authentication (2FA)** to **ON**. The two-factor authentication is enabled for all the users associated with a customer account.

Two-factor Authentication for Aruba Central Web Application

When two-factor authentication is enabled for a customer account, the users associated with that customer account are prompted for two-factor authentication when they log in to Aruba Central.

To complete two-factor authentication, perform the following actions:

1. Access the Aruba Central website.
2. Log in with your credentials. If two-factor authentication is enforced on your account, the two-factor authentication page opens.
3. Install the Google Authenticator app on your mobile device if not already installed.
4. Click **Next**.
5. If this is your first login since two-factor authentication is enforced on your account, open Google Authenticator on your mobile device.
6. Scan the QR Code. If you are unable to scan the QR code, perform the following actions:
   a. Click the **Problem in Reading QR Code** link. The secret key is displayed.
   b. Enter this secret key in the Google Authenticator app.
   c. Ensure that the **Time-Based** parameter is set. Aruba Central is added to the list of supported clients and a six-digit token is generated.
7. Click **Next**.
8. Enter the six-digit token.
9. Select the **Remember 2FA for 30 Days** check box if you want the authentication to expire only after 30 days.
10. Click **Finish**.

Two-factor Authentication for the Aruba Central Mobile App

Two-factor authentication must first be enabled for your account. If two-factor authentication is not enabled, you log in to the application directly after a successful SSO authentication.

To log in to Aruba Central app on your mobile device, perform the following actions:

1. Open the Aruba Central app on your mobile device.
2. Enter your username and password and click **Log in**. If the registration process is pending, an error message is displayed.

Please register for two-factor authentication in our web app to ensure secured authentication.

3. Enter the token. On successful authentication, the Aruba Central app opens.

Registering a New Mobile Device

If you have changed your mobile device, you need to install Google Authenticator app on your new device and register again using a web browser on your Desktop for two-factor authentication.

To register your new mobile device, complete the following steps:

1. Log in to Aruba Central web application. The two-factor authentication page is displayed.
2. Click the **Changed Your Mobile Device?** link.
3. To register your new device and receive a reset email with instructions, click **Send 2FA Reset Email**. A reset email with instructions will be sent to your registered email address.
4. Follow the instructions in the email and complete the registration.

Support Access

Aruba Central technical support may ask you to enable **Support Access** to debug issues. After you enable **Support Access**, the Aruba support team can access your Aruba Central account remotely.

Only users with administrator role can enable **Support Access**.

Enabling Support Access

To enable **Support Access**, complete the following steps:

1. Go to **Global Settings** > **User& Roles**. The **User & Roles** page opens.
2. From the **Actions** menu, turn on the **Support Access** toggle switch.
3. Set password expiry by clicking the number of days and click **Get Password**. A new password is generated
4. Copy the password and share it with the Aruba Central technical support representative.

Disabling Support Access

After the remote support session is complete, do the following to disable **Support Access**:

1. Go to **Global Settings** > **User& Roles**. The **User & Roles** page opens.
2. From the **Actions** menu, turn off the **Support Access** toggle switch.

The **Monitoring & Reports** app includes the following functional menu options for viewing the device and network details:

Network Overview

The **Monitoring & Reports** > **Network Overview** pane displays a summary of the bandwidth usage, client count, top APs by usage, top 5 clients, top Instant AP clusters by usage, top Instant 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.

Table 33: *Network Overview pane*

Data Pane Item	Description
Temporal Filter	Allows you to select a time range for the graphs displayed on the Overview pane. You can choose to view graphs for a time period of 3 hours, 1 day, 1 week, 1 month and 3 months.
Bandwidth Usage Graph	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 Instant AP over a specific duration.
Top APs By Usage	Displays the list of top Instant APs that utilize the maximum bandwidth in the network.
Application Usage	If Deep Packet Inspection is enabled, the Application Usage graphs display the applications, application categories, and web categories accessed by the clients in the network. The Web Reputation graph displays the web reputation score for the websites accessed by the clients connected to the network.
Top 5 Clients	Displays the top five clients connected to the currently available SSIDs that utilize the maximum bandwidth in the network.

Data Pane Item	Description
	The **Top 5 Clients** table displays data only for the clients that are connected to the network for a total duration of two or more hours.
Top IAP Clusters By Usage	Displays the list of top Instant AP clusters that utilize the maximum bandwidth in the network.
Top IAP Clusters by Clients	Displays the list of top Instant AP clusters connected to the client that utilize the maximum bandwidth in the network.
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.

APs

The **APs** monitoring dashboard provides all the metrics about the health, status, and clients information associated with the AP provisioned and managed through Aruba Central.

Page Views

To view the dashboard, go to **Monitoring & Reports** > **Network Overview** > **APs**.

The **APs** dashboard includes the following contents:

- **Usage**—Displays the overall usage metrics for the APs provisioned in your Aruba Central account.
  - **Usage**—Displays the incoming and outgoing data traffic to and from the device.
  - **Clients Count**—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 as per SSID over a specified time period.
  - **Application Usage**—If deep packet inspection is enabled, the **Application Usage** graphs display the applications, application categories, web categories, and web reputation accessed by the clients in the network. The **Web Reputation** graph displays the web reputation score for the websites accessed by the clients connected to the network.
- **Top N**—Displays a list of APs with maximum bandwidth usage. This component appears in the drop-down list of **Network Overview** > **APs** tab.
- **List of Offline APs**—Displays the total number of APs that are up.
- **List of Online APs**—Displays the total number of APs that are down.

Filters

To set your dashboard view to show only the data pertaining to a group, label, site, or device, use the **Filter Monitoring & Reports**. By default, Aruba Central displays data for all devices in your Aruba Central account.

To set your dashboard view to show data for specific duration, use the filtering options in **Temporal Filter**. By default, the data is displayed for a time range of 3 hours. To view the graphs for a different time range, click **Temporal Filter** and select a time range of your choice. You can choose to view data for a time period of 3 hours, 1 day, 1 week, 1 month, and 3 months.

Navigation and Granularity

To view more details about a specific AP, you can use the following page views:

- **List of Online APs**—To view the details of APs connected to Aruba Central.
- **List of Offline APs**—To view the details of APs that are currently not connected to Aruba Central.

Access Points Table

The **APs** table on **List of Offline APs** and **List of Online APs** pages displays a list of APs with the following information:

- **Device Name**—Name of the AP.
- **Clients**—Clients connected to the AP.
- **Channel**—Channels assigned under Radio 1 and Radio 2.
- **Power**—The transmit power of Radio 1 and Radio 2 measured in decibels.
- **Utilization**—The percentage of time (normalized to 255) that the channels of Radio 1 and Radio 2 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.
- **Noise Floor**—The noise at the radio receivers of Radio 1 and Radio 2. Along with the thermal noise, Noise Floor may be affected by certain types of interference sources, though not all interference types result in increased noise floor. Noise Floor value may vary depending on the noise introduced by components used in the computer or client device.
- **IP Address**—IP address of the AP.
- **Model**—The model number of the AP.
- **Serial**—The serial number of the device.
- **Mode**—The radio mode such as access or monitor.
- **MAC**—MAC address of the AP.
- **Virtual Controller**—Name of the Virtual Controller.
- **Location**—Location of the AP.
- **Group**—Group to which the device belongs.
- **Labels**—Labels associated with the AP. You can also add a new label to the AP by clicking on the edit icon.
- **Site**—The site to which the device belongs.
- **Firmware Version**—The firmware version running on the AP.
- **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 **List of Offline APs** 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 **List of Online APs** page.
- **Public IP**—IP address that is logged by servers when the device is connected through internet connection.
- **Search box**—The **Search** filter allows you to specify a criteria for searching devices. Aruba Central supports single column search. It filters the search results and sorts the list of devices based on the search string specified from a single column.

The **Search** filter is provided only for the **Device Name**, **IP Address**, **Model**, **Serial**, **Mode**, **MAC**, **Virtual Controller**, **Group**, **Labels**, and **Site** columns.

NOTE

To expand or collapse the column view, click the column settings icon next to the last column of the table. By default, the AP list table displays the **Device Name**, **Clients**, **Channel**, **Power**, **IP Address**, and **Model** columns. You can customize the view of AP list table with additional columns such as the **Utilization**, **Noise Floor**, **Mode**, **Serial**, **MAC**, **Virtual Controller**, **Group**, **Labels**, **Site**, **Firmware Version**, **Uptime**, **Last Seen**, and **Public IP**. 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** button provided in the drop-down list to reset the AP list with default columns only.

To delete a specific AP in the **List of Offline APs** page of the **Monitoring & Reports** > **Network Overview** > **APs** tab, click the AP listed in the AP list table. A confirmation message appears. Click the **Delete** button to delete the AP.

AP Details Page View

The **Access Points** table displays a list of APs in the group. To view the details of an AP, click the AP entry in the **Access Points** table. The following details of the selected AP are displayed:

AP Details Panel

The AP details page includes a header panel that provides the following information on the AP:

- **Access Points**—Displays the MAC address of the AP along with a message describing the operational status of the device for the time range selected in the Temporal Filter.
- **Device Health**—Displays the health status of the device that is measured based on the CPU and memory utilization of the device**.** For example, **Good** or **Bad.**
- **Radio 1**—Displays the health of Radio 1 indicated as **Good** or **Bad**. The health of the radios are scored based on the Noise Floor and RF Utilization values.
- **Radio 2**—Displays the health of Radio 2 indicated as **Good** or **Bad**. The health of the radios are scored based on the Noise Floor and RF Utilization values.
- **Virtual Controller**—Displays the name of the Virtual Controller to which the AP is connected, if the AP details page belongs to a slave device. Clicking the Virtual Controller name displays the AP details page corresponding to the Virtual Controller. If the AP details page belongs to a master AP, then the **Virtual Controller** field displays **Self**.

The AP details page includes tabs that displays information specific to the AP.

NOTE

The AP details page that is opened on Mozilla Firefox web browser displays blank sections in all the tabs when the time range is changed in the Temporal Filter or when the page undergoes auto-refresh. To populate data in the tabs, you must switch between the tabs of the AP details page or navigate back to the AP list view to revoke the AP details page.

Open Tools

The **Open Tools** button allows you access the troubleshooting utility to troubleshoot Access Point issues. For more information on troubleshooting Access Points, see Troubleshooting Device Issues at Advanced Level.

To view information on the tabs and **Go Live** button displayed on the AP details page, click through the following:

- Overview
- Usage
- Clients
- RF
- VPN

- Location
- Events
- Actions
- Go Live

APs—Overview Tab

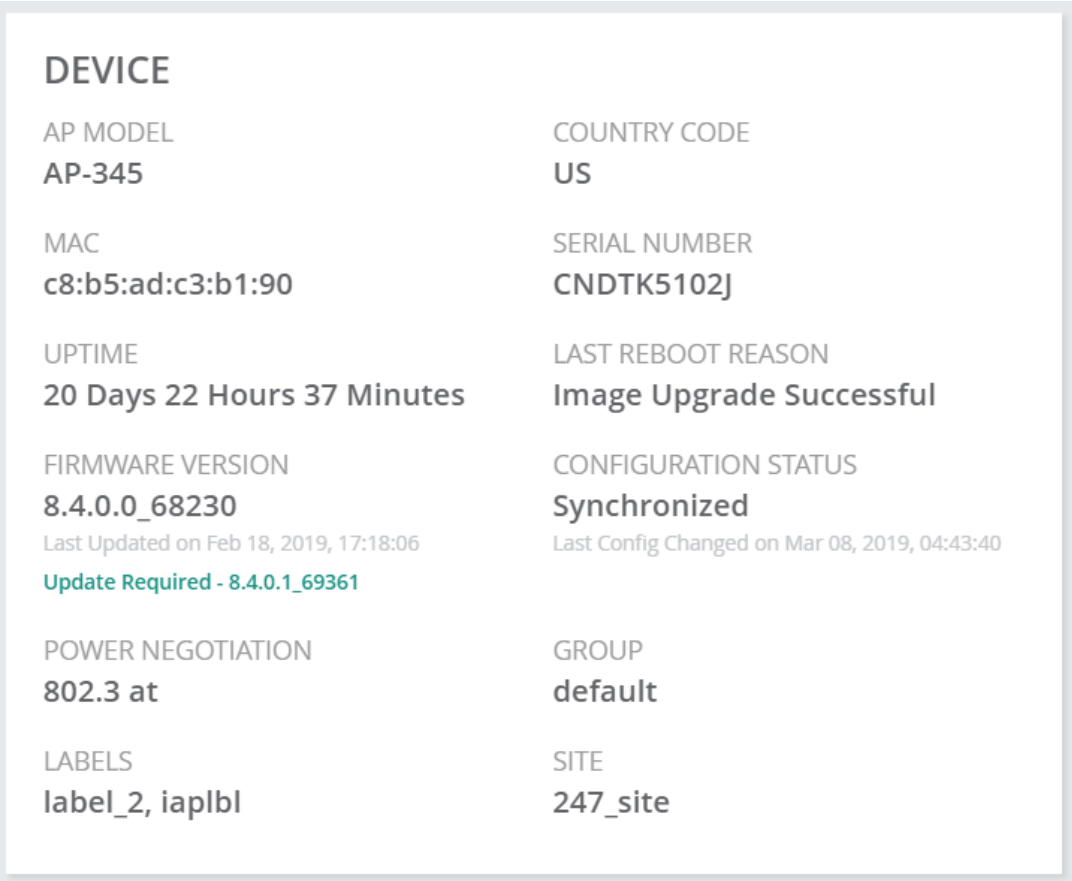
The **Overview** tab displays the AP device details,network information, radio details including the topology of clients connected to each radio, and the health status of the AP in the network. The **Overview** tab includes the following details:

Device

The **Device** section displays the following general information such as the state of the AP:

- **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**—The time when the device configuration was modified lately.
- **Power Negotiation**—The power in watts (W) negotiated on the ethernet port of the device in a wired network.
- **Group**—The group to which the AP belongs.
- **Labels**—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.
- **Blink LEDs—**To enable the blinking of LEDs on the AP to identify the location. The default blinking time is set to 5 minutes and it automatically stops after that. To stop the blink manually, click **Stop Blinking**.
- **Site**—The site to which the AP device belongs.

Figure 12 *Device*

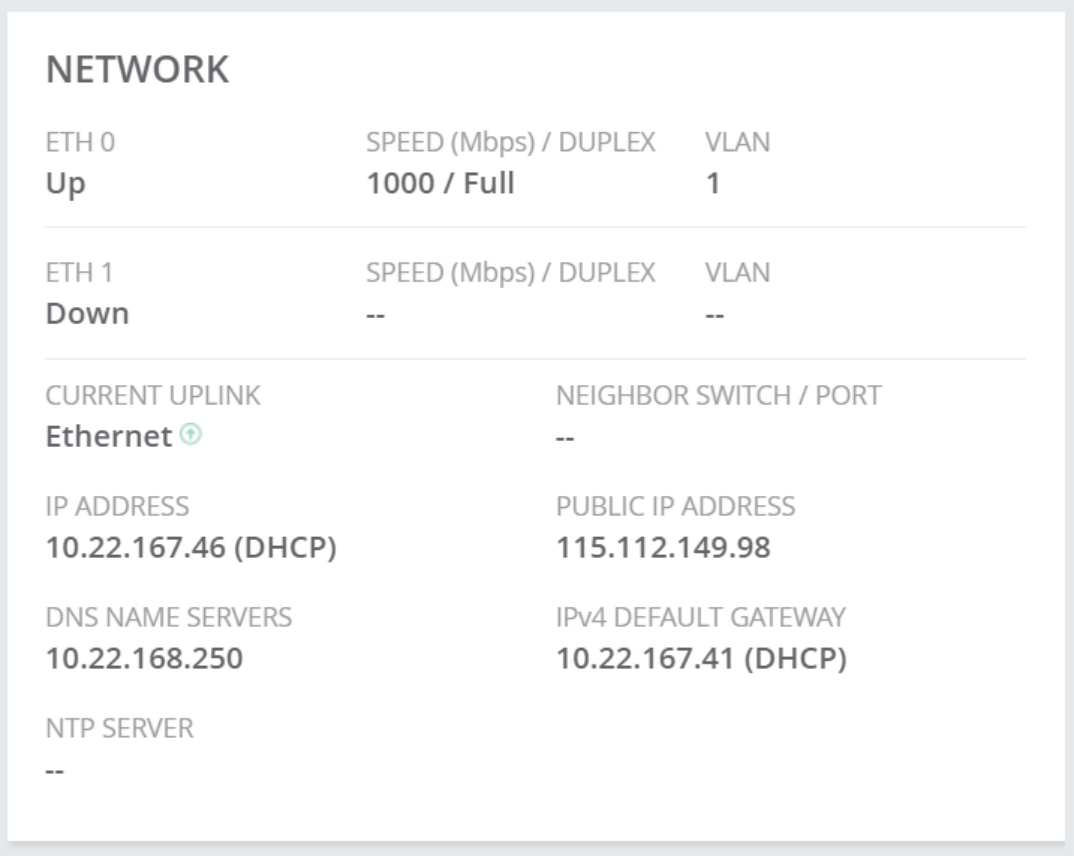


Network

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:

- **Speed/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**—Number of VLAN connections associated with the network.
- **Current Uplink**—Current uplink connection on the AP.
- **Neighbor Switch/Port**—Identification of the neighboring switch or port.
- **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.
- **iPv4 Default Gateway**—A 32 bit value which is used to uniquely identify the device on a public network.
- **NTP Server**—The information on NTP Server.

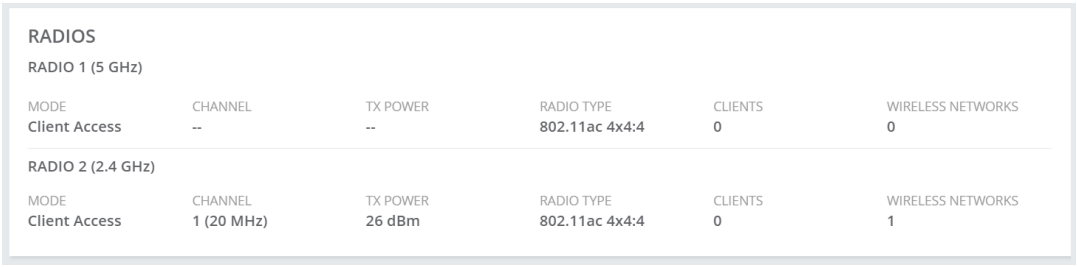
Figure 13 *Network*



Radios

The **Radios** section displays information on the related to **Radio 1** and **Radio 2** such as the **Mode**, **Channel**, **TX Power**, **Radio Type**, **Clients**, and **Wireless Networks.**

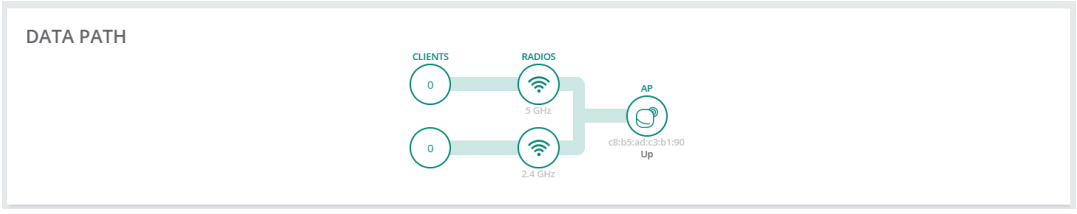
Figure 14 *Radios*



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.

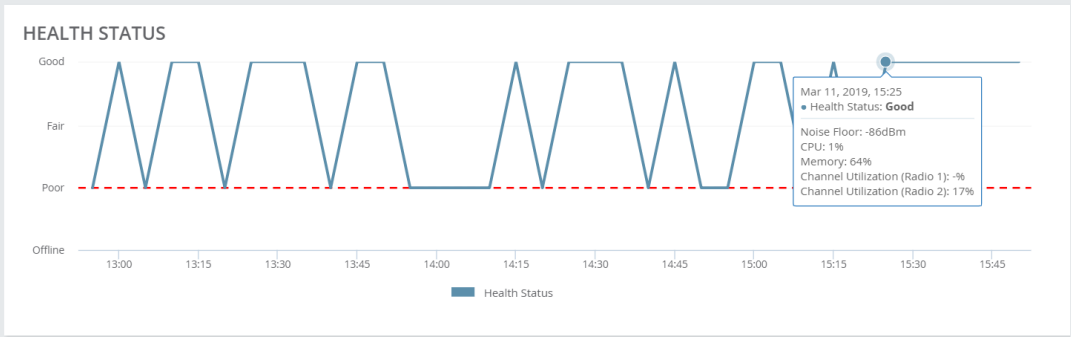
Figure 15 *Data Path*



Health Status

The **Health Status** trend graph indicates the health status of the device in the network for the time specified in the Temporal Filter. You can view information such as the Health Status, Noise Floor, CPU, memory, and channel utilization values when you move your mouse pointer to a specific area in the graph.

Figure 16 *Health Status*



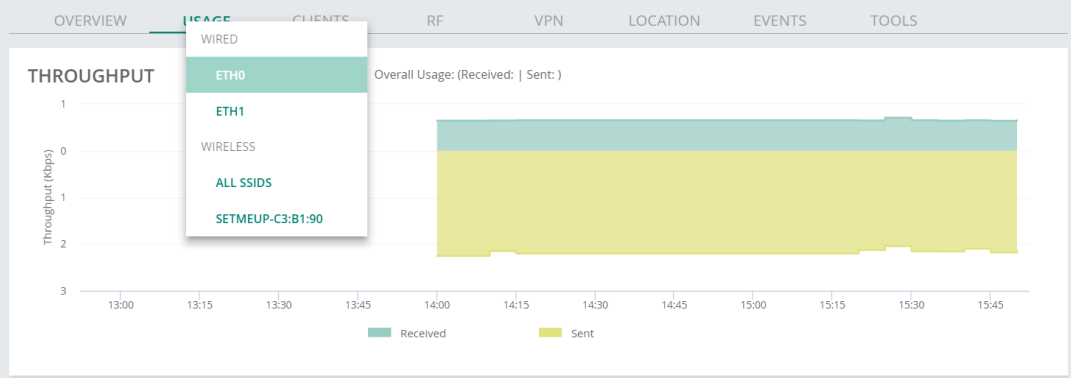
APs—Usage Tab

The **Usage** tab displays the size of data transmitted through the AP. This tab includes 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.

Figure 17 *Throughput*



Clients

The **Clients** graph indicates the number of clients connected to the device for a selected time range in the Temporal Filter. You can select a specific SSID or all SSIDs, Eth0, or Eth 1 from the drop-down list provided in the **Clients** section.

NOTE

You can also view the data for a specific time by moving the mouse on the graphs.

APs—Clients Tab

The **Clients** tab displays a table that lists the clients connected to the AP. You can view the table based on the **Connected**, **Offline**, or **Failed** clients that is selected from the **Status** drop-down list. The table includes the following columns:

- **Client Name**—Name of the client.
- **Status—**The status of the connected client. For example, **Connected**, **Offline**, or **Failed**.
- **Health**—The health of the connected client.
- **Failure Stage**—The stage at which the client had failed.
- **OS**—The operating system used by the client device**.**
- **SSID/Port**—The name of the wired or wireless network and the port to which the client is connected.

NOTE

The sorting option is available for the **Status** column. The search filter option is available for all the columns in the Clients table, except the **OS** column.

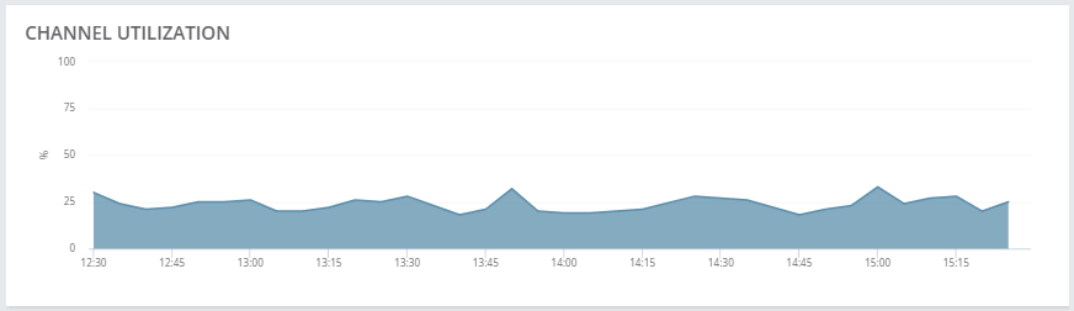
APs—RF Tab

The **RF** tab displays the following details corresponding to **Radio 1** and **Radio 2** radios of the AP:

Channel Utilization

The **Channel Utilization** graph indicates the percentage of channel utilization for the selected time range from the Temporal Filter.

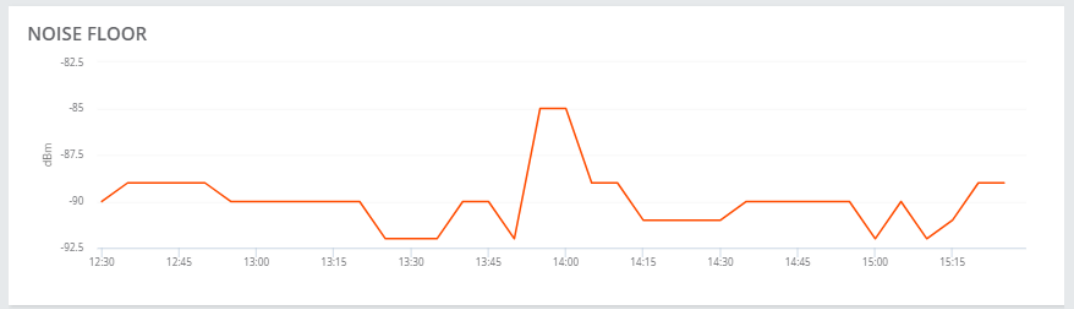
Figure 18 *Channel Utilization*



Noise Floor

The **Noise Floor** graph indicates the noise floor detected in the network to which the device belongs.

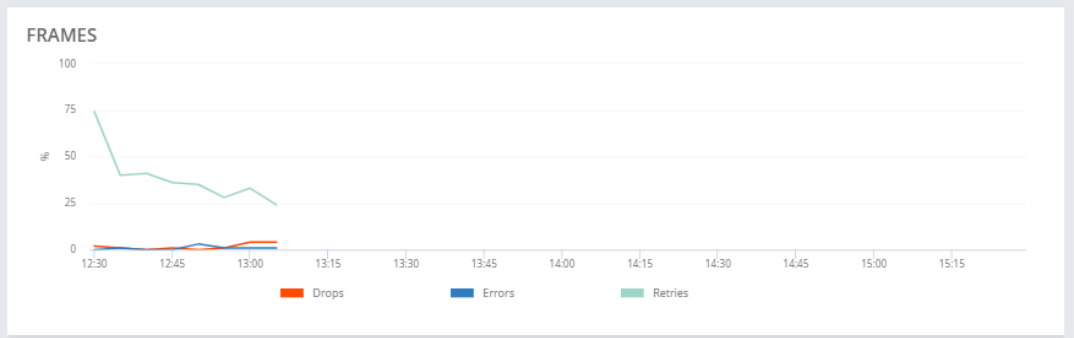
Figure 19 *Noise Floor*



Frames

The **Frames** 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, or encountered errors, or retried to be transferred, in a wireless network.

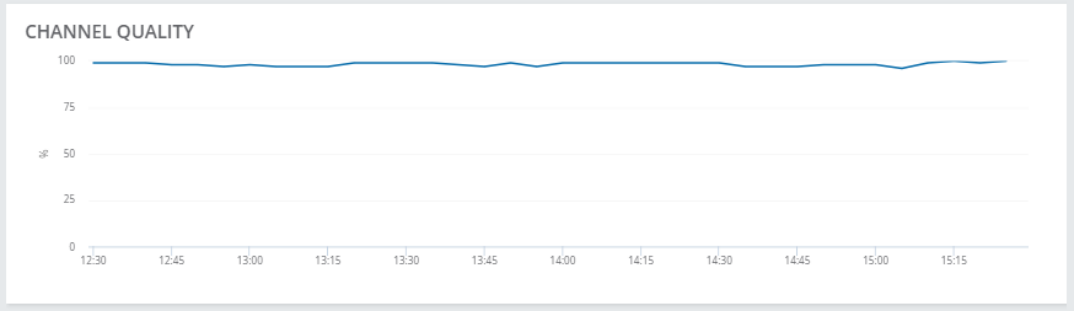
Figure 20 *Frames*



Channel Quality

The **Channel Quality** graph indicates the quality of channel in percentage.

Figure 21 *Channel Quality*



NOTE

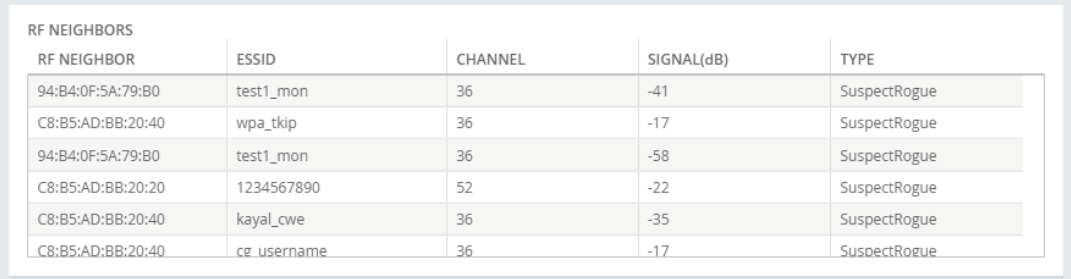
You can also view the data for a specific time of the day by moving the mouse over the **Channel Utilization**, **Noise Floor**, **Frames**, and **Channel Quality** graphs.

RF Neighbors

The **RF Neighbors** table displays details on all the RF neighbors connected to the AP. The table includes the following mandatory columns:

- **RF Neighbor**—The MAC address of the neighboring devices that belong to the same RF group as the AP.
- **ESSID**—The ESSID of the neighboring device.
- **Channel**—The channels assigned under Radio 1 and Radio 2.
- **Signal**—The signal-to-noise ratio in decibels.
- **Type**—The type of RF neighbor in the network. For example, Neighbor, Interferer, or SuspectRogue.

Figure 22 *RF Neighbors*



RF NEIGHBORS

RF NEIGHBOR	ESSID	CHANNEL	SIGNAL(dB)	TYPE
94:B4:0F:5A:79:B0	test1_mon	36	-41	SuspectRogue
C8:B5:AD:BB:20:40	wpa_tkip	36	-17	SuspectRogue
94:B4:0F:5A:79:B0	test1_mon	36	-58	SuspectRogue
C8:B5:AD:BB:20:20	1234567890	52	-22	SuspectRogue
C8:B5:AD:BB:20:40	kayal_cwe	36	-35	SuspectRogue
C8:B5:AD:BB:20:40	cg_username	36	-17	SuspectRogue

APs—VPN Tab

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. The VPN tab displays the following details:

Tunnels

The **Tunnels** 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.

Packet Loss

The **Packet Loss** graph indicates the percentage based on the number of packets lost during the data transmission in the VPN.

The VPN tab is displayed in the AP details page corresponding to Virtual Controllers only. This tab is not displayed for AP details page corresponding to slave APs.

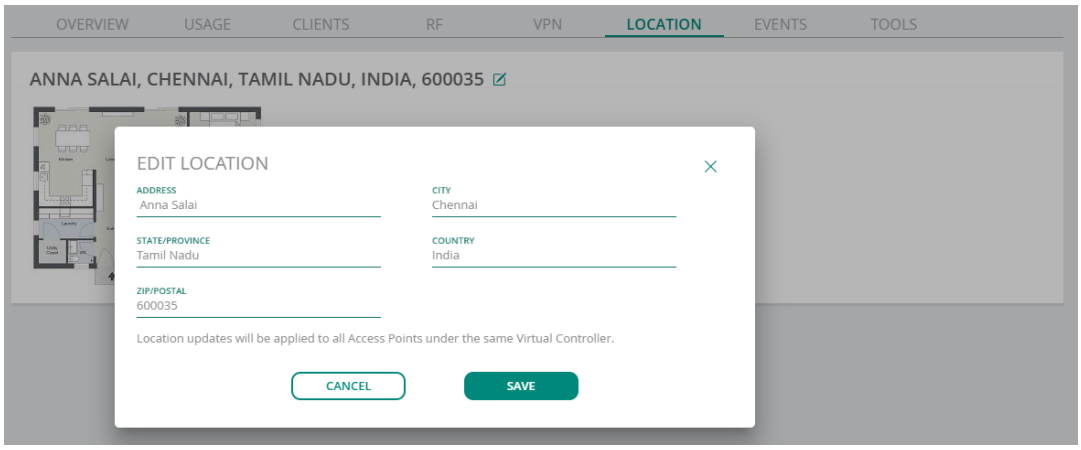
APs—Location Tab

The **Location** tab displays a sitemap or the floor plan showing the current location of the Instant AP device. The sitemap is derived from the Visual RF application, if Visual RF service is enabled for the Aruba Central account.

Figure 23 *Location*

You can also edit the location of the Instant AP device by clicking the edit icon provided next to the adress in the **Location** tab as shown below:

Figure 24 *Edit Location*



APs—Alerts & Logs Tab

The **Alerts & Logs** tab displays the total number of alerts, audit logs, and events generated for the AP. From the summary bar, click the number to drill down to the **Open Alerts**, **Audit Log**, or **Events** table.

Alerts

Alerts are categorized into four types: Critical, Major, Minor, and Warning. Click the number below the alert to view the list of alerts in the **Open Alerts** table. Drag the **Show Acknowledged Alerts** slider to view the acknowledged alerts in the **Acknowledged Alerts** table.

To acknowledge alert(s), select the alert(s) and click **Acknowledge** in the pop-up. To acknowledge all the alerts, click **Acknowledge All**.

The **Open Alerts** and **Acknowledged Alerts** tables display the following details:

- **Occurred On**—Timestamp of the alert. Use the sort option to sort the alerts by date and time.
- **Category**—Displays the category of the alert. Use the filter option to filter the alert by category.
- **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.

For more information about alerts, see Alert Types on page 221.

Audit Log

The audit log number displayed in the summary bar is the total number logs generated for all device management, configuration, and user management events triggered in Aruba Central. Click the number below the log to view the list of logs in the **Audit Log** table.

The **Audit Log** table displays the following details:

- **Occurred On**— Timestamp of the audit log. Use the sort option to sort the audio logs by date and time.
- **IP Address**—IP address of the client device.
- **Username**—Username of the admin user who applied the changes.
- **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. For detailed log information click the action icon. Complete details of the event can be seen by clicking the ellipsis. For example, if an event was not successful, clicking the ellipsis displays the reason for the failure.

For more information about audit logs, see Viewing Audit Trails on page 107.

Events

The events number displayed in the summary bar is the total number of events generated for the AP. Click the number below events to view the list of events in the **Events** table.

The **Events** table displays the following details:

- **Occurred On**—Timestamp of the event. Use the sort option to sort the events by date and time.
- **Category**—Type of event. Use the column filter to search for a particular type of event.
- **Description**—Description of the event. Use the column filter to filter an event based on the description.

APs—Actions

The **Actions** tab displays the following list of actions that can be performed on the AP device. The **Actions** tab displays the following tasks that can be performed on the AP:

- **Reboot AP**—To reboot the AP. Clicking this option displays a confirmation message stating that all clients connected to the device will be disconnected. Click **Yes** to reboot the AP.
- **Reboot Swarm**—To reboot the AP cluster. Clicking this option displays the **APs in the swarm will reboot and all clients connected to those will be disconnected** confirmation message. Click **Yes** to reboot the swarm.
- **Tech. Support**—To enable the administrators to generate a tech support dump required for troubleshooting the device. Clicking the **Tech.Support** option displays the **Maintenance** > **Tools** page of Aruba Central.
- **Console**—To open the remote console for a CLI session through SSH. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. Remote console access is supported only on VCs.

If the Copy and Paste function from the keyboard shortcut keys (CTRL+C and CTRL+V) do not work in your web browser, use the Copy and Paste functions available under the menu options in the web browser.

Live Instant AP Monitoring

Aruba Central supports live monitoring of AP details page corresponding to Instant APs that support Aruba Instant 8.4.0.0 firmware version and above. Aruba Central allows you to monitor live data that are updated in every 5 seconds, in the AP details page of the **Monitoring & Reports** module.

Enabling and Disabling Live Monitoring

To view the AP details page in a live-mode, perform the following steps:

1. From the app selector, click **Monitoring & Reports**.
2. Go to **Network Overview** > **APs** > **List of Online APs** page. The AP List page is displayed.

NOTE

The Live Monitoring feature is not applicable for offline Instant APs.

3. Click the Instant AP entry in the **Access Points** table that supports Aruba Instant 8.4.0.0 firmware version and above. The AP details page is displayed.
4. Click the **Go Live** button at the right corner of the page to view live data.

The **Go Live** button remains grayed-out for all the AP details that are not associated with Instant AP devices running Aruba Instant 8.4.0.0 firmware version and above.

NOTE

Aruba Central allows you to monitor live data for 15 minutes. After this time frame, Aruba Central reverts to the AP details page in a non-live mode to display the monitoring details for the time selected in the Temporal Filter. For more information on AP details page in a non-live mode, see APs.

5. Click the **Stop Live** button manually to switch to the non-live mode.

AP Details in Go Live Mode

Clicking the **Go Live** button displays a page with the following two tabs:

Table 34: *AP Details in Go Live Mode*

Card	Description
Overview	Displays live data related to the radios of the Instant AP such as the radio mode, channels or bands of the radios, and the transmission power for each of the radios in the **Mode**, **Channel/Band**, and **TX Power** fields, respectively. This tab displays constant data until there are any changes to the state of radios such as the power value, channel value, and so on.
RF	Displays live graphs based on noise floor, frames, channel quality of the neighboring RF devices for 15 minutes or till the **Stop Live** button is clicked. This tab displays graphs in the **Noise Floor**, **Frames**, and **Channel Quality** cards for both 5 GHz and 2.4 GHz radios.

Aruba Central allows you to monitor live data for 15 minutes. After this time frame, Aruba Central begins to display the monitoring details for the time selected in the Temporal Filter. For more information on AP Details page in a non-live mode, see APs.

In **Go Live** mode, AP Details page updates and displays data for every 5 seconds.

NOTE

The time range selected in the Temporal Filter becomes non-applicable when the **Go Live** button is enabled.

You can monitor one or more AP Details pages simultaneously on different tabs.

Deleting an Offline AP

To delete an offline AP:

1. Go to **Monitoring & Reports** > **Network Overview** > **APs** > **List of Offline APs**.

2. In the **APs** table, select the offline AP that you want to delete by clicking anywhere on the row, except the **Device Name** column.

Clicking on the **Device Name** column opens the corresponding AP details page.

3. In the pop-up window, click **Delete**.
4. Click **Yes** in the **Confirm Action** dialog box.

For a visual representation of the procedure, click here.

Monitoring Switches and Switch Stacks

The Switches monitoring dashboard provides rich metrics about the health and status of the switch and switch stacks provisioned and managed through Aruba Central.

Page Views

To view the Switches dashboard, go to **Monitoring & Reports** > **Network Overview** > **Switches**.

The Switches dashboard includes the following contents:

- **Usage**—Displays the following graphs:
  - **Usage**—Indicates aggregate client data traffic detected on the switches.
  - **Clients**—Indicates the number of clients connected to the switch.
- **Top N**—Displays a list of switches sorted based on maximum usage. It also shows the data traffic transmitted (Tx) by and received (Rx) from clients.
- **List of Online Switches**—Displays a list of switches that are up. To view the details of a switch, click the name of the device.
- **List of Offline Switches**—Displays a list of switches that are down or not connected to Aruba Central. To view the details of a switch, click the name of the device.

Filters

To set your dashboard view to show only the data pertaining to a group, label, site, or device, use the **Filter Monitoring & Reports** option. By default, Aruba Central displays data for all devices in your Aruba Central account.

To set your dashboard view to show data for specific duration, use the filtering options in **Temporal Filter**. By default, the data is displayed for a time range of 3 hours. To view the graphs for a different time range, click **Temporal Filter** and select a time range of your choice. You can choose to view data for a time period of 3 hours, 1 day, 1 week, 1 month, and 3 months.

Navigation and Granularity

To view more details about a specific switch device, you can use the following page views:

- **List of Online Switches**—To view the details of a switch connected to Aruba Central.
- **List of Offline Switches**—To view the details of a switch that is currently down or not connected to Aruba Central.

Switches Table

The **Switches** table in the **List of Online Switches** and **List of Offline Switches** pages display the following information about the switch or switch stack provisioned in Aruba Central:

- **Device Name**—Name of the switch or switch stack. For a switch stack, a stack icon is displayed next to the device name.
- **Clients**—Number of clients connected.
- **Alerts**—Number of alerts from the switch or switch stack.
- **Model**—Model number of the switch. For a switch stack, the term **Stack** is displayed.
- **Config Status**—Configuration status of the switch or switch stack.
- **Last Seen**—Time when the switch or switch stack connected last, and the time since when the switch or switch stack is operational.
- **Usage**—Data usage on the switches.
- **IP Address**—IP address of the switch or switch stack.
- **MAC**—MAC address of the switch or switch stack.
- **Firmware Version**—Firmware version of the switch or switch stack.
- **Group**—Name of the group to which the switch is assigned.
- **Labels**—Name of the label associated with the switch or switch stack.
- **Site**—Site under which the switch or switch stack is provisioned.
- **Uptime**—Time duration for which the switch is operational.
- **Serial**—Serial number of the switch or switch stack.
- **Uplink Ports**—Uplink ports configured on the switch or switch stack.
- **Port Utilization**—Utilization percentage of the port.

Open Tools

The **Open Tools** button allows you access the troubleshooting utility to troubleshoot Switch issues. For more information on troubleshooting Switches, see Troubleshooting Device Issues and Troubleshooting Device Issues at Advanced Level.

Switch Details

To view the details of specific switch, click the device name of the switch.

Switches—Overview Tab

The **Overview** tab provides a summary of the switch device details, network details, ports, hardware, uplink graph, usage graph, and details about the stack members.

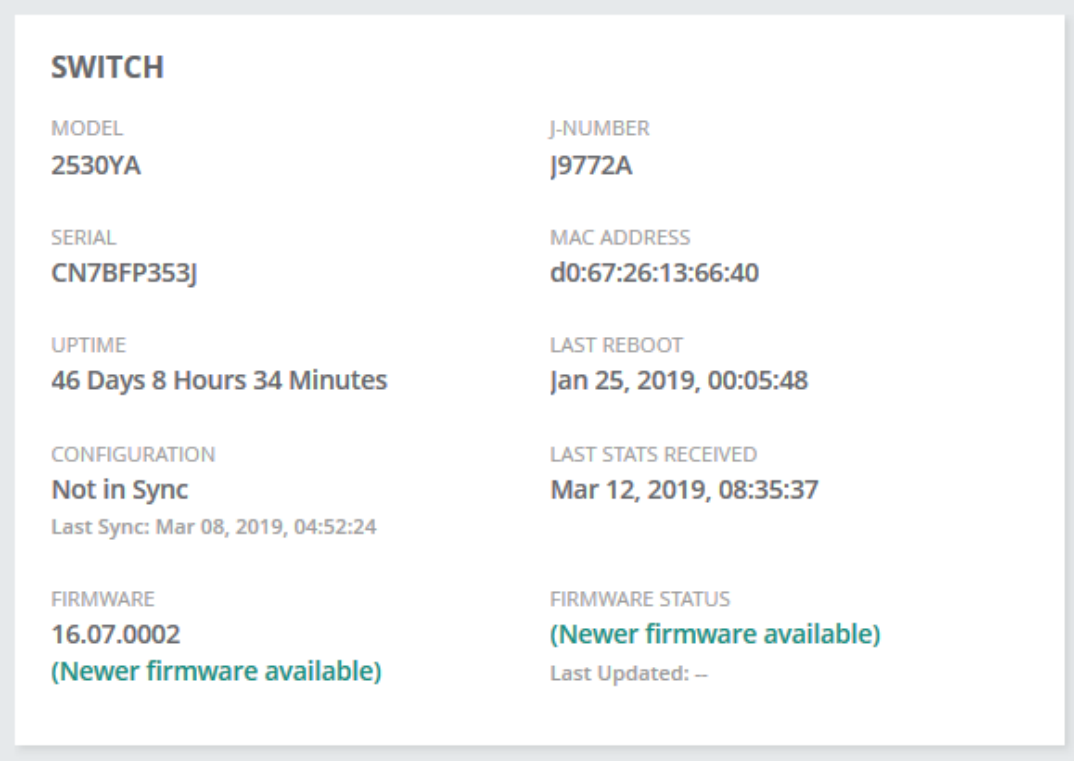
Switch

The **Switch** section displays the following details:

- **Model**—Hardware model of the switch.
- **Location**—Current location of the switch.
- **Contact**—E-mail address of the contact person.
- **Commander**—Name of the commander switch.
- **Serial**—Serial number of the switch.
- **Uptime**—Time duration for which the switches are operational.
- **Configuration**—Configuration status of the switch.

- **Firmware Version**—Firmware version of the switch. If an updated version is available, the version number is displayed and you can click the link to navigate to the firmware management page and upgrade the firmware.
- **J-Number**—Part number of the switch.
- **MAC Address**—MAC address of the switch
- **Last Reboot**—Timestamp of when the switch was last rebooted.
- **Last Stats Received**—Timestamp of when the last statistics were received.
- **Firmware Status**—Displays whether a new firmware version is available.
  - **Last Updated**—Timestamp of when the switch firmware was last changed.

Figure 25 *Switch Overview*

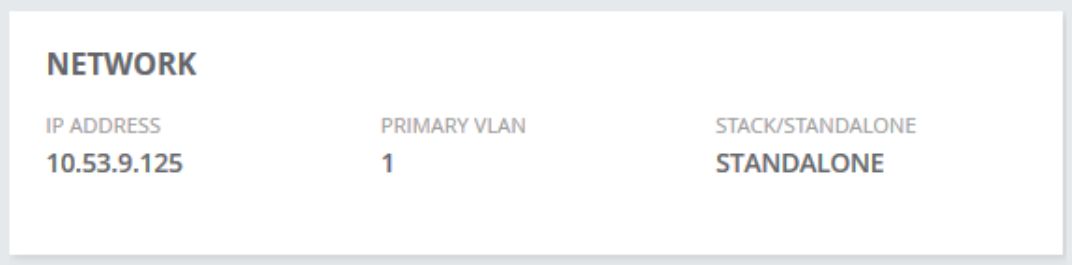


Network

The **Network** section displays the following details:

- **IP Address**—IP address of the switch.
- **Primary VLAN**—Default VLAN ID of the switch.
- **Stack/Standalone**— Indicates whether the switch is part of a stack or if it is a standalone switch.
- **Stack Members**—Total number of members in the stack.
- **Stack Topology**—Topology of the stack.
- **Stack ID**—Stack ID used to identify the stack.

Figure 26 *Network Details*

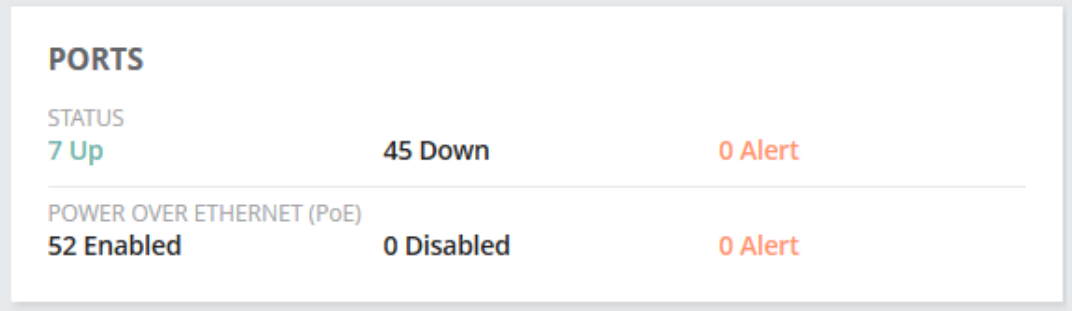


Ports

The **Ports** section displays the following details:

- **Status**—Number of ports in Up and Down state, and number of alerts.
- **Power Over Ethernet (PoE)**—Number of PoE ports enabled and disabled, and number of alerts.

Figure 27 *Port Summary*

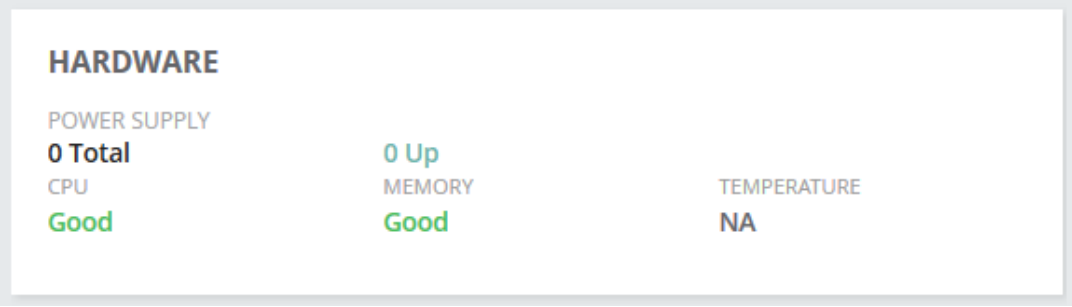


Hardware

The **Hardware** section displays the following details:

- **Power Supply**—Total number of power supplies and number of power supplies in Up state.
- **CPU**—CPU utilization status.
- **Memory**—Memory utilization status.
- **Temperature**—Temperature status. Hover your mouse over the status to view the temperature data.

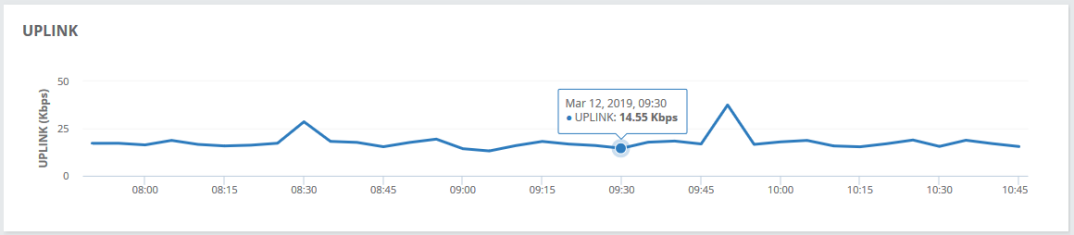
Figure 28 *Hardware Details*



Uplink

The **Uplink** section displays the uplink rate (Mbps) trend chart for the duration specified in the **Temporal Filter**. Hover your mouse over the trend chart to view the uplink rate at a particular time.

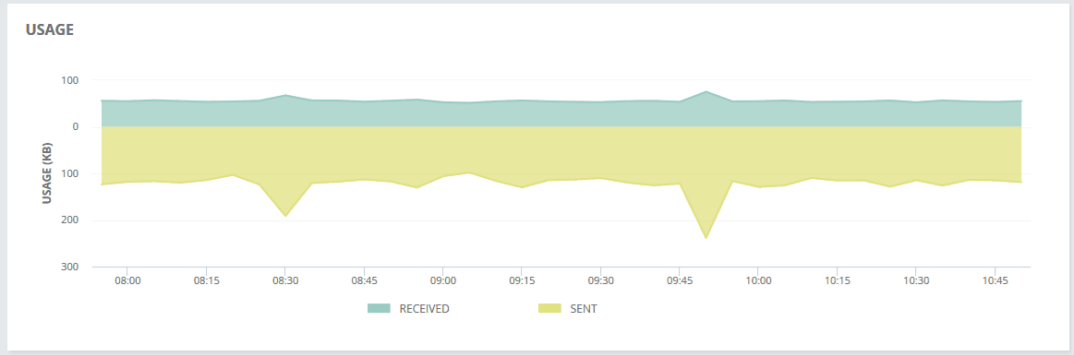
Figure 29 *Uplink Trend Chart*



Usage

The **Usage** section displays the trend chart for client data traffic detected on the switch. Hover your mouse over the trend chart to view data transmitted and received at a particular time.

Figure 30 *Usage Graph*

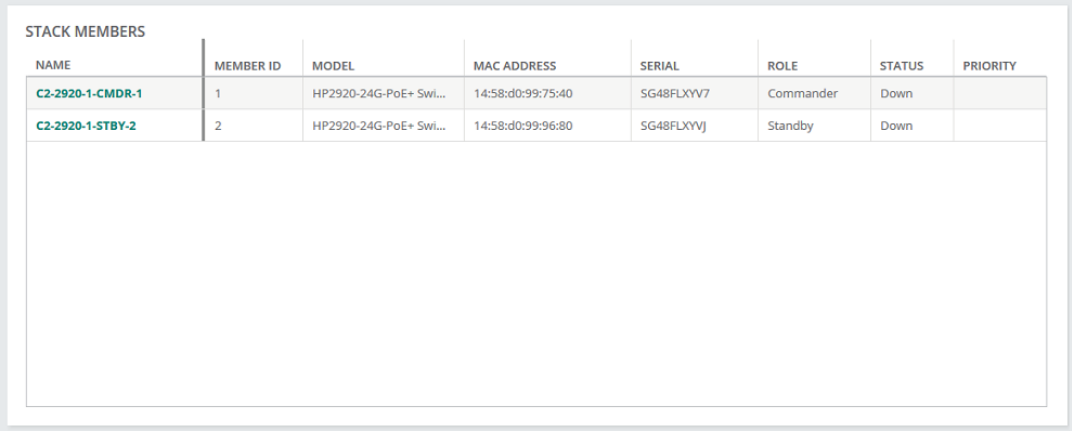


Stack Members

The **Stack Members** table displays the following details:

- Name of the stack member. Click on the name to navigate to the corresponding switch details page.
- Member ID.
- Model number.
- MAC address.
- Serial number.
- Role of the stack member—Commander or Standby.
- Status.
- Priority.

Figure 31 *Stack Members Table*



Switches—Ports Tab

The **Ports** tab displays the summary of ports, switch faceplate, and ports table.

NOTE

To view a visual representation of the **Ports** tab, click here.

Port Status

The **Port Status** section displays the total number of:

- Ports in up state
- Ports in down state
- Alerts generated
- Uplink ports

Faceplate

If the switch is a standalone switch, the faceplate of the switch is displayed. For a switch stack, faceplate of all the switches part of the stack is displayed. From the faceplate, click on the port to drill down and view port-level information. On the switch faceplate, hover your mouse over the port to view the following details: port number, port name, type, speed, and trunk group.

Ports

The **Ports** table displays the following details:

- **Port**—Port number. Use the column filter to search for a particular port and use the sort option to sort the ports in ascending or descending order.
- **Name**—Name of the switch.
- **Status**—Status of the switch. Use the column filter to filter by status.
- **Type**—Type of switch port. Use the column filter to filter by type.
- **MTU (Bytes)**—MTU size of the switch.
- **Port Speed (Mbps)**—Port speed of the switch.
- **Trunk Group**—If the port is part of a trunk group, the name of the trunk group is displayed.
- **Mode**—Operational mode of the port.
- **Admin**—Admin status of the switch.
- **MAC Address**-MAC address of the switch.

Viewing Port-Level Information

Use one of the following options to navigate to the port and view port-level information:

- In the switch faceplate, click on the port number.
- In the Ports table, click the port number.

The port-level information page consists of the following sections:

- **Status**—The **Status** section displays the following details:
  - Operational status
  - Admin status
  - Type of port
  - Description
  - MAC address
  - Name
  - Untagged VLAN
  - Trunk group
  - Data received
  - Data transmitted
- **Port Usage**—The **Port Usage** section provides a graphical representation of data received and transmitted by the port. Hover your mouse over the graph to view data for a particular time of the day.
- **Frame Counters**—The **Frame Counters** section provides a graphical representation of the interface frame counters. From the drop-down list, select one of the following options: **Unicast**, **Broadcast**, **Multicast**, **Discards**, or **Error**.

Switches—PoE Tab

The **PoE** tab displays details such as PoE status summary, PoE ports, and PoE consumption.

The **PoE** tab displays monitoring data only if the switch firmware version is 16.08.0001 or later.

PoE Status

The **PoE Status** section displays the following details:

- **Available**—Power available for consumption for the switch or stack.
- **Used**—Power used by various devices.
- **Remaining**—Power remaining to be utilized in the stack or device.
- **PoE Denied Ports**—Number of ports for which power is denied.

Faceplate

If the switch is a standalone switch, the faceplate of the switch is displayed. For a switch stack, faceplate of all the switches part of the stack is displayed. From the faceplate, click on the port to drill down and view port-level information. On the switch faceplate, hover your mouse over the PoE port to view the following details: port number, port name, type, class, and priority.

From the **Context** drop-down list, select the context:

- **POE-STATUS**—Displays the sate of each port. The state can be: Uplink, Drawing, Enabled, Disabled, or Alert.
- **POE-CLASS**—Power class of the PoE port. The class can be: 0, 1, 2, 3, 4, or 5.
- **POE PRIORITY**—PoE priority configured on the port. The priority can be: Critical, High, or Low.

NOTE

For a visual representation of how to set the context on the faceplate, click here.

Ports PoE

The **Ports PoE** table displays the following details:

- **Port**—Port number.
- **PoE**—PoE state: Enabled or Disabled.
- **Class**—Power class of the PoE port.
- **Priority**—PoE priority: Critical, High, or Low.
- **Status**—Current power status of the PoE port: Searching, Delivering, Disabled, or Fault.
- **Pre-STD Detect**—Displays whether PoE for pre-802.3af-standard powered devices is enabled on the switch: On or Off.
- **Alloc Actual**—Power actually being used on the port.
- **Alloc Configured**—The maximum amount of power allocated for the port.
- **PLC Type**—Physical layer classification type.

PoE Consumption

The **PoE Consumption** section displays a trend chart for the PoE power drawn from the Switch in watts. Hover your mouse over the trend chart to view the PoE power drawn at a particular time. For a stack, select the switch from the drop-down list to view the PoE consumption for the specific device.

NOTE

For a visual representation of how to view PoE consumption for a switch stack, click here.

Viewing PoE Port-Level Information

Use one of the following options to navigate to the PoE port and view port-level information:

- In the switch faceplate, click on the port number.
- In the **Ports PoE** table, click the port number.

NOTE

For a visual representation of how to navigate to the PoE port level, click here.

The port-level information page consists of the following tabs:

- Summary
- Slot Info & PoE Configuration
- LLDP Information

Summary

The **Summary** tab consists of the following sections:

- Summary—Displays the following details:
  - **PSE Reserved Power**—Power reserved for the port in the Power Sourcing Equipment (PSE).
  - **PSE Voltage**—Total voltage, in volts (V), currently being delivered to the powered device connected to the port
  - **PD Power Draw**—Power drawn by the powered device.
  - **PD Amperage Draw**—Amperage drawn by the powered device.

- **Over Current Count**—Number of times a powered device connected to the port attempted to draw more power than was allocated to the port.
- **MPS Absent Count**—Number of times the powered device has no longer requested power from the port MPS is Maintenance Power Signature.
- **Power Denied Count**—Number of power requests from the port that were denied because sufficient power was unavailable.
- **Short Count**—Number of times the switch provided insufficient current to the powered device connected to the port.

- **PoE Consumption**—Displays the trend chart for PoE consumption and power available for the duration specified in the **Temporal Filter**.

Slot Info & PoE Configuration

The **Slot Info & PoE Configuration** tab consists of the following sections:

- **PoE Slot Information**—Displays the following details:
  - **Slot**—Slot where the port is located.
  - **Operation Status**—Displays PoE power is available for the slot: On, Off, or Faulty.
  - **Maximum Power**—Maximum PoE wattage available to provision active PoE ports in the slot.
  - **Power In Use**—PoE power currently being used by the slot.
  - **Usage Threshold**—Configured percentage of available PoE power provisioning the switch must exceed to generate a usage notice.
- **PoE Configuration**—Displays the following details:
  - **PoE Power**—Displays whether PoE power is enabled on the port.
  - **Pre-Std Detect**—Displays whether PoE for pre-802.3af-standard powered devices is enabled on the switch: On or Off.
  - **PoE Port Status**—Current power status of the PoE port: Searching, Delivering, Disabled, or Fault.
  - **Power Priority**—Power priority configured on ports enabled for PoE: Low, High, or Critical.
  - **PLC Class Type**—Physical layer classification type.
  - **DLC Class Type**—Data link layer classification type.
  - **Configured Type**—If configured, shows the user-specified identifier for the port. If not configured, this field is empty.
  - **PoE Value Configuration**—PoE power value configured for the port.

LLDP Information

The **LLDP Information** tab displays the following details:

- **PSE Allocated Power**—Power allocated for the port in the PSE.
- **PD Requested Power**—Power requested by the powered device.

Switches—VLANs Tab

The **VLANs** tab displays VLAN name, VLAN ID, tagged and untagged ports, and faceplate. The VLANs tab consists of the following sections:

- VLANs table
- Faceplate of the switch or switch stack

VLANs

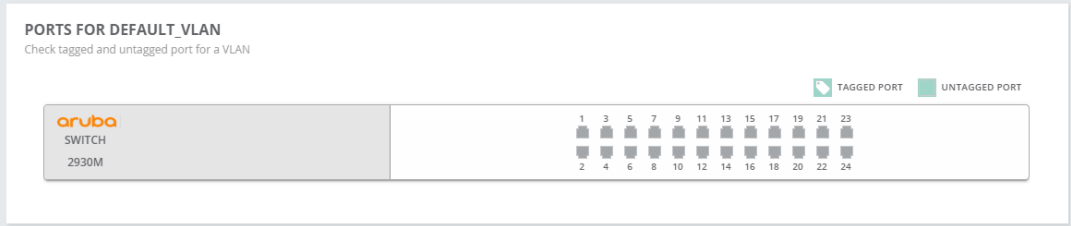
The **VLANs** table displays the following details:

- **Name**—VLAN name. Click the sort icon to sort the column.
- **ID**—VLAN ID.
- **Tagged Ports**—Displays the ports which have marked the VLAN as tagged.
- **Untagged Ports**—Displays the ports which have marked the VLAN as untagged.

Faceplate

From the **VLANs** table, select a VLAN to view the tagged and untagged ports in the faceplate.

The following is an illustration of the switch faceplate:



Switches—Hardware Tab

The **Hardware** tab displays information related to power supplies, fans, utilization and temperature.

Hardware

The **Hardware** table displays the overall hardware summary:

- **ID**—Identity of the hardware.
- **Name**—Name of the device.
- **Power Supplies**
  - **Total**—Total number of power supplies.
  - **Up**—Number of power supplies in Up state.
  - **Down**—Number of power supplies in Down state.
- **Fans**
  - **Total**—Total number of fans.
  - **Up**—Number of fans in Up state.
  - **Down**—Number of fans in Down state.
- **Utilization**
  - **CPU**—Current CPU utilization percentage.
  - **Memory**—Current memory utilization percentage.
- **Temperature**
  - **Current**—Current temperature.
  - **Min**—Minimum temperature.
  - **Max**—Maximum temperature.

Power Supplies

The **Power Supplies** table displays the following details:

- **Name**—Name of the power supply.

- **Status**—Current status of the power supply.

Fans

The **Fans** table displays the following details:

- **Name** —Name of the fan.
- **Status**—Current status of the fan.

CPU

The **CPU** section displays the current CPU utilization percentage and trend chart for the duration specified in the **Temporal Filter**. Hover your mouse over the trend chart to view the CPU utilization at a particular time.

Memory

The **Memory** section displays the current memory utilization percentage and trend chart for the duration specified in the **Temporal Filter**. Hover your mouse over the trend chart to view the memory utilization at a particular time.

Temperature

The **Temperature** section displays the current, minimum, and maximum temperature and trend chart for the duration specified in the **Temporal Filter**. Hover your mouse over the trend chart to view the temperature at a particular time.

Switches—Connected Tab

The **Connected** tab displays the number of intermediate and client devices connected to the switch or switch stack. From the switch faceplate section, you can navigate to the node details of the port. The node details page displays the authentication method used for the node.

Client Devices Table

The **Client Devices** table displays the following details:

- **Name**—Name of the client device.
- **Status**—Status of the client.
- **Port**—Port number of the switch that the device is connected to.
- **MAC Address**—MAC address of the client device. Use the sort option to sort MAC address.
- **IP Address**—IP address of the client device.

The wired client will show up in the **Client Devices** table 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.

Neighbor Devices Table

The **Neighbor Devices** table displays the following details:

- **MAC Address**—MAC address of the neighboring device.
- **Serial**—Serial number of the neighboring device.
- **IP Address**—IP address of the neighboring device.
- **Description**—Description of the neighboring device.
- **Local Port**—Local port number of the neighboring device.
- **Remote Port**—Remote port number of the neighboring device.
- **Capabilities**—Capabilities of the neighboring device.

Switches—Alerts & Logs Tab

The **Alerts & Logs** tab displays the total number of alerts, audit logs, and events generated for the switch. From the summary bar, click the number to drill down to the **Open Alerts**, **Audit Log**, or **Events** table.

Alerts

Alerts are categorized into four types: Critical, Major, Minor, and Warning. Click the number below the alert to view the list of alerts in the **Open Alerts** table. Drag the **Show Acknowledged Alerts** slider to view the acknowledged alerts in the **Acknowledged Alerts** table.

To acknowledge alert(s), select the alert(s) and click **Acknowledge** in the pop-up. To acknowledge all the alerts, click **Acknowledge All**.

The **Open Alerts** and **Acknowledged Alerts** tables display the following details:

- **Occurred On**—Timestamp of the alert. Use the sort option to sort the alerts by date and time.
- **Category**—Displays the category of the alert. Use the filter option to filter the alert by category.
- **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.

For more information about alerts, see Alert Types on page 221.

Audit Log

The audit log number displayed in the summary bar is the total number logs generated for all device management, configuration, and user management events triggered in Aruba Central. Click the number below the log to view the list of logs in the **Audit Log** table.

The **Audit Log** table displays the following details:

- **Occurred On**— Timestamp of the audit log. Use the sort option to sort the audio logs by date and time.
- **IP Address**—IP address of the client device.
- **Username**—Username of the admin user who applied the changes.
- **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. For detailed log information click the action icon. Complete details of the event can be seen by clicking the ellipsis. For example, if an event was not successful, clicking the ellipsis displays the reason for the failure.

For more information about audit logs, see Viewing Audit Trails on page 107.

Events

The events number displayed in the summary bar is the total number of events generated for the switch. Click the number below events to view the list of events in the **Events** table.

The **Events** table displays the following details:

- **Occurred On**—Timestamp of the event. Use the sort option to sort the events by date and time.
- **Category**—Type of event. Use the column filter to search for a particular type of event.
- **Description**—Description of the event. Use the column filter to filter an event based on the description.

Switches—Actions

The **Actions** tab displays the various options available for remote administration of the switch. The following options are available:

- **Reboot**—Reboots the switch.
- **Tech Support**—Allows the administrators to generate a tech support dump for troubleshooting the device.
- **Console**—Opens the remote console for a CLI session through SSH. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. For the Aruba Switch platforms, the remote console access is enabled only when the user credentials are configured in the **Wired Management** app.

NOTE

If the Copy and Paste function from the keyboard shortcut keys (CTRL+C and CTRL+V) do not work in your web browser, use the Copy and Paste functions available under the menu options in the web browser.

Deleting an Offline Switch

To delete an offline switch:

1. Go to **Monitoring & Reports** > **Network Overview** > **Switches** > **List of Offline Switches**.
2. In the **Switches** table, select the switch that you want to delete by clicking anywhere on the row, except the **Device Name** column.

NOTE

Clicking on the **Device Name** column opens the corresponding switch details page.

3. In the pop-up window, click **Actions** and select **Delete** from the drop-down list.
4. Click **Yes** in the **Confirm Action** dialog box.

NOTE

For a visual representation of the procedure, click here.

Switches—Assigning Uplink Ports

To assign uplink port(s):

1. Go to **Monitoring & Reports** > **Network Overview** > **Switches** > **List of Online Switches**.
2. In the **Switches** table, select the switch for which you want to assign uplink port(s) by clicking anywhere on the row.
3. In the pop-up window, click **Uplinks**.
4. In the pop-up window, click the **Assign Uplink Ports** drop-down list, select the port(s), and click **Assign**.

NOTE

For a visual representation of the procedure, click here.

Gateways

The **Gateways** monitoring dashboard provide rich metrics about the health and status of the SD-WAN devices provisioned and managed through Aruba Central.

Page Views

To view the Gateways dashboard, go to **Monitoring & Reports** > **Network Overview** > **Gateways**.

The **Gateways** dashboard includes the following contents:

- **Usage**—Displays the overall usage metrics for the Gateways provisioned in your Aruba Central account.

- **Usage**—Displays the incoming and outgoing data traffic in the WAN network.
- **WAN Compression**—The graph 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.
- **WAN Tag Provider Distribution**—Displays the number of online and offline uplinks per WAN provider.
- **WAN Type Provider Distribution**—Displays the number of online and offline uplinks per WAN circuit type.
- **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.

- **List of Offline Gateways**—Displays a list of Gateways that are currently down and not connected to Aruba Central.
- **List of Online Gateways**—Displays a list of Gateways that are connected to Aruba Central.
- **Distribution**—Displays the total percentage of Gateways distributed per hardware platform and software versions.

Filters

To set your dashboard view to show only the data pertaining to a group, label, site, or device, use the **Filter Monitoring & Reports**. By default, Aruba Central displays data for all devices in your Aruba Central account.

To set your dashboard view to show data for specific duration, use the filtering options in **Temporal Filter**. By default, the data is displayed for a time range of 3 hours. To view the graphs for a different time range, click **Temporal Filter** and select a time range of your choice. You can choose to view data for a time period of 3 hours, 1 day, 1 week, 1 month, and 3 months.

Navigation and Granularity

To view more details about a specific Gateway device, you can use the following page views:

- **List of Online Gateways**—To view the details of a Gateway connected to Aruba Central.
- **List of Offline Gateways**—To view the details of a Gateway that is currently down or not connected to Aruba Central. You can also delete an offline Gateway.

Gateways Table

The **Gateways** table on List of Offline and List of Online Gateways pages displays the following information about the Gateways provisioned in Aruba Central.

The default view of Gateways table shows only a few columns. To view the hidden columns, click the settings icon at the right side of the table. To reset the columns, click **Reset Columns**.

- **Device Name**—Name of the Gateway. This column also includes a search filter to allow users to search for a Gateway.
- **Model**—Hardware model of the Gateway.
- **Firmware Version**—The current firmware revision of the Gateway
- **Uptime**—Displays the uptime of each Gateway.
- **IP Address**—IP address of the Gateway.
- **Site**—Name of the site in which the Gateway is deployed.
- **MAC**—MAC address of the Gateway.

- **Group**—Group to which the Gateway is assigned.
- **Labels**—Name of the label. Clicking the label name opens the per label details.
- **Serial**—Serial number of the Gateway.

The **List of Offline Gateways** page allows you to delete a Gateway that is currently not connected to Aruba Central. To delete a Gateway, select the Gateway from the Gateways table, and click **Delete**.

Gateway Details Page View

To view the details of specific Gateway, click the device name of the Gateway. On clicking a Gateway, the dashboard provides detailed information about the Gateway operational status and WAN details.

The header panel of the Gateways dashboard displays the following information:

- **WAN**—Displays the total number of WAN interfaces that are currently operational or down. On clicking a number, the dashboard displays WAN interface details.
- **LAN**—Displays the total number of LAN interfaces that are currently operational or down. On clicking a number, the dashboard displays LAN and VLAN interface details.
- **Tunnels**—Displays the total number of VPN tunnels that are currently active or down. On clicking a number, the dashboard displays VPN tunnel details.
- **Path Steering**—Displays the total number of path steering policies that are compliant with the performance criteria (SLAs) defined for each type of traffic.
- **Alerts**—Displays the total number of open alerts that are yet to be acknowledged.

The header section of the Gateway monitoring dashboard also shows the uptime for Gateways that are online and connected to Aruba Central.

Actions Drop-down List

The **Actions** tab displays the following information:

- **Reboot Gateway**—Reboots the gateway.
- **Open Remote Console**—Opens the remote console for a CLI session through SSH. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device.

Open Tools

The **Open Tools** button allows you access the troubleshooting utility for troubleshoot Gateway issues.

Tabs

The Gateway monitoring dashboard includes the following tab views:

- Overview
- WAN
- LAN
- Tunnels
- Routing
- Path Steering
- Applications
- Alerts and Logs
- Sessions

Gateways—Overview Tab

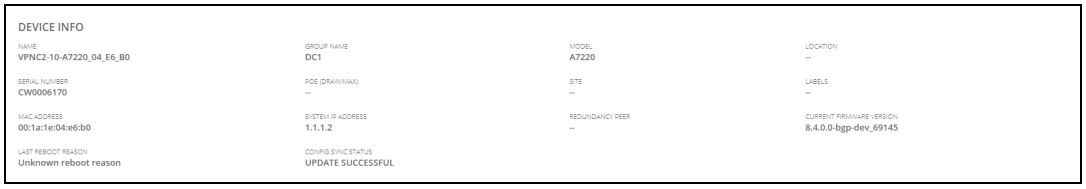
After you onboard and configure the gateways, you can view the branch health, monitor the WAN uplink, and view gateway performance from the **Gateways** page.

From the app selector, click **Monitoring & Reports** and go to **Network Overview** > **Gateways**. The **Gateways** page displays the following details for the gateways that are deployed in the WAN network.

The **Overview**dashboard provides gateway device details, WAN availability and performance information, and the list of top applications. The **Overview** tab displays the following details:

Device Info

Figure 32 *Device Info*



Displays the gateway device details. From the drop-down list, select **Overview** to view the following details:

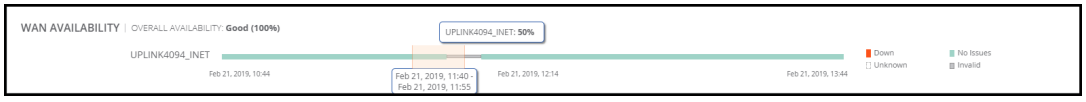
- **Name**—Name of the gateway.
- **Serial Number**—Serial number of the gateway.
- **MAC Address**—MAC address of the gateway.
- **Last Reboot Reason**—Reason for the last reboot.
- **Group Name**—Name of the group to which the gateway belongs.
- **POE (DRAW/MAX)**—The amount of power that the devices connected to the Branch Gateway consume and the maximum PoE power capacity. For example, if the value displayed is 6/120, the devices draw 6 watts and the maximum PoE power allocated is 120 watts.
- **System IP address**—IP address of the gateway.
- **Config Sync Status**—Status of the configuration sync.
- **Model**—Hardware model of the gateway.
- **Site**—Site name of the gateway location.
- **Redundancy Peer**—Displays the redundant gateway. Click the link to view the redundant gateway details. See the *Setting up Redundant Gateways for High Availability* section in the *Aruba Central Help Center*.
- **Location**—Physical location of the gateway.
- **Labels**—Labels attached to the gateway.
- **Current Firmware Version**—Firmware version running on the gateway.

The dashboard also displays additional overview information about WAN and VPN:

WAN Availability

Provides a graphical representation of the Branch Gateway's WAN uplink availability. The graph displays each WAN uplink availability for the selected time range. Availability is determined by default gateway, monitored IP, and data VPN Concentrator reachability.

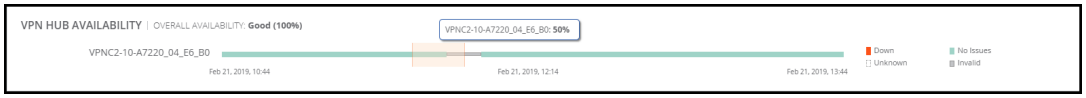
Figure 33 *WAN Availability*



VPN Hub Availability

Provides a graphical representation of the Branch Gateway's tunnel availability. Availability is determined by the probe settings configured using the **Health Check** option.

Figure 34 *VPN Hub Availability*



Aggregate WAN Usage

Displays the Branch Gateway's aggregate inbound and outbound traffic usage by WAN interface. Select one of the following options from the drop-down list:

Figure 35 *Aggregate WAN Usage—All Traffic*

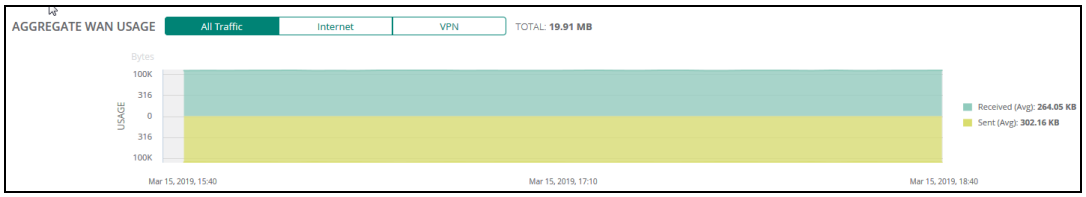


Figure 36 *Aggregate WAN Usage—Internet*

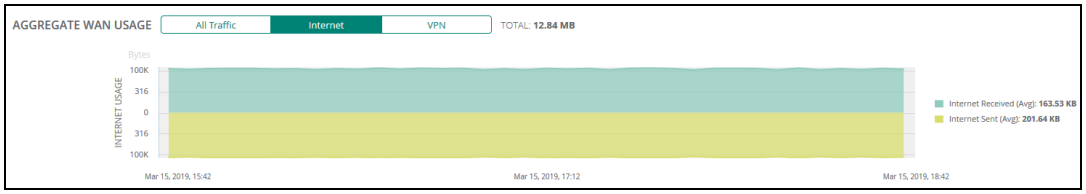
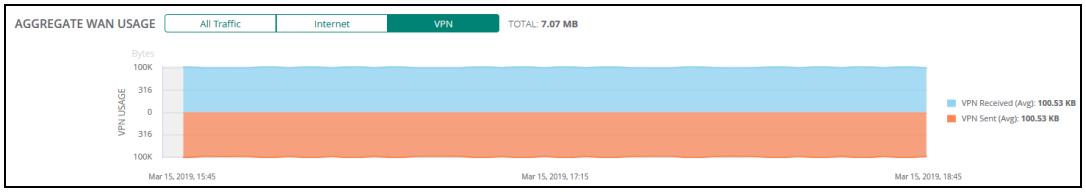


Figure 37 *Aggregate WAN Usage—VPN*



Aggregate WAN Compression

Displays the aggregate WAN compression details across all uplinks. The average bandwidth savings is displayed as a percentage. The compressed and uncompressed bandwidth is displayed as vertical grouped bar graphs. For more information about the process to enable data compression, see the *Configuring Uplink Interfaces* section in the *Aruba Central Help Center*.

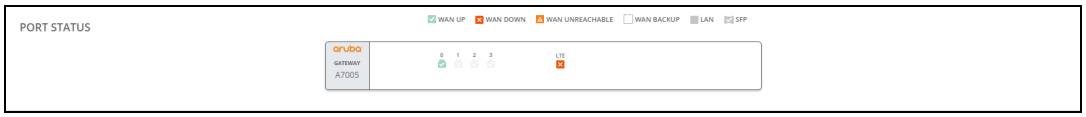
Figure 38 *Aggregate WAN Compression*

Gateway—WAN Tab

If the gateway is provisioned as a Branch Gateway, the **WAN** tab displays the following details:

- **Port Status**—Displays the WAN port status. Click a WAN port for more details.

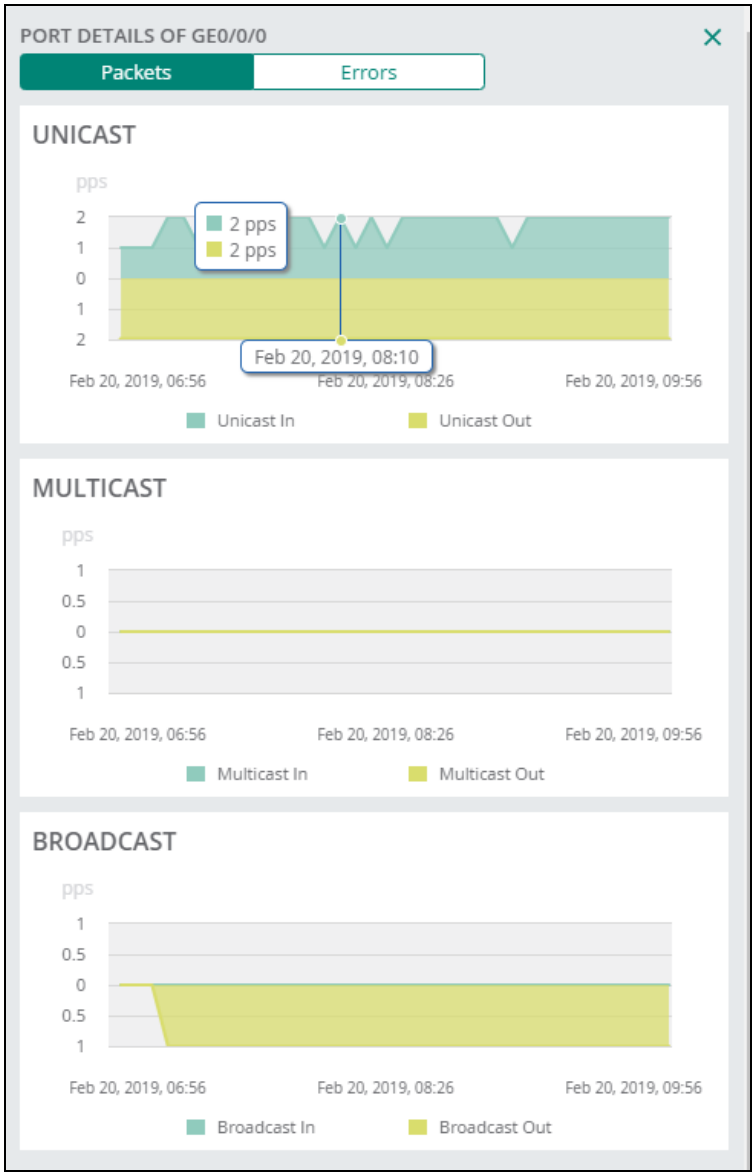
Figure 39 *Port Status*



In the **Port Status** table, click a port number to display the **Packets** and **Errors** details.

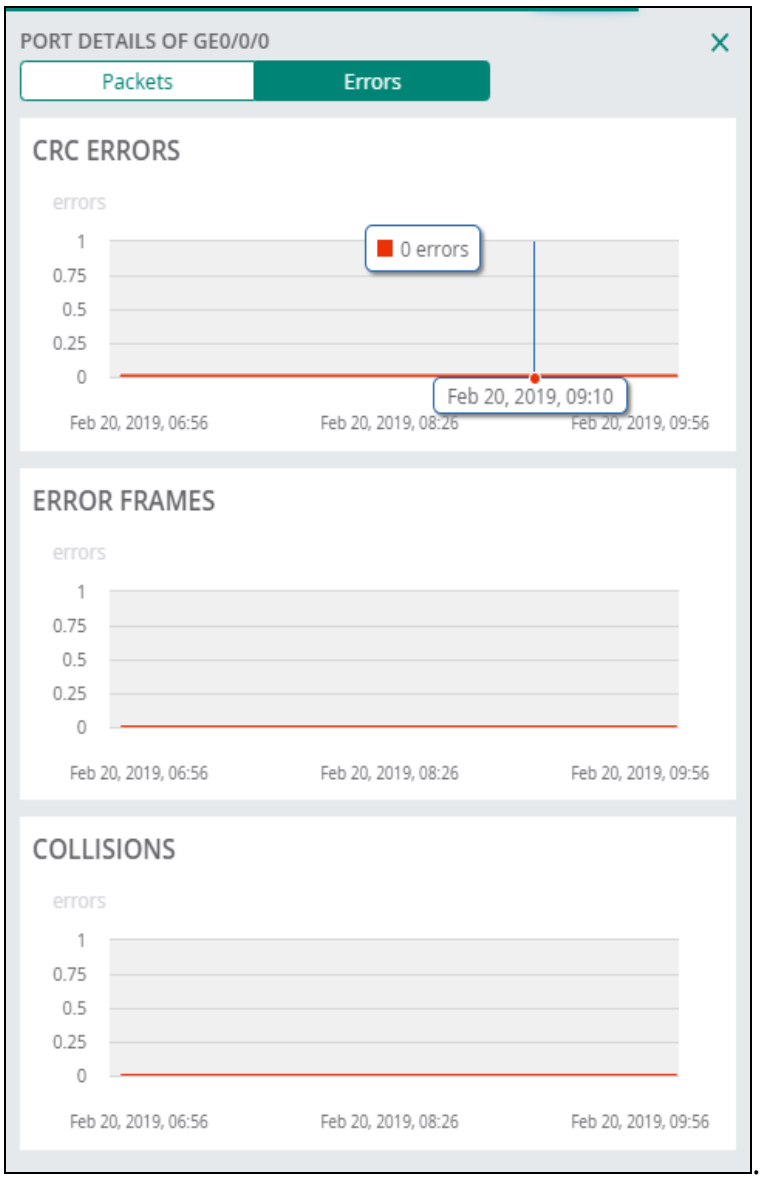
- The following graphs are displayed for the **Packets** interface:
  - **Unicast**—The number of unicast packets per second.
  - **Multicast**—The number of multicast packets per second.
  - **Broadcast**—The number of broadcast packets per second.

Figure 40 *Packet details of a port*



- The following graphs are displayed for the **Errors** interface:
  - **CRC Errors**—The number of cyclic redundancy errors logged.
  - **Error Frames**—The number of error frames logged.
  - **Collisions**—The number of collisions encountered.

Figure 41 *Error details of a port*



- **WAN Interfaces Summary**—The table lists the WAN interfaces and provides the total number of WAN interfaces. Displays the summary of WAN uplinks. The following details are displayed for the port:

NOTE

Click the Settings icon to reset or set the default columns that are displayed.

- **Total WAN Interfaces**—Total number of WAN interfaces available.
- **Port**— Port number.
- **Provider Tag/Type**—Service provider uplink tag or type.
- **Type**—WAN interface type.
- **VLAN ID**—VLAN identification number.
- **Oper. State**—Operational status.
- **Loss**—Loss percentage.
- **Latency**—The latency in microseconds.

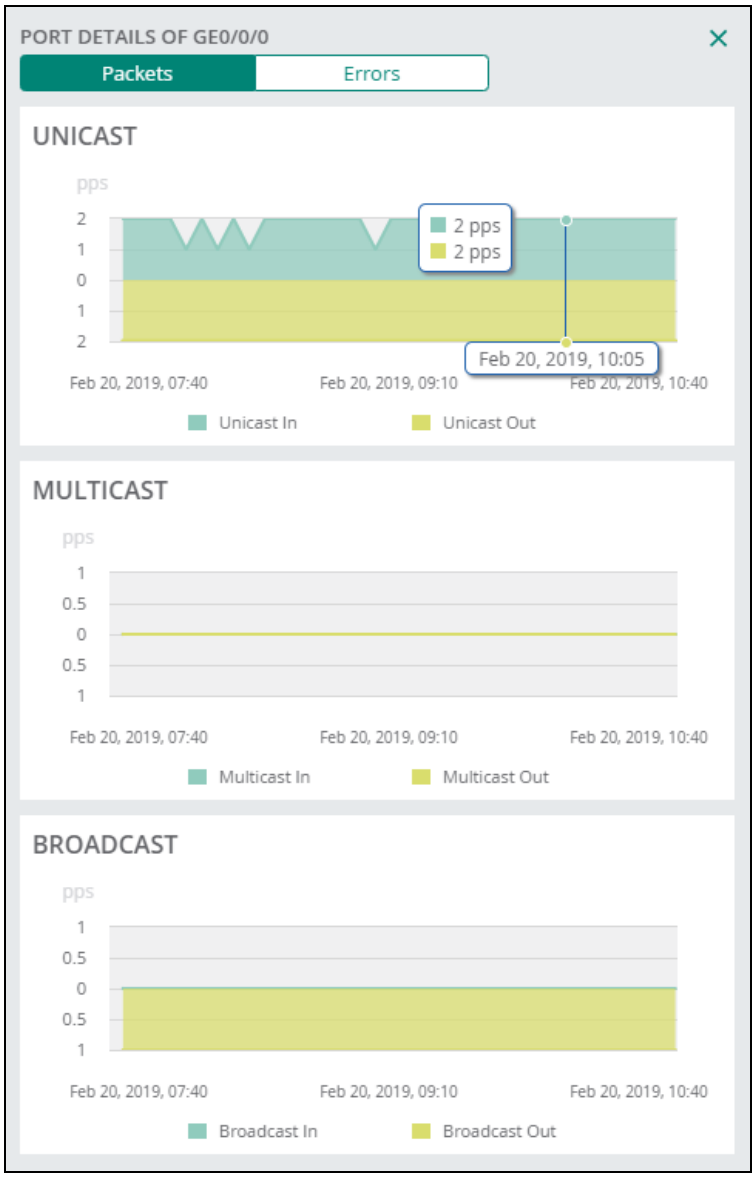
- **Private IP**—Private IP address.
- **Speed**—Indicated the type of connection, for example Auto, Full duplex or Half duplex.

Figure 42 *WAN interfaces summary*

In the **WAN Interfaces Summary** table, click a port number to display the **Packets** and **Errors** details.

- The following graphs are displayed for the **Packets** interface:
  - **Unicast**—The number of unicast packets per second.
  - **Multicast**—The number of multicast packets per second.
  - **Broadcast**—The number of broadcast packets per second.

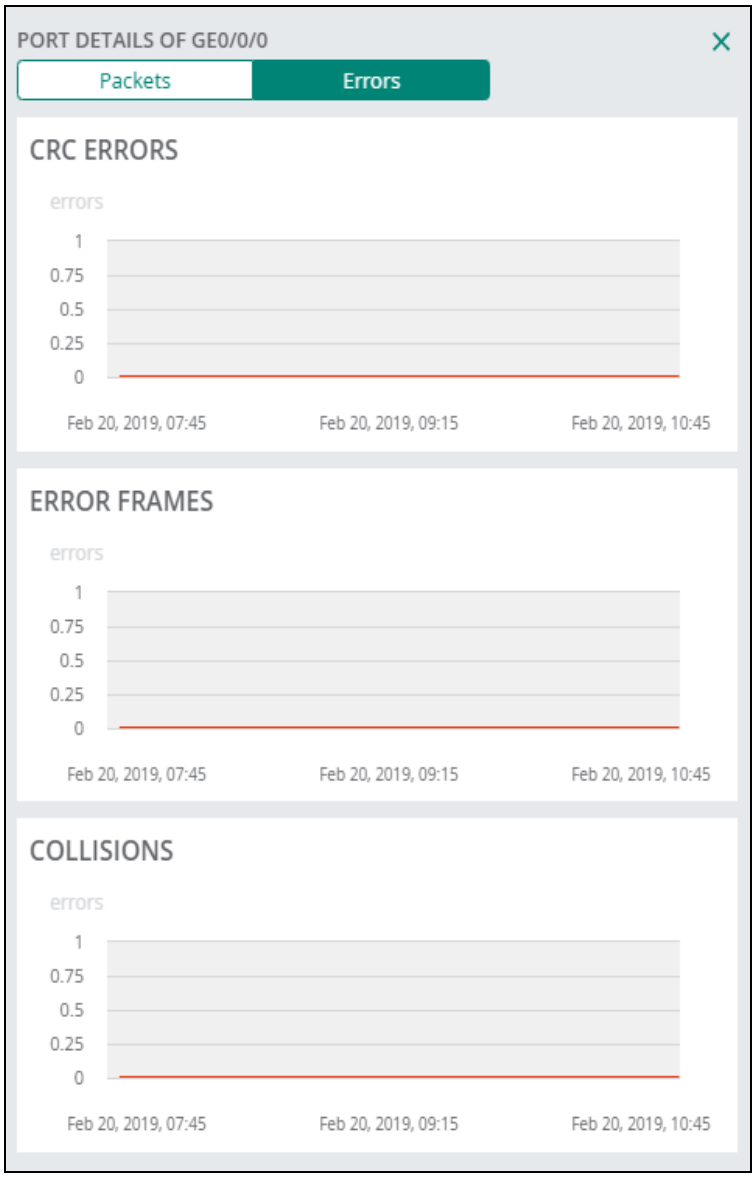
Figure 43 *Packet details of an interface*



- The following graphs are displayed for the **Errors** interface:

- **CRC Errors**—The number of cyclic redundancy errors logged.
- **Error Frames**—The number of error frames logged.
- **Collisions**—The number of collisions encountered.

Figure 44 *Error details of an interface*



- **WAN Interface Details**—In the **WAN Interfaces Summary** table, select a **Provider Tag/Type** to view the WAN interface details.

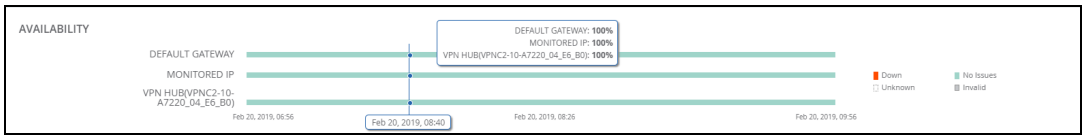
The following details are displayed for the WAN interface:

- **Status**—Operational status.
- **Provider Tag/Type**—Service provider uplink tag or type.
- **IP Address**—Private IP address.
- **Public IP Address**—Public IP address.
- **Default Gateway**—Default gateway.
- **Avg. MOS**—Indicates the transport health based on active monitoring probes. The field displays the average MOS score of all VPN probes.

Figure 45 *WAN interface details*

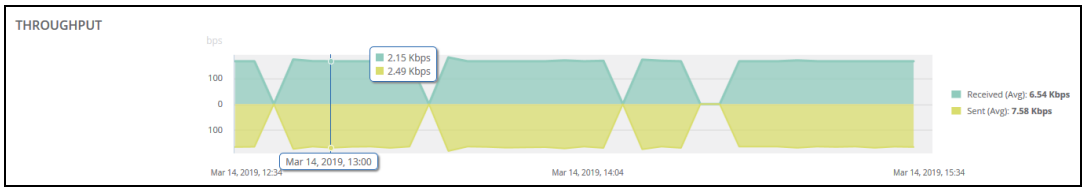
- **Availability**—Provides a graphical representation of the selected WAN interface's availability based on reachability. The graph shows the selected WAN port's ability to reach its default gateway, monitored IP, and VPN Concentrator.

Figure 46 *Availability of the interfaces*



- **Throughput**—Provides a graphical representation of the selected WAN interface's throughput. The graph displays the WAN interface's transmit and receive performance in Kbps.

Figure 47 *Throughput details*



- **WAN Usage**—Provides a snapshot of the WAN usage and is available for **All Traffic**, **Internet**, and **VPN** specific information. The graphs also display information that is sent and recieved.

Figure 48 *WAN Usage—All Traffic*

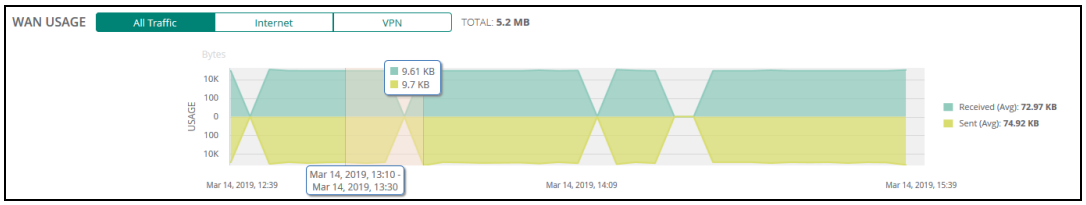


Figure 49 *WAN Usage—Internet*

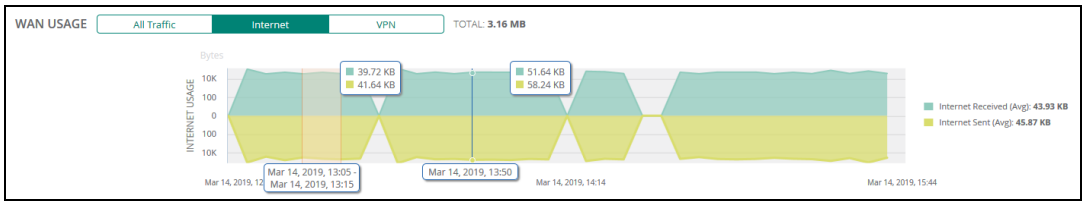
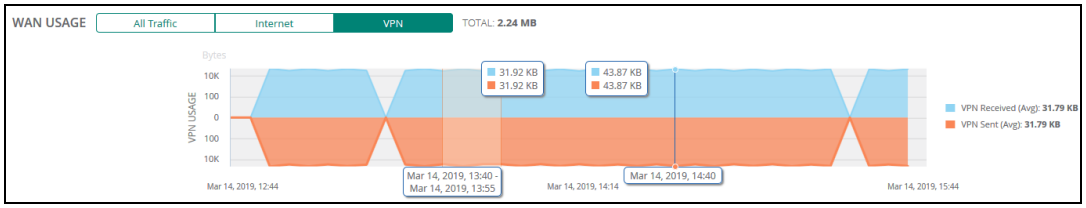


Figure 50 *WAN Usage—VPN*

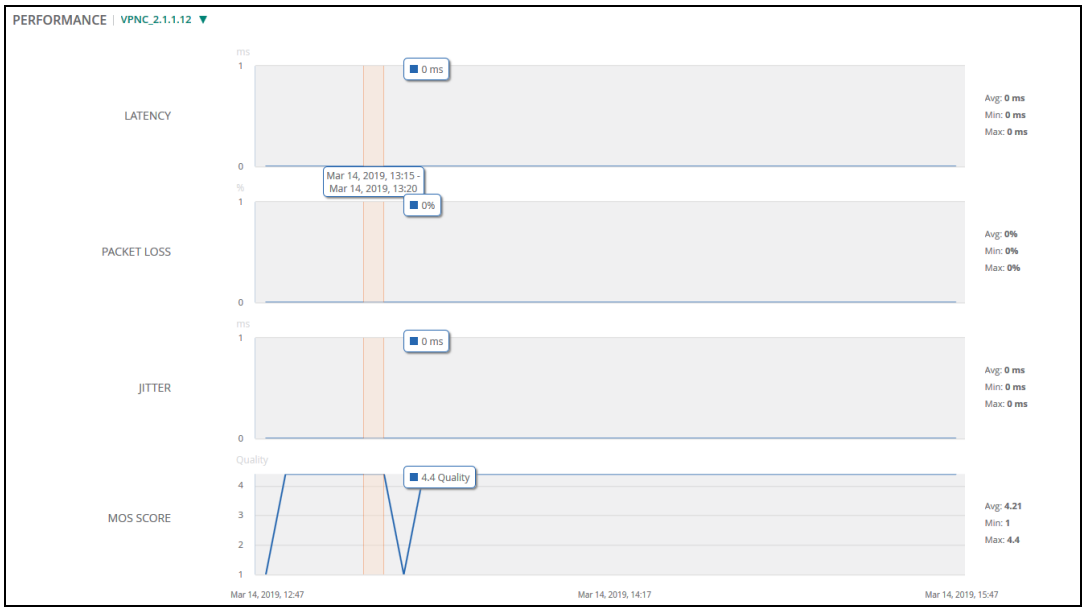


- **WAN Compression**—Provides informaton on the percentage of optimised and non optimized packetsand the average percentage of bandwidth saved.

Figure 51 *WAN Compression information*

- **Performance**—The Performance section displays the following details based on the interface that is selected:
  - **Latency**—The latency in milliseconds.
  - **Packet Loss**—Displays the packet loss in percentage.
  - **Jitter**—Displays the jitter in milliseconds.
  - **MOS Score**—Displays the MOS score.

Figure 52 *Performance details*



Gateways—LAN Tab

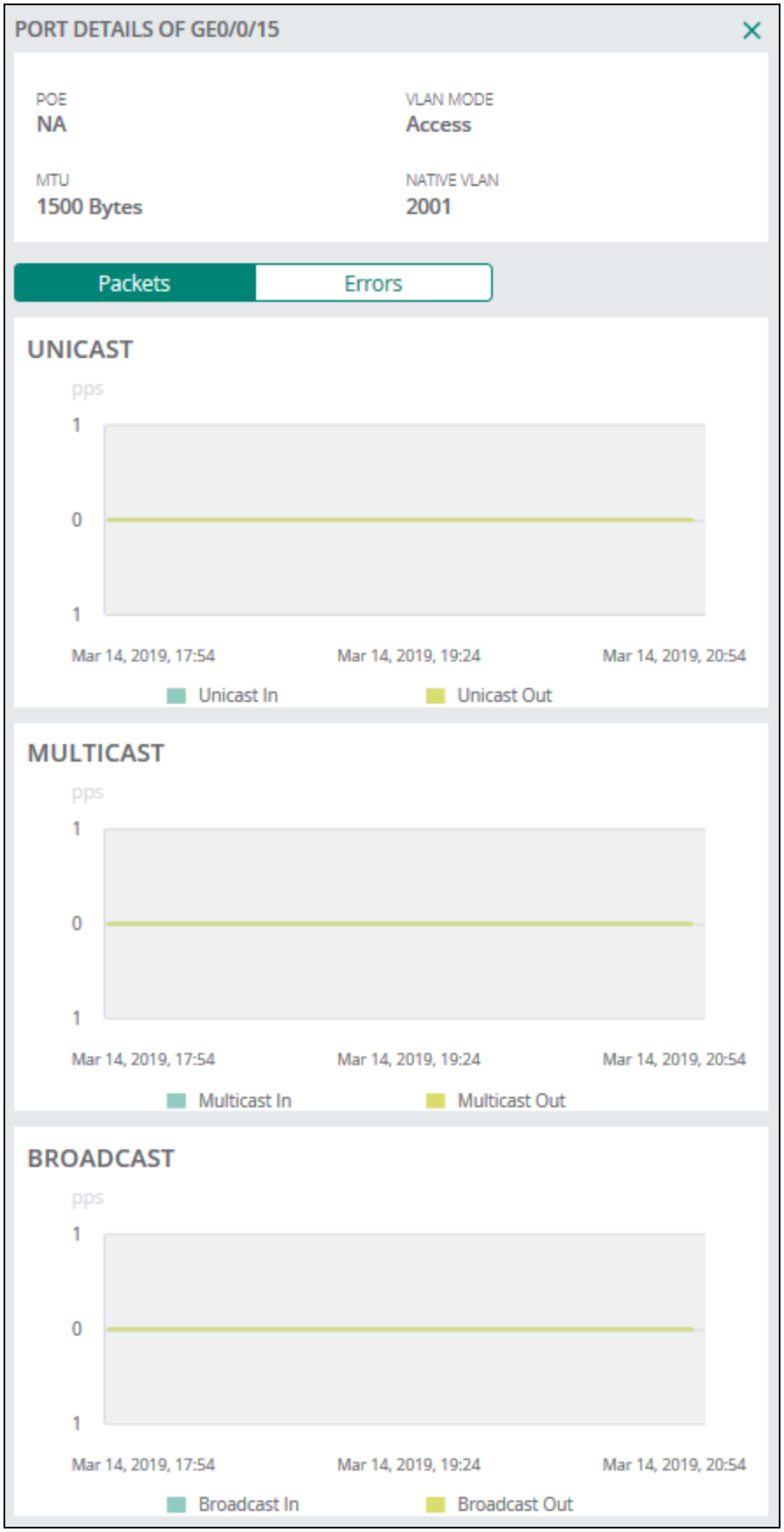
- **Port Status**—Provides a graphical representation of the Branch gateway's LAN link availability. Also provides a quick view of the LAN port status. Click a LAN port to view the port detail graphs based on Packets or Errors.

Figure 53 *LAN port status*

The following figure shows the Packet details displayed for the port:

- **Unicast**—The number of unicast packets per second.
- **Multicast**—The number of multicast packets per second.
- **Broadcast**—The number of broadcast packets per second.

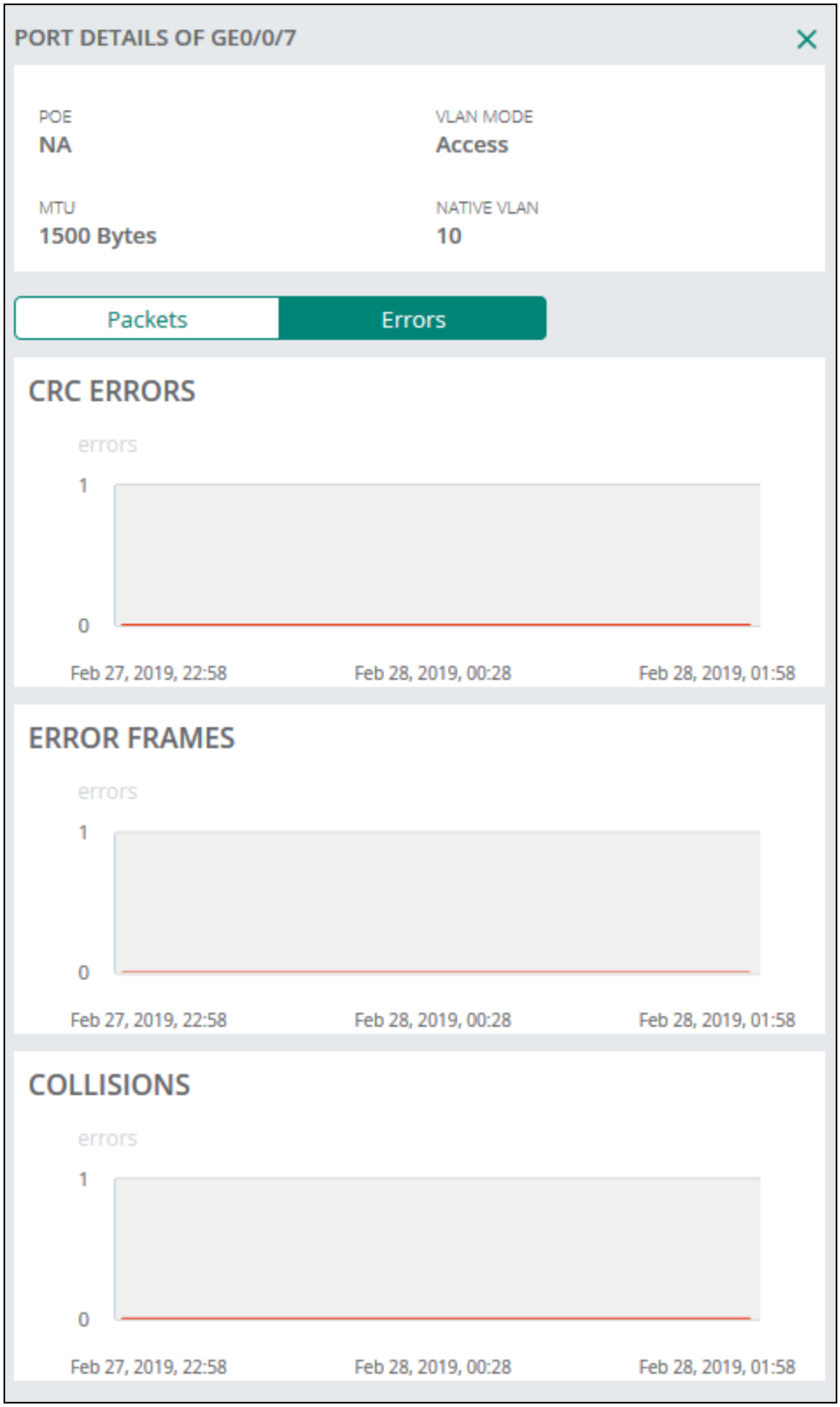
Figure 54 *Port Details—Packets*



The following figure shows the Error details displayed for the port:

- **CRC Errors**—The number of cyclic redundancy errors logged.
- **Error Frames**—The number of error frames logged.
- **Collisions**—The number of collisions encountered.

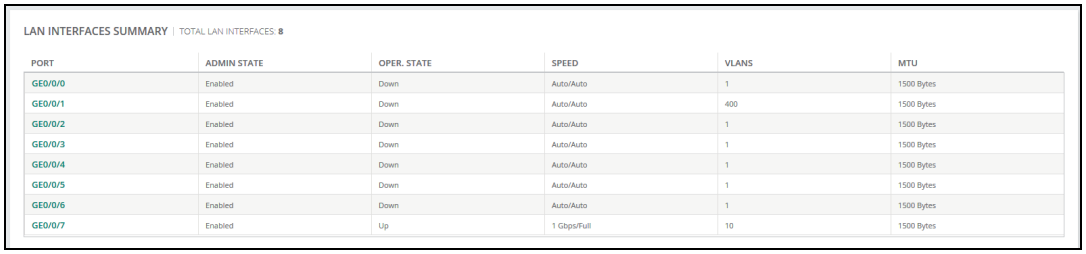
Figure 55 *Port Details—Errors*



- **LAN Interfaces Summary**—The table lists the LAN interfaces and provides the total number of LAN interfaces. Displays the summary of LAN interfaces. The following details are displayed for the port:
  - **Port**—Port number.
  - **Admin State**—Administrative state of the LAN interface.

- **Oper. State**—Operational state of the LAN interface.
- **Speed**—Speed.
- **VLANs**—Range of VLANs.
- **MTU**—MTU value.

Figure 56 *LAN Interfaces Summary*

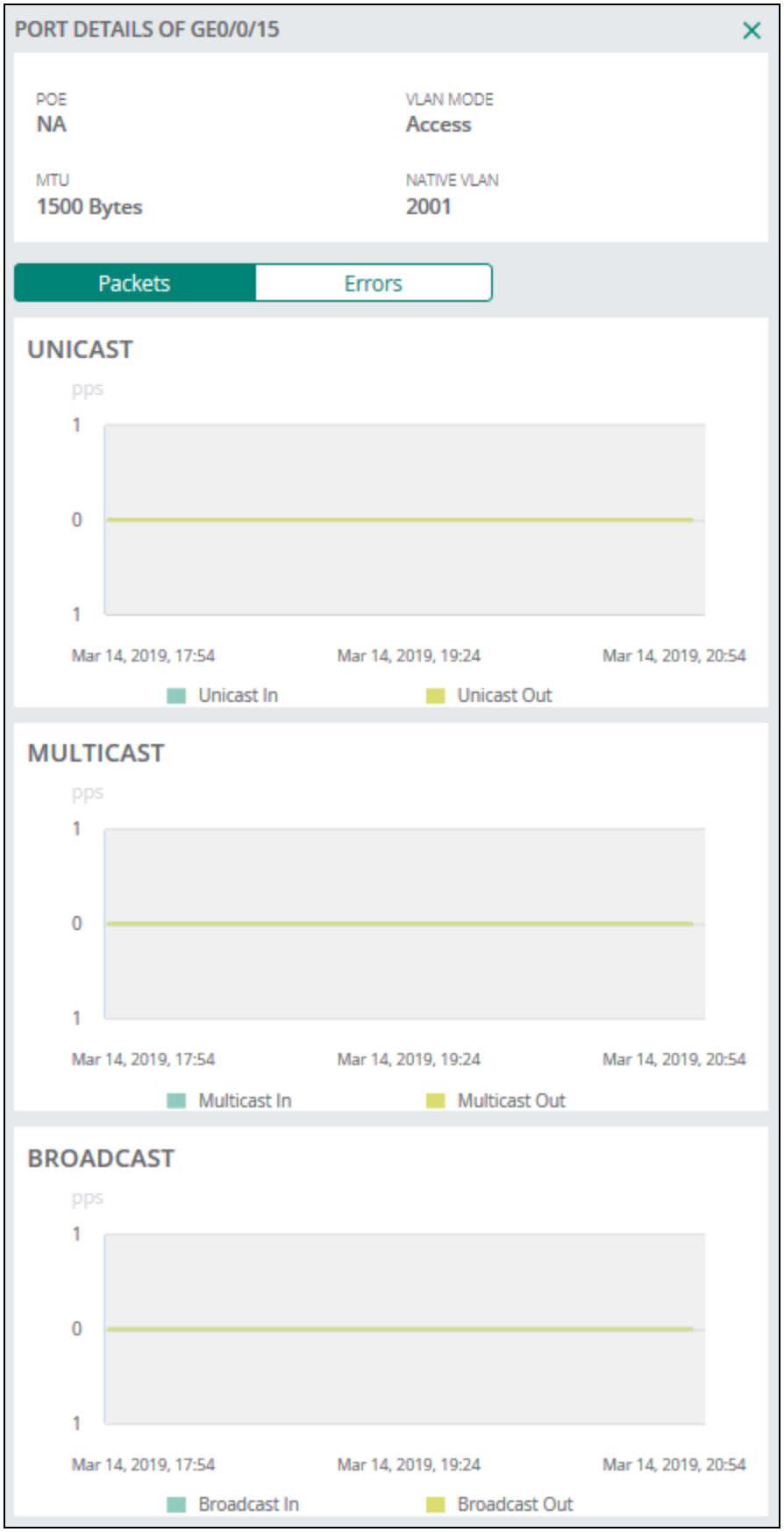


Click a LAN port to view the port detail graphs based on Packets or Errors.

The following Packet details are displayed for the port:

- **Unicast**—The number of unicast packets per second.
- **Multicast**—The number of multicast packets per second.
- **Broadcast**—The number of broadcast packets per second.

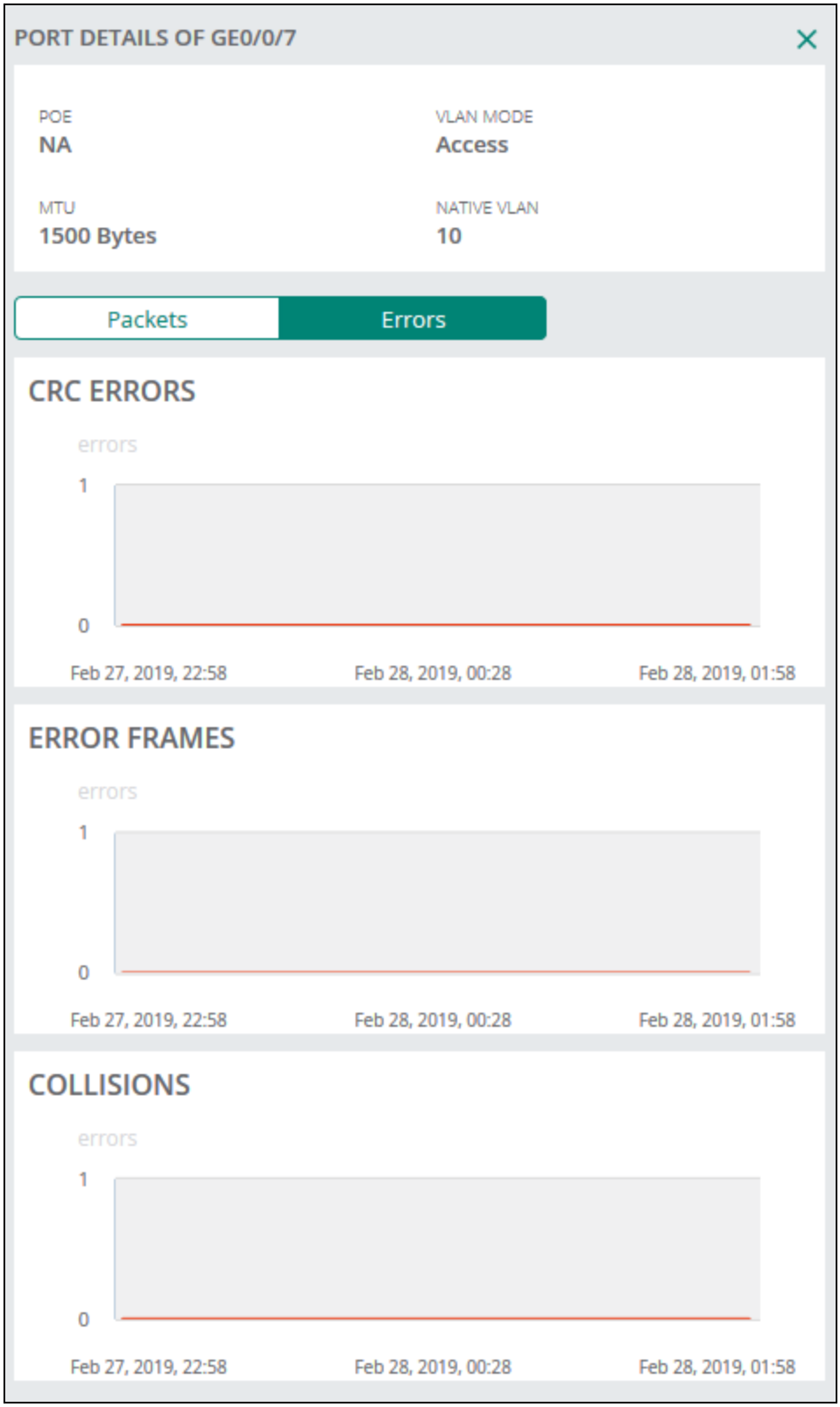
Figure 57 *Port Details—Packets*



The following Error details are displayed for the port:

- **CRC Errors**—The number of cyclic redundancy errors logged.
- **Error Frames**—The number of error frames logged.
- **Collisions**—The number of collisions encountered.

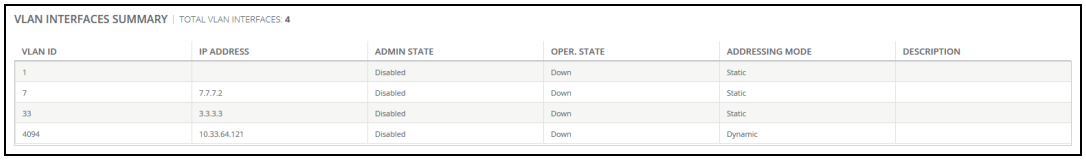
Figure 58 *Port Details—Errors*



- **VLAN Interfaces Summary**—The table lists the VLAN interfaces and provides the total number of VLAN interfaces. Displays the summary of LAN interfaces. The following details are displayed:
  - **VLAN ID**—VLAN ID number.
  - **IP Address**—IP address.

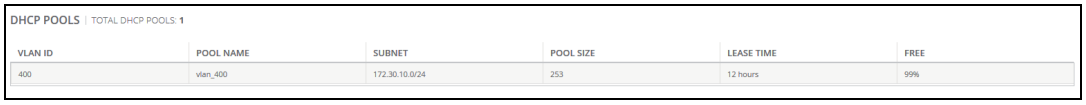
- **Admin State**—Administrative state of VLAN interface.
- **Oper. State**—Operational state of the VLAN interface.
- **Addressing Mode**—Type of addressing mode.
- **Description**—Description of the VLAN.

Figure 59 *VLAN Interfaces Summary*



- **DHCP Pools**—The table lists the DHCP pools and total number of DHCP pools. Displays the summary of DHCP pools. The following details are displayed:
  - **VLAN**—VLAN ID number.
  - **Pool Name**—Name of the DHCP pools.
  - **Subnet**—IP address of the client subnet.
  - **Pool type**—Type of pool.
  - **Pool size**—Size of the pool.
  - **Lease time**—Lease time of the pool.
  - **Allocated**—Number of addressed allocated.

Figure 60 *DHCP Pools*



- **Active Leases**—The table lists the active leases and the total number of active leases. Displays the summary of active leases. The following details are displayed:
  - **Pool Name**—Name of the DHCP pools
  - **IP Address**—IP address of the client subnet.
  - **MAC Address**—MAC address of the client.
  - **Start Date**—Start date and time of the lease.
  - **End Date**—End date and time of the lease.
  - **Remaining**—Remaining time for the lease to expire.

Figure 61 *Active Leases*

Gateways—Tunnels Tab

To access the Tunnels section follow these steps:

1. On the **Gateways** page, click **List of Online Gateways**. The list of gateways connected in Aruba Central are displayed.
2. Click the gateway link for which you want to see the details. A dashboard showing the details of the selected gateway opens.
3. Click the **Tunnels** tab to view details about the Tunnels status and health.

The **Tunnels** tab displays the following details:

- **Tunnels Summary**
- **Tunnels Details**

The following details are displayed in the **Tunnels Summary** table:

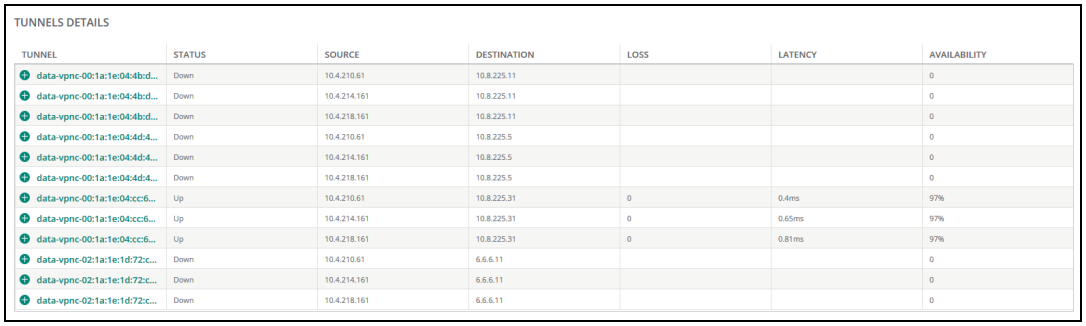
- **Total**—Total number of VPN tunnels.
- **Up**—Number of VPN tunnels in UP state.
- **Down**—Number of VPN tunnels in DOWN state.
- **Peers**—Total number of VPN peers.

Figure 62 *Tunnels Summary*

The following details are displayed in the **Tunnels Details** table:

- **Tunnel**—Tunnel number.
- **Status**—Status of the tunnel.
- **Source**—Source IP address of the tunnel.
- **Destination**—Destination IP address of the tunnel.
- **Loss**—Percentage of packet loss.
- **Latency**—The latency in microseconds.
- **Availability**—Availability graph of the tunnel. Displays the percentage of time the tunnel was in UP state.

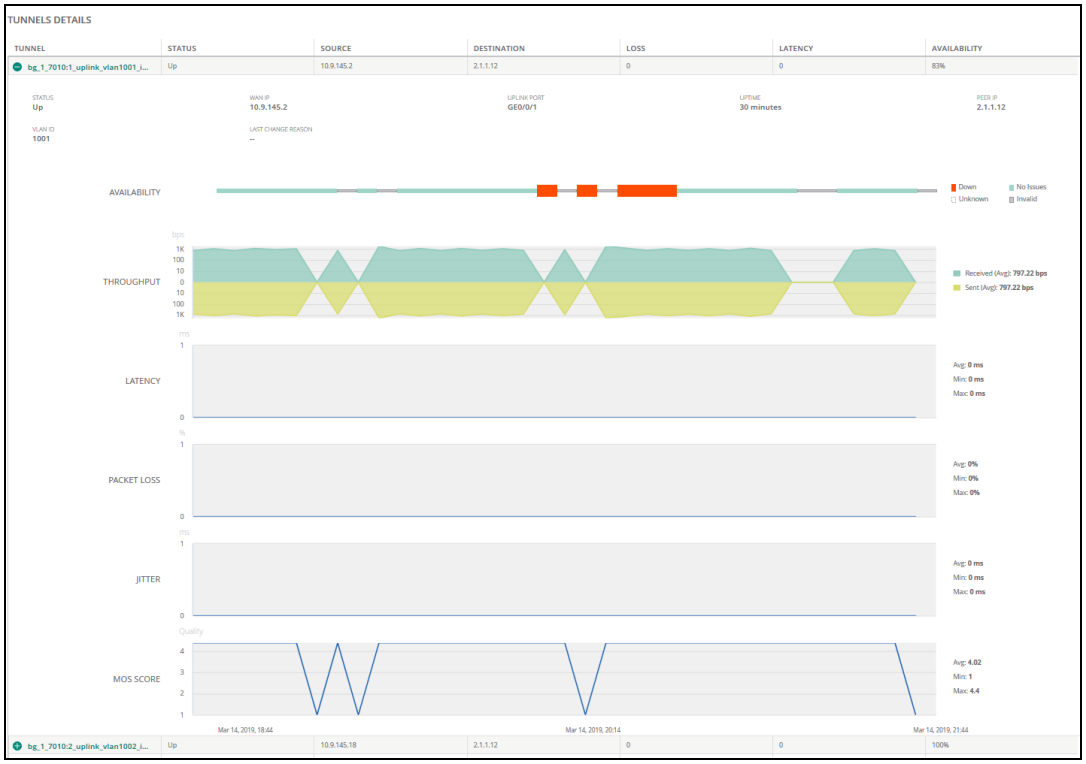
Figure 63 *Tunnels Details*



- **Tunnel Info**—Select a tunnel to view the following details:
  - **Status**—Status of the tunnel.
  - **VLAN ID**—VLAN ID.

- **WAN IP**—WAN IP address.
- **Last Change Reason**—Reason for the last status change of the tunnel.
- **Uplink Port**—Uplink port details.
- **Uptime**—Amount of time the tunnel has been active since it was last reset.
- **Peer IP**—Peer IP address.
- **Availability**—Availability of the tunnel.
- **Throughput**—Displays the inbound and outbound traffic rates for the selected tunnel.
- **Latency**—Latency in microseconds.
- **Packet Loss**—Percentage of packet loss.
- **Jitter**—Jitter in microseconds.
- **MOS Score**—MOS value.

Figure 64 *Tunnel details-information*



Gateways—Routing Tab

To access the Routing section follow these steps:

1. On the **Gateways** page, click **List of Online Gateways**. The list of gateways connected in Aruba Central are displayed.
2. Click the gateway link for which you want to see the details. A dashboard showing the details of the selected gateway opens.
3. Click the **Routing** tab to access the following route details for the gateway:

- **BGP**
- **OSPF**
- **Overlay**
- **Route Table**

BGP

The **BGP** tab displays the following details for the gateway:

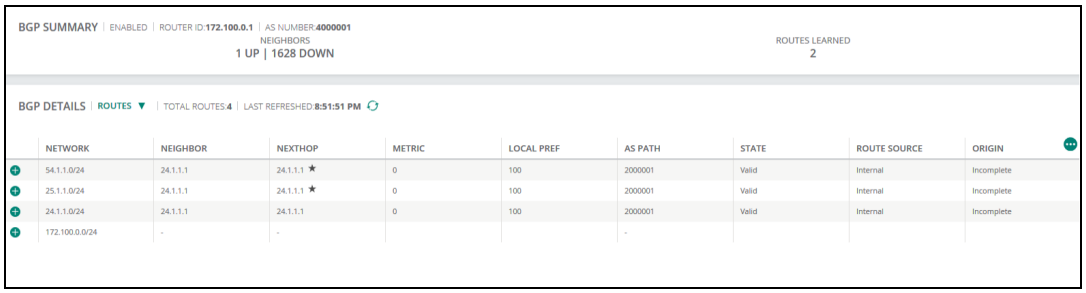
- **BGP Summary**

NOTE

Click the Settings icon to reset or set the default columns that are displayed.

- **Router ID**—Displays the Router ID.
- **AS Number**—Displays the private Autonomous System (AS) number.
- **Neighbors**—Displays the number of neighboring connections.
- **Routes Learned**—Displays the number of routes that have been learned.

Figure 65 *BGP—Summary*



- **BGP Details**—Displays the information categorized by **Neighbors** and **Routes**.
- **Neighbors**

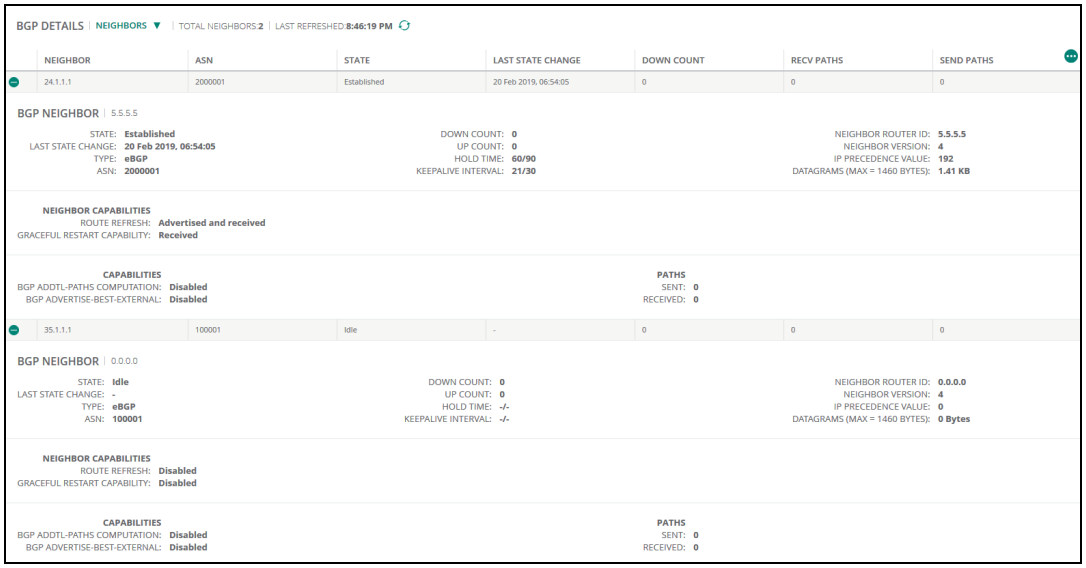
NOTE

Click the Settings icon to reset or set the default columns that are displayed.

- **Total Neighbors**—Displays the total number of neighbors.
- **Last Refreshed**—Indicates when the last refresh was completed.
- **Neighbor**—Displays the available neighbors.
- **ASN**—Displays the private Autonomous System (AS) number.
- **State**—Displays the current state.
- **Type**—Neighbor type.
- **Last State Change**—Displays the last state change.
- **Down Count**—Displays the number of neighbors that are down.
- **Up Count**—Displays the number of neighbors that are up.
- **Hold Time**—Displays the time spent on hold.
- **Keep Alive Interval**—Displays the time set for the Keep Alive Interval.
- **Router ID**—Displays the Router ID.
- **Neighbor Version**—Displays the firmware version of the connected neighbors.
- **IP Precedence Value**—Displays the IP precedence.
- **Datagrams (Max = 1400Bytes)**—Displays existing datagrams.
- **Route Refresh**—Displays the latest route refresh.
- **Graceful Restart Capability**—Displays whether graceful restart is supported.

- **BGP Addtl-Paths Computation**—Displays the additional paths computation.
- **Recv Paths**—Displays the receive path information.
- **Send Paths**—Displays the send path information.
- **Source Address**—Displays the source information.
- **Nexthop**—Displays information about the next hop.
- **Link Address**—Displays the link address.
- **CFfg Hold Time**— Displays the minimum acceptable hold time.
- **CFfg Keep Alive Time**— Displays the configuration keep alive time.
- **IS Route Reflector**—Displays the net hop path.
- **IS Router Server**—Displays the IS Router Server details.
- **BGP Advertise-Best_External**—Displays the backup external route.
- **Up Time**—Displays the time that the connection has been up.

Figure 66 *BGP—Neighbors Details*



- **Routes**

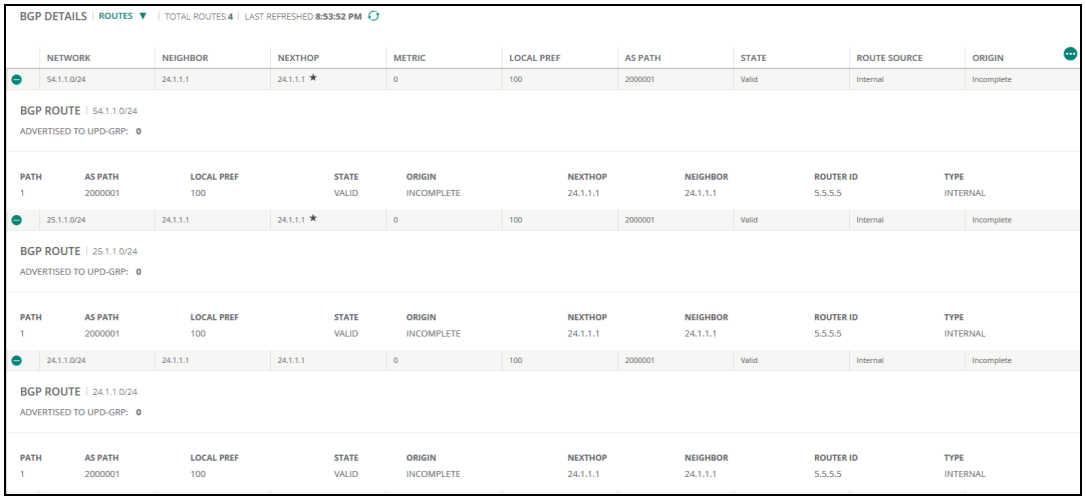
NOTE

Click the Settings icon to reset or set the default columns that are displayed.

- **Total Routes**—Displays the total number of routes.
- **Last Refreshed**—Indicates when the last refresh was completed.
- **Network**—Connected network.
- **Neighbor**—Displays the available neighbors.
- **Nexthop**—Displays information about the next hop.
- **Metric**—Distance for static routes. For a given route destination, there can be multiple next hops. A route metric enables the gateway to prefer one route over another or load-balance when the metric is the same.
- **Local Pref**—Displays the outbound external path.
- **AS Path**—Displays the private Autonomous System path.
- **State**—Displays the connection state of the connection.

- **Route Source**—Displays the specific route the packet should take.
- **Origin**—Displays the origin attribute value.
- **Advertised to Upd-Grp**—Displays the Advertised Update-Group status.
- **Router ID**—Displays the router ID.

Figure 67 *BGP—Routes Details*



OSPF

The **OSPF** tab displays the following details for the gateway:

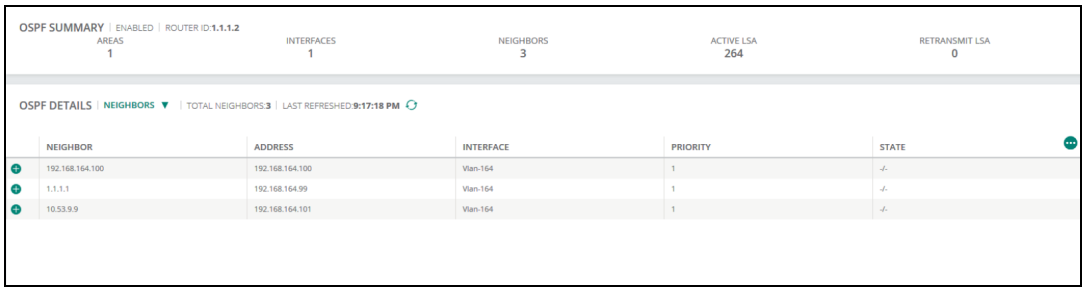
- **OSPF Summary**

NOTE

Click the Settings icon to reset or set the default columns that are displayed.

- **Status**—Status is either Enabled or Disabled.
- **Router ID**—The routers identification details.
- **Areas**—Area type as specified in the OSPF parameters.
- **Interfaces**—Displays the current interface.
- **Neighbors**—Displays the number of neighbors available.
- **Active LSA**—Displays the Active Link-State Advertisements.
- **Retransmit LSA**—Displays the Retransmitted Link-State Advertisements.

Figure 68 *OSPF—Summary*



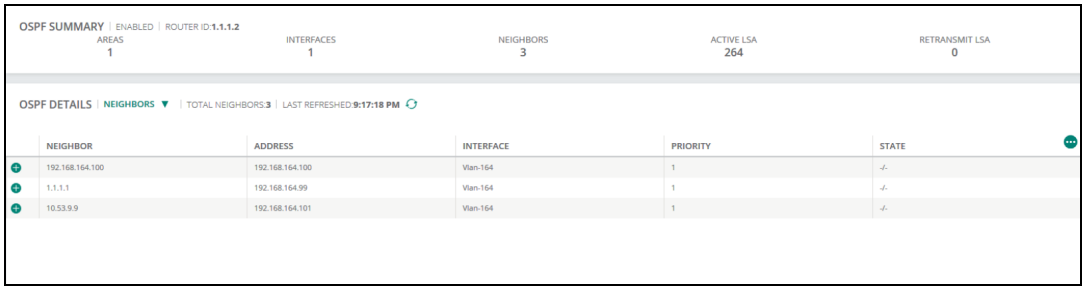
- **OSPF Details**—Displays the information categorized by **Neighbors**, **Interfaces**, **Areas**, and **Link State Databases**.
- **Neighbors**

NOTE

Click the Settings icon to reset or set the default columns that are displayed.

- **Total Neighbors**—The total number of neighbors.
- **Last Refreshed**—Indicates when the last refresh was completed.
- **Neighbor**—Details of the neighbors.
- **Address**—IP address of the neighbor.
- **Interface**—Displays the current interface for the neighbor.
- **Priority**—Displays the priority of each neighbor.
- **State**—Displays the state of the connection.
- **Area**—Displays the area of the neighbor.
- **Options**—Available neighbor options.
- **Dead Timer**—Displays the required time to wait before the neighbor connection is dead.
- **Retransmit Timer**—Displays the time between OSPF and LSA retransmissions.

Figure 69 *OSPF—Neighbor details*



- **Interfaces**

NOTE

Click the Settings icon to reset or set the default columns that are displayed.

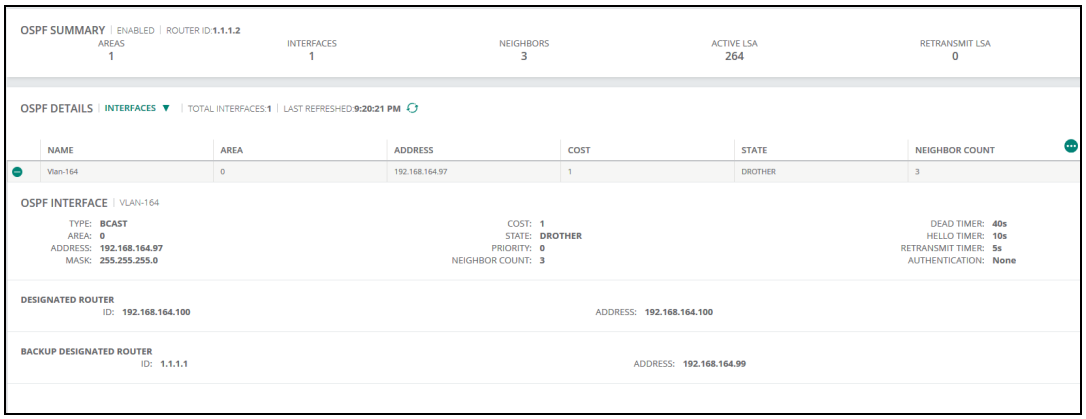
- **Total Interfaces**—The total number of interfaces.
- **Last Refreshed**—Indicates when the last refresh was completed.
- **Name**—Name of the interface.
- **Area**—Displays the logical collection of devices that share the same area.
- **Address**—IP address of the interface.
- **Mask**—IP mask of the interface.
- **State**—Displays the state of the connection.
- **Type**—Displays the type of connection.
- **Cost**—Displays the cost associated with the OSPF traffic on the tunnel interface.
- **Neighbor Count** —Displays the number of neighbors.
- **ID**—Displays the interface ID.
- **Address**—Displays the IP address of the interface.

- **Priority**—Displays the priority of the interface to determine the default router.
- **Hello Timer**—Displays the time interval between the hello packets to be sent on the interface.
- **Dead Timer**—Displays the time interval after which a router is declared dead if hello packets are not received.
- **Retransmit Timer** —Displays the retransmit interval time for link state advertisements.
- **Authentication**—Displays the status of this option that is used for enabling OSPF authentication mode for MD5.

Click on an interface listed in the table to view the following details:

- **Type**—Displays the type of connection.
- **Area**—Displays the logical collection of devices that share the same area.
- **Address**—IP address of the interface.
- **Mask**—IP mask of the interface.
- **Cost**—Displays the cost associated with the OSPF traffic on the tunnel interface.
- **State**—Displays the state of the connection.
- **Priority**—Displays the priority of the interface to determine the default router.
- **Neighbor Count**—Displays the number of neighbors.
- **Dead Timer**—Displays the time interval after which a router is declared dead if hello packets are not received.
- **Hello Timer**—Displays the time interval between the hello packets to be sent on the interface.
- **Retransmit Timer**—Displays the retransmit interval time for link state advertisements.
- **Authentication**—Displays the status of this option that is used for enabling OSPF authentication mode for MD5.

Figure 70 *OSPF— Interfaces details*



- **Areas**

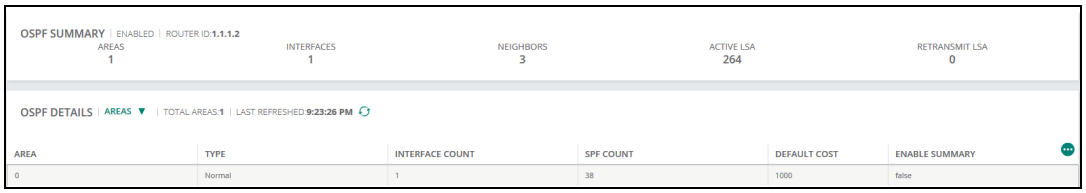
NOTE

Click the Settings icon to reset or set the default columns that are displayed.

- **Total Areas**—The total number of areas.
- **Last Refreshed**—Indicates when the last refresh was completed.
- **Area**—Displays the logical collection of devices that share the same area.
- **Type**—Displays the type of connection.
- **Interface count**—Displays the interface count.

- **SPF Count**—Displays the Shortest Path First count.
- **Default Count**—Displays the default count.
- **Enable Summary**—Displays if summary collection is enabled.

Figure 71 *OSPF— Areas details*

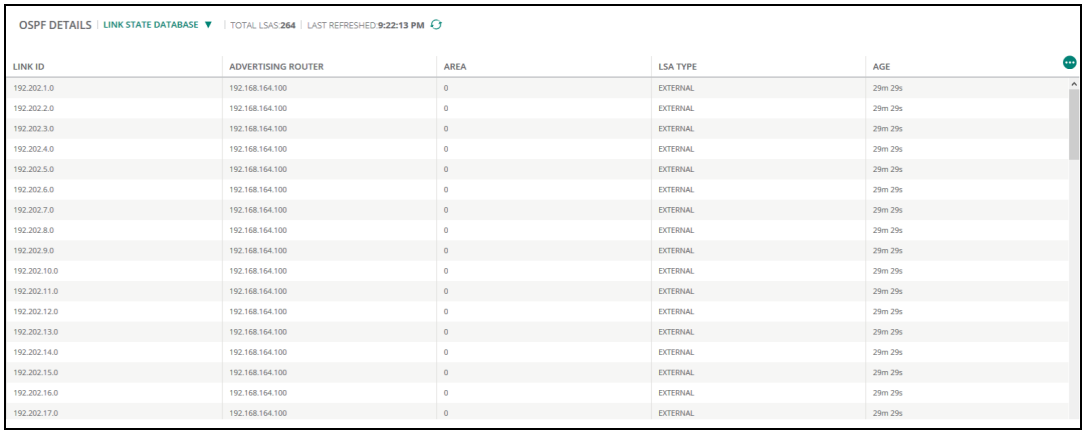


- **Link State Databases**

Click the Settings icon to reset or set the default columns that are displayed.

- **Total Link State Database**—The total number of Link State Databases.
- **Last Refreshed**—Indicates when the last refresh was completed.
- **Link ID**—Displays the router ID of the originating router.
- **Advertising Router**—Displays the routes that is advertising the link-state.
- **Area**—Displays the logical collection of devices that share the same area.
- **LSA Type**—Displays the aggregatiopn type.
- **Age**—Displays the age of the OSPF LSA.
- **State**—Displays the state of the connection.
- **Seq No.**—Displays the 32-bit OSPF Sequence number.
- **Checksum**—Displays the 16-bit checksum for the OSPF packet.

Figure 72 *OSPF—Link State Databases details*



- **LSA types**—There are various LSA types available and they are listed here:
  - **Router**—The Router page displays the following details:
    - Flags
    - Link ID
    - Link Data
    - Link Type

- Metric
- **Network**—The Network page displays the following details:
  - Mask
  - Attached router
- **Network Summary**—The Network Summary page displays the following details:
  - Address
  - Mask
  - Metric
- **ASBR Summary**—The ASBR Summary page displays the following details:
  - ASBR
  - Metric
- **External**—The External page displays the following details:
  - Mask
  - Metric
  - Type
  - Route Tag
  - Forwarding Address

Overlay

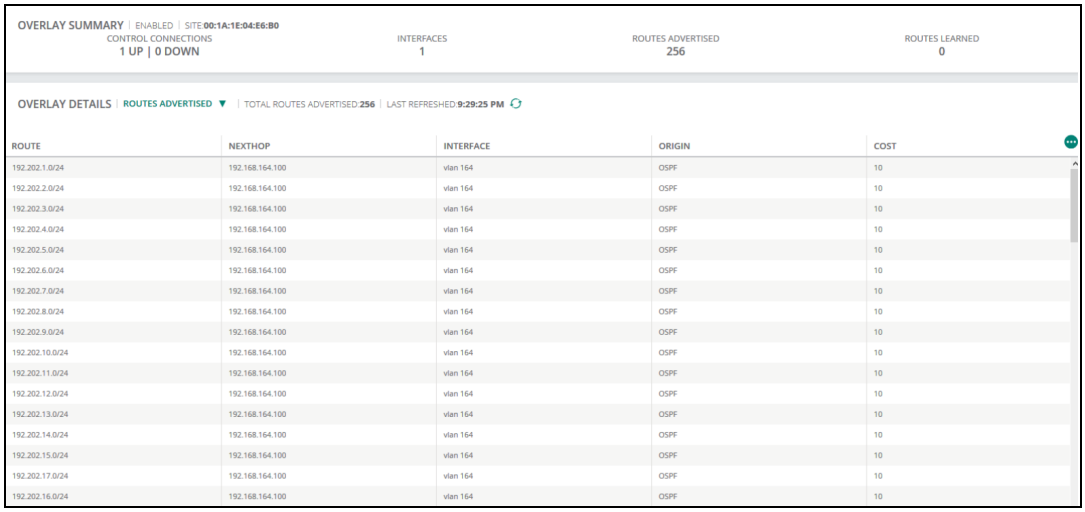
The **Overlay** tab displays the following details for the gateway:

Click the Settings icon to reset or set the default columns that are displayed.

Click the filter icon on each column header row to filter the displayed information

- **Overlay Summary**
  - **Status**—Status is either Enabled or Disabled.
  - **Site**—Displays the site location.
  - **Control Connections**—Displays the number of active control connections.
  - **Interfaces**—Displays the number of active interfaces.
  - **Routes Advertised**—Displays the number of routes that are advertised.
  - **Routes Learned**—Displays the number of routes that are learned.

Figure 73 *Overlay—Summary*



- **Overlay Details**—Displays the information categorized by **Control Connections**, **Interfaces**, **Routes Advertised**, and **Routes Learned**.
- **Control Connections**

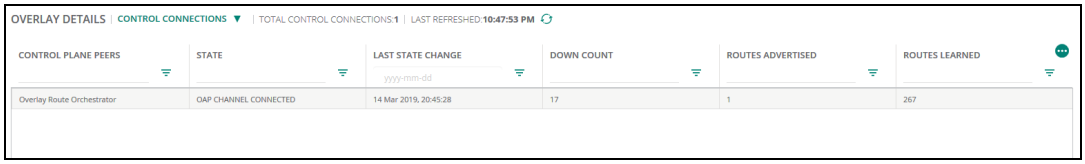
NOTE

Click the Settings icon to reset or set the default columns that are displayed.

Click the filter icon on each column header row to filter the displayed information

- **Total Control Connections**—Displays the total number of control connections.
- **Last Refreshed**—Indicates when the last refresh was completed.
- **Control Plane Peers**—Displays the Control Pane Peers.
- **State**—Displays the state of the connection.
- **Last State Change**—Indicates the Last State Change.
- **Down Count**—Displays the Down Count.
- **Routes Advertised**—Displays the advertised routes.
- **Routes Learned**—Displays the number of routes that are learned.

Figure 74 *Overlay Details —Control Connections*



- **Interfaces**

NOTE

Click the Settings icon to reset or set the default columns that are displayed.

Click the filter icon on each column header row to filter the displayed information

- **Total Interfaces**—Displays the total number of interfaces.
- **Last Refreshed**—Indicates when the last refresh was completed.
- **Interfaces**—Displays the number of active interfaces.
- **State**—Displays the state of the interface.

- **Tunnel Destination**—Displays the destination address.
- **Uptime**—Amount of time the tunnel has been active since it was last reset.
- **Routes Learned**—Displays the number of routes that are learned.

Figure 75 *Overlay Details —Interfaces*

- **Routes Advertised**

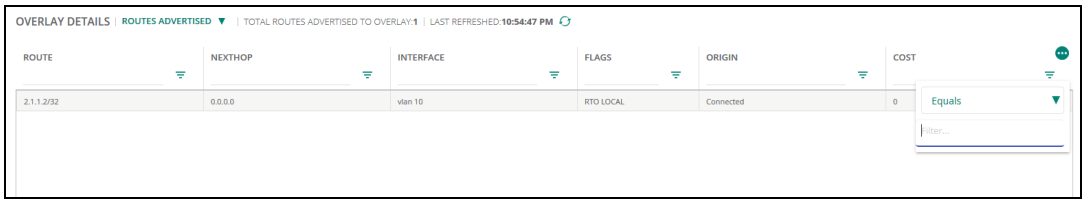
NOTE

Click the Settings icon to reset or set the default columns that are displayed.

Click the filter icon on each column header row to filter the displayed information.

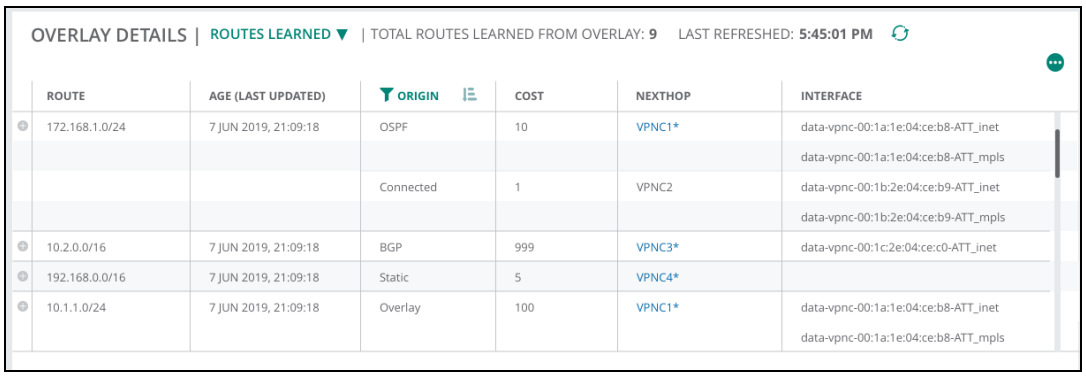
- **Route**—Displays the route name.
- **Nexthop**—Displays information about the next hop.
- **Interface**—Displays the number of active interfaces.
- **Flags**—Lists the number of active flags.
- **Origin**—Origin of the route.
- **Cost**—Cost associated with the route.

Figure 76 *Overlay Details—Routes Advertised*



- **Routes Learned**
  - **Total Routes Learned**—Displays the total number of routes that are learned.
  - **Last Refreshed**—Indicates when the last refresh was completed.
  - **Route**—The route IP address aand subnet.
  - **Age (Last Updated)**—Last updated date.
  - **Origin**—Orging of the connection, for example, Connected or Overlay.
  - **Flags**—Lists the number of active flags.
  - **Nexthop**—Displays information about the next hop.
  - **Interface**—Displays the number of active interfaces.

Figure 77 *Overlay Details—Routes Learned*



Route Table

NOTE

Click the Settings icon to reset or set the default columns that are displayed.

Click the filter icon on each column header row to filter the displayed information

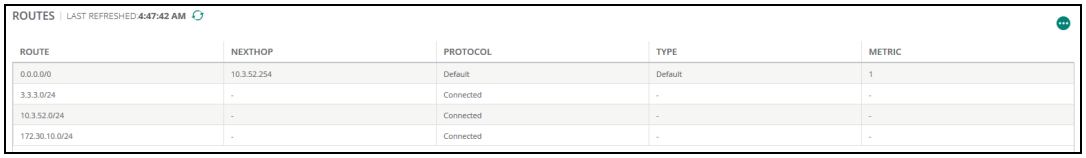
The **Route Table** tab displays the following route details for the gateway:

- **Route Summary**
  - **Total**—Total number of routes.
  - **Default**—Number of default routes.
  - **Static**—Number of static routes.
  - **Overlay**—Number of overlay connections.
  - **Connected**—Number of connected routes.
  - **Dynamic**—Number of dynamic routes.

Figure 78 *Routes Summary*

- **Routes**
  - **Last Refreshed**
  - **Route**—The route IP address aand subnet.
  - **Nexthop**—Displays information about the next hop.
  - **Protocol**—Routing protocol. Possible values are **Connected**, **Static**, **RAP-NG**, **Aggregated RAP-NG**, **OSPF**, **RIP**, **Default**, or **Aggregated Static**.
  - Type—
  - **Metric**—Distance for static routes. For a given route destination, there can be multiple next hops. A route metric enables the gateway to prefer one route over another or load-balance when the metric is the same.
  - **Flags**—Route flags. Possible value is either **Not Redistributed** or **CFG-SET**.

Figure 79 *Routes details*



Gateways—Path Steering Tab

In the **Path Steering** tab, you can view traffic path steering details for the Dynamic Path Steering policies configured on the Branch Gateway. The tab also displays the number of policies that are compliant along with the total number of policies configured on the Branch Gateway.

From the list of Dynamic Path Steering polices, select the policy for which you want to view the path steering details.

The **Path Steering** section displays the following information:

- **Path Steering Summary**
  - **State**—Displays whether the path steering feature is enabled.
  - **Policy Compliance**—Displays the compliance status of all the configured policies.

Figure 80 *Path Steering Summary*

- **Path Steering Details** section displays the following information:
  - **Policy Name**—The name of the Dynamic Path Steering policy
  - **Bandwidth**— The threshold percentage set for bandwidth utilization
  - **Latency**—The threshold value set for a round-trip ping time in milliseconds
  - **Jitter**—The threshold value set for jitters in packet transmission in milliseconds
  - **Packet Loss**—The percentage of packet loss allowed for the traffic type
  - **Path Preference**—The path preference in the primary, secondary, and tertiary order
  - **Status**—The compliance status of the uplinks
  - **Overall Compliance**—Overall compliance (%) of the policy

Figure 81 *Path Steering Details*

Click a policy to view the **Compliance Summary** that consists of the **Status** and **Session** information.

- **Status**—Provides a graphical representation of the configured uplink statuses. The following details are displayed:
  - Overall status
  - The status of each of the uplinks configured for the Dynamic Path Steering policy on that gateway

Hover over the status bar to view the compliance status details of all the configured uplinks. You can view the compliance status of the uplinks and the probe IPs. If the probe IPs are non-compliant, it displays the reason for non-compliance such as latency, jitter, or packet loss. The following list contains the various colors and the corresponding compliance status:

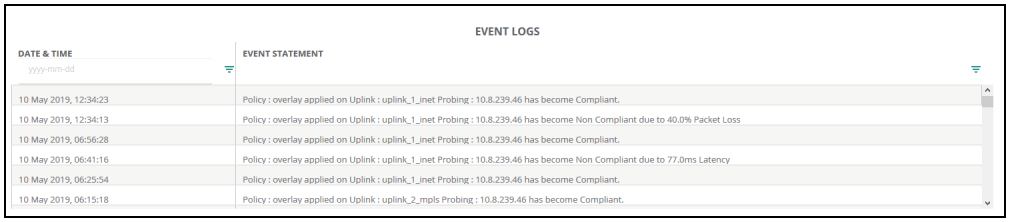
- **Green**—An uplink is **Compliant** when all of the associated probe IPs meet the set SLAs and threshold settings.
- **Orange**—An uplink is **Partially Compliant** when you have multiple probe IPs and not all of them are compliant.
- **Red**—An uplink is **Non-Compliant** when all of the probe IPs are non-compliant.
- **Yellow**—This is the **Hold Period** when an uplink changes it's status from Non-compliant to Compliant (usually the first 3 minutes of the transition phase).
- **Grey**—Uplink status is **Unknown** when the Dynamic Path Steering feature does not send any compliance information to the cloud.

- **Sessions**—Provides a graphical representation of the total number of sessions. The following details are displayed:
  - Overview
  - The sessions count on each of the uplinks configured for the Dynamic Path Steering policy on that gateway

Figure 82 *Path Steering Details—Compliance Summary*

- **Event Logs**—When an uplink becomes non-compliant, an event is recorded, when the same uplink becomes compliant adhering to the set SLAs, another event is recorded. The **Event Logs** table provides information about all such events. It displays the timestamp and a detailed event statement that contains the policy name, the uplink name, the probe IP, and the reason for non-compliance, if it is a non-compliance event.

Figure 83 *Event Logs*



Gateways—Applications Tab

Displays charts showing client traffic trends to application, application categories, website categories, and websites of a specific security reputation score. To view the traffic classification based on application, application category, and website category, you must enable **Deep Packet Inspection** on the Branch Gateways.

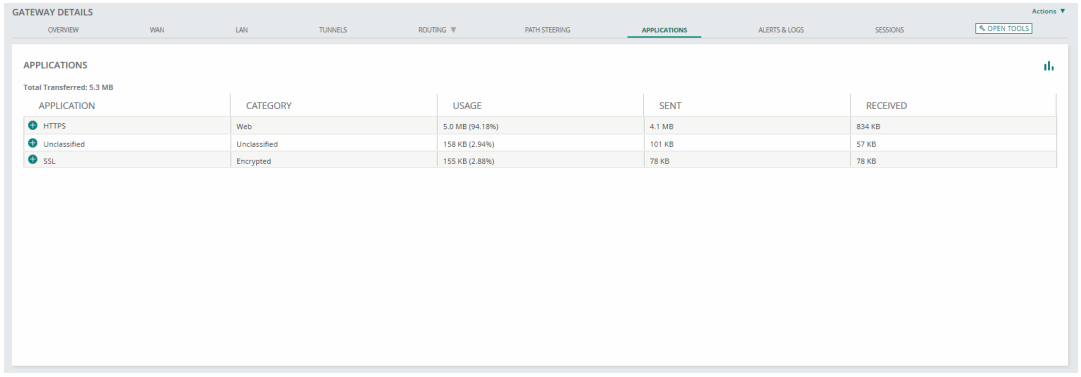
NOTE

Click the Grid or Graph icon on the **Application** and **Websites** sections to toggle the views.

The **Applications** tab displays the following:

- **Application / Categories**—Displays top N application categories based on total bandwidth usage. Apart from the top N, the rest of the application categories are grouped under the **Unclassified** category.
  - **Applications**—Displays top N applications based on total bandwidth usage. Apart from the top N, the rest of the applications are grouped under the **Unclassified** category. Click the **+** next to the service name to expand the view and display additional information.
  - **Categories**—Displays top N web categories based on total bandwidth usage. Apart from the top N, the rest of the web categories are grouped under the **Unclassified** category.
  - **Usage**—Displays the bandwidth usage of each application.
  - **Sent**—Displays the amount of data sent.
  - **Received**—Displays the amount of data received.

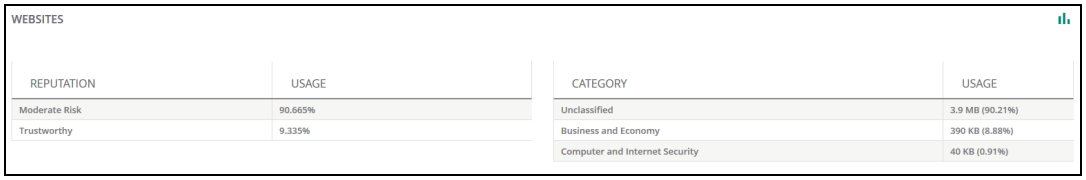
Figure 84 *Applications*



The **Websites** tab displays the following tables:

- **Reputation and Usage**—Displays the reputation and usage percentage.
- **Category and Usage**—Displays the WebCC category and the usage percentage.

Figure 85 *Websites*



Gateway—Alerts & Logs Tab

The **Alerts & Logs** tab features an **Alerts** and **Audit Log** dashboard for a quick view of the of alerts and logs.

Alerts

The alerts are categorized into four types **Critical**, **Major**, **Minor**, and **Warning**. Click the number below the alert to display the warning(s) in the **Open Alerts** table.

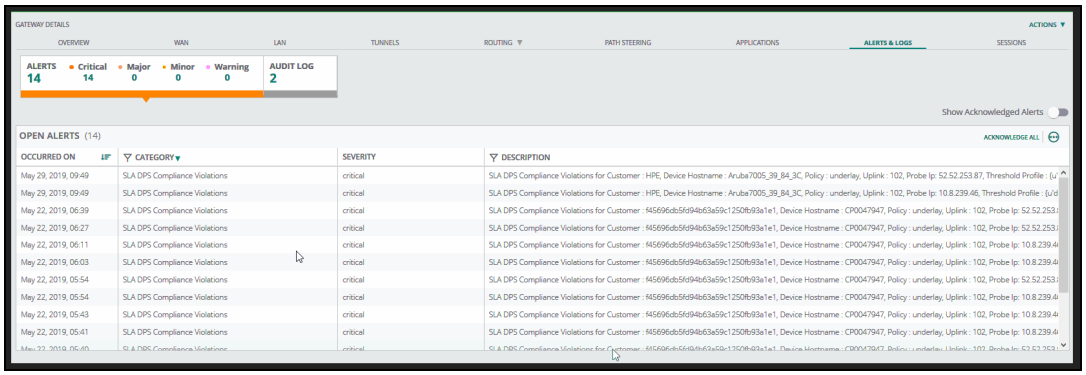
The Audit Logs lists the number of logs recorded. Click the number below the log to display the log(s) in the **Audit Log** table.

- **Open Alerts**—Displays a list of alerts based on the selection made in the dashboard.
  - To acknowledge the alerts, select the alert(s) and click **Acknowledge** in the pop-up or to acknowledge all the alerts, click **Acknowledge All** at the top of the table.
  - To view the acknowledged alerts, click the **Show Acknowledged Alerts** slider.

The Open Alerts table lists the information based on the following:

- **Occurred on**— Displays the date and time the alert was generated.
- **Category**—Lists the category under which the alert was raised.
- **Severity**—Displays the severity level of the alert, the available options are Critical, Major, Minor, and Warning.
- **Description**—Displays a description of the alert.

Figure 86 *Alerts information*



Audit Log

On the dashboard, click the number below Audit Log to display the Audit Log table.

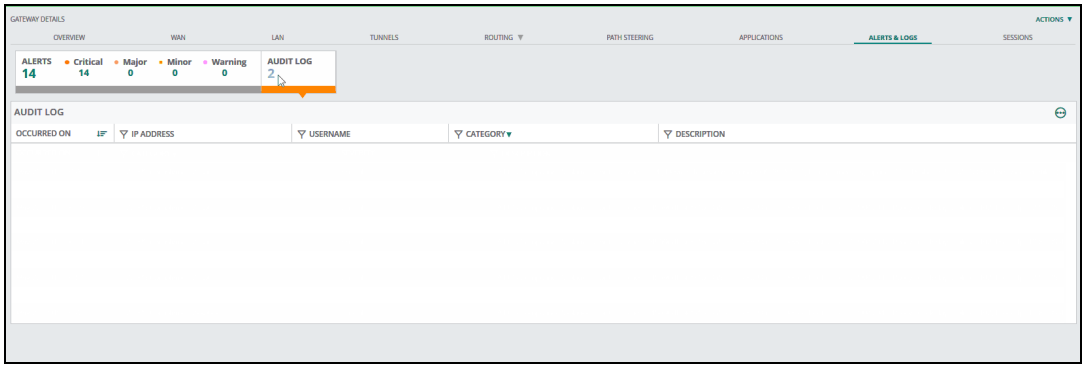
- **Audit Log**—Displays a list of audit logs.

The following details are displayed for audit logs:

- **Occurred on**— Displays the date and time the alert was generated.
- **IP Address**—Displays the description of the alert.
- **Username**—Displays the severity level of the alert.

- **Category**—Lists the category under which the alert was raised.
- **Description**—Brief description of the log information. For detailed log information click the action icon.

Figure 87 *Audit logs information*



For more information about gateway alerts, see the *Gateway Alerts* section in the *Aruba Central Help Center*.

Gateways—Sessions Tab

The **Sessions** tab displays the following information:

- **Session Summary**—Displays a summary of all the running sessions.
- **Sessions**—Displays filtered Session information.

The following details are displayed in the **Session Summary** pane:

- **Current entries**—Displays the number of currant and active entries.
- **Max entries**—Displays the total entries made with the time period.
- **High water mark**—Displays the highest number active entries.
- **Allocation failures**—Displays the number no failed allocations.
- **Denied entries**—Displays the number of entries that were denied.

The **Session** pane displays information filtered by the **IP Address**.

Click the Settings icon to reset or set the default columns that are displayed.

The Session table displays information about:

- **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.
- **App port** —Displays the port number used by the application.
- **Action**—Displays the application specific action.
- **Packets**—Displays the number of packets.
- **State**—Displays the connection state of the application. The state can either be Active, Inactive, or Denied.
- **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.

To view additional information of individual sessions click the **+** icon to expand and display session specific information. The information in the tables is categorized as:

- **Details**
  - **User policy name (ACL)**—Displays the user policy name.
  - **User policy rule (ACE)**—Displays the user policy rule.
  - **Start time**—Displays the session start time.
  - **Receive time**—Displays the session receive time.
  - **WebCC category**—Displays the WebCC categorization.
  - **WebCC reputation**—Displays the site reputation.
  - **Application category**—Displays the application category.
- **Nexthop**
  - **Uplink interface**—Displays the uplink interface details.
  - **Uplink VLAN**—Displays the uplink VLAN details.
  - **Tunnel**—Displays the tunnel details.
- **Dynamic Path Selection (DPS)**
  - **Policy name**—Displays the policy name.
  - **Path preference**—Displays the path interface details.
  - **Compliance**—Displays the compliance details.

Figure 88 *Session summary and session information*

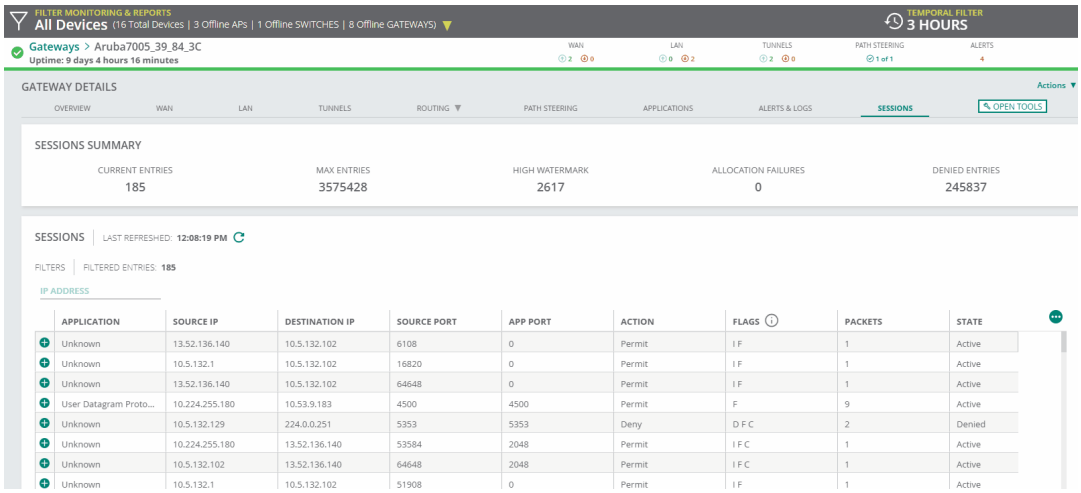
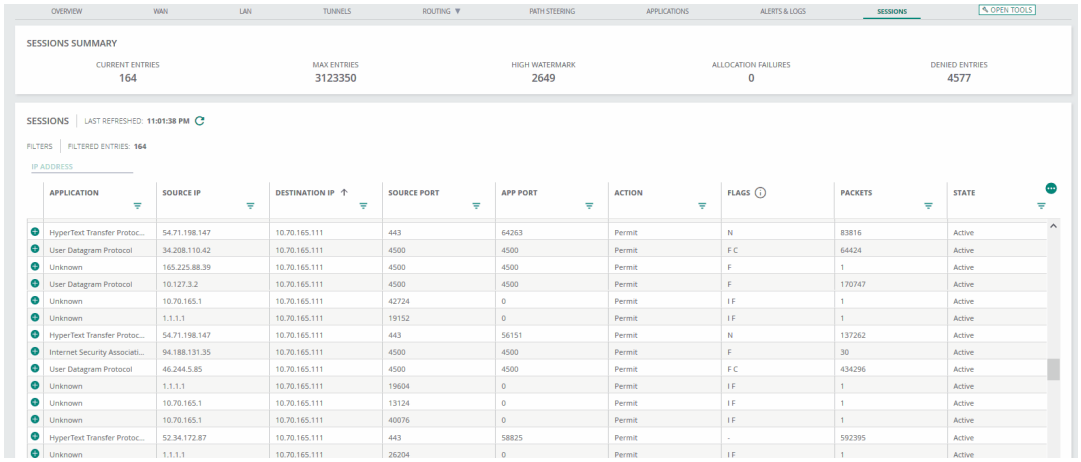


Figure 89 *Session Details*



Deleting an Offline Gateway

To delete an offline Gateway:

1. Go to **Monitoring & Reports** > **Network Overview** > **Gateways** > **List of Offline Gateways**.
2. From the **Gateway**s table, select the Gateway that you want to delete. To select a Gateway, click on any column (except **Device Name**).

NOTE

Clicking on a device name in the **Device Name** column opens the Gateway dashboard.

3. Click **Delete**.
4. Confirm deletion.

NOTE

For a visual representation of the procedure, click here.

Security

The Security tab provides details on rogue APs, interfering APs, infrastructure attacks, and WIDS events.

Viewing Rogue AP Detectors

To view detectors of rogue APs:

1. From the app selector, click **Monitoring & Reports**.
2. In the default **Network Overview** page, click **Security > Rogues/Interferers**. A graph showing Top 5 detectors of Rogue APs is displayed.

Viewing Intrusion Detection Attacks

To view detectors of rogue APs:

1. From the app selector, click **Monitoring & Reports**.
2. In the default **Network Overview** page, click **Security > Intrusion Detection**. The following graphs are displayed:
    a. Top 5 detectors of infrastructure attacks.
    b. Top 5 detectors of client attacks.
    c. Detected intrusion detection system attacks.

Viewing WIDS Events

To view WIDS events:

1. From the app selector, click **Monitoring & Reports**.
2. In the default **Network Overview** page, click **Security > WIDS Events**. The **WIDS Events** pane is displayed.

The **Security** pane provides a summary of the rogue Instant APs, interfering Instant APs, and the total number of wireless attacks detected on an AP and client devices for a given duration.

Table 35: *Security pane*

Data Pane Content	Description
Temporal Filter	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. You can choose to view graphs for a time period of 3 hours, 1 day, and 1 week.
Rogues	Displays a graph showing the top 5 rogue AP detectors in the network.
Interferences	Displays a graph showing the top 5 interferences detected in the network.

Table 35: *Security pane*

Data Pane Content	Description
Intrusion Detection	Displays graphs showing the top 5 infrastructure, client, and intrusion detection attacks.
WIDS Events	Displays a list of the WIDS events. The table displays information for the following types of WIDS events: ■ Rogues ■ Interferences ■ Infrastructure Attacks ■ Client Attacks The **Rogues** table displays the following information for the WIDS events: ■ **First Seen**—The time relative to the current moment (for example, 6 minutes; an hour) at which the rogue device was f detected in the network. ■ **Last Seen**—The time relative to the current moment (for example, 6 minutes; an hour) at which the rogue device was last detected in the network. ■ **Reason For Classification**—Reason for classification of the rogue device (Instant AP). ■ **Detecting AP**—The AP that detected the rogue device in the network. ■ **Station MAC**—MAC address of the station. ■ **Containment Status**—Details of the containment status. ■ **ESSID**—The ESSIDs broadcast by the rogue device. ■ **Channel**—Number of radio channels detected on the rogue device. ■ **Radio**—Radio band on which the interference was detected. The **Interferences** table, **Infrastructure Attacks** table, and the **Client Attacks** table display the following information: ■ **Type**—The type of the interference, infrastructure attack, or client attack detected. ■ **Level**—The level of the interference, infrastructure attack, or client attack detected. ■ **Date/Time**—Date and time of the interference, infrastructure attack, or client attack detected. ■ **Description**—A description of the interference, infrastructure attack, or client attack detected. ■ **Detecting AP**—The MAC address of the AP that detected the interference or attack. ■ **Virtual Controller**—The VC name of the Instant AP cluster in which the interference or attack was detected. ■ **Station MAC**—The MAC address of the station. ■ **Radio**—The radio band on which the interference or attack was detected.

Network Health

The **Network Health** menu option in the **Monitoring & Reports** application provides detailed information of the network health status and usage for the sites configured in your setup.

Data Source

The **Network Health** page displays network and site health data for the overall network and gateways.

Page Views

The **Network Health** page offers the following views:

- **Grid**—Primarily provides numerical representation of the data. The **Site Type** and **Connectivity Status** columns provide textual values.
- **Status**—Uses the following indicators to present information on status of the network health:

- **Small black bullet icon**—Indicates no issues.
- **Big red bullet icon**—Indicates potential issues.

- **Map**—The map provides a pictorial view of the network across various sites. The sites are color coded; red indicates potential issues and gray indicates that there are no issues. To change the zoom level, click the zoom icons.
  - From the **Pin Radius** drop-down list, select one of the following: No Grouping, 5 miles, 10 miles, 15 miles, 20 miles, or 50 miles.
  - From the **Data Column For Map** drop-down list, select one of the following: Status, High Mem Usage, High CPU Usage, High CH utilization, High Noise, Uplinks Down, or Tunnels Down.

Legend

The following indicators are used present information on status of network health:

- **Small black bullet icon**—Indicates no issues
- **Big red bullet icon**—Indicates potential issues

Summary

If the data source is set to **Summary**, the **Network Health** page displays the following information:

Table 36: *Summary Page View*

Header	Description
Site Name	Name of the site. Clicking on the site name opens the **Site Health** page. For more information, see the *Site Health* section in the *Aruba Central Help Center*..
Number of Devices	Displays the following details for devices: ■ **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: ● 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: ● 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: ● WLAN CPU High ● Wired CPU High ● Branch CPU High ■ **High Channel Utilization**—Number of APs with a higher channel utilization per radio band. ■ **High Noise**—Number of APs with a high RF noise.
User	Displays the following details for WLAN clients: ■ **Client Health Score** ■ **Client Connectivity Score** To sort the table content based on client health or connectivity score, click the filter icon and specify a value.
WAN	Displays the following details for the WAN: ■ **Uplinks Down** ■ **Tunnels Down**

Table 36: *Summary Page View*

Header	Description
	The range is from 0 to 100 percent. To filter uplinks and tunnels, click the column filter bar and enter values in the **Min** and **Max** text boxes.

Gateway

Table 37: *Gateway 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 *Site Health* section in the *Aruba Central Help Center*.
Site Type	Displays the total number of sites for each site type.	Displays whether the device is deployed as a hub or spoke. ■ To filter gateways provisioned as a hub, click **Hub**. ■ To filter gateways provisioned as a spoke, click **Spoke**.
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. ■ To filter devices in UP sate, click **Up**. ■ To filter devices in DOWN sate, click **Down**.
Connectivity	Displays the total number of links and the average bandwidth consumed.	Displays the following information: ■ **Status**—Displays the overall connectivity status. Hover your mouse over the column to view the circuit status, tunnel status, overlay status, and underlay status separately. One of the following statuses is displayed: ● Up ● Partial ● Down ■ **Bandwidth**—Displays bandwidth details. ● **Configured**—Displays the bandwidth that is configured on the Branch 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.
Performance	Displays the average value for site availability and policy compliance.	Displays the following metrics: ■ **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.

Site Health

In the **Network Health** page, click the site name to view details of a specific site. The **Site Health** page is displayed. The **Site Health** page view can be set to the **Summary** or the **Gateways** view.

The **Summary** view displays details for the wired and wireless devices deployed on the site. The **Gateway** view displays the details of the WAN setup deployed on the site.

Summary

The **Site Health Summary** page displays the following details:

Table 38: *Site Health Summary Page*

Content	Description
Site Name	Name of the site. To search for a specific site, click the **Site Name** drop-down and enter the search text.
Data View	Data source. For example, if the data view is set to **Summary**, the page displays data for the wired and WLAN devices deployed on a site.
Time Range	Time range selection drop-down for viewing site health. You can set the time range to 3 hours, 1 day, 1 week, 1 month, or 3 months.
Summary	The following details are available: ■ **Name**—Name of the site. ■ **Location**—Location of the site. ■ **APs**—Number of APs deployed on the site. ■ **Switches**—Number of switches deployed on the site. ■ **Gateways**—Number of gateways deployed on the site. ■ **Topology** icon—Link to topology view. The topology page displays the network topology of the site. ■ **Summary Statistics**—A graphical representation of the number of clients and bandwidth usage for the selected time range. ■ **Change Log**—A visual representation of change logs for configuration, firmware, and reboot changes in the selected time range. The number of changes logged for configuration, firmware upgrades and reboots are represented in gray, green, and red indicators.
System Health Indicators Graphs	The following details are displayed: **Down Devices**—This graph shows the count or percentage of devices with DOWN status. You can set the filter to view either the total count or the percentage of the devices that are in Down status. The graph displays the following information: ■ Total number of devices ■ Number of unique devices that were DOWN ■ Minimum and maximum device downtime. When you click any point in time range within the graph, the **See Devices** option is displayed. Click **See Devices**. A pop-up window opens and displays the details of devices with DOWN status and their UP and Down Time in percentage. You can also add other metrics such as CPU, Memory, Channel Utilization (5 GHz, 2.4 GHz), or Noise Floor (5 GHz, 2.4 GHz) for this devices list.
	High Memory Utilization—This graph shows the total count or percentage of devices with high memory utilization. ■ **Filter**—You can set the filter to count or percentage to view the total count or percentage of devices with a higher memory utilization. ■ **Device Details**—The graph also displays the total number of devices, number of unique devices, the minimum and maximum number of devices with high memory utilization. You can also view the total count or percentage of maximum and minimum number of devices with high memory utilization for specific time when you hover your mouse over the graph. ■ **Threshold Setting**—You can also choose to view the graph details based on one of the following criteria by selecting an option from the **Temporary Baseline Override** list (threshold setting widget): ● >70% memory utilization

Table 38: *Site Health Summary Page*

Content	Description
	● >80% memory utilization ● >90% memory utilization To view more details, click **See Devices**. A pop-up window opens and provides the details of devices with high memory utilization and their minimum and maximum memory utilization values. You can add other metrics such as CPU, Channel Utilization (5 GHz, 2.4 GHz), Noise Floor (5 GHz, 2.4 GHz), or Device Downtime for the devices.
	High CPU Utilization—This graph shows the total count or percentage of devices with high CPU utilization. ■ **Filter**—You can set the filter to total count or percentage to view the total count or percentage of devices with a higher CPU utilization. ■ **Device Details**—The graph also displays the total number of devices, number of unique devices with high CPU utilization, and minimum and maximum number of devices with high CPU utilization. You can also view the total count or percentage of maximum and minimum number of devices with high CPU utilization for a specific time when you hover your mouse over the graph. ■ **Threshold setting**—You can also choose to view the graph details based on one of the following criteria by selecting an option from the **Temporary Baseline Override** list (threshold setting widget): ● >70% CPU utilization ● >80% CPU utilization ● >90% CPU utilization To view more details, click **See Devices**. A pop-up window opens and displays the details of devices with high CPU utilization and their individual minimum and maximum CPU utilization values. You can add other metrics such as Memory , Channel Utilization (5 GHz, 2.4 GHz), Noise Floor (5 GHz, 2.4 GHz), and Device Downtime for the devices.
RF Health Indicators Graphs	You can view the following RF health status for the 2.4GHz and 5GHz bands: **5 GHz Utilization and Noise**—This graph displays the total count or percentage of devices with high channel utilization and high noise floor levels for 5GHz band. ■ **Filter**—You can set the filter to total count or percentage to view the total count or percentage of devices with a higher channel utilization for the 5GHz radio band. ■ **Device Details**—The graph displays total number of devices, number of unique devices with high 5 GHz channel utilization and high noise floor levels, and the minimum and maximum number of devices with high channel utilization. You can also view the total count or percentage of maximum and minimum number of devices with high CPU utilization for a specific time when you hover your mouse over the graph. ■ **Threshold setting**—You can also choose to view the graph details based one of the following criteria by selecting an option from the Temporary Baseline Override list (threshold setting widget): ● >60% 5 GHz Utilization ● >70% 5 GHz Utilization ● >80% 5 GHz Utilization ● >-75 dBm 5 GHz Noise ● >-80 dBm 5 GHz Noise ● >-85 dBm 5 GHz Noise To view more details, click **See Devices**. A pop-up window opens and displays details of devices with high 5 GHz channel utilization (minimum and maximum values) and Noise Floor (minimum and maximum) values. You can add other metrics such as 2.4 GHz Channel Utilization, 2.4 GHz Noise Floor, CPU, Device Downtime, or Memory for the list of devices.
	2.4 GHz Utilization and Noise: —This graph displays the total count or percentage of devices with a higher channel utilization and high noise floor levels for 2.4 GHz channel. ■ **Filter**—You can set the filter to total count or percentage to view the total count or percentage of devices with a higher channel utilization for the 2GHz radio band. ■ **Device Details**—The graph displays the total number of devices, number of unique devices with high 2.4 GHz channel utilization and noise floor levels, minimum and maximum number of devices with high channel utilization and noise levels. You can also view the total

Table 38: *Site Health Summary Page*

Content	Description
	count or percentage of maximum and minimum number of devices with high 2.4 GHz Utilization and Noise. ■ **Threshold Setting**—You can also choose to view the graph details based one of the following criteria by selecting an option from the Temporary Baseline Override list (threshold setting widget): ●>60% 2.4 GHz Utilization ●>70% 2.4 GHz Utilization ●>80% 2.4 GHz Utilization ●>-75 dBm 2.4 GHz Noise ●>-80 dBm 2.4 GHz Noise ●>-85 dBm 2.4 GHz Noise To view more details, click **See Devices**. A pop-up window opens and provides the details of devices with high 2.4 GHz channel utilization (minimum and maximum values) and Noise Floor (minimum and maximum) values. You can add other metrics such as CPU, Memory, 5 GHz Channel Utilization, 5 GHz Noise Floor, and Device Downtime for the list of devices.
Client Health Indicators Graph	Displays the graph showing the overall health indicators for the clients connected to the devices. The devices with low client connectivity scores are displayed for the selected time range.
NOTE: The threshold setting widget (⚙) is visible only when you bring the mouse pointer closer to its position slightly above the right-hand side of each graph.	

Gateways

The Site Health Gateway page displays the following information:

Table 39: *Site Health Gateways Page*

Content	Description
Site Name	Name of the site. From the drop-down list, select a site.
Data View	Data source. From the drop-down list, select either **Summary** or **Gateway**. For example, if the data view is set to **Gateways**, the page displays data for the gateways deployed on the site.
Time Range	Time range selection drop-down for viewing site health. You can set the time range to 3 hours, 1 day, 1 week, 1 month, or 3 months.
Summary	The following details are available: ■ **Name**—Name of the site. ■ **Location**—Location of the site. ■ **APs**—Number of APs deployed on the site. ■ **Switches**—Number of switches deployed on the site. ■ **Gateways**—Number of gateways deployed on the site. ■ **Topology** Icon—Link to topology view. The topology page displays the network topology of the site.

Table 39: *Site Health Gateways Page*

Content	Description
Site Availability graph	Site availability metrics per provider represented in a chart. The graph displays detailed metrics for the number of sites in the down status, percentage of site availability, and the number of unknown sites.
Policy Compliance graph	Policy compliance metrics for the site. The path steering data is used to calculate this metric.
Bandwidth graph	Bandwidth utilization of the selected site. From the drop-down list, select one of the following: ■ All Traffic ■ Internet vs. VPN
Bandwidth Provider graph	Bandwidth utilization of the selected uplink. From the drop-down list, select the uplink.
Transport Health graph	Displays the transport health of the site based on active monitoring probes. Site transport health is an average of MOS score across all probes.
NOTE: If you hover over any graph, a pop-up window opens and displays the data specific to that graph. Click on the graph to lock the time range. After you lock the selection, the same time range is selected across all the graphs in the **Site Health** page. **NOTE:** If you click on any graph, a **see devices** button in enabled below all the graphs. Click **see details** to view the list of devices. From the **Add Metric** drop-down list, select one or more of the following: Site Availability, Policy Compliance, Bandwidth, Internet vs. VPN, or Transport Health.	

Label Health

The **Label Health** menu option in the **Monitoring & Reports** application provides detailed information on the health and performance of the devices attached to each label in your setup.

Data Source

The **Label Health** page displays details for all the wired and WLAN devices attached to the labels configured in your setup.

Page Views

The **Label Health** page offers the following views:

- **Grid**—The grid view displays label health information in numerical values.
- **Status**—The status view displays health indicators. The following indicators are used present information on status of network health:
  - **Small black bullet icon**—Indicates no issues.
  - **Big red bullet icon**—Indicates potential issues.

Summary

The **Label Health** > **Summary** page displays the following information:

Table 40: *Summary Page View*

Header	Description
Label Name	Name of the label. To view details for a specific label, click the label from the list.
Number of Devices	The page displays the following details for devices: ■ **Status**—Number of devices that are in Up or Down. ■ **High Memory Usage**—Number of devices with high memory utilization. ■ **High CPU Usage**—Number of devices with high CPU usage. ■ **RF High Channel Usage**—Number of APs with a higher channel utilization per radio band. ■ **RF High Noise**—Number of APs with a high RF noise.
User	The page displays the connectivity health score details for WLAN clients. You can set the minimum and maximum filters to view clients within a specific range of connectivity score. The client connectivity health score refers to a cumulative score that is computed based on client onboarding performance of the network. The connectivity score below 69% is indicated in red and hints at potential issues in the client onboarding experience.
WAN	The page displays the following details for WAN. To sort the table content based on the uplink and tunnel status, click the filter icon and specify a value. ■ **Uplinks Down** ■ **Tunnels Down**

Per Label Details

To view device health and performance details per label, click the label name in the **Label Health** page.

Table 41: *Label Health Summary Page*

Content	Description
Site Name	Name of the label. To search for a label, click the drop-down and enter the search text.
Data View	Data source. For example, if the data view is set **Summary**, the page displays data for the wired and WLAN devices attached to a label.
Time Range	Time range selection drop-down for viewing device health per label. You can set the time range to 3 hours, 1 day, 1 week, 1 month, or 3 months.
Summary	The following details are displayed: ■ **Name**—Name of the site. ■ **Location**—Location of the site. ■ **APs**—Number of APs deployed on the site. ■ **Switches**—Number of switches deployed on the site. ■ **Gateways**—Number of gateways deployed on the site. ■ **Topology** icon—Link to topology view. The topology page displays the network topology of the site. ■ **Summary Statistics**—A graphical representation of the number of clients and bandwidth usage for the selected time range. ■ **Change Log**—A visual representation of change logs for configuration, firmware, and reboot changes in the selected time range. The number of changes logged for configuration, firmware upgrades and reboots are represented in gray, green, and red indicators.

Table 41: *Label Health Summary Page*

Content	Description
System Health Indicators Graphs	The following details are displayed: **Down Devices**—This graph shows the count or percentage of devices with DOWN status. You can set the filter to view either the total count or the percentage of the devices that are in Down status. The graph displays the following information: ■ Total number of devices ■ Number of unique devices that were DOWN ■ Minimum and maximum device downtime. When you click any point in time range within the graph, the **See Devices** option is displayed. Click **See Devices**. A pop-up window opens and displays the details of devices with DOWN status and their UP and Down Time in percentage. You can also add other metrics such as CPU, Memory, Channel Utilization (5 GHz, 2.4 GHz), or Noise Floor (5 GHz, 2.4 GHz) for this devices list.
	High CPU & High Memory—This graph shows the total count or percentage of devices with high CPU and memory utilization. ■ Filter—You can set the filter to count or percentage to view the total count or percentage of devices with a higher memory utilization. ■ Device Details—The graph also displays the total number of devices, number of unique devices, the minimum and maximum number of devices with high memory utilization. You can also view the total count or percentage of maximum and minimum number of devices with high memory utilization for specific time when you hover your mouse over the graph. ■ Threshold Setting—You can also choose to view the graph details based on one of the following criteria by selecting an option from the **Temporary Baseline Override** list (threshold setting widget): ●>70% memory utilization ●>80% memory utilization ●>90% memory utilization When you click any point in time range within the graph, the **See Devices** option is displayed. Click **See Devices**. A pop-up window opens and provides the details of devices with high memory utilization and their minimum and maximum memory utilization values. You can add other metrics such as CPU, Channel Utilization (5 GHz, 2.4 GHz), Noise Floor (5 GHz, 2.4 GHz), or Device Downtime for the devices.
	High CPU Utilization—This graph shows the total count or percentage of devices with high CPU utilization. ■ Filter—You can set the filter to total count or percentage to view the total count or percentage of devices with a higher CPU utilization. ■ Device Details—The graph also displays the total number of devices, number of unique devices with high CPU utilization, and minimum and maximum number of devices with high CPU utilization. You can also view the total count or percentage of maximum and minimum number of devices with high CPU utilization for a specific time when you hover your mouse over the graph. ■ Threshold setting—You can also choose to view the graph details based on one of the following criteria by selecting an option from the **Temporary Baseline Override** list (threshold setting widget): ●>70% CPU utilization ●>80% CPU utilization ●>90% CPU utilization When you click any point in time range within the graph, the **See Devices** option is displayed. Click **See Devices**. A pop-up window opens and displays the details of devices with high CPU utilization and their individual minimum and maximum CPU utilization values. You can add other metrics such as Memory , Channel Utilization (5 GHz, 2.4 GHz), Noise Floor (5 GHz, 2.4 GHz), and Device Downtime for the devices.
RF Health Indicators Graphs	You can view the following RF health status for the 2.4GHz and 5GHz bands: **5 GHz Utilization and Noise**—This graph displays the total count or percentage of devices with high channel utilization and high noise floor levels for 5GHz band. ■ Filter—You can set the filter to total count or percentage to view the total count or

Table 41: *Label Health Summary Page*

Content	Description
	percentage of devices with a higher channel utilization for the 5GHz radio band. ■ Device Details—The graph displays total number of devices, number of unique devices with high 5 GHz channel utilization and high noise floor levels, and the minimum and maximum number of devices with high channel utilization. You can also view the total count or percentage of maximum and minimum number of devices with high CPU utilization for a specific time when you hover your mouse over the graph. ■ Threshold setting—You can also choose to view the graph details based one of the following criteria by selecting an option from the Temporary Baseline Override list (threshold setting widget): ●>60% 5 GHz Utilization ●>70% 5 GHz Utilization ●>80% 5 GHz Utilization ●>-75 dBm 5 GHz Noise ●>-80 dBm 5 GHz Noise ●>-85 dBm 5 GHz Noise When you click any point in time range within the graph, the **See Devices** option is displayed. Click **See Devices**. A pop-up window opens and displays details of devices with high 5 GHz channel utilization (minimum and maximum values) and Noise Floor (minimum and maximum) values. You can add other metrics such as 2.4 GHz Channel Utilization, 2.4 GHz Noise Floor, CPU, Device Downtime, or Memory for the list of devices.
	2.4 GHz Utilization and Noise: —This graph displays the total count or percentage of devices with a higher channel utilization and high noise floor levels for 2.4 GHz channel. ■ Filter—You can set the filter to total count or percentage to view the total count or percentage of devices with a higher channel utilization for the 2GHz radio band. ■ Device Details—The graph displays the total number of devices, number of unique devices with high 2.4 GHz channel utilization and noise floor levels, minimum and maximum number of devices with high channel utilization and noise levels. You can also view the total count or percentage of maximum and minimum number of devices with high 2.4 GHz Utilization and Noise. ■ Threshold Setting—You can also choose to view the graph details based one of the following criteria by selecting an option from the Temporary Baseline Override list (threshold setting widget): ●>60% 2.4 GHz Utilization ●>70% 2.4 GHz Utilization ●>80% 2.4 GHz Utilization ●>-75 dBm 2.4 GHz Noise ●>-80 dBm 2.4 GHz Noise ●>-85 dBm 2.4 GHz Noise When you click any point in time range within the graph, the **See Devices** option is displayed. Click **See Devices**. A pop-up window opens and provides the details of devices with high 2.4 GHz channel utilization (minimum and maximum values) and Noise Floor (minimum and maximum) values. You can add other metrics such as CPU, Memory, 5 GHz Channel Utilization, 5 GHz Noise Floor, and Device Downtime for the list of devices.
Client Health Indicators Graph	Displays the graph showing the overall health indicators for the clients connected to the devices. The devices with low client connectivity scores are displayed for the selected time range.
NOTE: The threshold setting widget (⚙) is visible only when you bring the mouse pointer closer to its position slightly above the right-hand side of each graph.	

Client Overview

The **Monitoring & Reports** > **Client Overview** page displays the details of clients connected to the devices in Aruba Central.

The **Client Overview** page displays the total number of clients, bandwidth usage, and the application usage by the clients connected to the wired and wireless networks.

Table 42: *Client Overview Page*

Data Pane Content	Description
Temporal Filter	By default, the graphs on the **Client Overview** pane are plotted for a time range of 3 hours. To view the graphs for a different time range, click the **Temporal Filter** link. You can choose to view graphs for a time period of 3 hours, 1 day, 1 week, 1 month and 3 months. However, the Distribution data (Client OS) under the **Distribution** tab does not honor the time range you selected in the temporal filter.
Total	Displays the total number of clients.
Wired	Displays the total number of clients connected to the wired network.
Wireless	Displays the total number of clients connected to wireless network.
Usage	Displays the following: ■ **Bandwidth Usage**—Displays the incoming and outgoing throughput traffic for all the clients during a specific time range. The graph will not show any data for the clients that are connected to the network for less than two hours. ■ **Applications**—Displays a table with details on the client traffic flow to and from various applications. Click the bar graph icon to view bar graphs indicating the traffic flow. ■ **Websites**—Displays a table with details on client traffic flow and their data usage by various websites. Click the bar graph icon to view bar graphs indicating the data usage by various websites. For more information about enabling **Application Visibility**, list of supported Instant APs , and the data displayed on the **Applications** and **Websites** sections, see Application Visibility on page 204.
Distribution	Displays the type of client device connected to the wireless network.
Top N	Displays a list of clients connected to the currently available SSIDs that utilize the maximum bandwidth in the network. The **Top Clients by Usage** table displays data only for the clients that are connected to the network for a total duration of two or more hours.

Unified Clients

The **Monitoring & Reports** > **Clients** page provides a summary view of all the clients connected to the network. From this page, you can filter clients based on the network to which the clients are connected. The page displays key client information and also allows you to drill down to a specific client detail page.

By default, the **Clients** page displays a unified list of clients for the selected group. The list of clients is populated for a time range of 3 hours. To view the list of clients for a different time range, click the **Temporal Filter** link and choose the time period. Total data usage for the selected time period is displayed above the client summary bar.

To filter clients based on the device to which the clients are connected, select the device type from the **Clients** drop-down list:

- **Unified**—Displays a unified list of clients connected to the network.
- **AP**—Displays a list of clients connected to the Instant AP.
- **Switch**—Displays a list of clients connected to the switch.
- **Gateway**—Displays a list of clients connected to the Aruba Gateway.

The wired client will show up in the **Unified Clients** page only if the client is connected to an Aruba 2540 Series, Aruba 2920 Series, Aruba 2930F Series, Aruba 2930M Series, Aruba 3810 Series, or Aruba 5400R Series switch.

To filter clients based on the network to which the clients are connected, click the network type from the **Client Summary** bar:

- **Wireless**—Displays a list of clients connected to the wireless network.
- **Wired**—Displays a list of clients connected to the wired network.

The **Clients** table lists the details of each client. By default, the table displays the following columns: **Client Name**, **Status**, **IP Address**, **VLAN**, **Connected To**, **Link**, **AP Role**, **Gateway Role**, and **Health**. Click the ellipsis icon to perform additional operations:

- **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.

If a filter icon appears next to the column header, click it enter the filter criteria or select the 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: **Connected**, **Offline**, or **Failed**.

For a visual representation of the **Clients** page, click here.

Table 43: *Unified Client Details*

Column	Applicability	Description
Client Name	■ Unified ■ AP ■ Switch ■ Gateway	Username, hostname, or MAC address of the client. Click the client name to view the client details page.
Status	■ Unified ■ AP ■ Switch	Client connection status. Use the filter option to view the following: ■ Connected clients ■ Offline clients ■ Failed clients. Hover your mouse over the status to view: ■ Client name ■ IP address ■ **Connected**—Date and time at which the client connected. ■ **Offline**—Last seen time. ■ **Failed**—Failure reason and last seen time.
IP Address	■ Unified ■ AP ■ Switch	IP address of the client.
VLAN	■ Unified ■ AP ■ Switch ■ Gateway	VLAN of the device to which the client is connected.
Connected To	■ Unified	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.
Link	■ Unified	Displays SSID for wireless clients and port number for wired clients.
AP Role	■ Unified ■ AP	Role assigned by the Instant AP.
Gateway Role	■ Unified ■ Gateway	Role assigned by the Aruba Gateway.
Health	■ Unified ■ AP ■ Gateway	Client health. The value can be one of the following: ■ **Good**—51-100. ■ **Fair**—26-50. ■ **Poor**—0-25.
Failure Stage	■ Unified ■ AP	Failure status of the client that failed to connect. The failure reasons could be: ■ Association error ■ MAC authentication error ■ 802.1X authentication error ■ Key exchange error ■ DHCP error ■ Captive Portal error
Group Name	■ Unified ■ AP ■ Switch ■ Gateway	Group name of the device managed by Aruba Central.
Site Name	■ Unified	Name of the site in which the devices managed by Aruba Centralare installed.

Table 43: *Unified Client Details*

Column	Applicability	Description
	■ AP ■ Switch ■ Gateway	
MAC Address	■ Unified ■ AP ■ Switch ■ Gateway	MAC address of the client.
Hostname	■ Unified ■ AP ■ Gateway	Host name of the client.
User Name	■ Unified ■ AP ■ Switch ■ Gateway	Username of the client.
Key Management	■ Unified ■ AP	Security mode used by the client.
Authentication	■ Unified ■ AP	Authentication type.
IPV6 Address	■ Unified ■ AP	IPv6 address of the client.
Capabilities	■ Unified ■ AP	Client capabilities.
Usage	■ Unified ■ AP ■ Switch ■ Gateway	Total data usage for the selected time period.
OS	■ Unified ■ AP ■ Gateway	Operating system of the client.
Last Seen Time	■ Unified ■ AP ■ Switch ■ Gateway	Date and time at which the client was last seen.
Connected Since	■ Unified ■ AP ■ Switch ■ Gateway	Date and time since when the client was connected.
AP Name	■ Unified ■ AP	Name of the Instant AP.
SSID	■ AP	SSID to which the client is connected.

Table 43: *Unified Client Details*

Column	Applicability	Description
BSSID	■ AP	BSSID of the Instant AP.
AP Mac Address	■ Unified ■ AP	MAC address of the Instant AP.
Speed(TX/RX)	■ AP	Last known connection speed of the client.
SNR	■ AP	Signal-to-Noise Ratio reported by the Instant AP.
Channel/Band	■ Unified ■ AP	Last connected channel and band.
Switch Name	■ Unified ■ Switch	Name of the switch.
Port	■ Unified ■ Switch ■ Gateway	Port number of the switch.
Gateway Name	■ Unified ■ Gateway	Name of the Aruba Gateway.

Client Details

The **Monitoring & Reports** > **Clients** page shows the clients connected to the wireless and wired networks. By default, the **Clients** page displays a unified list of clients for the selected group.

The client details page shows a summary of the client and allows you to navigate to the corresponding device details page.

The wired client shows up in the **Unified Clients** page only if the client is connected to an Aruba 2540 Series, Aruba 2920 Series, Aruba 2930F Series, Aruba 2930M Series, Aruba 3810 Series, or Aruba 5400R Series switch.

This section includes the following topics:

Viewing Clients Connected to Wireless Networks

To view the details of a client connected to the wireless network:

1. Go to **Monitoring & Reports** > **Clients**. By default, the **Clients** table displays a unified list of clients for the selected group.
2. 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.

For a visual representation of the procedure, click here.

Client Summary Bar

The client summary bar displays the following information:

Table 44: *Client Summary Bar*

Field	Description
MAC address and connection status	MAC address of the device to which the client is connected and connection status. Connection status is updated immediately on state change.
Device Health	Signal strength of the client device. The signal strength value is displayed in percentage: ■ 0-25—Poor ■ 26-50—Fair ■ 50-100—Good
SNR	SNR for the client as measured by the AP. The SNR value is displayed in decibels: ■ 0-20—Poor ■ 21-35—Fair ■ >35—Good
TX Rate	Data transmission rate.
RX Rate	Data reception rate.
Connected To	Name of the AP that broadcasts the SSID to which the client is connected. Click the name of the AP to view the device details page.

Live Client Monitoring

Click **Go Live** to start live monitoring of the client. Live monitoring is supported only if the Instant AP is running 8.4.0.0 firmware version. Live monitoring stops after 15 minutes. At any point, you can click **Stop Live** to go back to the historical view.

Five seconds after you start live monitoring, the following data starts getting populated:

- **Usage** graph—The Instant AP sends bandwidth usage data every five seconds and the usage graph is live for 15 minutes.
- For the following fields, data is refreshed every five seconds and the average for the last 60 seconds is displayed:
  - **Device Health**
  - **SNR**
  - **TX Rate**
  - **RX Rate**

For a visual representation of the procedure, click here.

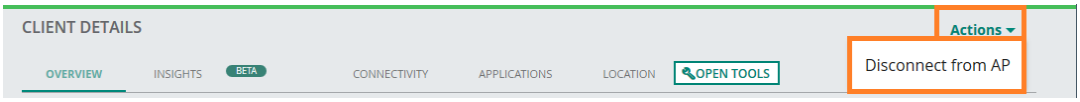
Disconnecting a Wireless Client from an AP

To disconnect a wireless client from an online AP:

1. Go to **Monitoring & Reports** > **Clients**. By default, the **Clients** table displays a unified list of clients for the selected group.

2. 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.

3. From the **Actions** drop-down list, click **Disconnect from AP**:



NOTE

The **Actions** drop-down is disabled if the AP is offline.

Wireless Client Details

The wireless client details page consists the following tabs:

- Overview
- Connectivity
- Applications
- Location
- Events
- Open Tools
- AI Insights

Overview

The **Overview** tab consists of four sections. The following table describes the information displayed in each section:

Table 45: *Overview Tab*

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: ■ **Client** > **SSID** > **AP** ■ **Client** > **SSID** > **AP** > **Switch** ■ **Client** > **SSID** > **AP** > **Switch** > **Gateway** ■ **Client** > **SSID** > **AP** > **Gateway**
Client Info	Displays the following information: ■ **Username**—User name of the client. ■ **Hostname**—Hostname of the client. ■ **IP Address**—IP address of the client. ■ **Client Type**—Type of the client device. ■ **Connected Since**—Date and time since when the client is connected. ■ **Device OS**—Operating system running on the client device.
Network Info	Displays the following information: ■ **VLAN**—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 by AP to the client. ■ **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

Table 45: *Overview Tab*

Section	Description
	profile. ■ **Gateway Role**—Displays the role assigned by the Gateway. ■ **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.
Connection Info	Displays the following information: ■ **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.

Connectivity

The **Connectivity** tab displays the following information:

Table 46: *Connectivity Tab*

Section	Description
Bandwidth Usage graph	Displays the incoming and outgoing throughput traffic for the client during a specific time range.
UCC Call Detail Records	Displays call detail records for the client if any. To view this data, ensure that the **Unified Communication** application service is enabled on the APs. The table displays the following information for the client: ■ **Start Time**—Start time of the call. ■ **End Time**—Time at which the call ended. ■ **Call Type**—Type of the call. For example, audio or video. ■ **Protocol**—Application protocol used for the call. ■ **Connectivity Type**—Type of connection used to make a call. For example, call from Wi-Fi to an external device. ■ **End to End Call Quality**—Quality of the call. ■ **Status**—Status of the session.
Association History	Displays details of the Instant AP and client association. The widget displays the following information: ■ **Time**—Displays the time stamp and details of the Instant AP and client association. ■ **AP Name**—AP to which the client is connected.

Applications

To view application usage metrics for the client connected to the wireless network, enable **Deep Packet Inspection**.

The **Applications** tab consists of two sections:

- **Applications**—Displays a table with details on the client traffic flow to and from various applications. Click the bar graph icon to view bar graphs indicating the traffic flow.
- **Websites**—Displays a table with details on client traffic flow and their data usage by various websites. Click the bar graph icon to view bar graphs indicating the data usage by various websites.

For more information about enabling **Application Visibility**, list of supported Instant APs, and the data displayed on the **Applications** and **Websites** sections, see Application Visibility on page 204.

Location

The **Location** tab displays the current physical location of the client device on the floor map.

Events

The **Events** tab displays the time stamp and description of events generated by the AP and client association.

Open Tools

Click **Open Tools** to open the **Tools** page. The **Tools** page is automatically filtered based on the client you select. This enables network administrators to perform checks on the client and debug client connectivity issues. For more information, see Using Troubleshooting Tools on page 1.

AI Insights

The **Client AI Insight** page displays information about Client performance issues such as, excessive 2.4G dwell and low SNR links. AI Insights are displayed for a selected time period based on the time selected in **Temporal Filter**. The user can select the following time range from the **Temporal Filter** to view the insight data:

- 3 hours —Displays 4 bar graphs with exact hourly data
- 1 week —Displays 7 bars with past 7 days' daily data
- 1 day—Displays 24 bars with exact hourly data
- 1 month—Displays 30 bars with past 30 days' daily data

3 months Temporal Filter is not supported. If the user selects 3 months in the Temporal Filter, it displays 1 month time series.

The graphs represent severity in different colors:

- **Red**—High
- **Yellow**—Medium
- **Grey**—Low

Each Insight further includes categories of information present in form of tabs like, reason, band, channel, SNR and so on. These tabs are clickable and display the detailed information found in that section of the Insight.

The **Client AI Insights** page displays the performance issues based on the following criteria:

Excessive 2.4G Dwell

The **Excessive 2.4G Dwell** insight shows information about the number of dual-band (2.4G and 5G) devices that spend a significant amount of time in the 2.4G band. 5G channels are often preferable, as they typically offer faster Wi-Fi connections and lower levels of interference than 2.4G channels.

Insight Details

The **Excessive 2.4G Dwell** insight includes the categories of information listed below. Click the tabs to display details about the information found in that section of the insight.

- **Band**—Displays if devices experiencing a low signal-quality link were using 2.4G or 5G radio bands. The graph on this tab shows the proportion of time (minutes) and usage of the client.
- **Tx Power**—Displays the percentage of Tx Power distribution (dBm) in both the 2.4G and 5G band.
- **SNR**—Displays the percentage of SNR (dB) in both 2.4G and 5G band.

Low SNR Links

The **Low SNR Links** insight report shows information about client devices that have a low-quality signal-strength connection to their access point.

Insight Details

The **Low SNR Links** insight includes the categories of information listed below. Click the tabs to display details about the information found in that section of the insight.

- **SNR**—Displays four views, Signal-to-Noise Ratio, Data Rate, Upload and Download overtime for the selected temporal filter.
- **Band**—Displays if devices experiencing a low signal-quality link were using 2.4G or 5G radio bands. The graph on this tab shows the proportion of time and usage of the client.
- **Good vs Bad**—Displays the amount of time (minutes) with Low SNR (Bad) and High SNR (Good). The data is represented in the form of a pie chart.
- **By AP**—Displays the total time (High and Low SNR) that the client connected to all the APs in the network.

Viewing Clients Connected to Wired Networks

To view the details of a client connected to the wired network:

1. From the **Monitoring & Reports** app, click **Clients**. By default, the **Clients** table displays a unified list of clients for the selected group.
2. Click the client name to view the client details page. If there are many clients connected to the network, click **Wired** to filter the clients connected to the wired network and enter the client name in the **Client Name** column.

For a visual representation of the procedure, click here.

Wired Client Details

The wired client details page consists the following sections:

- **Client Summary** bar—Displays the following:
  - MAC address of the device to which the client is connected and connection status.
  - **Connected To**—Name of the Gateway to which the client is connected. Click the name of the Gateway to view the device details page.
- **Tabs**—Consists of the following tabs:
  - Overview
  - Connectivity
  - Applications

Overview

The **Overview** tab consists of three sections. The following table describes the information displayed in each section:

Table 47: *Overview Tab*

Section	Description
Data Path	Displays the data path of the client in the network. Click the device icon to view the corresponding device details page. The data path can be one of the following: ■ **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 Info	Displays the following information: ■ **Username**—User name of the client. ■ **Hostname**—Hostname of the client. ■ **IP Address**—IP address of the client. ■ **Client Type**—Type of the client device. ■ **Connected Since**—Date and time since when the client is connected. ■ **Device OS**—Operating system running on the client device.
Network Info	Displays the following information: ■ **VLAN**—VLAN ID on which the client is connected to the AP. ■ **VLAN Derivation**—Displays how the dynamic VLAN is derived. ■ **AP Role**—AP role associated to the client. ■ **AP Derivation**—Displays how the AP role is derived. ■ **Gateway Role**—Gateway role associated to the client. ■ **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.

Connectivity

The **Connectivity** tab displays the incoming and outgoing throughput traffic for the client during a specific time range.

Applications

To view application usage metrics for the client connected to the wired network, enable **Deep Packet Inspection**.

The **Applications** tab consists of two sections:

- **Applications**—Displays a table with details on the client traffic flow to and from various applications. Click the bar graph icon to view bar graphs indicating the traffic flow.
- **Websites**—Displays a table with details on client traffic flow and their data usage by various websites. Click the bar graph icon to view bar graphs indicating the data usage by various websites.

For more information about enabling **Application Visibility**, list of supported Instant APs, and the data displayed on the **Applications** and **Websites** sections, see Application Visibility on page 204.

Application Visibility

The **Monitoring & Reports** > **Application Visibility** tab provides detailed information on data usage by the clients connected to APs in the network. Clicking the **Application Visibility** tab displays a 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 **Application Visibility** dashboard.

Application Visibility is supported for Instant APs running 6.4.3.1-4.2.0.0 or later release version.

Aruba Central supports Application Visibility monitoring, DPI configuration, and web filtering for IAP-103, RAP-108/109, IAP-114/115, RAP-155, IAP-224/225, IAP-274/275, IAP-228, IAP-277, IAP-205, IAP-214, and IAP-324/325, IAP-304/305. IAP-207, IAP-334, and IAP-314/315.

The Instant AP-104/105, Instant AP-134/135, RAP3WNP, and Instant AP-175 devices support only web policy enforcement.

To view application usage metrics for Instant AP clients, you must enable the Application Visibility feature on Instant APs.

To enable the Application Visibility feature, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Services**. The **Services** page opens.
4. Click **Application Visibility.**
5. 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.

Application Visibility Dashboard

The **Application Visibility** dashboard displays metrics and graphs related to client traffic flow in the following sections:

- **Applications**
- **Websites**
- **Blocked Traffic**

To view the client traffic details, ensure that the DPI access rules are enabled on the Instant AP device.

The **Blocked Traffic** section is only displayed in the **Monitoring & Reports > Application Visibility** page.

Applications

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.

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.

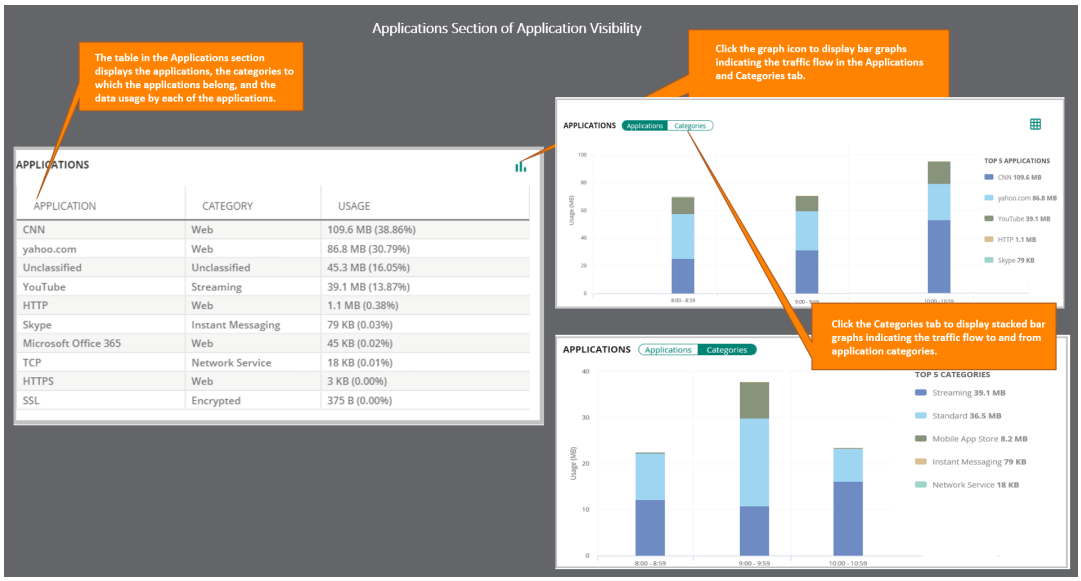
These graphs are displayed for a specific time frame (3 Hours, 1 Day, 1 Week, 1 Month, 3 Months). By default, the graphs display real-time client traffic data or usage trend in the last three hours.

Application Visibility data is updated every 0th minute of every hour. The data population on the **Application Visibility** dashboard may be delayed by an hour when compared to the Application Visibility data displayed in the **Monitoring & Reports > Network Overview > APs** and **Monitoring & Reports > Client Overview** pages.

Quick Reference Illustration of Applications Section

See the following figure for an illustration of Applications section:

Figure 90 *Applications Section UI*



Websites

The **Websites** section 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:

- **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.
- **Reputation**—The reputation of the application categories, for example, **Trustworthy**, **Unknown**, **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.

Graph View in Websites Section

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.

The application (Apps) and Web Categories charts are also displayed in the **Monitoring & Reports > Network Overview > APs** and **Monitoring & Reports > Client Overview** pages.

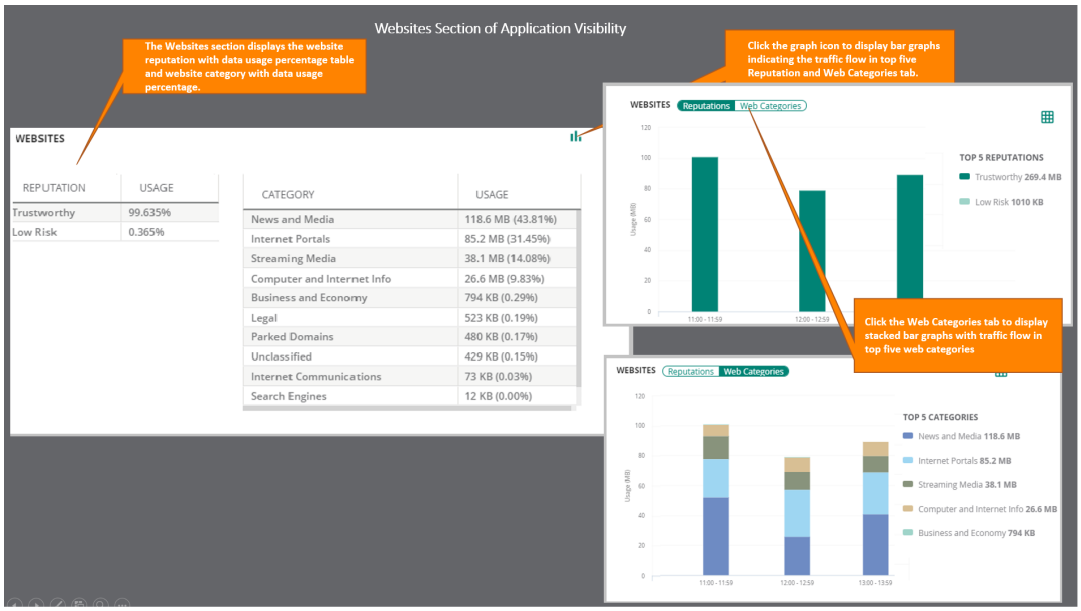
NOTE

Application Visibility data is updated every 0th minute of every hour. The data population on the **Application Visibility** dashboard may be delayed by an hour when compared to the Application Visibility data displayed in the **Monitoring & Reports > Network Overview > APs** and **Monitoring & Reports > Client Overview** pages.

Quick Reference Illustration of Websites Section

See the following figure for an illustration of Websites section:

Figure 91 *Websites Section UI*



Blocked Traffic

Based on the group selection from the **Blocked Traffic** drop-down list, the **Blocked Traffic** section of the **Application Visibility** 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**.

NOTE

The blocked traffic details are shown only for the APs on which the Application Visibility or DPI ACLs are enabled. For more information, see Configuring ACLs for Application Usage Analysis and Configuring ACLs on Instant APs for Website Content Classification .

Downloading Blocked Session Details

To download the blocked session details in the CSV format, complete the following steps:

1. Go to **Blocked Traffic** of **Monitoring & Reports** > **Application Visibility** tab. If the group filter is set to **All Devices**, select the device group from the **Device 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.
2. To download the blocked sessions report, click **Download CSV**. Aruba Central generates the CSV report with data from the last 7 days.

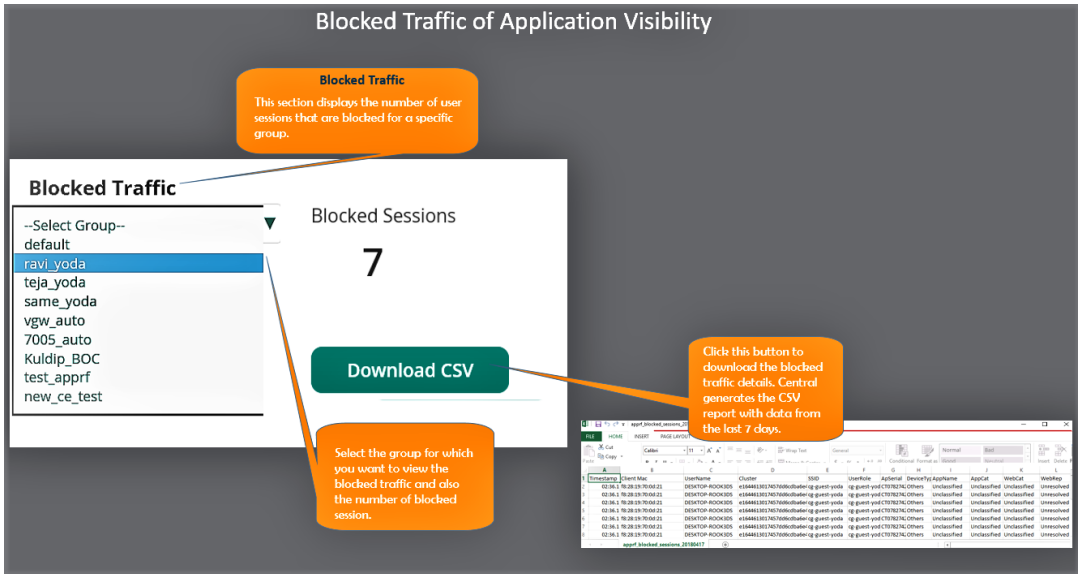
NOTE

The CSV file shows up to 50000 blocked sessions for a single Instant AP cluster.

Quick Reference Illustration of Blocked Traffic Section

See the following figure for an illustration of Blocked Traffic section:

Figure 92 *Blocked Traffic Section UI*



VisualRF

VisualRF allows you to plan sites, create and manage floor plans, and provision APs. You can use VisualRF Plan to do basic planning procedures, such as, creating a floor plan and provisioning APs.

VisualRF provides 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. The VisualRF puts this information at your fingertips through integrated mapping and location data.

VisualRF uses sophisticated RF fingerprinting to accurately display coverage patterns and calculate the location of every wireless device in range. VisualRF does not require dedicated RF sensors or a costly additional location appliance, because

it gathers all the necessary information from your existing devices.

NOTE

VisualRF is supported only on Instant APs running 6.5.2.0 or later.

NOTE

In VisualRF, do not use the internet browser for back and front navigation. Instead, use the breadcrumbs.

VisualRF offers the following features:

- Floor plan import and creation
- Pictorial navigation that allows you to view the floor plans associated with Instant APs, clients, buildings, and floors.

- Accurate calculation of the location of all client devices (laptops and Phones) using RF data from your devices.
- A tree view that allows you to navigate to a specific campus.
- A map view that shows the location of devices and heatmaps that depict the strength of RF coverage in each location.
- Unique URLs when you drill down to a site, campus, or building map, in the following formats: /vrf, /vrf/site/<id>, /vrf/campus/<id>, and /vrf/building/<id>

VisualRF Dashboard

To view the VisualRF dashboard:

1. From the app selector, click **Monitoring & Reports**.
2. Click **VisualRF**. The VisualRF dashboard opens.

The VisualRF dashboard allows you set your view to one of the following options:

- Network—The network icon allows you to navigate to a specific site.
- Map—The map view shows the location of the sites. Clicking on a specific site leads you to a campus, buildings, floor plans, and devices.
  - You can also search for a specific site in the search box.
  - To move or drag a site to different location on the map, click the lock icon.
- List—The list view provides a complete list of sites, links to the corresponding buildings and floor plans, size of the floor, grid size, the number of APs on the floor, and the number of clients connected to APs on the floor.

Viewing Network Information

The **Network** link displays a page for viewing campuses, buildings, and floors within a network. You can click the **Map** link to view the site map. Click the **List** link to view the list of sites.

To view more information, perform the following actions:

- To view the details of a network within a campus, select a campus, and click on a building within the selected campus.
- To view the floor plan, select a floor. The floor plan displays the Instant APs and clients on that floor.
- To view information about the devices, select an AP or client.

Customizing the Floor Plan View

To customize your floor plan view, click the **View** tab on the right sliding panel. The **View** tab displays the list of campuses and the devices.

- To increase the icon size of campus, click the arrow next to **Campuses**.
- Click **APs** to view the details of the Instant AP and the RF environment.
- Click **Clients** to view the client details.

Viewing Campus, Sites, Buildings, and Floors

The VisualRF navigation menu on the right pane consists of the **Properties**, **View**, and **Edit** tabs. The following table describes the menu options available for network locations such as campus, building, and floor.

Table 48: *VisualRF—Network Menu Options*

Networks Property Tab	View Tab	Edit Tab
Displays the total number of APs, buildings, clients, and floors	Displays the following menu options: ■ **Campuses** ● Displays the complete list of campus sites within your network. Click the links to view details of the campus sites. ● Enables or disables the campus icons on the map. ● Allows you to decrease or increase campus icon size on the map ■ **Labels**—Shows or hides the labels assigned to campus sites.	Displays the following menu options: ■ **Select All**—Selects all campus sites. You can perform the following actions when the campus sites are selected: ● **Remove**—Removes the selected sites. ● **Bill of Materials**—Enables showing or hiding heatmap, speed, sensor coverage, wired range and other details. ● **Auto match planned devices**—Automatically matches the devices that are planned for deployment and reloads the page. ■ **Undo**—Cancels the previous action. ■ **New Floorplan**—Allows you to create a new floor plan ■ **Set Background**—Allows you set a background image. You can upload a custom image or set a specific location from the world map as a background. ■ **New Campus**—Allows you create a new campus. ■ **Auto-arrange Campuses**—Arranges campus icons on the map.

Table 49: *VisualRF—Campus Menu Options*

Campus Property Tab	View Tab	Edit Tab
Displays the name of campus and the total number of APs in the campus site.	Displays the following menu options: ■ **Buildings** ● Displays the complete list of buildings within the campus. Click the links to view the details of the buildings in the campus site. ● Enables or disables the building icons on the map. ● Allows you to decrease or increase the building icon size on the map ■ **Labels**—Shows or hides the labels assigned to buildings.	Displays the following menu options: ■ **Select All**—Selects all buildings. You can perform the following actions when buildings are selected: ● **Remove**—Removes the selected buildings. ● **Navigate**—Navigates to the building. ● **Bill of Materials**—Enables showing or hiding heatmap, speed, sensor coverage, wired range and other details. ● **Auto match planned devices**—Automatically matches the devices that are planned for deployment and reloads the page. ■ **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. ■ **Set Background**—Allows you set a background image. You can upload a custom image or set a specific location from the world map as a background. ■ **New Building**—Allows you to create a new building. ■ **Auto-arrange Buildings**—Arranges building cons on the map.

Table 50: *VisualRF—Building Menu Options*

Building Property Tab	View Tab	Edit Tab
Displays the name and location details of the building, and the total number of floors and APs in the building.	Displays the complete list of floors in the building. Click the links to view the floor plan of the floors in the building.	Displays the following menu options: ■ **Select All**—Selects all floors. You can perform the following actions when floors are selected: ● **Remove**—Removes the selected buildings. ● **Navigate**—Navigates to the building. ● **Bill of Materials**—Enables showing or hiding heatmap, speed, sensor coverage, wired range and other details. ● **Auto match planned devices**—Automatically matches the devices that are planned for deployment and reloads the page. ● **Duplicate**—Creates a duplicate of the selected floor. ■ **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.

Table 51: *VisualRF—Floor Menu Options*

Property Tab	View Tab	Edit Tab
Displays the floor details, total number of APs on the floor, and clients. The **Advanced** option allows you to set the values to indicate if the environment is related to an office space, cubicles, offices, or concrete.	Displays the following menu options: ■ **Devices**—Displays APs, Clients, and rogues devices detected on the floor. ■ **AP Overlay**—Shows the heatmap for the current and adjacent floors. ■ **Floor Plan Features**—Displays the following details: ● **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. VisualRF uses 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.	Displays the following menu options: ■ **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: ● **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. ● **Refresh**—Refreshes the page.

Viewing AP Overlay Information

The AP Heatmap overlay displays information for adjacent floors to determine how the bleed through from adjacent floors affects the viewed floor. Besides the current floor, you can view all floors, or data from APs located on the floor above or below.

The **AP Overlay** > **Heatmap** option that allows you to view details of signal cutoff, and for each radio band and floors. The **Heatmap** option also allows you to change the overlay display to grid.

Viewing Rogue Devices

To view the rogue devices on a floor plan, navigate to the floor plan and click the **Devices** > **Rogues** in the **Properties** tab. Clicking on **Rogues** shows or hides the rogue icons on the floor plan. The rogue device presence is marked with orange circle. The floor plan also shows if the rogue devices is associated with any Instant AP.

Planning and Provisioning Devices

VisualRF provides the capability to plan campuses, buildings, floors, and location for device provisioning before the actual deployment. Using VisualRF, you can create a floor plan and add devices to this floor plan.

The planning and provisioning workflow includes the following procedures:

- Creating a Campus
- Creating a Building
- Creating a Floor Plan
- Modifying Floor Plan Properties
- Adding Devices to the Floor Plan
- Printing a Bill of Materials Report

Creating a Campus

To create a new campus, perform the following actions:

1. From the app selector, click **Monitoring & Reports** > **VisualRF**. The VisualRF dashboard opens.
2. Click **Floor Plans** > **Network** view.
3. Click the **Network** slide out pane on the right and then click the **Edit** link.
4. Click **New Campus**.
5. Enter the name of the campus and click **Save**. The new campus icon appears on the campus background.
6. To set a background image for the campus, complete the following steps:

   a. Click **Set Background**.

   - To set a custom background, select the **Custom Image** option and upload the image file.
   - To set the background to a specific geographical map, click the **World Map** option and select the country map from the drop-down list.

   b. Click **Save**.

   c. Drag the new campus icon to the appropriate location on the map background, or right-click the background or

   Or

   Click **Auto Arrange Campuses** to arrange the campus in alphabetical order across the background.

Creating a Building

To create a building, complete the following steps:

1. From the app selector, click **Monitoring & Reports** > **VisualRF**. The VisualRF dashboard opens.
2. Click **Floor Plans** > **Network** view.
3. Select the campus under which you want to create a building. The **Campus** slide out pane opens.
4. Click the **Edit** tab.
5. Click **New Building**. Enter the following information:

Table 52: *New Building Configuration Parameters*

Field	Description
Name	Name of the building located in an existing campus.
Address	Building or Campus address.
Latitude	Latitude as seen from Google Earth.
Longitude	Longitude as seen from Google Earth.
Ceiling Height	The normal distance between floors in the building (in feet). This value can be overridden as each floor is created, but this is the default value for every new floor added to the system.
Attenuation	Enter the attenuation loss (in dBm) between floors. This value can be overridden as each floor is created, but this is the default value for every new floor added to the system.

6. Click **Save**. You can add multiple buildings if required.
7. To automatically arrange buildings, click **Auto-arrange Buildings**.

Creating a Floor Plan

VisualRF allows 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. From the app selector, click **Monitoring & Reports** > **VisualRF**. The VisualRF dashboard opens.
2. Click **Floor Plans** > **Network** view.
3. Click the **Edit** tab in the **Network** slide out panel.
4. Click **New Floorplan**. The **New Floorplan** pop-up window opens.
5. Click **Browse** and locate a floor plan image file from your local file system. You can import the floor plan image file in the bmp, jpg, jpeg, gif, and png format.
6. Select the campus and building from the **Campus** and **Building** drop-down lists, respectively.
7. Assign a floor name and a floor number in the **Floor name** and **Floor number** text boxes, respectively.
8. Click **Save**.

Importing a Floor Plan

To import a floor plan exported from VisualRF Plan, AirWave, or Aruba Central, complete the following steps:

1. From the app selector, click **Monitoring & Reports** > **VisualRF**. The VisualRF dashboard opens.
2. Click the **Import** menu option.
3. Click **Browse** and select the floor plan zip file to import.

4. 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. From the app selector, click **Monitoring & Reports** > **VisualRF**. The VisualRF dashboard opens.
2. Click **Floor Plans** > **Network** view.
3. Click **List**. The list of sites is displayed.
4. Click the floor number or floor name link. The **<Floor Name>** slide out pane is displayed.
5. Click **Properties** and modify the following properties.

Table 53: *Floor Plan Properties*

Setting	Default	Description
Floor Name	Floor [Number]	A descriptive name for the floor. It inherits the floor number as a name if nothing is entered.
Floor Number	0.0	The floor number. You can enter negative numbers for basements. **NOTE:** Each floor plan within a building must have a unique floor number.
WidthHeight	N/A	These fields display the current width and height of the floor plan. To change these settings, click the **Measure** icon and measure a portion of the floor.
Gridsize	5 x 5 feet	Size of the grid. Decreasing the grid size will enable the location to place clients in a small grid which will increase accuracy.
Advanced		
Environment	N/A	Environment indicator. The values on the slider range from 1–4 to indicate if the environment is related to an office space, cubicles, offices, or concrete.

6. Click **Save**.

Adding Devices to the Floor Plan

You can add the planned devices (for example, APs) or the already deployed devices to floor plan.

To add the already deployed devices to the floor plan, complete the following steps:

1. From the app selector, click **Monitoring & Reports** > **VisualRF**. The VisualRF dashboard opens.
2. Click **Floor Plans** > **Network** view.
3. Click **List**. The list of sites is displayed.
4. Click the floor number or name link. The **<Floor Name>** slide out pane is displayed.
5. Click **Edit**.
6. Click the **Add Deployed Devices** icon. A list of devices is displayed.
7. 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 VisualRF are hidden. To show them, clear the **Hide Devices that are already added** check box at the bottom of the list.
8. Click and drag an AP (or a Group or Folder of APs) to its proper location on the floor.
9. Click **Save**.
10. To remove a device from the floor plan, right-click that device and then click **Remove.**

To provision new devices when creating a new floor plan, complete the following steps:

1. From the app selector, click **Monitoring & Reports** > **VisualRF**. The VisualRF dashboard opens.
2. Click **Floor Plans** > **Network** view.
3. Click **List**. The list of sites is displayed.
4. Click the floor number or name link. The **<Floor Name>** slide out pane is displayed.
5. Click **Edit**.
6. Click **Planned Devices** and select a device type (model) from the list of available devices.
7. In the **Count** field, enter the number of devices of that type to add to the new floor.
8. (Optional) Click and drag the **Deployment Type** slider bar to adjust data rates for a high-density or low-density environment.
9. (Optional) Click the **Advanced** link and configure the advanced deployment options
   - **Service level**: Select **Speed** or **Signal** to plan coverage by adjusting data rate requirements (Speed) or AP signal strength settings. Click **Calculate AP** count to recalculate the suggested number of APs based on these advanced settings.
   - **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 advanced settings.
10. Click **Add APs to Floorplan**.
11. Click and drag the device, to the desired location.
12. Click **Finish**.
13. To remove a planned device from the floor plan, right-click that device and then click **Remove**.

Printing a Bill of Materials Report

To generate a Bill of Materials (BOM) Report from within VisualRF, complete the following steps:

1. From the app selector, click **Monitoring & Reports** > **VisualRF**. The VisualRF dashboard opens.
2. Click **Floor Plans** > **Network**.
3. Right-click a campus icon, a building icon, or a building floor and select **Show Bill of Materials**. A report pop-up window opens.
4. Select options such as heat map, speed, sensor coverage, wired range, and summary.
5. Select **OK**.

VisualRF APIs

Aruba Central supports the following APIs for retrieving client location and floor plan information:

- **GET /visualrf_api/v1/campus**—Retrieves a list of all campus sites.
- **GET /visualrf_api/v1/campus/{campus_id}**—Retrieves information about a specific campus and its buildings.
- **GET /visualrf_api/v1/building/{building_id}**—Retrieves information about specific building and its floors.
- **GET /visualrf_api/v1/floor/{floor_id}**—Retrieves details about a specific floor.
- **GET /visualrf_api/v1/floor/{floor_id}/image**—Retrieves background image from a specific floor plan.
- **GET /visualrf_api/v1/floor/{floor_id}/access_point_location**—Retrieves information about the location of the APs on a specific floor plan.
- **GET /visualrf_api/v1/access_point_location/{macaddr}**—Retrieves location details of a specific AP.
- **GET /visualrf_api/v1/client_location/{macaddr}**—Retrieves location details of a specific client.

- **GET /visualrf_api/v1/floor/{floor_id}/client_location**—Retrieves information about the location of clients on a specific floor.

For more information on APIs, see Aruba Central APIs and refer to API documentation at https://app1-apigw.central.arubanetworks.com/swagger/central.

Topology

The **Topology** map in Aruba Central provides a graphical representation of the network layout, details of the devices deployed in a branch site, and the health of the WAN uplinks and tunnels. The minimum required ArubaOS version for Topology is ArubaOS version 8.1.0.0-1.0.1.1.

On Switches, LLDP is enabled by default. On Branch Gateways, if the port type is LAN, LLDP is enabled by default and you can view the topology map.

For more information, see the following sections in the *Aruba Central Help Center*:

- *Configuring Ports for LAN Interfaces*
- *Configuring Other Parameters for Port*

Before You Begin

The topology map filters devices based on sites. To view the topology map, ensure that you have assigned the devices to sites. For more information, see the *Assigning Devices to Sites* in the *Aruba Central Help Center*.

Viewing Topology Map

To access the topology map:

1. From the app selector, click **Monitoring & Reports**.
2. Click **Topology**.
3. From the filter bar, select a site.

Navigating the Topology Map

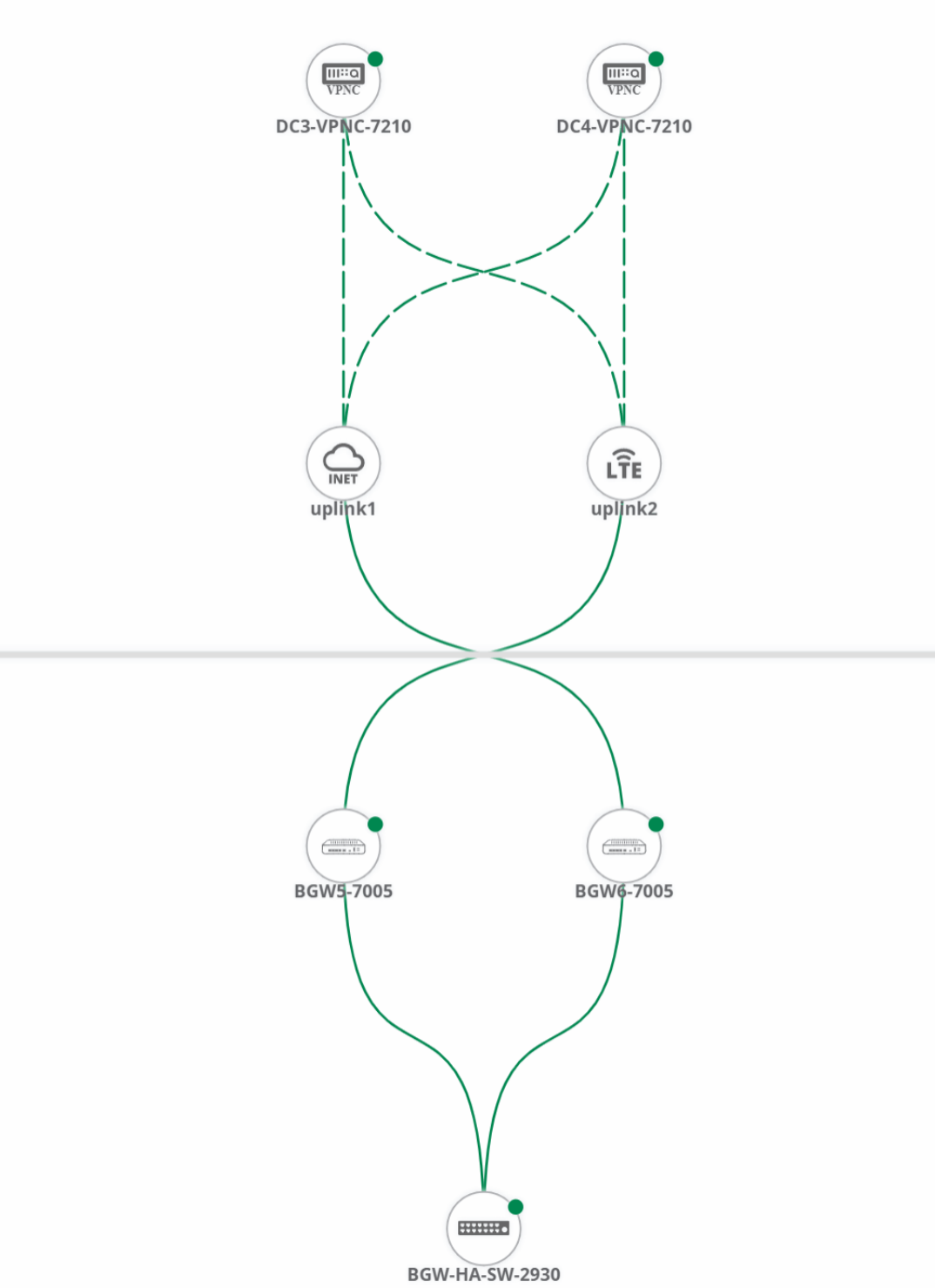
The topology map provides a pictorial view of the devices deployed in the branch site, uplink health, and tunnel status. A task pane on the right provides a summary of the devices, uplinks, and tunnel details. The red and green indicators show the current status and health of the WAN uplinks and tunnels.

- To view the name, type, and hardware model of the device, hover your mouse on the device.
- To view details of the uplink interfaces, click the lines on the map.
- To know the tunnel mapping, hover over the tunnel or the uplink, and the uplink path is highlighted.
- To change the zoom level, click the zoom icons.

An example of a Topology map:

An example Topology where the Branch Gateways are connected to both the VPN Concentrators through both the uplinks.

Figure 93 *Site Topology*



NOTE

Active tunnels are green in color and inactive tunnels are red in color. If there are multiple tunnels connecting to one VPNC, and even if one of those tunnels is down, the tunnel mapping is displayed in red dotted lines.

Task Pane

The task pane consists of the following tabs:

- **Details**—Provides a detailed summary of the devices, uplink interfaces, and tunnels. It also highlights the status of the device and uplinks.
- **Filter**—Allows you to apply a filter criteria for displaying devices on the map. The following options are available:
  - Branch Gateway—filters out Branch Gateways (feature is currently not available).
  - Switch—filters out switches.
  - IAP—filters out Instant Access Points.
  - VPNC—filters out VPNCs and Virtual gateways.
  - Security Cloud—filters out Zscaler and Palo Alto Networks GlobalProtect™ Cloud Service.

  For example, if you set the filter to VPNC, only the VPNC details are displayed. Similarly, you can set the filter to show or hide the devices that are linked on uplink ports.

The **Details** tab displays the following information:

Table 54: *Contents of the Details Tab*

Type	Description
Device details	
Branch Gateway	Displays the following details: ■ **Name**—Hostname of the Branch Gateway. ■ **Serial**—Serial number of the Branch Gateway. ■ **IP**—IP address of the Branch Gateway. ■ **MAC**—MAC address of the device. ■ **Type**—Type of device deployment. For Branch Gateways, the type shows up as Gateway. ■ **Model**—Hardware model of the device. ■ **Status**—Operational status of the device. ■ **Health**—Operational health of the device.
Switch	Displays the following details: ■ **Name**—Hostname of the switch. ■ **Serial**—Serial number of the switch. ■ **IP**—IP address of the switch. ■ **MAC**—MAC address of the switch. ■ **Type**—Type of the device. ■ **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. ■ **IP**—IP address of the switch. ■ **MAC**—MAC address of the switch. ■ **Type**—Type of the device. ■ **Stack Role**—Role of the switch in the stack. ■ **Model**—Hardware model of the switch. ■ **Status**—Operational status of the switch stack. ■ **Health**—Operational health of the switch stack. ■ **Stack Members**—Lists the members of the stack, the role (member or commander), and state.
Instant AP	Displays the following details: ■ **Name**—Hostname of the Instant AP. ■ **Serial**—Serial number of the Instant AP. ■ **IP**—IP address of the Instant AP. ■ **MAC**—MAC address of the Instant AP.

Type	Description
	■ **Type**—Type of the device. ■ **Model**—Hardware model of the Instant AP. ■ **Status**—Up and down arrows indicating the operational status of the Instant AP. ■ **Health**—Operational health of the Instant AP.
Tunnel, Uplink, and Edge details	
Tunnel	Displays the following information about tunnels configured on the Branch Gateway: ■ **Map Name**—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.
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**—Public IP address. ■ **Device MAC**—MAC address of the device. ■ **Serial**—Serial number of the device. ■ **Port Number**—Port number of the device. ■ **Tunnels**—List of tunnels mapped to the uplink. A green bullet icon indicates that the tunnel is up and a red bullet icon indicates that the tunnel is down.
Edge	Displays the following information about the link: ■ **Interface numbers**—The devices' interface numbers. ■ **Interface**—Interface number of the individual device. ● **Serial**—Serial number of the individual device. ● **Device Name**—The name of the individual device. ● **Port Number**—The Port number of the individual device. **NOTE:** In case of 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.

Alerts

The **Alerts** pane displays all types of alerts generated for events pertaining to device provisioning, configuration, and user management.

Viewing the Alerts Summary and Acknowledging Alerts

To view a summary of alerts and acknowledge alerts, complete the following steps:

1. From the app selector, click **Monitoring & Reports**.
2. Click **Alerts**. The **Alerts** page shows a summary of alerts and the **Configure Alerts** and **Acknowledge All** buttons.

Table 55: *Alerts pane*

Data Pane Content	Description
Open	■ Displays the number of alerts in the following categories: ● Critical ● Major ● Minor ● Warning ■ **Search box**—Allows you to search for alerts using keywords. ■ **Acknowledge**—The **Acknowledge** button appears when you hover your mouse over any alert. Click **Acknowledge** to acknowledge that specific alert. ■ **Acknowledge All**—Allows you to acknowledge all alerts at once.
Acknowledged	Displays a list of acknowledged alerts. Use the search box to search for an alert.

Configuring Alerts

To configure alerts, complete the following steps:

1. From the app selector, go to **Monitoring & Reports > Alerts**.
2. On the **Alerts** page, click **Configure Alerts**. By default, the **Alerts** > **User** category is displayed.
3. Use the tabs to navigate between the alert categories. See Alert Types on page 221 for a complete list of alerts that you can configure. 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. 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. To set the threshold value, select the alert and in the **exceeds** text box, enter the value. The alert is triggered when one of the threshold values exceed the duration.

   b. **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.

   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.
   - **Webhook**—Select the **Webhook** check box and select the Webhook from the drop-down list. For more information, see Webhooks on page 393.

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.

Viewing Enabled Alerts

To view alerts that you have enabled:

1. From the app selector, go to **Monitoring & Reports > Alerts**.
2. On the **Alerts** page, click **Configure Alerts**.
3. In the **Configure Alerts** page, click **Enabled**. Use the tabs to navigate between the alert categories. The alerts enabled for each category are displayed in the respective tabs.

Alert Types

Aruba Central allows you to configure and enable the alerts described in this section:

IAP Alerts

Aruba Central allows you to configure and enable the following IAP alerts:

- **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 Instant AP is detected.
- **AP Disconnected**—Generates an alert when an Instant 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 Instant 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.
- **AP CPU Utilization**—Generates an alert when the Instant 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 Instant 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.
- **Radio Channel Utilization**—Generates an alert when the Instant 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**—Generates an alert when the number of connected clients exceed 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.

- **Modem Plugged**—Generates an alert when the modem is plugged.

User Alerts

Aruba Central allows you to configure and enable the following user management alerts:

- **New User Account Added**—Generates an alert when a new user account is added. This alert is enabled by default and the alert severity is **Major**.
- **User Account Deleted**—Generates an alert when a user account is deleted.
- **User Account Edited**—Generates an alert when a user account is edited.

Switch Alerts

Aruba Central allows you to configure and enable the following switch alerts:

- **New Switch Detected**—Generates an alert when a new switch is detected. This alert is enabled by default and the alert severity is **Major**.
- **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
- **New Switch Detected**—Generates an alert when a new switch is detected. This alert is enabled by default and the alert severity is **Major**.
- **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 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.

Gateway Alerts

See the *Gateway Alerts* section in the *Aruba Central Help Center*.

Clarity Alerts

Aruba Central allows you to configure and enable the following Clarity alerts:

- **DNS Delay Detected**—Generates an alert when DNS delay is detected. 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 DNS failure is detected. 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 DHCP delay is detected. 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 DHCP failure is detected. 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 authentication delay is detected. 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 authentication failure is detected. 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. 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. 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.

Reports

The **Reports** pane allows you to create various reports. You can configure the reports to be run on demand or periodically. You must have read/write privileges or you must be an Admin user to be able to create reports. The **Reports** page has the following sections:

- **Configure Reports**—Displays the reports configured using the **Create Report** option.
- **Generated Reports**—Displays the reports generated.

This section includes the following topics:

Types of reports

The following table lists the different types of reports that you can generate in Aruba Central.

Table 56: *Types of reports*

Report Type	Parameters Displayed
All	Displays all scheduled and generated reports.
Network	Displays the following parameters: ■ Number of Instant APs ■ Instant AP Model ■ Top Ten Wireless Clients By Usage ■ Top Ten Instant APs By Usage ■ Total Usage By SSID ■ Device Types ■ Wireless Clients ■ Wireless Data Usage ■ Wireless Data Peak Usage ■ Top Ten Applications By Usage ■ Top Ten Web Categories By Usage ■ Switches ■ Switch Model ■ Top Ten Switches By Usage (Tx/Rx) ■ Top Ten Ports By Usage (Tx/Rx) ■ Wired Uplink Stats ■ Wired Peak Uplink Stats
Security	Displays the following parameters: ■ Rogue APs ■ Total Rogue APs Detected ■ Wireless Intrusions ■ Total Wireless Intrusions
PCI Compliance	Displays the PCI Compliance result as **Fail** or **Pass**.
Client Inventory	Displays the client details summarized by all aggregation fields. The report includes the following details: ■ Number of APs, APs and the AP model ■ Number of Clients, Top 10 Clients by Usage, and the type of client device ■ Top Ten APs by Usage ■ Total Usage by SSID ■ Wireless Clients ■ Wireless Data Usage graphs such as Top Ten APs by Usage, Total Usage by SSID, Wireless Clients, Wireless Data Usage, Wireless Data Peak Usage, Top 10 applications by usage, Top 10 web categories by usage ■ Switch information such as the Switches in the network, Switch model, Top 10 Switches by Usage, Top 10 Ports by Usage, wired uplink stats, and wired peak uplink stats graphs.
Infra Inventory	Displays the inventory and subscription information for the devices that are online during a specific duration. The report includes the following details: ■ Number of Instant APs ■ Number of Switches ■ AP interfaces summary ■ Model and Firmware version for APs ■ Model and Firmware version for Switches ■ Instant AP and Switches subscription information ■ Subscription utilization graph
Client Usage	Displays information about the client usage, client count, and client traffic to applications, application categories, web categories, and applications with web reputation score assigned.

Report Type	Parameters Displayed
New Infra Inventory	Displays the inventory and subscription information to the devices that are newly added in Aruba Central.
Capacity Planning	Displays the throughput and client density information for devices provisioned in Aruba Central. The report includes the following details: ■ Top 25 APs by throughput ■ Top-25 APs by peak client density ■ Top-25 APs by average client density ■ Top-25 Switches by throughput ■ Subscription usage
AppRF	Displays application usage report for a specific device group. The report displays the following widgets: ■ Top 10 applications accessed by the clients ■ Top 10 web categories accessed by the clients ■ Top 10 applications accessed by each type of the client device. ■ Top 10 applications for the user roles assigned to the client devices. ■ Top 10 applications for the SSIDs on which the client devices are connected.
Client Session	Displays the details of client sessions for the SSIDs provisioned on Instant APs. The report also displays the client count, the number of sessions, cumulative duration, and the usage based on the following parameters : ■ Client Device OS ■ Connection mode ■ SSIDs ■ User roles ■ MAC address vendors of the device
RF Health	Displays the following RF usage statistics for the AP radios. ■ Channel changes ■ Transmission power changes ■ Average Noise (in dBm) ■ Average channel utilization (%) ■ Total error (%) ■ Interfering devices ■ Clients ■ Usage **NOTE:** For APs that support 5 GHz dual band in synchronization with Aruba Instant 8.3.0.0, the **Device** column in the **RF Health Report** shows the radio number of the operating radio along with the model number of the device.
Configuration Audit Status	Displays the last configuration action audited for devices assigned to groups in Aruba Central. This report shows the following information categories: ■ Aggregate Statistics—Shows configuration status for all the devices. ■ Detailed Statistics—Shows detailed configuration status for each device.
Unified Communications	Displays a variety of charts that allow you to assess the quality of voice and video traffic on the network. The page displays the following details: ■ UC Health ■ Poor Sessions ■ Total Sessions ■ UC Clients ■ Audio ■ Video ■ Desktop Sharing ■ Session Count by Type ■ Session Quality by Session Type ■ Operating Systems

Report Type	Parameters Displayed
	■ Session Quality by Client Health ■ Session Quality by SSID ■ Session Count by Protocol For more information, see Activity on page 429.
WAN Inventory	See the *Gateway Reports* section in the *Aruba Central Help Center*.
WAN Policy Compliance	
WAN Transport Health	
WAN Availability	
WAN Utilization	

Creating a report

You can generate reports for devices associated with a group, site, or label. You can also set a periodicity for running the reports.

NOTE

Although your page view is set to a specific group, site, or label, you can create reports for a different group, site, or label. However, if your page view is set to an Instant AP cluster or Switch, you can schedule report generation only for that Instant AP cluster or Switch.

To create a report, complete the following steps:

1. From the App selector, click **Monitoring & Reports** and select **Reports**. The **Reports** page is displayed.
2. Click **Create Report**. The
   - To generate reports for the devices attached to a group, select **Groups** and then select a device group.
   - To generate reports for devices attached to a label, click **Labels** and then select a label.
   - To generate reports for devices deployed on a specific site, click **Sites** and select a site.
3. Enter the name for the report in **Title**.
4. From the **Report Type** drop-down, select the type of the report to generate.
5. From the **Period** drop-down, select the period for which you want to view the report.
6. Select **Now** from **Schedule** to generate the report immediately. To run reports at a later time, select **Later** and specify the date and time.
7. From the **Run Report** drop-down, select how often you want to generate the report by choosing **One Time**, **Daily Interval**, **Weekly Interval**, or **Monthly Interval**.
8. If you are creating a PCI Compliance report, specify the Cardholder Data Environment (CDE) subnets or CDE SSIDs for which you want to generate the report. You can also run report on all SSIDs.

NOTE

Aruba Central does not support creating or filtering AppRF and PCI Compliance reports based on labels or sites.

9. To email the generated report, specify the email address of the recipient in **Email Report**.
10. Click **Create**.

Generated Reports

In the **Generated Reports** section of the **Reports** page, a table listing the parameters used for generating a report is displayed.

Table 57: *Reports Pane*

Parameter	Description
Title	Displays the title name of the report generated.
Date Run	Displays the date on which report was generated.
Saved By	Indicates the user login name using which the report was generated.
Device Group	Indicates the device group or groups for which the report was generated.
Labels	Indicates the labels for which the report was generated.
Report Type	Indicates the type of report.
Status	Displays the current status of the report generated.
Periodicity	Indicates when the report is triggered.

Viewing generated reports

To view a generated report, complete the following steps:

1. From the App selector, click **Monitoring & Reports** and select **Reports**.
2. From the **Report Type** drop-down in the **Generated Reports** section of the **Reports** page, select the report type. The following types of reports are available:
   - Network
   - PCI Compliance
   - Security
   - Client Inventory
   - Infra Inventory
   - Client Usage
   - New Infra Inventory
   - Capacity Planning
   - AppRF
   - Client Session
   - RF Health
   - Configuration Audit Status
   - Unified Communications
   - WAN Inventory
   - WAN Policy Compliance
   - WAN Transport Health
   - WAN Availability

- WAN Utilization

3. To send the report through email, click the email icon, enter the email address, and then click **Send email**.

Editing a report

To edit view a configured report, complete the following steps:

1. In the **Reports** page, go to the **Configure Reports** table.
2. Select the report that you want to edit and click the edit icon.
3. Edit the field(s) as necessary and click **Update**.

Deleting report(s)

In the **Reports** page, go to the **Configure Reports** table.

- To delete a configured report, complete the following steps:
  - Select the report that you want to delete and click the delete icon.
  - In the **Confirm Action** pop-up, click **Yes**.
- To delete multiple configured reports, complete the following steps:
  - Press and hold the **Ctrl** key and select the reports that you want to delete and click **Batch Remove Reports**.
  - In the **Confirm Action** pop-up, click **Yes**.

In the **Reports** page, go to the **Generated Reports** table.

- To delete a generated report, complete the following steps:
  - Select the report that you want to delete and click the delete icon.
  - In the **Confirm Action** pop-up, click **Yes**.
- To delete multiple generated reports, complete the following steps:
  - Press and hold the **Ctrl** key and select the reports that you want to delete and click **Batch Remove Reports**.
  - In the **Confirm Action** pop-up, click **Yes**.

Exporting a report

To export a generated report, complete the following steps:

1. In the **Reports** page, go to the **Generated Reports** table.
2. Select the report that you want to export and click the export icon.

This section describes how to configure WLAN SSIDs, radio profiles, DHCP profiles, VPN routes, security and firewall settings, uplink interfaces, logging servers on Instant APs.

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

Setting Country Code

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

Country Code Configuration in Aruba Central from UI

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

Table 58: *Instant AP Provisioned To Aruba Central*

Country Code Configured at Instant AP	Country Code Configured in Group	Behavior
No	Yes	The country code of the group is pushed to the newly added Instant AP.
No	No	Aruba Central displays the **Country Code not set. Config not updated** message in the Audit Trail. A notification is also displayed at the bottom of the main window to set the country code of the new Instant AP. To set the country code, perform the following actions: 1. Click **Set Country Code Now** link on the notifications pane. The **Set Country Code** pop up opens. 2. Select the device and click the edit icon. 3. Specify a country code from the **Country Code** drop-down list. 4. Click **Save**.

If an Instant AP already has a country code, and then joins the Central using ZTP configuration, the country code of the Instant AP is retained. In this case, Central would not push the group's country code.

Setting Country Code At Group Level

To set the country code of the Instant AP at the group level, perform the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select the group to be modified.
3. Click **System** > **General**. The page to set the configurations for the group is displayed.
4. Select the country code for Instant AP from the **Set Country code for group** drop-down list.
5. Click **Save Settings.**
6. Reboot Instant 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 Instant AP with different country codes can be a part of the group.

Once 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 Instant AP also will be updated accordingly.

Setting Country Code At Device Level

To set the country code of the Instant AP at the device level, perform the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select the Instant AP device for which the country code must be modified.
3. Click **System** > **General**. The page to set the configuration for the device is displayed.
4. Click the edit icon.
5. Select the new country code from the **Country Code** drop-down list.
6. Click **Ok**.
7. Reboot Instant AP for changes to take effect.

NOTE

By default, the value corresponding to the **Country code** is the country code set at the group level which can be then modified at the device level from the drop-down list. The country code of the Instant AP will always be the most recently set country code at the group level or device level.

Country Code Configuration at Group Level from API

Aruba Central provides an option to set and get the country code at group level through the APIs in **Maintenance > API Gateway**.

To set or get the country code at group level through API:

1. Go to **Maintenance > API Gateway**.
2. Click **Authorized Apps & Tokens** tab and generate a token key.
3. Download and copy the generated token.
4. Click the link displayed in the **APIs** tab of the **API Gateway**. The **Central Network Management APIs** page opens.
5. On the left navigation pane, select **Configuration** from the **URL** drop-down list.
6. Paste the token key in the **Token** field and press enter.
7. Click **NB UI Group Configuration.** The following options are displayed**:**

- **Set country code at group level ([PUT]/configuration/v1/country)** — This API allows to set country code for multiple groups at once. Aruba Central currently allows country codes of up to 50 Instant AP device groups to be configured simultaneously. To set the country codes of multiple groups, enter the group names and country code as inputs corresponding to the **groups** and **country** labels respectively in the script { "groups": ["string"], "country": "string" } within the **set_ group_config_ country_ code** text box.
- **Get country code set for group ([GET]/configuration/v1/{group}/country)** — This API allows to retrieve the country code set for a specific Instant AP group. To get the country code information of the Instant AP group, enter the name of the group for which the country code is being queried corresponding to the **country** label in the script { "country": "string"} within the **group** text box.

NOTE

The APIs for setting and retrieving country code information are not available for the Instant AP devices deployed in template groups.

The following are the response messages displayed in the **Set country code at group level** and **Get country code set for group** sections:

Table 59: *Response Messages*

Set country code at group level	Get country code set for group
■ 201 - Successful operation ■ 400 - Bad Request ■ 401 - Unauthorized access, authentication required ■ 403 - Forbidden, do not have write access for group ■ 413 - Request-size limit exceeded ■ 417 - Request-size limit exceeded ■ 429 - API Rate limit exceeded ■ 500 - Internal Server Error ■ 503 - Service unavailable, configuration update in progress	■ 400 - Bad Request ■ 401 - Unauthorized access authentication required ■ 403 - Forbidden, do not have read access for group ■ 413 - Request-size limit exceeded ■ 417 - Request-size limit exceeded ■ 429 - API Rate limit exceeded ■ 500 - Internal Server Error ■ 503 - Service unavailable, configuration update in progress

For further details on API help, refer to https://app1-apigw.central.arubanetworks.com/swagger/central.

Configuring Device Parameters

To configure device parameters for an Instant AP, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the navigation pane, click **Access Points**. The **Access Points** page opens.
4. To edit an AP, click the edit icon **Edit** on the Access Point row. The **Edit** pane for modifying the Instant AP parameters opens.
5. Configure the parameters described below:

Table 60: *Access Points Configuration*

UI	Parameters	Description
Basic Info	**Name**	Configures a name for the Instant AP. You can specify a character string of up to 32 ASCII or non-ASCII characters.
	AP Zone	Configures the Instant AP zone. For Instant APs running firmware versions 6.5.4.7 or later, and 8.3.0.0 or later, you can configure multiple AP zones by adding zone names as comma separated values. **NOTE:** Aruba recommends that you do not configure zones in both SSID (**Wireless Management** > **Networks**) and in the Per AP settings of an Instant AP (**Wireless Management** > **Access Points**). If the same zones are configured in SSID and Per AP settings, APs may broadcast the SSIDs, but if the SSIDs and Per AP settings have different zones configured, it may lead to a configuration error. For more information on AP zones, see *Aruba Instant User Guide*.
	RF Zone	Allows you to create an RF zone for the AP. With RF zone, you can configure different power transmission settings for APs in different zones or sections of a deployment site. For example, you can configure power transmission settings to make Wi-Fi available only for the devices in specific areas of a store. You can also configure separate RF zones for the 2.4 GHz and 5 GHz radio bands for the Instant APs in a cluster. For more information, see Configuring Radio Parameters on page 281. **NOTE:** Aruba recommends that you configure RF zone for either individual AP or for the cluster. Any discrepancy in the RF zone names may lead to configuration errors.
	Swarm Mode	Allows to set one of the following operation modes: ■ **Cluster**—Allows Instant AP join an Instant AP cluster. ■ **Standalone**—Allows Instant AP to function in the standalone mode. After changing the AP operation mode, ensure that you reboot the AP.
	Preferred Master	Provisions the Instant AP as a master Instant AP. By default, the **Preferred Master** toggle button remains disabled.
	IP Address for Access Point	Allows IP to get an IP address from the DHCP server. By default, the Instant APs obtain IP address from a DHCP server. The users can also assign a static IP address to the Instant AP. To specify a static IP address for the Instant AP, complete the following steps: 1. Enter the new IP address for the Instant AP in the **IP Address** text box. 2. Enter the subnet mask of the network in the **Netmask** text box. 3. Enter the IP address of the default gateway in the **Default Gateway** text box. 4. Enter the IP address of the DNS server in the **DNS Server** text box. 5. Enter the domain name in the **Domain Name** text box.
Radio	**Mode**	Select any of the following options:

UI	Parameters	Description
		■ **Access**—In the **Access** mode, the Instant AP serves clients, while also monitoring for rogue Instant APs in the background. ■ **Monitor**—In the **Monitor** mode, the Instant AP acts as a dedicated monitor, scanning all channels for rogue Instant APs and clients. ■ **Spectrum Monitor**—In the **Spectrum Monitor** mode, the Instant AP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference, whether from the neighboring Instant APs or from non-Wi-Fi devices such as microwaves and cordless phones. **NOTE:** In the **Monitor** and **Spectrum Monitor** modes, the Instant APs do not provide access services to clients. **NOTE:** In the dual-5Ghz band, the **Mode** remains as **Access** and is non-editable. This dual 5 GHz band is only supported on AP-344 and AP-345 that run on Instant AP 8.3.0.0. For more information, see the Configuring Dual 5 GHz Radio Bands on an Instant AP section. To get accurate monitoring details and statistics, it is highly recommended to reboot the Instant APs once the Instant APs are toggled from the 2.4/5GHz mode to dual-5GHz radio mode or vice-versa.
		You can configure a radio profile on an Instant AP either manually or by using the **Adaptive radio management assigned**(ARM) feature. ARM is enabled on Aruba Central by default. It automatically assigns appropriate channel and power settings for the Instant APs.
		You can also Administrator Assigned and select the number of channels in the **Channel** drop-down list. In the **Transmit Power** field, enter the signal strength measured in dBm.
External Antenna	**Antenna Gain**	If the Instant AP has external antenna connectors, you need to configure the transmit power of the system. You can also measure or calculate additional attenuation between the device and the antenna before configuring the antenna gain. For more information, see the Configuring External Antenna section.
	Antenna Polarization Type	The wireless bridge's integrated antenna sends a radio signal that is polarized in a particular direction. The antenna's receive sensitivity is also higher for radio signals that have the same polarization. To maximize the performance of the wireless link, both antennas must be set to the same polarization direction. To maximize the performance of the wireless link, both antennas must be set to the same polarization direction.
Installation Type	**Installation Type**	Configure the Installation Type of the Instant AP you have selected. The Installation Type drop-down consists of the following options: ■ **Indoor** ■ **Outdoor** You can either select the Indoor option to change the installation to Indoor mode or select the Outdoor option to change the installation to the Outdoor mode. **NOTE:** The options in the **Installation Type** drop-down are listed based on the Instant AP model.
Mesh	**Mesh enable**	Enable this option to allow mesh access points to form mesh network. The mesh feature ensures reliability and redundancy by allowing the network to continue operating even when an Instant AP is non-functional or if the device fails to connect to the network. For more information, see the Mesh Network and Mesh Instant AP section. **NOTE:** For more information on mesh network, you can also refer to the *Mesh Instant AP Configuration* chapter of *Aruba Instant 8.4.0.0 User Guide*.

UI	Parameters	Description
	Clusterless mesh name	Enter the name of mesh access points that do not belong to any cluster. The **Clusterless mesh name** field is disabled when the **Mesh enable** option is enabled.
	Clusterless mesh key	Enter the key of the mesh access points that do not belong to any cluster. The **Clusterless mesh key** field is disabled when the **Mesh enable** option is enabled.
	Retype	Re-enter the clusterless mesh key. The **Retype** is disabled when the **Mesh enable** option is enabled.
Uplink	**Uplink Management VLAN**	The uplink traffic on Instant AP is carried out through a management VLAN. However, you can configure a non-native VLAN as an uplink management VLAN. After an Instant AP is provisioned with the uplink management VLAN, all management traffic sent from the Instant AP is tagged to the management VLAN. To configure a non-native uplink VLAN, click **Uplink** and specify the VLAN in **Uplink Management VLAN**.
	Eth0 Bridging	If you want to convert the Eth0 uplink port to a downlink port, enable **Eth0 Bridging**. Enable this option to support wired bridging on the Ethernet 0 port of an Instant AP.
	USB Port	Enable the USB port if you do not want to use the cellular uplink or 3G/4G modem in your current network setup.
	PEAP User	Create the PEAP user credentials for certificate based authentication. Provide the user name and password in the **Username** and **Password** field for creating the PEAP user.

6. Click **Save Settings**.
7. Reboot the Instant AP if required.

Configuring External Antenna

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

EIRP = Tx RF Power (dBm)+GA (dB) - FL (dB)

The following table describes this formula:

Table 61: *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 Instant APs with external connectors, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the navigation pane, click **Access Points**. The **Access Points** page opens.
4. Under **Basic Info**, select the access point to configure and then click **Edit**.
5. Select **Radio** 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 2.4 GHz and 5 GHz bands.
7. Click **Save Settings**.

Adding an Instant AP

To add an Instant AP to Aruba Central, assign an IP address and a subscription.

After an Instant AP is connected to the network and if the **Auto Join Mode** feature is enabled, the Instant AP inherits the configuration from the virtual controller and is listed in the **Access Points** tab.

Deleting an Instant AP from the Network

To delete an Instant AP from the network:

1. From the app selector, click **Monitoring & Reports**. The **Network Overview** page opens.
2. Click **APs** and select **List** from the APs drop-down. The list of APs in the network is displayed.
3. Click the AP to delete. The AP details page opens.
4. From the **Actions** drop-down, click **Delete AP**.

The **Delete AP** button is available only if the AP is down.

Configuring System Parameters an Instant AP Cluster

To configure system parameters for an Instant AP cluster:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. Click **System**. The **System** details for the selected group or the device are displayed.
4. Click **General** and configure the following parameters:

Table 62: *System parameters*

Data Pane Item	Description
Virtual Controller	To configure the virtual controller name and IP address, click edit icon and update the name and IP address. The IP address serves as a static IP address for the multi-AP network. When configured, this IP address is automatically provisioned on a shadow interface on the Instant AP that takes the role of a virtual controller. The AP sends three ARP messages with the static IP address and its MAC address to update the network ARP cache. ■ **Name**—Name of the virtual controller. ■ **IP address**—IPv4 address configured for the virtual controller. The IPv4 address uses the 0.0.0.0 notation. ■ **IPv6 address**—IPv6 address configured for the virtual controller. You can configure IPv6 address for the virtual controller only if the Allow IPv6 Management feature is enabled. IPv6 is the latest version of IP that is suitable for large-scale IP networks. IPv6 supports a 128-bit address to allow 2128, or approximately 3.4×1038 addresses while IPv4 supports only 232 addresses. The IP address of the IPv6 host is always represented as eight groups of four hexadecimal digits separated by colons. For example *2001:0db8:0a0b:12f0:0000:0000:0000:0001*. However, the IPv6 notation can be abbreviated to compress one or more groups of zeroes or to compress leading or trailing zeroes; for example *2001:db8:a0b:12f0::0:0:1*.
Set Country code for group	To configure a country code for the Instant 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 Instant AP device groups. When a country code is configured for the group, it takes precedence over the country code setting configured t the device level.
Timezone	To configure a timezone, select a timezone 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. **NOTE:** Reboot the Instant AP after modifying the radio profile for changes to take effect.
NTP Server	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: ■ Trace and track security gaps, network usage, and troubleshoot network issues. ■ Validate certificates. ■ Map an event on one network element to a corresponding event on another. ■ Maintain accurate time for billing services and similar. NTP helps obtain the precise time from a server and regulate the local time in each network element. Connectivity to a valid NTP server is required to synchronize the Instant AP clock to set the correct time. If NTP server is not configured in the Instant AP network, an Instant AP reboot may lead to variation in time data. By default, the Instant 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. 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.
Virtual Controller Netmask **Virtual Controller Gateway** **Virtual Controller VLAN**	**NOTE:** The IP configured for the virtual controller can be in the same subnet as Instant AP or can be in a different subnet. Ensure that you configure the virtual controller VLAN, gateway, and subnet mask details only if the virtual controller IP is in a different subnet. **NOTE:** Ensure that virtual controller VLAN is not the same as native VLAN of the Instant AP.

Table 62: *System parameters*

Data Pane Item	Description
DHCP Option 82 XML	Option 82 can be customized to cater to the requirements of any ISP using the master Instant AP. To facilitate customization using a XML definition, multiple parameters for Circuit ID and Remote ID options of DHCP Option 82 are introduced. The XML file is used as the input and is validated against an XSD file in the master Instant 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. From the drop-down list, select one of the following XML files: ■ default_dhcpopt82_1.xml ■ default_dhcpopt82_2.xml For information related to the **Option 82** drop-down list, see Option 82 on page 321 .
Dynamic CPU Utilization	Instant APs perform various functions such as wired and wireless client connectivity and traffic flows, wireless security, network management, and location tracking. If an AP is overloaded, prioritize the platform resources across different functions. Typically, the Instant APs manage resources automatically in real time. However, under special circumstances, if dynamic resource management needs to be enforced or disabled altogether, the dynamic CPU management feature settings can be modified. To configure dynamic CPU management, select any of the following options from **Dynamic CPU Utilization**. ■ **Automatic**—When selected, the CPU management is enabled or disabled automatically during run-time. This decision is based on real time load calculations taking into account all different functions that the CPU needs to perform. This is the default and recommended option. ■ **Always Disabled in all APs**— When selected, this setting disables CPU management on all APs, typically for small networks. This setting protects user experience. ■ **Always Enabled in all APs**—When selected, the client and network management functions are protected. This setting helps in large networks with high client density.
Auto Join Mode	When enabled, Instant APs can automatically discover the virtual controller and join the network. The **Auto Join Mode** feature is enabled by default.
APs allowed for Auto-Join Mode	When Auto Join is enabled, the Instant APs are automatically discovered and are allowed to join the cluster. When the Auto Join feature is disabled on the Instant AP, the list of allowed APs on Aruba Central may not be synchronized or up-to-date. In such cases, you can manually add a list of APs that can join the Instant AP cluster in the Aruba Central UI. To manually add the list of allowed AP devices, complete the following steps: 1. From the group selector, select the desired AP. 2. Under **System**, click the **Manage APs** link next to **APs allowed for Auto-Join Mode** field. 3. Add the MAC address of AP that you want to allow. 4. Click **Save Settings**.
Allow IPv6 Management	Enables IPv6 address configuration for the virtual controller. **NOTE:** You can configure an IPv6 address for a virtual controller IP only when **Allow IPv6 Management** feature is enabled.
Uplink switch native VLAN	Allows you to specify a VLAN ID, to prevent the AP from sending tagged frames for clients connected on the SSID that uses the same VLAN as the native VLAN of the switch. By default, the AP considers the native VLAN of the upstream switch, to which it is connected, as the VLAN ID 1.
Terminal Access	When enabled, the users can access the Instant AP CLI through SSH.
Console Access	When enabled, the users can access Instant AP through the console port.

Table 62: *System parameters*

Data Pane Item	Description
WebUI Access	If an Instant AP is connected to Aruba Central, you can use this option to disable Instant AP Web UI access and any communication via HTTPS or SSH. If you enable this option, you can manage the Instant AP only from Aruba Central.
Telnet Server	When enabled, the users can start a Telnet session with the Instant AP CLI.
LED Display	Enables or disables the LED display for all Instant APs in a cluster. **NOTE:** The LED display is always enabled during the Instant AP reboot.
Extended SSID	**Extended SSID** is enabled by default in the factory default settings of Instant APs. This disables mesh in the factory default settings. **NOTE:** For Instant AP devices that support Aruba Instant 8.4.0.0 firmware versions and above, you can configure up to 14 SSIDs. By enabling Extended SSID, you can create up to 16 networks.
Deny Inter-user Bridging	If you have security and traffic management policies defined in upstream devices, you can disable bridging traffic between two clients connected to the same AP on the same VLAN. When inter-user bridging is denied, the clients can connect to the Internet but cannot communicate with each other, and the bridging traffic between the clients is sent to the upstream device to make the forwarding decision. To disable inter-user bridging, move the slider to the right.
Deny Local Routing	If you have security and traffic management policies defined in upstream devices, you can disable routing traffic between two clients connected to the same Instant AP on different VLANs. When local routing is disabled, the clients can connect to the Internet but cannot communicate with each other, and the routing traffic between the clients is sent to the upstream device to make the forwarding decision. To disable local routing, move the slider to the right.
Dynamic RADIUS Proxy	If your network has separate RADIUS authentication servers (local and centralized servers) for user authentication, you may want to enable **Dynamic RADIUS proxy** to route traffic to a specific RADIUS server. When **Dynamic RADIUS proxy** is enabled, the IP address of the virtual controller is used for communication with external RADIUS servers. To enable **Dynamic RADIUS Proxy**, you must configure an IP address for the Virtual Controller and set it as a NAS client in the RADIUS server profile.
Dynamic TACACS Proxy	If you want to route traffic to different TACACS servers, enable **Dynamic TACACS Proxy**. When enabled, the Instant AP cluster uses the IP address of the Virtual Controller for communication with external TACACS servers. If an IP address is not configured for the Virtual Controller, the IP address of the bridge interface is used for communication between the Instant AP and TACACS servers. However, if a VPN tunnel exists between the Instant AP and TACACS server, the IP address of the tunnel interface is used.
Cluster Security	Enables or disables the cluster security feature. When enabled, the control plane communication between the Instant AP cluster nodes is secured. The **Disallow Non-DTLS Slaves** toggle appears. Enable this toggle to allow slave Instant APs to join a DTLS enabled cluster. For secure communication between the cluster nodes, the Internet connection must be available, or at least a local NTP server must be configured. **NOTE:** After enabling or disabling cluster security, ensure that the configuration is synchronized across all devices in the cluster, and then reboot the cluster. **NOTE:** The **Disallow Non-DTLS Slaves** toggle is only supported in Instant AP devices supporting Aruba Instant 8.4.0.0 firmware versions and above.
Low Assurance PKI	Enable this option to allow low assurance devices that use non-TPM chip, in the network. **NOTE:** To enable the cluster security feature, set the **Low Assurance PKI** toggle to **Enable.**

Table 62: *System parameters*

Data Pane Item	Description
	For more information on *Low Assurance PKI*, refer to *Cluster Security* section in *Aruba Instant 8.4.0.0 User Guide*. **NOTE:** The **Low Assurance PKI** toggle is supported in Instant AP devices running Aruba Instant 6.5.3.0 firmware versions and above.
Mobility Access Switch Integration	Enables LLDP protocol for Mobility Access Switch integration. With this protocol, Instant APs can instruct the Switch to turn off ports where rogue access points are connected, as well as take actions such as increasing PoE priority and automatically configuring VLANs on ports where Instant APs are connected.
URL Visibility	Enables URL data logging for client HTTP and HTTPS sessions and allows Instant APs to extract URL information and periodically log them on ALE for DPI and application analytics.

Configuring VLAN Name and VLAN ID

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

To map a VLAN Name to a VLAN ID, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **System**. The **System** page for the selected group opens.
4. Click the **Named VLAN Mapping** section**.**
5. Click the **+** icon in the **Named VLAN Mapping** section. The **VLAN Name to VLAN ID Mapping** page is displayed.
6. Enter the VLAN Name and VLAN ID that is required to be mapped.
7. Click **OK**. The **VLAN Name to VLAN ID Mapping** table in the **Named VLAN Mapping** section lists all the mapped VLAN.

You can find the Named VLAN Mapping feature applied in the following fields of corresponding UI pages of Aruba Central:

- The **VLANID** field of **Wireless Management** > **Wireless SSIDs** > **Add SSID** > **VLAN** tab when **Custom** for Instant AP Assigned and **Static** for External DHCP server assigned is selected.
- The **VLANID** field of **Wireless Management** > **Access Point Ports** > **Add SSID** > **VLAN** tab when **Custom** for **Instant AP Assigned** and **Static** for **External DHCP server assigned** is selected.
- The **Access Rule** page of the **Wireless Management** > **Access Point Ports** > **Access** tab and **Wireless Management** > **Wireless SSIDs** > **Access** tab when you add rules for selected roles. Select **VLAN Assignment** as the rule type in the **Access Rule** page to find the mapped VLAN name in the **VLANID** field.

Points to remember

- The maximum number of Named VLAN ID mappings allowed in Aruba Central is **32**.
- VLAN mapping cannot be performed if the VLAN name does not exist.
- The VLAN mapping record is deleted from the **VLAN Name to VLAN ID Mapping** table when the VLAN name is deleted.
- You can only map a single VLAN id to a VLAN name.
- The VLAN name field is not case-sensitive.

Configuring Dual 5 GHz Radio Bands on an Instant AP

Aruba Central provides an option to retrieve the radio numbers of Instant AP through the APIs. It also provides an option to filter AP details using radio numbers in the Monitoring dashboard.

For regular Instant APs with non-dual band, Central automatically assigns radio 1 to 2.4GHz band and radio 0 to 5GHz band respectively.

To get the radio numbers through API:

1. Go to **Maintenance > API Gateway**.
2. Click **Authorized Apps & Tokens** tab and generate a token key.
3. Download and copy the generated token.
4. Click the link displayed in the **APIs** tab of the **API Gateway**. The **Central Network Management APIs** page opens.
5. On the left navigation pane, select **Monitoring** from the **URL** drop-down list.
6. Paste the token key in the **Token** field and press enter.
7. Click **API Reference > AP.** The following are the APIs related to access points that allow to retrieve and filter data for a specific radio number:

Table 63: *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 neighbouring 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/bandwith_ 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.

8. On the left navigation pane, click **API Reference > Client.**
9. The following APIs allows to retrieve the radio number for the total connected clients:

Table 64: *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 API help, refer to https://app1-apigw.central.arubanetworks.com/swagger/central.

Configuring Network Profiles on Instant APs

This section describes the following procedures:

- Configuring Wireless Network Profiles on Instant APs on page 242
- Configuring Wireless Networks on Guest Users on Instant APs on page 253
- Configuring Wired Port Profiles on Instant APs on page 268
- Editing a Network Profile on page 272
- Deleting a Network Profile on page 272

Configuring Wireless Network Profiles on Instant APs

You can configure up to 14 SSIDs. By enabling **Extended SSID** in the **Wireless Management > System > General** tab, you can create up to **16** networks.

If more than 16 SSIDs are assigned to a zone and the extended zone option is disabled, an error message is displayed.

Creating a Wireless Network Profile

To configure WLAN settings, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click the **Wireless SSIDs**. The **Wireless SSIDs** page opens.
4. To create a new SSID profile, click **+ Add SSID**. The **Create a New Network** pane opens.
5. In **General** tab, configure the following parameters for basic configuration:
   a. Enter a name that is used to identify the network in the **Name (SSID)** text box.
   b. 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.
6. Under **Advanced Settings**, configure the parameters as mentioned in the Advanced WLAN Configuration Parameters table.

Table 65: *Advanced WLAN Configuration Parameters*

Parameter	Description
Broadcast/Multicast	
Broadcast Filtering	Select any of the following values: ■ **All**—The Instant AP drops all broadcast and multicast frames except DHCP and ARP, IGMP group queries, and IPv6 neighbor discovery protocols. ■ **ARP**—The Instant 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 Instant AP is configured to ARP mode. ■ **Unicast ARP Only**—This options enables Instant AP to convert ARP requests to unicast frames thereby sending them to the associated clients. ■ **Disabled**—The Instant AP forwards all the broadcast and multicast traffic is forwarded to the wireless interfaces.
DTIM Interval	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 Instant AP delivers the buffered broadcast and multicast frames to the associated clients in the power save mode. Range is 1 to 10 beacons. The default value is 1, which means the client checks for buffered data on the Instant AP at every beacon. You can also configure a higher DTIM value for power saving.
Multicast Transmission Optimization	Select the check box if you want the Instant AP to select the optimal rate for sending broadcast and multicast frames based on the lowest of unicast rates across all associated clients. When this option is enabled, multicast traffic can be sent up to a rate of 24 Mbps. The default rate for sending frames for 2.4 GHz is 1 Mbps and that for 5 GHz is 6 Mbps. This option is disabled by default.
Dynamic Multicast Optimization	Select the check box to allow Instant 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. **NOTE:** When you enable DMO on multicast SSID profiles, ensure that the DMO feature is enabled on all SSIDs configured in the same VLAN.
Dynamic Multicast Optimization Channel Utilization Threshold	Specify a value to set a threshold for DMO channel utilization. With DMO, the Instant 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 Instant AP sends multicast traffic over the wireless link. **NOTE:** This option will be enabled only when **Dynamic Multicast Optimization** is enabled.
Transmit Rates (Legacy Only)	
2.4 GHz	If the 2.4 GHz band is configured on the Instant 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 Instant 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.
Zone	
Zone	Specify the zone for the SSID. If a zone is configured in the SSID, only the Instant AP in that zone broadcasts this SSID. If there are no Instant APs in the zone, SSID is broadcast. If the Instant AP cluster has devices running Aruba Instant firmware versions 6.5.4.7 or later, and 8.3.0.0 or later, you can configure multiple AP zones by adding zone names as comma separated values.

Parameter	Description
	NOTE: Aruba recommends that you do not configure zones in both SSID (**Wireless Management** > **Wireless SSIDs**) and in the Per AP settings of an Instant AP (**Wireless Management** > **Access Points**). If the same zones are configured in SSID and Per AP settings, APs may broadcast the SSIDs, but if the SSIDs and Per AP settings have different zones configured, it may lead to a configuration error. For more information on AP zones, see *Aruba Instant User Guide*.
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.
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.
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 a per AP 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 a per AP level and not cluster level.
Enable 11ac	When this option is selected, VHT is enabled on the 802.11ac devices for the 5GHz radio band. If VHT is enabled for the 5 GHz radio profile on an Instant AP, it is automatically enabled for all SSIDs configured on an Instant AP. By default, VHT is enabled on all SSIDs. **NOTE:** If you want the 802.11ac Instant APs to function as 802.11n Instant 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 Instant AP, it is automatically enabled for all SSIDs configured on an Instant AP. By default, VHT is enabled on all SSIDs.
WiFi Multimedia	
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	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. **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.

Parameter	Description
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-save mechanism that is an optional part of the IEEE amendment 802.11e, QoS.
Miscellaneous	
Content Filtering	Select this check box to route all DNS requests for the non-corporate domains to OpenDNS on this network.
Primary Usage	Based on the type of network profile, select one of the following options: ■ **Mixed Traffic**—Select this option to create an employee or guest network profile. The employee network is used by the employees in an organization and it supports passphrase-based or 802.1X-based authentication methods. Employees can access the protected data of an enterprise through the employee network after successful authentication. The guest network is created for guests, visitors, contractors, and any non-employee users who use the enterprise Wi-Fi network. The VC assigns the IP address for the guest clients. Captive portal or passphrase-based authentication methods can be set for this wireless network. Typically, a guest network is an unencrypted network. However, you can specify the encryption settings when configuring a guest network. ■ **Voice Only**—Select this option to configure a network profile for devices that provide only voice services such as handsets or applications that require voice traffic prioritization. **NOTE:** When a client is associated with the voice network, all data traffic is marked and placed into the high priority queue in QoS.
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.
Deauth Inactive Clients	Select this option to allow the Instant AP to send a deauthentication frame to the inactive client and the clear client entry.
Hide SSID	Select this check box if you do not want the SSID to be visible to users.
Disable Network	Select this check box if you want to disable the SSID. When selected, the SSID is disabled, but is not removed from the network. By default, all SSIDs are enabled.
Can Be Used Without Uplink	Select this check box if you do not want the SSID profile to use the uplink.
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.
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.
Out of service (OOS)	Enable or disable the SSID based on the following OOS states of the Instant AP:

Parameter	Description
	■ VPN down ■ Uplink down ■ Internet down ■ Primary uplink down The network turns out of service when selected event occurs and the SSID is enabled or disabled as per 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.
OOS time (global)	Configure a hold time interval in seconds within a 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.
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.
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.
Time Range Profiles	
Time Range Profiles	Click **+ New Time Range Profile** to create a new time range profile. For more information, see Configuring Time-Based Services for Wireless Network Profiles on page 275.

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 for Wireless Network

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

1. In the **VLAN** tab, select any of the following options for **Client IP Assignment**:
   - **Instant AP assigned**—When selected, the client obtains the IP address from the VC.
   - **External DHCP server assigned**—When selected, the client obtains the IP address from the network.
2. Based on the type of client IP assignment mode selected, you can configure the VLAN assignment for clients as described in the following table:

Table 66: *VLAN Assignment*

Parameter	Description
Instant AP assigned	On selecting this option, the client obtains the IP address from the Virtual Controller. The Virtual Controller creates a private subnet and VLAN on the Instant 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 Instant APs on page 318. If this option is selected, specify any of the following options: ■ **Internal VLAN**—Assigns IP address to the client in the same subnet as the Instant 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, enter the scope of VLAN that is allowed 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.
External DHCP server assigned	If this option is selected, specify any of the following options: ■ **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. For more information, see Configuring VLAN Assignment Rule. ■ **Native Vlan**—Assigns the client VLAN to the native VLAN.

3. Click **Next** to configure security settings.

Configuring Security Settings for a Wireless Network

To configure security settings for mixed traffic or voice network, complete the following steps:

1. In the **Security** tab, specify any one of the following options in the **Security Level**:
   - **Enterprise**—On selecting the security level, the authentication options applicable to the network are displayed.
   - **Personal**—On selecting **Personal** security level, the authentication options applicable to the personalized network are displayed.
   - **Captive Portal**—On selecting **Captive Portal** security level, the authentication options applicable to the captive portal is displayed. For more information on captive portal, see Configuring Access Points Ports Networks on Guest Users on Instant APs.
   - **Open**—On selecting **Open** security level, the authentication options applicable to an open network are displayed.

The default security setting for a network profile is **Personal**.

2. Based on the security level specified, configure the following basic parameters:

Table 67: *Basic WLAN security settings*

Data pane item	Description
Key Management	For **Enterprise** security level, select any of the following options from **Key Management**: ■ **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. **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.
	For **Personal** security level, select an encryption key from **Key Management**. For **WPA-2 Personal**, **WPA Personal**, **Both (WPA-2&WPA)**, and **WPA-3 Personal** keys, specify the following parameters: ■ **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 the authentication server.
	For **Captive Portal** security level, select an encryption key from **Key Management**. For **WPA-2 Personal**, **WPA Personal**, **Both (WPA-2&WPA)**, and **WPA-3** keys, specify the following parameters: ■ **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. 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 information on configuring captive portal, see Configuring Wireless Networks on Guest Users on Instant APs on page 253.
	For **Open** security level, the Key Management includes **Open**, and **Enhanced Open** options.
EAP Offload	This option is applicable to **Enterprise** security levels only. To terminate the EAP portion of 802.1X authentication on the Instant AP instead of the RADIUS server, set **EAP Offload** to Enabled. Enabling **EAP Offload** can reduce network traffic to the external RADIUS server by terminating the authorization protocol on the Instant AP. By default, for 802.1X authorization, the client conducts an EAP exchange with the RADIUS server, and the Instant AP acts as a relay for this exchange. When EAP Offload is enabled, the Instant AP by itself acts as an authentication server and terminates the outer layers of the EAP protocol, only relaying the innermost layer to the external RADIUS server. It can also reduce the number of exchange packets between the Instant AP and the authentication server.

Data pane item	Description
	NOTE: Instant supports the configuration of primary and backup authentication servers in an EAP termination-enabled SSID. **NOTE:** If you are using LDAP for authentication, ensure that Instant AP termination is configured to support EAP.
Authentication Server	■ **Primary Server**—Sets a primary authentication server. The **Primary Server** option appears only for Enterprise security level, internal and external captive portal types. Select one of the following options from the drop-down list: ● **Internal Server**—To use an internal server, select **Internal Server** and add the clients that are required to authenticate with the internal RADIUS Server. Click **Users** to add the users. ● To add a new server, click +. For information on configuring external servers, see Configuring External Authentication Servers for an Instant AP Cluster on page 294. ■ **Secondary Server**—To add another server for authentication, configure another authentication server. ■ **Authentication Survivability**—If an external server is configured for authentication, you can enable authentication survivability. Specify a value in hours for **Cache Timeout** to set the duration after which the authenticated credentials in the cache expires. When the cache expires, the clients are required to authenticate again. You can specify a value within range of 1 to 99 hours.By default, authentication survivability is disabled. ■ **Load Balancing**—Set this to **Enabled** 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 on page 294.
Users	Click **Users** to add the users. The registered users of **Employee** type will be able to access the users of **Enterprise** network. To add a new user, click **+ Add User** and enter the new user in the **Add User** page. The **Primary Server** option appears only for **Enterprise** security level, internal and external captive portal types.

3. Based on the security level specified, specify the following parameters in the **Advanced Settings** section:

Table 68: *Advanced WLAN security settings*

Data pane item	Description
Use Session Key for LEAP	Select this option to use the session key for Lightweight Extensible Authentication Protocol. This option is available only for **Enterprise** level**.**
Opportunistic Key Caching (OKC)	Select the **Opportunistic key caching (OKC)** options that helps reduce the time needed for authentication. When OKC is used, multiple APs can share Pairwise Master Keys (PMKs) among themselves, and the station can roam to a new access points that has not visited before and reuse a PMK that was established with the current AP. OKC allows the station to roam quickly to an access point it has never authenticated to, without having to perform pre-authentication. OKC is available specifically on WPA2 SSIDs only.
MAC Authentication for Enterprise Networks	To enable MAC address based authentication for **Personal** and **Open** security levels, set **MAC Authentication** to **Enabled**. For **Enterprise** security level, the following options are available: ■ **Perform MAC Authentication Before 802.1X** — Select this to use 802.1X authentication only when the MAC authentication is successful. ■ **MAC Authentication Fail-Thru** — On selecting this, the 802.1X authentication is attempted when the MAC authentication fails. If MAC authentication is enabled, configure the following parameters: ■ **Delimiter Character**—Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the Instant AP uses the delimiter in the MAC

Data pane item	Description
	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 Instant AP to use uppercase letters in MAC address string for MAC authentication. This option is available only if MAC authentication is enabled.
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. If the re-authentication interval is configured: ■ 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 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. ■ 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.
Blacklisting	By default, this option is disabled. To enable blacklisting of the clients with a specific number of authentication failures, select **Blacklisting** 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 blacklisted. By default, the **Blacklisting** option is disabled.
Enforce DHCP	Enforces WLAN SSID on Instant AP clients. When DHCP is enforced: ■ A layer-2 user entry is created when a client associates with an Instant 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 Instant APs, the DHCP state and the client IP address is synchronized with the new Instant AP.
PA3 Transition	Enable this option to allow transition from WPA3 to WPA2 and vice versa. The WPA3 Transition appears only when WPA-3 is selected in the **Key Management** for **Personal, Captive Portal,** and **Open** level.
Legacy Support	Enable this option to allow backward compatibility of encryption modes in networks. The **Legacy Support** appears only when WPA-3 is selected in the **Key Management** for **Personal, Captive Portal,** and **Open** level.
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: ■ **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	Enable this option to configure client IP address as calling station ID. When this option is enabled, the following options are displayed: ■ **Called Station ID Type**—Select any of the following options for configuring called station ID:

Data pane item	Description
	● **Access Point Group**—Uses the VC ID as the called station ID. ● **Access Point Name**—Uses the host name of the Instant 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 Instant AP as the called station ID. ● **MAC address**—Uses the MAC address of the Instant 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.
Delimiter Character	Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the Instant 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 Instant AP to use uppercase letters in MAC address string for MAC authentication. This option is available only if MAC authentication is enabled.
Fast Roaming	Enable the following fast roaming features as per your requirement: ■ **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 to another within the same cluster. The **802.11r** option is not available for **Enterprise** level. Once you enable the **802.11r**, the following text box is displayed: ● **MDID**— In the **MDID** text box, enter the mobility domain identifier to configure a mobility domain identifier. In a network of standalone Instant APs within the same management VLAN, 802.11r roaming does not work. This is because the mobility domain identifiers do not match across Instant APs. They are auto-generated based on a virtual controller key. You can set a mobility domain identifier for 802.11r SSIDs. For standalone Instant APs in the same management VLAN, 802.11r roaming works only when the mobility domain identifier is configured with the same value. ■ **802.11k**—Select **802.11k** to enable 802.11k roaming. The 802.11k protocol enables Instant APs and clients to dynamically measure the available radio resources. When 802.11k is enabled, Instant 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 management enhancements and BSS transition management. It allows the client devices to exchange information about the network topology and RF environment. The BSS transition management mechanism enables an AP to request a voice client to transition to a specific AP, or suggest a set of preferred APs to a voice client, due to network load balancing or BSS termination. It also helps the voice client identify the best AP to transition to as they roam.

4. Click **Next** to configure access rules.

Configuring ACLs for User Access to a Wireless Network

You can configure up to 64 access rules for a wireless network profile. To configure access rules for a network, complete the following steps:

1. Enable the **Downloadable User** option to allow downloading of pre-existing user roles. The CPPM Settings table with **Name**, **CPPM Username** and **Actions** columns related to the radius servers are displayed. For more information on Downloadable User Roles feature, see Downloadable User Roles.

The **Downloadable User Role** feature is optional.

The Downloadable User Roles feature is available only for networks that include APs that run a minimum of Aruba Instant 8.4.0.0 firmware version with a minimum of ClearPass server version 6.7.8.

At least one radius server must be configured to apply the Downloadable User Roles feature. For more information on configuring radius server, see Authentication Servers for Instant 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 following details:
   - **CPPM Username**—Enter the ClearPass Policy Manager admin username.
   - **Password**—Enter the password.
   - **Retype**—Retype the password.
4. Click **Ok**.
5. 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.
     - Create a role assignment rule.
6. Click **Save Settings**.

Viewing Wireless 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 Wireless Networks on Guest Users on Instant APs

Instant 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 Instant 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 Instant AP.

The Instant 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

Instant APs support the following types of splash page profiles:

- **Internal Captive portal**— Select this splash page to use an internal server for hosting the captive portal service. Internal captive portal supports the following types of authentication:
  - **Internal Authenticated**— When **Internal Authenticated** is enabled, a guest user who is pre-provisioned in the user database has to provide the authentication details.
  - **Internal Acknowledged**—When **Internal Acknowledged** is enabled, a guest user has to accept the terms and conditions to access the Internet.
- **External Captive portal**—Select this splash page to use an external portal on the cloud or on a server outside the enterprise network for authentication.
- **Cloud Guest**—Select this splash page to use the cloud guest profile configured through the **Guest Management** tab.

Selecting **None** disables the captive portal authentication.

For information on how to creating splash page profiles, see the following sections:

- Creating a Wireless Network Profile for Guest Users on page 253
- Configuring an Internal Captive Portal Splash Page Profile on page 254
- Configuring an External Captive Portal Splash Page Profile on page 256
- Configuring a Cloud Guest Splash Page Profile on page 258
- Disabling Captive Portal Authentication on page 259

Creating a Wireless Network Profile for Guest Users

To create an SSID for guest access, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Wireless SSIDs**.
4. To create a new SSID profile, click the + icon. The **Create a New Network** pane opens.

5. Under **Basic Settings**, enter a name that is used to identify the network in the **Name (SSID)** box.
6. In **Miscellaneous** section, select the **Primary Usage** as **Mixed Traffic**.
7. If configuring a wireless guest profile, set the required WLAN configuration parameters described in Table 65.
8. Click **Next** to configure VLAN settings. The VLAN details are displayed.
9. Select any of the following options for **Client IP Assignment**:

Table 69: *VLAN Assignment*

Parameter	Description
Instant AP assigned	On selecting this option, the client obtains the IP address from the Virtual Controller. The Virtual Controller creates a private subnet and VLAN on the Instant 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 Instant APs on page 318. If this option is selected, specify any of the following options: ■ **Default**—Assigns IP address to the client in the same subnet as the Instant 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, enter the scope of VLAN that is allowed.
External DHCP server assigned	If this option is selected, specify any of the following options: ■ **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. 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. ■ **Native Vlan**—Assigns the client VLAN is assigned to the native VLAN.

Configuring an Internal Captive Portal Splash Page Profile

To configure internal captive portal profile, complete the following steps:

1. Open the guest SSID to edit and configure the following parameters in the **Wireless SSIDs** > **Security** page.

Table 70: *Internal Captive Portal Configuration Parameters*

Parameter	Description
Captive Portal Type	Select any of the following: ■ **Internal - Authenticated**—When **Internal Authenticated** 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. ■ **Internal - Acknowledged**—When **Internal Acknowledged** is enabled, the guest users are required to accept the terms and conditions to access the Internet. ■ **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. Also enter the details in **Walled Garden**, and **Advanced** section. ■ **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.
Captive Portal Location	Select **Acknowledged** or **Authenticated** from the drop-down list.
Splash Page Properties	Under **Splash Page Properties** when **Customize Captive Portal** is clicked, use the editor to specify text and colors for the initial page that is displayed to the users connecting to the network. The initial page asks for user credentials or email, depending on the splash page type (Internal - Authenticated or Internal - Acknowledged) for which you are customizing the splash page design. Perform the following steps to customize the splash page design. ■ **Top Banner Title**—Enter a title for the banner. To preview the page with the new banner title, click **Preview Splash Page**. ■ **Header fill color**—Specify a background color for the header. ■ **Welcome Text**—To change the welcome text, click the first square box in the splash page, enter the required text in the **Welcome Text**box, and click **OK**. Ensure that the welcome text does not exceed 127 characters. ■ **Policy Text**—To change the policy text, click the second square in the splash page, enter the required text in the **Policy Text** box, and click **OK**. Ensure that the policy text does not exceed 255 characters. ■ **Page Fill Color**—To change the color of the splash page, click the Splash page rectangle and select the required color from the color palette. ■ **Redirect URL**—To redirect users to another URL, specify a URL in **Redirect URL**. ■ **Logo Image**—To upload a custom logo, click **Upload**, browse the image file, and click **upload image**. Ensure that the image file size does not exceed 16 KB. To delete an image, click **Delete**. ■ To preview the captive portal page, click **Preview** splash page. ■ Captive-portal proxy server IP and Port—If you want 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.
Encryption	By default, this field is disabled. Select **Enabled** and configure the following encryption parameters: ■ **Key Management**—Specify an encryption and authentication key ■ **Passphrase format**—Specify a passphrase format. ■ **Passphrase**—Enter a passphrase and retype to confirm.
Authentication	Configure the following parameters: ■ **MAC Authentication**—To enable MAC address based authentication for **Personal** and **Open** security levels, set **MAC Authentication** to **Enabled**. ■ **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.

Table 70: *Internal Captive Portal Configuration Parameters*

Parameter	Description
	● To add a new server, click +. For information on configuring external servers, see Configuring External Authentication Servers for an Instant AP Cluster on page 294. ■ **Secondary Server**—To add another server for authentication, configure another authentication server. ■ **Load Balancing**—Set this to **Enabled** if you are using two RADIUS authentication servers, to balance the load across these servers. For more information on the dynamic load balancing mechanism, see Configuring DHCP Server for Assigning IP Addresses to Instant AP Clients on page 323.
Advanced Settings > Captive Portal Proxy Server IP	Specify the **Captive Portal Proxy Server IP**.
Advanced Settings > Captive Portal Proxy Server Port	Specify the **Captive Portal Proxy Server Port**.
Advanced Settings > Reauth Interval	Specify a value for **Reauth Interval**. When set to a value greater than zero, APs periodically re-authenticate all associated and authenticated clients.
Advanced Settings > 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.
Advanced Settings > Blacklisting	If you are configuring a wireless network profile, select **Enabled** to enable blacklisting of the clients with a specific number of authentication failures. This is applicable for WLAN SSIDs only.
Advanced Settings > Disable If Uplink Type Is	To exclude uplink, select an uplink type.

2. Click **Save Settings**.

Configuring an External Captive Portal Splash Page Profile

You can configure external captive portal profiles and associate these profiles to a user role or SSID. You can create a set of captive portal profiles in the **Security** > **External Captive Portal** data pane and associate these profiles with an SSID or a wired profile. You can also create a new captive portal profile under the **Security** tab of the WLAN wizard or a Wired Network pane. You can configure up to eight external captive portal profiles.

When the captive portal profile is associated to an SSID, it is used before user authentication. If the profile is associated to a role, it is used only after the user authentication. When a captive portal profile is applied to an SSID or wired profile, the users connecting to the SSID or wired network are assigned a role with the captive portal rule. The guest user role allows only DNS and DHCP traffic between the client and network, and directs all HTTP or HTTPS requests to the captive portal unless explicitly permitted.

To configure an external captive portal profile, complete the following steps:

1. Open the guest SSID to edit and configure the following parameters in the **Wireless SSIDs** > **Security** page.

2. Select the Splash Page type as **External**.

3. 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.

4. Select a captive portal profile. To add a new profile, click **+** and configure the following parameters:

Table 71: *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: ■ **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 Whitelisting	On enabling this for the external captive portal authentication, the URLs that are allowed for the unauthenticated users to access are automatically whitelisted.
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.

5. Click **Save**.

6. On the external captive portal splash page configuration page, specify encryption settings if required.

7. Specify the following authentication parameters under **Advanced Settings**:

- **MAC Authentication**—To enable MAC address based authentication for **Personal** and **Open** security levels, set **MAC Authentication** to **Enabled**.
- **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 an Instant AP Cluster on page 294.

- **Secondary Server**—To add another server for authentication, configure another authentication server.
- **Load Balancing**—Set this to **Enabled** if you are using two RADIUS authentication servers, to balance the load across these servers.

8. If required, under **Walled Garden**, create a list of domains that are blacklisted and also a white list of websites that the users connected to this splash page profile can access.
9. To exclude uplink, select an uplink type.
10. 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 Instant 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 Instant AP to use uppercase letters in MAC address string for MAC authentication. This option is available only if MAC authentication is enabled.

11. Configure the **Reauth Interval**. Specify a value for **Reauth Interval**. When set to a value greater than zero, Instant APs periodically re-authenticate all associated and authenticated clients.
12. If required, enable blacklisting. Set a threshold for blacklisting clients based on the number of failed authentication attempts.
13. Click **Save Settings**.

Configuring a Cloud Guest Splash Page Profile

For information on how to create a cloud guest network profile, see Configuring a Cloud Guest Splash Page Profile

Associating a Cloud Guest Splash Page Profile to a Guest SSID

To use the Cloud Guest Splash page profile for the guest SSID, ensure that the Cloud Guest Splash Page profile is configured through the **Guest Access** app.

To associate a Cloud Guest splash page profile to a guest SSID, complete the following steps:

1. Open the guest SSID to edit and click **Security**:
   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 click **Next**.
   c. To enable encryption, set **Encryption** to **Enabled** 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**.
2. Click **Save Settings**.

Configuring ACLs for Guest User Access

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

1. Open the guest SSID that you want to edit.
2. Under **Access**, select any of the following types of access control:

- **Unrestricted** — Select this to set unrestricted access to the network.
- **Network Based** — Select **Network Based** to set common rules for all users in a network. By default, **Allow any to all destinations** access rule is enabled. This rule allows traffic to all destinations. To define an access rule:

    a. Click **(+)** icon and select appropriate options for **Rule Type**, **Service**, **Action**, **Destination**, and **Options** fields.

    b. Click **Save**.

- **Role Based** — Select **Role Based** to enable access based on user roles.

For role-based access control:

1. Create a user role:

    a. Click **New** in **Role** pane.

    b. Enter a name for the new role and click **OK**.

2. Create access rules for a specific user role:

    a. Click **(+)** icon and select appropriate options for **RuleType**, **Service**, **Action**, **Destination**, and **Options** fields.

    b. Click **Save**.

3. Create a role assignment rule.

    a. Under **Role Assignment Rule**, click **New**. The **New Role Assignment Rule** pane is displayed.

    b. Select appropriate options in **Attribute**, **Operator**, **String**, and **Role** fields.

    c. Click **Save**.

3. Click **Save Settings**.

Disabling Captive Portal Authentication

To disable captive portal authentication, perform the following steps:

1. Select the guest network profile for which you want to disable captive portal authentication.
2. Under **Security**, select **None** for **Splash Page Type**.
3. Click **Save Settings.**

Configuring Access Points Ports Networks on Guest Users on Instant APs

Instant 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 centres, or Wi-Fi hotspots. The webpage also prompts the guest users to authenticate or accept the usage policy and terms. Captive portals are used at Wi-Fi hotspots and can be used to control wired access as well.

The captive portal solution for an Instant 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 Instant AP.

The Instant 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

Instant APs support the following types of splash page profiles:

- **Internal Captive portal**— Select this splash page to use an internal server for hosting the captive portal service. Internal captive portal supports the following types of authentication:
  - **Internal Authenticated**— When **Internal Authenticated** is enabled, a guest user who is pre-provisioned in the user database has to provide the authentication details.
  - **Internal Acknowledged**—When **Internal Acknowledged** is enabled, a guest user has to accept the terms and conditions to access the Internet.
- **External Captive portal**—Select this splash page to use an external portal on the cloud or on a server outside the enterprise network for authentication.
- **Cloud Guest**—Select this splash page to use the cloud guest profile configured through the **Guest Management** tab.

Selecting **None** disables the captive portal authentication.

For information on how to creating splash page profiles, see the following sections:

- Configuring Access Points Ports Networks on Guest Users on Instant APs on page 259
- Configuring an Internal Captive Portal Splash Page Profile on page 261
- Configuring an External Captive Portal Splash Page Profile on page 263
- Configuring a Cloud Guest Splash Page Profile on page 265
- Disabling Captive Portal Authentication on page 266

Creating a Wired Network Profile for Guest Users

To create an SSID for guest access, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Access Points Ports**.
4. To create a new SSID profile, click the +**Add Port Profile**. The **Create a New Network** pane opens.
5. Under the basic settings, enter a name that is used to identify the network in the **Port Profile Name** box.
6. Click **Next** to configure VLAN settings. The VLAN details are displayed.
7. Select any of the following options for **Client IP Assignment**:

Table 72: *VLAN Assignment*

Parameter	Description
Instant AP assigned	On selecting this option, the client obtains the IP address from the Virtual Controller. The Virtual Controller creates a private subnet and VLAN on the Instant 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 Instant APs on page 318. If this option is selected, specify any of the following options: ■ **Default**—Assigns IP address to the client in the same subnet as the Instant 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, enter the scope of VLAN that is allowed.
External DHCP server assigned	If this option is selected, specify any of the following options: ■ **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. 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. ■ **Native Vlan**—Assigns the client VLAN is assigned to the native VLAN.

Configuring an Internal Captive Portal Splash Page Profile

To configure internal captive portal profile, complete the following steps:

1. Open the guest SSID to edit and configure the following parameters in the **Wireless Management** > **Access Points Ports** > **Security** page.

Table 73: *Internal Captive Portal Configuration Parameters*

Parameter	Description
Captive Portal Type	Select any of the following: ■ **Internal - Authenticated**—When **Internal Authenticated** 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. ■ **Internal - Acknowledged**—When **Internal Acknowledged** is enabled, the guest users are required to accept the terms and conditions to access the Internet. ■ **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. Also enter the details in **Walled Garden**, and **Advanced** section. ■ **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.
Captive Portal Location	Select **Acknowledged** or **Authenticated** from the drop-down list.
Splash Page Properties	Under **Splash Page Properties** when **Customize Captive Portal** is clicked, use the editor to specify text and colors for the initial page that is displayed to the users connecting to the network. The initial page asks for user credentials or email, depending on the splash page type (Internal - Authenticated or Internal - Acknowledged) for which you are customizing the splash page design. Perform the following steps to customize the splash page design. ■ **Top Banner Title**—Enter a title for the banner. To preview the page with the new banner title, click **Preview Splash Page**. ■ **Header fill color**—Specify a background color for the header. ■ **Welcome Text**—To change the welcome text, click the first square box in the splash page, enter the required text in the **Welcome Text**box, and click **OK**. Ensure that the welcome text does not exceed 127 characters. ■ **Policy Text**—To change the policy text, click the second square in the splash page, enter the required text in the **Policy Text** box, and click **OK**. Ensure that the policy text does not exceed 255 characters. ■ **Page Fill Color**—To change the color of the splash page, click the Splash page rectangle and select the required color from the color palette. ■ **Redirect URL**—To redirect users to another URL, specify a URL in **Redirect URL**. ■ **Logo Image**—To upload a custom logo, click **Upload**, browse the image file, and click **upload image**. Ensure that the image file size does not exceed 16 KB. To delete an image, click **Delete**. ■ To preview the captive portal page, click **Preview** splash page. ■ Captive-portal proxy server IP and Port—If you want 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.
Encryption	By default, this field is disabled. Select **Enabled** and configure the following encryption parameters: ■ **Key Management**—Specify an encryption and authentication key ■ **Passphrase format**—Specify a passphrase format. ■ **Passphrase**—Enter a passphrase and retype to confirm.
Authentication	Configure the following parameters: ■ **MAC Authentication**—To enable MAC address based authentication for **Personal** and **Open** security levels, set **MAC Authentication** to **Enabled**. ■ **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.

Table 73: *Internal Captive Portal Configuration Parameters*

Parameter	Description
	● To add a new server, click +. For information on configuring external servers, see Configuring External Authentication Servers for an Instant AP Cluster on page 294. ■ **Secondary Server**—To add another server for authentication, configure another authentication server. ■ **Load Balancing**—Set this to **Enabled** if you are using two RADIUS authentication servers, to balance the load across these servers. For more information on the dynamic load balancing mechanism, see Configuring DHCP Server for Assigning IP Addresses to Instant AP Clients on page 323.
Users	Create and manage users in the captive portal network. Only registered users of type **Guest Employee** will be able to access this network.
Advanced Settings > MAC Authentication	To enable MAC address based authentication for **Personal** and **Open** security levels, set **MAC Authentication** to **Enabled**.
Advanced Settings > Reauth Interval	Specify a value for **Reauth Interval**. When set to a value greater than zero, APs periodically re-authenticate all associated and authenticated clients.
Advanced Settings > Blacklisting	If you are configuring a wireless network profile, select **Enabled** to enable blacklisting of the clients with a specific number of authentication failures. This is applicable for WLAN SSIDs only.
Advanced Settings > Disable If Uplink Type Is	To exclude uplink, select an uplink type.

2. Click **Save Settings**.

Configuring an External Captive Portal Splash Page Profile

You can configure external captive portal profiles and associate these profiles to a user role or SSID. You can create a set of captive portal profiles in the **Security** > **External Captive Portal** data pane and associate these profiles with an SSID or a wired profile. You can also create a new captive portal profile under the **Security** tab of the WLAN wizard or a Wired Network pane. You can configure up to eight external captive portal profiles.

When the captive portal profile is associated to an SSID, it is used before user authentication. If the profile is associated to a role, it is used only after the user authentication. When a captive portal profile is applied to an SSID or wired profile, the users connecting to the SSID or wired network are assigned a role with the captive portal rule. The guest user role allows only DNS and DHCP traffic between the client and network, and directs all HTTP or HTTPS requests to the captive portal unless explicitly permitted.

To configure an external captive portal profile, complete the following steps:

1. Open the guest SSID to edit and configure the following parameters in the **Wireless Management** > **Access Points Ports** > **Security** page.
2. Select the Splash Page type as **External**.
3. 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.
4. Select a captive portal profile. To add a new profile, click **+** and configure the following parameters:

Table 74: *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: ■ **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 Whitelisting	On enabling this for the external captive portal authentication, the URLs that are allowed for the unauthenticated users to access are automatically whitelisted.
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.

5. Click **Save**.
6. On the external captive portal splash page configuration page, specify encryption settings if required.
7. Specify the following authentication parameters in **Advanced Settings**:

- **MAC Authentication**—To enable MAC address based authentication for **Personal** and **Open** security levels, set **MAC Authentication** to **Enabled**.
- **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 an Instant AP Cluster on page 294.
- **Secondary Server**—To add another server for authentication, configure another authentication server.
- **Load Balancing**—Set this to **Enabled** if you are using two RADIUS authentication servers, to balance the load across these servers.

8. If required, under **Walled Garden**, create a list of domains that are blacklisted and also a white list of websites that the users connected to this splash page profile can access.

9. To exclude uplink, select an uplink type.

10. 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 Instant 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 Instant AP to use uppercase letters in MAC address string for MAC authentication. This option is available only if MAC authentication is enabled.

11. Configure the **Reauth Interval**. Specify a value for **Reauth Interval**. When set to a value greater than zero, Instant APs periodically re-authenticate all associated and authenticated clients.

12. If required, enable blacklisting. Set a threshold for blacklisting clients based on the number of failed authentication attempts.

13. Click **Save Settings**.

Configuring a Cloud Guest Splash Page Profile

For information on how to create a cloud guest network profile, see Configuring a Cloud Guest Splash Page Profile

Associating a Cloud Guest Splash Page Profile to a Guest SSID

To use the Cloud Guest Splash page profile for the guest SSID, ensure that the Cloud Guest Splash Page profile is configured through the **Guest Access** app.

To associate a Cloud Guest splash page profile to a guest SSID, complete the following steps:

1. Open the guest SSID to edit and click **Security**:
   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 click **Next**.
   c. To enable encryption, set **Encryption** to **Enabled** 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**.
2. Click **Save Settings**.

Configuring ACLs for Guest User Access

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

1. Open the guest SSID that you want to edit.
2. Under **Access**, select any of the following types of access control:

- **Unrestricted** — Select this to set unrestricted access to the network.
- **Network Based** — Select **Network Based** to set common rules for all users in a network. By default, **Allow any to all destinations** access rule is enabled. This rule allows traffic to all destinations. To define an access rule:

a. Click **(+)** icon and select appropriate options for **Rule Type**, **Service**, **Action**, **Destination**, and **Options** fields.

b. Click **Save**.

- **Role Based** — Select **Role Based** to enable access based on user roles.

For role-based access control:

1. Create a user role:

   a. Click **New** in **Role** pane.

   b. Enter a name for the new role and click **OK**.

2. Create access rules for a specific user role:

   a. Click **(+)** icon and select appropriate options for **RuleType**, **Service**, **Action**, **Destination**, and **Options** fields.

   b. Click **Save**.

3. Create a role assignment rule.

   a. Under **Role Assignment Rule**, click **New**. The **New Role Assignment Rule** pane is displayed.

   b. Select appropriate options in **Attribute**, **Operator**, **String**, and **Role** fields.

   c. Click **Save**.

3. Click **Save Settings**.

Disabling Captive Portal Authentication

To disable captive portal authentication, perform the following steps:

1. Select the guest network profile for which you want to disable captive portal authentication.
2. Under **Security**, select **None** for **Splash Page Type**.
3. Click **Save Settings.**

Downloadable User Roles

Aruba Central allows you to download pre-existing user roles when you create network profiles.

The Downloadable User Roles feature is available only for networks that include APs that run a minimum of Aruba Instant 8.4.0.0 firmware version with a minimum of ClearPass server version 6.7.8.

Aruba Instant and ClearPass Policy Manager include support for centralized policy definition and distribution.

When ClearPass Policy Manager successfully authenticates a user, the user is assigned a role by ClearPass Policy Manager. If the role is not defined on the Instant AP, the role attributes can also be downloaded automatically. In order to provide highly granular per-user level access, user roles can be created when a user has been successfully authenticated. During the configuration of a policy enforcement profile in ClearPass Policy Manager, the administrator can define a role that should be assigned to the user after successful authentication. In RADIUS authentication, when ClearPass Policy Manager successfully authenticates a user, the user is assigned a role by ClearPass Policy Manager.

If the role is not defined on the Instant AP, the role attributes can also be downloaded automatically. This feature supports roles obtained by the following authentication methods:

- 802.1X (WLAN and wired users)
- MAC authentication
- Captive Portal

ClearPass Policy Manager Certificate Validation for Downloadable User Roles (DUR)

When a ClearPass Policy Manager server is configured as the domain for RADIUS authentication for downloading user roles, in order to validate the ClearPass Policy Manager customized CA, Instant APs are required to publish the root CA for the HTTPS server to the well-known URI (**http://<clearpass-fqdn>/.wellknown/ aruba/clearpass/https-root.pem**). The Instant AP must ensure that an FQDN is defined in the above URI for the RADIUS server and then attempt to fetch the trust anchor by using the RADIUS FQDN. Upon configuring the domain of the ClearPass Policy Manager server for RADIUS authentication along with a username and password, the Instant AP tries to retrieve the CA from the above well-known URI and store it in flash memory. However, if there is more than one ClearPass Policy Manager server configured for authentication, the CA must be uploaded manually.

Enabling Downloadable User Roles Feature for Wireless Networks in Aruba Central

To enable the Downloadable User Roles feature, perform the following steps:

1. Go to **Wireless Management** > **Wireless SSIDs** > **Create a New Network** page to create a wireless network.
2. Configure the WLAN settings and VLAN settings.
3. In the Security tab, select the radius server in **Primary Server** field.

At least one radius server must be configured to apply the the Downloadable User Roles feature. For more information on configuring radius server, see Authentication Servers for Instant APs

4. Click **Next**, the **Access** tab is displayed.
5. Enable the **Downloadable User** option to allow downloading of pre-existing user roles. The **CPPM Settings** table with **Name**, **CPPM Username** and **Actions** columns related to the radius servers are displayed.

The Downloadable User Roles feature is available only for networks that include APs that run a minimum of Aruba Instant 8.4.0.0 firmware version with a minimum of ClearPass server version 6.7.8.

At least one radius server must be configured to apply the the Downloadable User Roles feature. For more information on configuring radius server, see Authentication Servers for Instant APs

6. Click the action corresponding to the radius server listed in the **CPPM Settings** table. The **Edit Server** page is displayed.

The **Edit Server** page displays the name of the radius server name. The **Name** field is non-editable.

7. Enter the following details:
   - **CPPM Username**—Enter the ClearPass Policy Manager admin username.
   - **Password**—Enter the password.
   - **Retype**—Retype the password.
8. Click **Ok**.

Enabling Downloadable User Roles Feature for Wired Networks in Aruba Central

To enable the Downloadable User Roles feature, perform the following steps:

1. Go to **Wireless Management** > **Access Point Ports** > **Create a New Network** page to create a wireless network.
2. Configure the WLAN settings and VLAN settings.
3. In the **Security** tab, select the radius server in **Primary Server** field.

NOTE

At least one radius server must be configured to apply the the Downloadable User Roles feature. For more information on configuring radius server, see Authentication Servers for Instant APs

4. Click **Next**, the **Access** tab is displayed.
5. Enable the **Downloadable User** option to allow downloading of pre-existing user roles. The **CPPM Settings** table with **Name**, **CPPM Username,** and **Actions** columns related to the radius servers are displayed.

NOTE

The Downloadable User Roles feature is available only for networks that include APs that run a minimum of Aruba Instant 8.4.0.0 firmware version with a minimum of ClearPass server version 6.7.8.

NOTE

At least one radius server must be configured to apply the the Downloadable User Roles feature. For more information on configuring radius server, see Authentication Servers for Instant APs

6. Click the action corresponding to the radius server listed in the **CPPM Settings** table. The **Edit Server** page with the radius server name is displayed.

NOTE

The **Edit Server** page displays the radius server name. The **Name** field is non-editable.

7. Enter the following details:
   - **CPPM Username**—Enter the ClearPass Policy Manager admin username.
   - **Password**—Enter the password.
   - **Retype**—Retype the password.
8. Click **Ok**.

Configuring Wired Port Profiles on Instant APs

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

The access point ports of an Instant 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 settings, complete the following steps in each of the tabs:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Access Points Ports**. The **Wired Port Profiles** page is displayed.
4. To create a new SSID profile, click the **+ Add Port Profiles**. The **Create a New Network** pane is displayed.

Complete the configuration for each of the tabs in the **Create a New Network** page as described in the below sections:

Configuring General Network Profile Settings

To configure general network profile settings, complete the following steps in the **General** tab:

1. Enter a name that is used to identify the network in the **Port Profile Name** box.
2. Under **Advanced Settings** section, configure the following parameters:

   a. **Speed/Duplex**—Ensure that appropriate values are selected for **Speed/Duplex**. Contact your network administrator if you need to assign speed and duplex parameters.

   b. **PoE**—Set **PoE** to **Enabled** to enable Power over Ethernet.

   c. **Admin Status**—The **Admin Status** indicates if the port is up or down.

   d. **Content Filtering**—To ensure that all DNS requests to non-corporate domains on this wired port network are sent to OpenDNS, select **Enabled** for **Content Filtering**.

   e. **Uplink**—Select **Enabled** to configure uplink on this wired port profile. If **Uplink** is set to **Enabled** and this network profile is assigned to a specific port, the port is enabled as an Uplink port.

   f. **Spanning Tree**—Set the **Spanning Tree** to **Enabled** 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 Instant APs with three or more ports. By default, STP is disabled on wired port profiles.

   g. **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.

   h. **802.3az**—Select **Enabled** 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 Instant APs that support a minimum of Aruba Instant 8.4.0.0 firmware version.
3. Click **Next**. The **VLANs** pane is displayed.

Configuring VLAN Settings

To configure VLAN-specific settings, complete the following steps in the **VLAN** tab:

1. On the VLANs pane, configure VLANs for the wired port network:

   a. **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.
   - **Trunk**—Select this mode to allow the port to carry packets for multiple VLANs specified as allowed VLANs.

   b. Specify any of the following values for **Client IP Assignment**:

   - **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.
   - **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.

   c. If the **Trunk** mode is selected:

   - Specify the **Allowed VLAN**, enter a list of comma separated digits or ranges 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.

d. 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.

2. Click **Next**. The **Security** pane details are 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**—Select **Enabled** to enable 802.1X authentication. Configure the basic parameters such as the authentication server, and MAC Authentication Fail-Through. Select any of the following options for authentication server:
  - **New**—On selecting this option, an external RADIUS server must be configured to authenticate the users. For information on configuring an external server, see Configuring External Authentication Servers for an Instant AP Cluster on page 294.
  - **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 this to **Enabled** 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 on page 294.
- **MAC Authentication**—To enable MAC authentication, select **Enabled**. The MAC authentication is disabled by default.
- **Captive Portal**—Select **Enabled** captive portal authentication. For more information on configuring security on captive portal, see Configuring Access Points Ports Networks on Guest Users on Instant APs.
- **Open**—Select **Enabled** to set security for open network.

2. Enable the **Port Type Trusted** option to connect uplink and downlink to a trusted port only.
3. In the **Primary Server** field, perform one of the following steps:

- **Internal Server**—To use an internal server, select Internal Server and add the clients that are required to authenticate with the internal RADIUS Server. Click **Users** to add the users. To add a new server, click +. For information on configuring external servers, see Configuring External Servers for Authentication on page 1.
- **Secondary Server**—To add another server for authentication, configure another authentication server.
  - **Load Balancing**—Select **Enabled** 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 on page 294.

4. **MAC Authentication Fail-Thru**—Select **Enabled** 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**—Select **Enabled** to configure client IP address as calling station ID and enter the **Called Station ID Type** as follows:
  - **Access Point Group**—Uses the VC ID as the called station ID.
  - **Access Point Name**—Uses the host name of the Instant 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 Instant AP as the called station ID.
- **MAC address**—Uses the MAC address of the Instant AP as the called station ID.

- **Reauth Interval**—Specify the interval at which all associated and authenticated clients must be reauthenticated.

6. Click **Next**. The **Access** pane is displayed.

Configuring Access Settings

To configure access-specific settings, complete the following steps in the **Access** tab:

1. Enable the **Downloadable User** option to allow downloading of pre-existing user roles. The CPPM Settings table with **Name**, **CPPM Username** and **Actions** columns related to the radius servers are displayed.

The Downloadable User Role feature is optional.

The Downloadable User Roles feature is available only for networks that include APs that run a minimum of Aruba Instant 8.4.0.0 firmware version with a minimum of ClearPass server version 6.7.8.

At least one radius server must be configured to apply the Downloadable User Roles feature. For more information on configuring radius server, see Authentication Servers for Instant 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 SSID successfully.

Configuring Network Port Profile Assignment

To map the Access Point Ports profile to Ethernet ports, perform the following:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Access Points Ports**. The **Wired Port Profiles** page is displayed.
4. In the **Port Profiles Assignments** section, assign wired port profiles to Ethernet ports:

   e. Select a profile from the **0/0** drop down list.

   f. Select the profile from the **0/1** drop down list.

   g. If the Instant AP supports Enet2, Enet3 and Enet4 ports, assign profiles to these ports by selecting a profile from the **0/2**, **0/3**, and **0/4** drop-down list respectively.
5. Click **Save Settings**.

Viewing Summary Table

You can view the list of Access Point Ports profile that are configured in the **Wireless Management** >**Access Point Ports** page in the summary table of **Create a New Network** page. The table includes the list of Access Point Ports SSID profiles with the following details:

- **Name—**Displays the name provided to the SSID profile.
- **Type—**Indicates the type of SSIDs, for example, **Mixed Traffic**, or **Voice**.
- **Access Type—**Displays scope of access to the SSID profile, for example, **Unrestricted**, **network-based**, or **Restricted**.
- **Actions**—Includes actions to enable or disable the Wi-Fi, edit the SSID profile, and delete the SSID profile.

Editing a Network Profile

To edit a network profile, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Networks**. The **Networks** page is displayed.
4. Select the network that you want to edit.
5. Click the **Edit** icon under the **Actions** column. The network details are displayed.
6. Modify the profile.
7. Save the changes.

Deleting a Network Profile

To delete a network profile, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Networks**. The **Networks** page is displayed.
4. Select the network that you want to delete.
5. Click the **Delete** icon under **Actions** column.
6. Click **OK** to confirm deletion.

Mesh Network and Mesh Instant AP

Mesh Network Overview

The mesh solution effectively expands and configures network coverage for outdoor and indoor enterprises in a wireless environment. The mesh network automatically reconfigures broken or blocked paths when traffic traverses across mesh Instant AP. This feature provides increased reliability by allowing the network to continue operating even when an Instant AP is non-functional or if the device fails to connect to the network.

A mesh network requires at least one valid wired or 3G uplink connection.

The mesh network must be provisioned by plugging into the wired network for the first time.

Mesh Instant APs

The Instant APs that are configured for mesh can either operate as mesh portals or as mesh points based on the uplink type.

Instant AP as Mesh Portal

Any provisioned Instant AP that has a valid wired or 3G uplink connection functions as a mesh portal. A mesh portal acts as a gateway between the wireless mesh network and the enterprise wired LAN. The mesh roles are automatically assigned based on the Instant AP configuration. The mesh portal can also act as a virtual controller.

The mesh portal reboots after 5 minutes when it loses its uplink connectivity to a wired network.

Instant AP as Mesh Point

The Instant AP without an ethernet link functions as a mesh point. The mesh point establishes an all-wireless path to the mesh portal and provides traditional WLAN services such as client connectivity, IDS capabilities, user role association, and QoS for LAN-to-mesh communication to the clients, and performs mesh backhaul or network connectivity. The mesh points authenticate to the mesh portal and establish a secured link using AES encryption.

A mesh point also supports LAN bridging by connecting any wired device to the downlink port of the mesh point. In the case of single ethernet port platforms such as Instant AP-105, you can convert the Eth0 uplink port to a downlink port by enabling Eth0 Bridging.

Redundancy is observed in a mesh network when two Instant APs have valid uplink connections, and most mesh points try to mesh directly with one of the two portals.

There can be a maximum of eight mesh points per mesh portal in a mesh network. When mesh Instant APs boot up, they detect the environment to locate and associate with their nearest neighbor. The mesh Instant APs determine the best path to the mesh portal ensuring a reliable network connectivity.

In a dual-radio Instant AP, the 2.4 GHz radio is always used for client traffic, and the 5 GHz radio is always used for both mesh-backhaul and client traffic.

Automatic Mesh Role Assignment

Aruba Central supports enhanced role detection during Instant AP boot-up and Instant 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.

Mesh Role Detection during System Boot-Up

If the ethernet link is down during Instant AP boot-up, the Instant AP acts as a mesh point. If the ethernet link is up, the Instant AP continues to detect if the network is reachable in the following scenarios:

- In a static IP address scenario, the Instant AP acts as a mesh portal if it successfully pings the gateway. Otherwise, it acts as a mesh point.
- In case of DHCP, the Instant AP acts as a mesh portal when it obtains the IP address successfully. Otherwise, it acts as a mesh point.
- In case of IPv6, Instant APs do not support the static IP address but only support DHCP for detection of network reachability.

If the Instant AP has a 3G or 4G USB modem plugged, it always acts as a mesh portal. If the Instant AP is set to Ethernet 0 bridging, it always acts as a mesh point.

Mesh Role Detection during System Running Time

The mesh point uses the Loop Protection for Secure Jack Port feature to detect the loop when the ethernet is up. If the loop is detected, the Instant AP reboots. Otherwise, the Instant AP does not reboot and the mesh role continues to act as a mesh point.

Setting up Instant Mesh Network

- To provision Instant APs as mesh Instant APs:
- Connect the Instant APs to a wired switch.
- Ensure that the virtual controller key is synchronized and the country code is configured.
- Ensure that a valid SSID is configured on the Instant AP.
- If the Instant AP has a factory default SSID (Instant SSID), delete the SSID.
- If an ESSID is enabled on the virtual controller, disable it and reboot the Instant AP cluster.
- Disconnect the Instant APs that you want to deploy as mesh points from the switch, and place the Instant APs at a remote location. The Instant APs come up without any wired uplink connection and function as mesh points. The Instant APs with valid uplink connections function as mesh portals.

Configuring Wired Bridging on Ethernet 0 for Mesh Point

Aruba Central supports wired bridging on the Ethernet 0 port of anInstant AP. You can configure wired bridging, if the Instant AP is configured to function as a mesh point.

Perform the following steps to configure support for wired bridging on the Ethernet 0 port of an Instant AP from Aruba Central UI:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the navigation pane, click the **Access Points** tab. The **Access Points** page opens.
4. To edit an Instant AP, click the edit icon corresponding to the AP. The edit pane to modify the Instant AP parameters opens.
5. Expand the **Uplink** section.
6. To configure a non-native uplink VLAN, specify the number of VLANs in the **Uplink Management VLAN** text box.
7. Enable the **Eth0 Bridging** toggle button.

8. Click **OK**.
9. Reboot the Instant AP.

Mesh Cluster Function

Aruba Central introduces the mesh cluster function for easy deployments of Instant APs. You can configure the ID, password, and also provision Instant APs to a specific mesh cluster.

In a cluster-based scenario, you can configure unlimited mesh profiles in a network. When an Instant AP boots up, it attempts to find a mesh cluster configuration. The Instant AP fetches a pre-existing mesh cluster configuration, if any. Otherwise, it uses the default mesh configuration in which the SSID, password, and cluster name are generated by the virtual controller key.

Instant APs that belong to the same mesh network can establish mesh links with each other. The Instant APs can establish a mesh link in a standalone scenario also. However, the network role election does not take place in a standalone environment. Users can set the same mesh cluster configuration to establish mesh links with other networks. For more information on mesh cluster configuration, refer to the *Mesh Instant AP Configuration* chapter of *Aruba Instant 8.4.0.0 User Guide*.

Configuring Time-Based Services for Wireless Network Profiles

Aruba Central allows you to configure the availability of a WLAN SSID at a particular time of the day. You can now create a time range profile and assign it to a WLAN SSID, so that you can enable or disable access to the SSID and thus control user access to the network during a specific time period.

Instant 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.

Before You Begin

Before you configure time-based services, ensure that the NTP server connection is active.

Creating a Time Range Profile

To create a time range profile, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **System**. The **System** page opens.
4. Click **Time-Based Services**.
5. Click **+** under the time range profiles in the Time-Based Profiles table. The **New profile** window for creating a time range profile opens. Configure the parameters that are listed in the following table:

Table 75: *Time Range Profile Configuration Parameters*

Parameter	Description
Name	Specify a name for the time range profile.
Type	Select the type of time range profile: ■ **Periodic**—Allows you configure a specific periodicity and recurrence pattern for a time range profile. ■ **Absolute**—Allows you to configure an absolute day and time range.
Repeat	Specify the frequency for the periodic time range profile: ■ **Daily**—Enables daily recurrence. ■ **Weekly**—Allows you define a specific time range with specific start and end days in a week.
Day Range	**Absolute Time Range** 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. **Periodic Time Range** For a periodic time range profile, the following **Day Range** options are available: ■ For daily recurrence—If the **Repeat** option is set to **Daily**, this field allows you to select the following time ranges: ● **Monday—Sunday (All Days)** ● **Monday—Friday (Weekdays)** ● **Saturday—Sunday (Weekend)** 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. ■ 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. For example, if you set **Start day** as Monday and **End day** as Friday, and **Start time** as 1 and **End time** as 2, the applied time range profile is Monday 1 am to Friday 2 am every week; that is, on Monday at 3 am, the profile will be applied or enabled.
Start Time	Select the start time for the time range profile from the **Hours** and **Minutes** drop-down lists, respectively.
End Time	Select the end time for the time range profile from the **Hours** and **Minutes** drop-down lists, respectively.
Visualization Graph for Time	The Visualization graph (approximated to the hour) provides a visual display of the selected time range (Day range, Start Time, and End Time) for periodic profiles.

Associating a Time Range Profile to an SSID

To apply a time range profile to an SSID, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Networks**. The **Networks** page is displayed.
4. Click the edit icon next to the SSID for which you want to apply the time range profile. You can also add a time range profile when configuring an SSID.
5. Click **Time Range Profiles**.

6. Select a time range profile from the list and select a value from the **Status** drop-down list.
   - When a time range profile is enabled on SSID, the SSID is made available to the users for the configured time range. For example, if the specified time range is 12:00 to 13:00, the SSID becomes available only between 12 PM to 1 PM on a given day.
   - If a time range is disabled, the SSID becomes unavailable for the configured time range. For example, if configured time-range is 14:00 to 17:00, the SSID is made unavailable from 2 PM to 5 PM on a given day.
7. Click **Save**.

Associating a Time Range Profile to ACL

Aruba Central allows you to configure time-based services for specific ACL. To apply a time range profile to an access rule, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Security**. The **Security** page is displayed.
4. In the Roles section, click the edit icon listed for access rules under **Access Rules For Selected Roles** to which you want to apply the time range profile.
5. The **Access Rule** page is displayed.
6. In the **Options** section, select the **Time Range** check box and select the time range profile from the drop-down list.
   - When a time range profile is associated with an ACL, the configured time range is applied on all the WLAN SSID with the specific ACL.
   - If a time range is disabled or if the time range profile is deleted for an ACL, all WLAN SSID with the specific ACL will be able to access the network without any time constraint.
7. Click **Save**.

For more information on time range configuration, see the *Aruba Instant User Guide*.

Configuring ARM and RF Parameters on Instant APs

This section provides the following information:

ARM Overview

ARM is a radio frequency management technology that optimizes WLAN performance even in the networks with highest traffic by dynamically and intelligently choosing the best 802.11 channel and transmitting power for each Instant AP in its current RF environment. ARM works with all standard clients, across all operating systems, while remaining in compliance with the IEEE 802.11 standards. It does not require any proprietary client software to achieve its performance goals. ARM ensures low-latency roaming, consistently high performance, and maximum client compatibility in a multi-channel environment. By ensuring the fair distribution of available Wi-Fi bandwidth to mobile devices, ARM ensures that data, voice, and video applications have sufficient network resources at all times. ARM allows mixed 802.11a, b, g, n, and ac client types to inter operate at the highest performance levels.

When ARM is enabled, an Instant AP dynamically scans all 802.11 channels within its 802.11 regulatory domain at regular intervals and sends reports on WLAN coverage, interference, and intrusion detection to the Virtual

Controller. ARM computes coverage and interference metrics for each valid channel, chooses the best performing channel, and transmit power settings for each Instant AP RF environment. Each Instant AP gathers other metrics on its ARM-assigned channel to provide a snapshot of the current RF health state.

Instant APs support the following ARM features:

- Channel or Power Assignment—Assigns channel and power settings for all the Instant APs in the network according to changes in the RF environment.
- Voice Aware Scanning—Improves voice quality by preventing an Instant AP from scanning for other channels in the RF spectrum during a voice call and by allowing an Instant AP to resume scanning when there are no active voice calls.
- Load Aware Scanning—Dynamically adjusts the scanning behavior to maintain uninterrupted data transfer on resource intensive systems when the network traffic exceeds a predefined threshold.
- Bandsteering—Assigns the dual-band capable clients to the 5 GHz band on dual-band Instant APs thereby reducing co-channel interference and increasing the available bandwidth for dual-band clients.
- Client Match—Continually monitors the RF neighborhood of the client to support the ongoing band steering and load balancing of channels, and enhanced Instant AP reassignment for roaming mobile clients.

When Client Match is enabled on 802.11n capable Instant APs, the Client Match feature overrides any settings configured for the legacy band steering, station hand-off assist or load balancing features. The 802.11ac capable Instant APs do not support the legacy band steering, station hand off or load balancing settings, so these Instant APs must be managed using Client Match.

- Airtime Fairness—Provides equal access to all clients on the wireless medium, regardless of client type, capability, or operating system to deliver uniform performance to all clients.

For more information on ARM features supported by the APs, see the *Aruba Instant User Guide*.

Configuring ARM Features

To configure ARM features such as band steering, and airtime fairness mode and Client Match, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **RF**. The **RF** page opens.
4. Under **Adaptive Radio Management(ARM)**, the **Client Control** section display the following components: **Band Steering Mode, Airtime Fairness Mode**, **ClientMatch, ClientMatch Calculating Interval** ,**ClientMatch Neighbor Matching, ClientMatch Threshold**, **Spectrum Load Balancing Mode**.
5. For **Band Steering Mode**, configure the following parameters:

Table 76: *Band Steering Mode Configuration Parameters*

Data pane item	Description
Prefer 5 GHz	Enables band steering in the 5 GHz mode. On selecting this, the Instant AP steers the client to the 5 GHz band (if the client is 5 GHz capable), but allows the client connection on the 2.4 GHz band if the client persistently attempts for 2.4 GHz association.
Force 5 GHz	Enforces 5 GHz band steering mode on the Instant APs.
Balance Bands	Allows the Instant AP to balance the clients across the two radios to best utilize the available 2.4 GHz bandwidth. This feature takes into account the fact that the 5 GHz band has more channels than the 2.4 GHz band, and that the 5 GHz channels operate in 40 MHz, while the 2.5 GHz band operates in 20 MHz.
Disable	Allows the clients to select the band to use.

6. For **Airtime Fairness Mode**, specify any of the following values:

Table 77: *Airtime Fairness Mode Configuration Parameters*

Data Pane Item	Description
Default Access	Allows access based on client requests. When **Air Time Fairness** is set to default access, per user and per SSID bandwidth limits are not enforced.
Fair Access	Allocates air time evenly across all the clients.
Preferred Access	Sets a preference where 802.11n clients are assigned more air time than 802.11a/11g. The 802.11a/11g clients get more airtime than 802.11b. The ratio is 16:4:1.

7. For **Client Match**, configure the following parameters:

Table 78: *Additional ARM Configuration Parameters*

Data Pane Item	Description
Client Match	Enables the Client Match feature on APs. When enabled, client count is balanced among all the channels in the same band. When Client Match is enabled, ensure that scanning is enabled. **NOTE:** When the Client Match is disabled, channels can be changed even when the clients are active on a BSSID.
Client MatchCalculating Interval	Configures a value for the calculating interval of Client Match. The interval is specified in seconds and the default value is 30 seconds. You can specify a value within the range of 10-600.
Client MatchNeighbor Matching%	Configures the calculating interval of Client Match. This number takes into account the least similarity percentage to be considered as in the same virtual RF neighborhood of Client Match. You can specify a percentage value within the range of 20-100. The default value is 75%.

Data Pane Item	Description
Client MatchThreshold	Configures a Client Match threshold value. This number takes acceptance client count difference among all the channels of Client Match. When the client load on an AP reaches or exceeds the threshold in comparison, Client Match is enabled on that AP. You can specify a value within range of 1-20. The default value is 2.
Spectrum Load Balancing Mode	Enables the **Specturm Load Balancing Mode** to determine the balancing strategy for Client Match. The following options are available: ■ Channel ■ Radio ■ Channel + Radio

8. Click **Access Point Control**, and configure the following parameters:

Table 79: *AP Control Configuration Parameters*

Data pane item	Description
Customize Valid Channels	Allows you to select a custom list of valid 20 MHz and 40 MHz channels for 2.4 GHz and 5 GHz bands. By default, the AP uses valid channels as defined by the Country Code (regulatory domain). On selecting **Customize Valid Channels**, a list of valid channels for both 2.4.GHz and 5 GHz are displayed. The valid channel customization feature is disabled by default. The valid channels automatically show in the **static channel assignment** data pane.
Min Transmit Power	Allows you to configure a minimum transmission power within a range of 3 to 33 dBm in 3 dBm increments. If the minimum transmission EIRP setting configured on an AP is not supported by the AP model, this value is reduced to the highest supported power setting. The default value for minimum transmit power is 18 dBm.
Max Transmit Power	Allows you to configure the maximum transmission power within a range of 3 to 33 dBm in 3 dBm increments. If the maximum transmission EIRP configured on an AP is not supported by the local regulatory requirements or AP model, the value is reduced to the highest supported power settings.
Client Aware	Allows ARM to control channel assignments for the Instant APs with active clients. When the Client Match mode is set to **Disabled**, an Instant AP may change to a more optimal channel, which disrupts current client traffic. The **Client Aware** option is **Enabled** by default.
Scanning	Allows the Instant 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. **NOTE:** For Client Match configuration, ensure that scanning is enabled.
Wide Channel Bands	Allows the administrators to configure 40 MHz channels in the 2.4 GHz and 5.0 GHz bands. 40 MHz channels are two 20 MHz adjacent channels that are bonded together. The 40 MHz channel effectively doubles the frequency bandwidth available for data transmission. For high performance, you can select 5 GHz. If the AP density is low, enable in the 2.4 GHz band.
80 MHz Support	Enables or disables the use of 80 MHz channels on APs. This feature allows ARM to assign 80 MHz channels on APs with 5 GHz radios, which support a very high throughput. This setting is enabled by default. **NOTE:** Only the APs that support 802.11ac can be configured with 80 MHz channels.

9. Click **Save Settings**.

Configuring Radio Parameters

To configure RF parameters for the 2.4 GHz and 5 GHz radio bands on an Instant AP, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **RF**. The **RF** page opens.
4. Click **Radio**.
5. Under 2.4 GHz, 5 GHz, or both, configure the following parameters.

Table 80: *Radio Configuration Parameters*

Data Pane Item	Description
Zone	Allows you to configure a zone per radio band for Instant APs in a cluster. You can also configure an RF zone per Instant AP. **NOTE:** Aruba recommends that you configure RF zone for either individual AP or for the cluster. Any discrepancy in the RF zone names may lead to configuration errors.
Legacy Only	When set to **ON**, the Instant AP runs the radio in the non-802.11n mode. This option is set to **OFF** by default.
802.11d / 802.11h	When set to **ON**, the radios advertise their 802.11d (Country Information) and 802.11h (Transmit Power Control) capabilities. This option is set to **OFF** by default.
Beacon Interval	Configures the beacon period for the Instant AP in milliseconds. This indicates how often the 802.11 beacon management frames are transmitted by the AP. You can specify a value within the range of 60–500. The default value is 100 milliseconds.
Interference Immunity Level	Configures the immunity level to improve performance in high-interference environments. The default immunity level is 2. ■ **Level 0** — No ANI adaptation. ■ **Level 1** — Noise immunity only. This level enables power-based packet detection by controlling the amount of power increase that makes a radio aware that it has received a packet. ■ **Level 2** — Noise and spur immunity. This level also controls the detection of OFDM packets, and is the default setting for the Noise Immunity feature. ■ **Level 3** — Level 2 settings and weak OFDM immunity. This level minimizes false detects on the radio due to interference, but may also reduce radio sensitivity. This level is recommended for environments with a high-level of interference related to 2.4 GHz appliances such as cordless phones. ■ **Level 4** — Level 3 settings, and FIR immunity. At this level, the AP adjusts its sensitivity to in-band power, which can improve performance in environments with high and constant levels of noise interference. ■ **Level 5** — The AP completely disables PHY error reporting, improving performance by eliminating the time the Instant AP spends on PHY processing. **NOTE:** Increasing the immunity level makes the AP lose a small amount of range.
Channel Switch Announcement Count	Configures the number of channel switching announcements to be sent before switching to a new channel. This allows the associated clients to recover gracefully from a channel change.

Table 80: *Radio Configuration Parameters*

Data Pane Item	Description
Background Spectrum Monitoring	When set to **ON**, the APs in the access mode continue with their normal access service to clients, while performing additional function of monitoring RF interference (from both neighboring APs and non Wi-Fi sources such as, microwaves and cordless phones) on the channel they are currently serving the clients.
Customize ARM Power Range	Configures a minimum (Min Power) and maximum (Max Power) power range value for the 2.4 GHz and 5GHz band frequencies. The default value is 3 dBm. Unlike the configuration in the ARM profile, the transmit power of all radios in the Radio profile do not share the same configuration.
Enable 11ac	When set to **ON**, VHT is enabled on the 802.11ac devices for the 5GHz radio band. If VHT is enabled for the 5 GHz radio profile on an Instant AP, it is automatically enabled for all SSIDs configured on an Instant AP. By default, VHT is enabled on all SSIDs. **NOTE:** If you want the 802.11ac Instant APs to function as 802.11n Instant APs, clear this check box to disable VHT on these devices.
Smart antenna	Set to **Enabled** to combine an antenna array with a digital signal-processing capability to transmit and receive in an adaptive, spatially sensitive manner.
ARM/WIDS Override	When **ARM/WIDS Override** is off, the Instant AP will always process frames for WIDS. WIDS is an application that detects the attacks on a wireless network or wireless system. purposes even when it is heavily loaded with client traffic. When **ARM/WIDS Override** is on, the Instant AP will stop process frames for WIDS.

6. Click **Save Settings**.

Configuring IDS Parameters on Instant APs

Aruba Central supports the IDS feature that monitors the network for the presence of unauthorized Instant APs and clients. It also logs information about the unauthorized Instant 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. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click Wireless IDS/IPS. The **IDS** page opens.
4. Configure the following options:

- **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.
- **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. The detection levels can be configured using the **IDS** pane. The following levels of detection can be configured in the WIP Detection page:

- **Off**
- **Low**
- **Medium**
- **High**

The following table describes the detection policies enabled in the Infrastructure Detection **Custom settings** field.

Table 81: *Infrastructure Detection Policies*

Detection level	Detection policy
Off	Rogue Classification
Low	■ **Detect AP Spoofing** ■ **Detect Windows Bridge** ■ **IDS Signature — Deauthentication Broadcast** ■ **IDS Signature — Deassociation Broadcast**
Medium	■ **Detect ad hoc networks using VALID SSID** ■ **Detect Malformed Frame — Large Duration**
High	■ **Detect AP Impersonation** ■ **Detect ad hoc Networks** ■ **Detect Valid SSID Misuse** ■ **Detect Wireless Bridge** ■ **Detect 802.11 40 MHz intolerance settings** ■ **Detect Active 802.11n Greenfield Mode** ■ **Detect AP Flood Attack** ■ **Detect Client Flood Attack** ■ **Detect Bad WEP** ■ **Detect CTS Rate Anomaly** ■ **Detect RTS Rate Anomaly** ■ **Detect Invalid Address Combination** ■ **Detect Malformed Frame — HT IE** ■ **Detect Malformed Frame — Association Request** ■ **Detect Malformed Frame — Auth.** ■ **Detect Overflow IE** ■ **Detect Overflow EAPOL Key** ■ **Detect Beacon Wrong Channel** ■ **Detect devices with invalid MAC OUI**

The following table describes the detection policies enabled in the Client Detection **Custom settings** field.

Table 82: *Client Detection Policies*

Detection level	Detection policy
Off	All detection policies are disabled.
Low	Detect Valid Station Misassociation
Medium	■ **Detect Disconnect Station Attack** ■ **Detect Omerta Attack** ■ **Detect FATA-Jack Attack** ■ **Detect Block ACK DOS** ■ **Detect Hotspotter Attack** ■ **Detect unencrypted Valid Client** ■ **Detect Power Save DOS Attack**
High	■ **Detect EAP Rate Anomaly** ■ **Detect Rate Anomaly** ■ **Detect Chop Chop Attack** ■ **Detect TKIP Replay Attack** ■ **IDS Signature — Air Jack** ■ **IDS Signature — ASLEAP**

The following levels of detection can be configured in the WIP Protection page:

- **Off**
- **Low**
- **High**

The following table describes the protection policies that are enabled in the Infrastructure Protection **Custom settings** field.

Table 83: *Infrastructure Protection Policies*

Protection level	Protection policy
Off	All protection policies are disabled
Low	■ Protect SSID — Valid SSID list is auto derived from AP configuration ■ Rogue Containment
High	■ Protect from Adhoc Networks ■ Protect AP Impersonation

The following table describes the detection policies that are enabled in the Client Protection **Custom settings** field.

Table 84: *Client Protection Policies*

Protection level	Protection policy
Off	All protection policies are disabled
Low	Protect Valid Station
High	Protect Windows Bridge

Containment Methods

You can enable wired and wireless containment measures to prevent unauthorized stations from connecting to your Aruba Central network.

Aruba Central supports the following types of containment mechanisms:

- Wired containment — When enabled, Instant 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.

The FCC and some third parties have alleged that under certain circumstances, the use of containment functionality violates 47 U.S.C. §333. Before using any containment functionality, ensure that your intended use is allowed under the applicable rules, regulations, and policies. Aruba is not liable for any claims, sanctions, or other direct, indirect, special, consequential or incidental damages related to your use of containment functionality.

Configuring Authentication and Security Profiles on Instant APs

This section describes the authentication and security parameters to configure on an Instant AP provisioned in:

- Supported Authentication Methods on page 286
- Authentication Servers for Instant APs on page 292
- Configuring External Authentication Servers for an Instant AP Cluster on page 294
- Configuring Users Accounts for the Instant AP Management Interface on page 296
- Configuring Guest and Employee User Profiles on Instant APs on page 297
- Configuring Roles and Policies on Instant APs for User Access Control on page 298
- Enabling ALG Protocols on Instant APs on page 311
- Blacklisting Instant AP Clients on page 311

Supported Authentication Methods

Authentication is a process of identifying a user through a valid username and password. Clients can also be authenticated based on their MAC addresses.

The authentication methods supported by the Instant 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 Instant AP. The wireless client can pass data traffic only after successful 802.1X authentication.

The NAS acts as a gateway to guard access to a protected resource. A client connecting to the wireless network first connects to the NAS.

Configuring 802.1X Authentication for a Network Profile

To configure 802.1X authentication for a wireless network profile, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Networks**. The **Networks** page opens.
4. Select a network profile for which you want to enable 802.1X authentication, and click **Edit**.
5. In **Edit <profile-name>**, ensure that all required WLAN and VLAN attributes are defined, and then click the **Security** tab.
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 Instant 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 Instant 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.

Configuring MAC Authentication for a Network Profile

To configure MAC authentication for a wireless profile, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Networks**. The **Networks** page opens.

4. Select a network profile for which you want to enable MAC authentication and click **Edit**.
5. In the **Edit <profile-name>,** ensure that all required WLAN and VLAN attributes are defined, and then click the **Security** tab**.**
6. In **Security**, for **MAC Authentication**, select **Enabled** for **Personal** or **Open** security level.
7. Specify the type of authentication server to use.
8. Click **Save Settings**.

MAC Authentication with 802.1X Authentication

The administrators can enable MAC authentication for 802.1X authentication. MAC authentication shares all the authentication server configurations with 802.1X authentication. If a wireless or wired client connects to the network, MAC authentication is performed first. If MAC authentication fails, 802.1X authentication does not trigger. If MAC authentication is successful, 802.1X authentication is attempted. If 802.1X authentication is successful, the client is assigned an 802.1X authentication role. If 802.1X authentication fails, the client is assigned a **deny-all** role or **mac-auth-only** role.

You can also configure the following authentication parameters for MAC+802.1X authentication:

- MAC authentication only role—Allows you to create a **mac-auth-only** role to allow role-based access rules when MAC authentication is enabled for 802.1X authentication. The **mac-auth-only** role is assigned to a client when the MAC authentication is successful and 802.1X authentication fails. If 802.1X authentication is successful, the **mac-auth-only** role is overwritten by the final role. The **mac-auth-only** role is primarily used for wired clients.
- L2 authentication fall-through—Allows you to enable the **l2-authentication-fallthrough** mode. When this option is enabled, the 802.1X authentication is allowed even if the MAC authentication fails. If this option is disabled, 802.1X authentication is not allowed. The **l2-authentication-fallthrough** mode is disabled by default.

Configuring MAC Authentication with 802.1X Authentication

To configure MAC authentication with 802.1X authentication for wireless network profile, configure the following parameters:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Networks**. The **Networks** page opens.
4. Select a network profile for which you want to enable MAC and 802.1X authentication and click **Edit**.
5. Click **Security**.
6. Select **Perform MAC Authentication Before 802.1X** to use 802.1X authentication only when the MAC authentication is successful.
7. Select **MAC Authentication Fail Through** to use 802.1X authentication even when the MAC authentication fails.
8. Click **Save Settings**.

Captive Portal Authentication

Captive portal authentication is used for authenticating guest users. For more information, see Configuring Wireless Networks on Guest Users on Instant APs on page 253.

MAC Authentication with Captive Portal Authentication

The following conditions apply to a network profile with MAC authentication and Captive Portal authentication enabled:

- If the captive portal splash page type is **Internal-Authenticated** or **External-RADIUS Server**, MAC authentication reuses the server configurations.
- If the captive portal splash page type is **Internal-Acknowledged** or **External-Authentication Text** and MAC authentication is enabled, a server configuration page is displayed.
- If the captive portal splash page type is **none**, MAC authentication is disabled.

The MAC authentication with captive portal authentication supports the **mac-auth-only** role.

Configuring MAC Authentication with Captive Portal Authentication

To configure the MAC authentication with captive portal authentication for a network profile, complete the following steps:

1. Select an existing wireless profile for which you want to enable MAC with captive portal authentication.
2. Under **Access**, specify the following parameters for a network with **Role Based** rules:

   a. Select **Enforce Machine Authentication** when MAC authentication is enabled for captive portal. If the MAC authentication fails, the captive portal authentication role is assigned to the client.

   b. For wireless network profile, select **Enforce MAC Auth Only Role** when MAC authentication is enabled for captive portal. After successful MAC authentication, the **MAC auth only** role is assigned to the client.
3. Click **Next** and then click **Save Settings**.

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 on Guest Users on Instant APs on page 253.

WISPr Authentication

WISPr authentication allows a smart client to authenticate on the network when they roam between wireless Internet service providers, even if the wireless hotspot uses an ISP with whom the client may not have an account.

If a hotspot is configured to use WISPr authentication in a specific ISP and a client attempts to access the Internet at that hotspot, the WISPr AAA server configured for the ISP authenticates the client directly and allows the client to access the network. If the client only has an account with a *partner* ISP, the WISPr AAA server forwards the client's credentials to the partner ISP's WISPr AAA server for authentication. When the client is authenticated on the partner ISP, it is also authenticated on your hotspot's own ISP as per their service agreements. The Instant AP assigns the default WISPr user role to the client when your ISP sends an authentication message to the Instant AP.

Instant APs support the following smart clients:

- iPass
- Boingo

These smart clients enable client authentication and roaming between hotspots by embedding iPass Generic Interface Specification (GIS) *redirect*, *authentication*, and *logoff* messages within HTML messages that are sent to the Instant AP.

Configuring WISPr Authentication

To configure WISPr authentication, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **System**. The **System** page opens.
4. Under **WISPr**, configure the following parameters:

- **ISO Country Code**—The ISO Country Code for the WISPr Location ID.
- **E.164 Area Code**—The E.164 Area Code for the WISPr Location ID.
- **Operator Name**—The operator name of the hotspot.
- **E.164 Country Code**—The E.164 Country Code for the WISPr Location ID.
- **SSID/Zone**—The SSID/Zone for the WISPr Location ID.
- **Location Name**—Name of the hotspot location. If no name is defined, the name of the Instant AP, to which the user is associated, is used.

5. Click **Save Settings** to apply the changes.

The WISPr RADIUS attributes and configuration parameters are specific to the RADIUS server used by your ISP for the WISPr authentication. Contact your ISP to determine these values. You can find a list of ISO and ITU country and area codes at the ISO and ITU websites (www.iso.org and http://www.itu.int).

A Boingo smart client uses a NAS identifier in the format <CarrierID>_<VenueID> for location identification. To support Boingo clients, ensure that you configure the NAS identifier parameter in the RADIUS server profile for the WISPr server.

Walled Garden

On the Internet, a walled garden typically controls access to web content and services. The Walled garden access is required when an external captive portal is used. For example, a hotel environment where the unauthenticated users are allowed to navigate to a designated login page (for example, a hotel website) and all its contents.

The users who do not sign up for the Internet service can view the allowed websites (typically hotel property websites). The website names must be DNS-based and support the option to define wildcards. When a user attempts to navigate to other websites that are not in the whitelist of the walled garden profile, the user is redirected to the login page. Instant AP supports Walled Garden only for the HTTP requests. For example, if you add yahoo.com in Walled Garden whitelist and the client sends an HTTPS request (https://yahoo.com), the requested page is not displayed and the users are redirected to the captive portal login page.

In addition, a blacklisted walled garden profile can also be configured to explicitly block the unauthenticated users from accessing some websites.

Configuring Walled Garden Access

To configure walled garden access, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Security**. The **Security** page opens.
4. Click **Walled Garden**.
5. To allow access to a specific set of websites, create a whitelist, click + and add the domain names. This allows access to a domain while the user remains unauthenticated. Specify a POSIX regular expression (regex(7)). For example:

- yahoo.com matches various domains such as news.yahoo.com, travel.yahoo.com and finance.yahoo.com
- www.apple.com/library/test is a subset of www.apple.com site corresponding to path /library/test/*

- favicon.ico allows access to /favicon.ico from all domains.

6. To deny users access to a domain, click + under Blacklist, and enter the domain name in the window. This prevents the unauthenticated users from viewing specific websites. When a URL specified in the blacklist is accessed by an unauthenticated user, Instant AP sends an HTTP 403 response to the client with an error message.
7. Save the changes.

Support for Multiple PSK in WLAN SSID

Aruba Central allows you to configure multiple PSK (MPSK) in WLAN network profiles that include APs running a minimum of Aruba Instant 8.4.0.0 firmware version and later. MPSK enhances the WPA2 PSK mode by allowing device-specific or group-specific passphrases, which are generated by ClearPass Policy Manager and sent to the Instant 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 Instant 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 Instant 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 Instant 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 Instant AP stores the MPSK passphrase in its local cache for client roaming. The cache is shared between all the Instant APs within a single cluster. The cache can also be shared with standalone Instant APs in a different cluster provided the APs belong to the same multicast VLAN. Each Instant AP first searches the local cache for the MPSK information. If the local cache has the corresponding MPSK passphrase, the Instant 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 Blacklisting

- MPSK and internal RADIUS server

Configuring Multiple PSK for Wireless Networks

1. Go to **Wireless Management** > **Wireless SSIDs** and click **+Add SSID**.
2. To modify an existing profile, go to **Wireless Management** > **Wireless SSIDs**, select a wireless SSID from the list of networks to edit.
3. Click the **Security** tab.
4. Select **Personal** from the **Security Level**. The authentication options applicable to the Enterprise network are displayed.
5. From the **Key Management** drop-down list, select the **MPSK-AES** option.
6. From the **Primary Server** drop-down list, select a server. The radius server selected from the list is the CPPM server.
7. Click **Next** to complete the encryption configuration.

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**.

When you select WPA3 as the encryption option in the **Key Management**, the **WPA3 Transition** option is displayed in the **Advanced Settings** section. Enable this option to allow transition from WPA3 to WPA2 and vice versa.

WPA3-Enterprise

WPA3-Enterprise enforces top secret security standards for an enterprise Wi-Fi in comparison to secret security standards. Top secret security standards includes:

- Deriving at least 384-bit PMK/MSK using Suite B compatible EAP-TLS.
- Securing pairwise data between STA and authenticator using AES-GCM-256.
- Securing group addressed data between STA and authenticator using AES-GCM-256.
- Securing group addressed management frames using BIP-GMAC-256.

Aruba Instant supports WPA3-Enterprise only in non-termination 802.1X and tunnel-forward modes. WPA3-Enterprise compatible 802.1x authentication occurs between STA and CPPM.

WPA3-Enterprise advertises or negotiates the following capabilities in beacons, probes response, or 802.11 association:

- AKM Suite Selector as 00-0F-AC:12
- Pairwise Cipher Suite Selector as 00-0F-AC:9
- Group data cipher suite selector as 00-0F-AC:9
- Group management cipher suite (MFP) selector as 00-0F-AC:12

If WPA3-Enterprise is enabled, STA is successfully associated only if it uses one of the four suite selectors for AKM selection, pairwise data protection, group data protection, and group management protection. If a STA mismatches any one of the four suite selectors, the STA association fails.

Configuring WPA3 for Enterprise Security for Wireless Network

1. Go to **Wireless Management** > **Wireless SSIDs** and click **+**.
2. To modify an existing profile, go to the **Wireless Management** > **Wireless SSIDs** page, select a WLAN SSID from the list of networks to edit.
3. Click the **Security** tab.
4. Select **Enterprise** from the **Security Level**. The authentication options applicable to the Enterprise network are displayed.
5. 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.
6. Click **Next**.

Configuring WPA3 for Personal Security

1. Go to the **Wireless Management** > **Wireless SSIDs** and click **+**.
2. To modify an existing profile, go to the **Wireless Management** > **Wireless SSIDs** page, select a WLAN SSID from the list of networks to edit.
3. Click the **Security** tab.
4. Select **Personal** from the **Security Level**. The authentication options applicable to the Enterprise network are displayed.
5. Select **WPA-3 Personal** from the **Key Management** drop-down list.
6. Click **Next**.

Authentication Servers for Instant 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 Instant 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 Instant 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 Instant 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 Instant 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 Instant 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 Instant 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.

Authentication Termination on Instant 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 Instant 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 Instant APs to perform load balancing of authentication requests destined to authentication servers such as RADIUS or LDAP.

The load balancing in Instant 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 an Instant AP Cluster

You can configure an external RADIUS server, TACACS or LDAP server for user authentication. To configure a server, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Security**. The **Security** page opens.
4. Click **Authentication Server**.
5. To create a new server, click **+**.
6. Configure any of the following types of server for authentication:

Table 85: *Authentication Server Configuration*

Type of Server	Parameters
RADIUS	Configure the following parameters: ■ **Name**—Name of the external RADIUS server. ■ **IP Address**— IP address or the FQDN of the external 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. ■ **Shared Key and Retype Shared Key**—Shared key for communicating with the external RADIUS server. ■ **Timeout**—The timeout duration for one RADIUS request. The Instant 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 Instant AP. You can specify a value within the range of 1–5. The default value is 3 requests. ■ **RFC 3576**—To allow the APs to process RFC 3576-compliant CoA and disconnect messages from the RADIUS server, select **Enabled**. Disconnect messages terminate the user session immediately, whereas the CoA messages modify session authorization attributes such as data filters. ■ **NAS IP Address**—Enter the VC IP address. The NAS IP address is the VC IP address that is sent in data packets. ■ **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 Instant 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. ■ **Dynamic RADIUS Proxy Parameters**—If Dynamic RADIUS Proxy is enabled in the system parameters of the Instant AP, configure the following dynamic RADIUS proxy 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** ● **MAC** ● **Captive Portal**
LDAP	Configure the following 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-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.

Type of Server	Parameters
	■ **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	Configure the following parameters: ■ **Name**—Name of the server. ■ **Shared Key and Retype Key**—The secret key to authenticate communication between the TACACS client and server. ■ **Auth Port**—The TCP IP port used by the server. The default port number is 49. ■ **Timeout**—A number between 1 and 30 seconds to indicate the timeout period for TACACS+ requests. The default value is 20 seconds. ■ **IP Address**—IP address of the server. ■ **Retry Count**—The maximum number of authentication attempts to be allowed. The default value is 3. ■ **Dead Time (in mins)**—Specify a dead time for authentication server in minutes. When two or more authentication servers are configured on the Instant 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.
Change of Authorization Only	Configure the following parameters: ■ **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.

7. Click **Save Server**.

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.

NOTE

You can also add an external RADIUS server by selecting New for Authentication Server when configuring a WLAN or wired profile.

Configuring Users Accounts for the Instant AP Management Interface

You can configure RADIUS or TACACS authentication servers to authenticate and authorize the management users of an Instant 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 Instant 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.

NOTE

In Aruba Central, the Instant 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 Instant APs provisioned in the template and UI groups. If a pre-configured Instant 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 Instant AP. In other words, Aruba Central hashes management user passwords irrespective of the management user configuration settings running on an Instant AP.

To configure authentication parameters for local admin, read-only, and guest management administrator account settings.

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.

3. On the left navigation pane, click **System**. The **System** page opens.
4. Under **Administrator**, configure the following parameters:

Table 86: *Configuration Parameters for the Instant AP Users*

Type of the User	Authentication Options	Steps to Follow
Client Control	**Internal**	Select **Internal** if you want to specify a single set of user credentials. If using an internal authentication server: 1. Enter a **Username** and **Password**. 2. Retype the password to confirm.
	Authentication server	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 w/ fallback to internal	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 (**username** and **password**) for internal server based authentication.
	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 Dynamic Load Balancing between Authentication Servers on page 294.
	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: 1. Specify a **Username** and **Password**. 2. Retype the password to confirm.
Guest Registration Only		To configure a guest user account with the read-only privileges: 1. Specify the **Username** and **Password**. 2. Retype the password to confirm.

3. Click **Save Settings**.

Configuring Guest and Employee User Profiles on Instant APs

The local database of an Instant 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 Instant 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. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Security**. The **Security** page opens.
4. Click **Users for Internal Server**.
5. Enter the username in the **Username** text box.
6. Enter the password in the **Password** text box and reconfirm.
7. Select a type of user from the **Type** drop-down list.
8. Click **Add** and click **OK.** The users are listed in the **Users** list.
9. To edit user settings:
   a. Select the user to modify under **Users**
   b. Click **Edit** to modify user settings.
   c. Click **OK**.
10. To delete a user:
    a. In the **Users** section, select the username to delete
    b. Click **Delete**.
    c. Click **OK**.
11. To delete all or multiple users at a time:
    a. Select the user names that you want to delete
    b. Click **Delete All**.
    c. Click **OK**.

Deleting a user only removes the user record from the user database, and will not disconnect the online user associated with the username.

Configuring Roles and Policies on Instant APs for User Access Control

Instant 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 Instant 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.

Instant APs supports a role-based stateful firewall. In other words, Instant firewall can recognize flows in a network and keep track of the state of sessions. The firewall logs on the Instant 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 Instant 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 Instant AP clients are associated with user roles, which determine the client's network privileges and the frequency at which clients re-authenticate. Instant 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.

Instant 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.

For more information on roles and policies, see the following topics:

- Configuring Network Service ACLs on page 299
- Configuring ACLs for Application Usage Analysis
- Configuring User Roles for Instant AP Clients on page 301
- Configuring Role Derivation Rules for Instant AP Clients on page 302
- Configuring Firewall Parameters for Inbound Traffic on page 308

Configuring Network Service ACLs

This section describes the procedure for configuring ACLs to control access to network services. For information on:

- Configuring ACLs for DPI, see Configuring ACLs for Application Usage Analysis on page 305.
- Configuring ACLs website content classification, see Configuring ACLs on Instant APs for Website Content Classification on page 306.

To configure access rules, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Security**. The **Security** page opens.
4. Click **Roles**.
5. Under **Access Rules For Selected Roles**, click **+ Add Rule** to add a new rule. The new rule window is displayed.
6. Under **Rule Type**, select **Access Control.**
7. To configure access to applications or application categories, select a service category from the following list:

- **Network**
- **Application Category**
- **Application**
- **Web Category**
- **Web Reputation**

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

Table 87: *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: ■ **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. **NOTE:** If TCP and UDP uses the same port, ensure that you configure separate access rules to permit or deny access.
Action	Select any of following attributes: ■ 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. ■ **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 Aruba Central firewall supports firewall based logging. Firewall logs on the Instant APs are generated as security logs.
Blacklist	Select **Blacklist** to blacklist the client when this rule is triggered. The blacklisting lasts for the duration specified as **Auth failure blacklist time** on the **BLACKLISTING** tab of the **Security** window. For more information, see Blacklisting Instant AP Clients on page 311.
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: ■ Video: Priority 5 (Critical) ■ Voice: Priority 6 (Internetwork Control)

Table 87: *Access rule configuration parameters*

Data Pane Item	Description
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. For more information, see Configuring Radio Parameters on page 281.
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.
802.1 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. For more information on time range profiles, see Configuring Time-Based Services for Wireless Network Profiles on page 275.

9. Save the changes.

Configuring User Roles for Instant 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 Instant AP involves the following procedures:

- Creating a User Role on page 301
- Assigning Bandwidth Contracts to User Roles on page 301

Creating a User Role

To create a user role, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Security**. The **Security** pane is displayed.
4. Click **Roles**. The **Roles** pane contents are displayed.
5. Under **Roles**, click **New**.
6. Enter a name for the new role and click **OK**.

You can also create a user role when configuring wireless profile. For more information, see Configuring ACLs for User Access to a Wireless Network on page 251.

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 Instant AP) or downstream (Instant 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:

1. Select **Configuration** > **Wireless** > **Security**. The **Security** pane contents are displayed.
2. Click **Roles**. The **Roles** pane contents are displayed.
3. Create a new role or select an existing role.
4. Under **Access Rues For Selected Roles**, click **(+)**.
5. Select **Bandwidth Contract** under **Rule-Type**.
6. Specify the downstream and upstream rates in Kbps. If the assignment is specific for each user, select **Peruser**.
7. Click **Save**.
8. 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 Instant 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. For more information on derivation rules, see *Aruba Instant User Guide*.

Creating a Role Derivation Rule

You can configure rules for determining the role that is assigned for each authenticated client.

When creating more than one role assignment rule, the first matching rule in the rule list is applied.

To create a role assignment rule, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Wireless SSIDs**. The **Wireless SSIDs** page opens.
4. Select a network profile and click **Edit**.
5. Under **Access**, set the slider to **Role Based**.
6. Under **Role Assignment Rules**, click **New**. 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.
7. Select the attribute from the **Attribute** list that the rule it matches against. The list of supported attributes includes RADIUS attributes, dhcp-option, dot1x-authentication-type, mac-address, and mac-address-and-dhcp-options. For information on a list of RADIUS attributes, see RADIUS Server Authentication with VSA on page 293.
8. 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.

9. Enter the string to match in the **String** box.
10. Select the appropriate role from the **Role** list.
11. Click **Save**.

Configuring VLAN Assignment Rule

To configure VLAN assignment rules for an SSID profile:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Wireless SSIDs**. The **Wireless SSIDs** page opens.
4. Click **+Add SSID** to create a new network profile or click the edit icon corresponding to the network profile that is required to be modified.
5. Perform the configurations in the **General**, **VLAN**, and **Security** tab. For more information, see Configuring Wireless Network Profiles on Instant APs.
6. Click **Next**. The **Access** tab is displayed.
7. Select the access rule from **Access Rules**.
8. In the **Access Rules For Selected Roles**, click + **Add Rule** to add a new rule. The **Access Rule** page is displayed.

The **VLAN Assignment** option is also listed in the **Access Rule** page when you create or edit a rule for wired port profiles in the **Wireless Management** > **Access Point Ports** > **Create a New Network > Access** tab.

9. From the **Rule Type** drop-down list, select **VLAN Assignment** option.
10. Enter the VLAN ID in the **VLAN ID** field under **Service** section. Alternatively , you can select the VLAN ID or the VLAN name from the drop-down list provided next to the VLAN ID field.

The VLAN name for a specific VLAN is available only after mapping the VLAN ID with the VLAN name in the **Wireless Management** > **Systems** >**Named VLAN Mapping** section. For more information, see Configuring VLAN Name and VLAN ID.

11. Click **Save** to apply the changes.

Configuring VLAN Derivation Rules

The users are assigned to a VLAN based on the attributes returned by the RADIUS server after users authenticate.

To configure VLAN derivation rules for an SSID profile:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Wireless SSIDs**. The **Wireless SSIDs** page opens.
4. Select a network profile and click **Edit**.
5. Under **VLAN**, select **Dynamic** under **Client VLAN Assignment**.

6. Click **New** 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.
7. Select an attribute from the **Attribute** list.
8. 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.
9. Enter the string to match in the **String** field.
10. Select the appropriate VLAN ID from **VLAN**.
11. Ensure that all other required parameters are configured.
12. Click **Save** to apply the changes.

Configuring Firewall Parameters for Wireless Network Protection

To configure firewall settings, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Security**. The **Security** page opens.
4. Click **Firewall Settings.**
5. In the **Application Layer Gateway (ALG) Algorithms** section, select **Enabled** from the corresponding drop-down lists to enable **SIP**, **VOCERA**, **Alcatel NOE**, and **Cisco Skinny** protocols.
6. In the **Protection Against Wired Attacks** section, set the following options to **Enabled** :
   - **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.

Disabling Auto Topology Rules

If the firewalls rules are configured, the **Auto Topology Rules** are enabled by default. When the inbound firewall settings are enabled:

- ACEs must be configured to block auto topology messages, as there is no default rule at the top of predefined ACLs.
- ACEs must be configured to override the guest VLAN auto-expanded ACEs. In other words, the user defined ACEs take higher precedence over guest VLAN ACEs.

To disable the auto topology rules, set **Auto Topology Rules** to **OFF**.

Configuring ACLs for Application Usage Analysis

This section describes the procedure for configuring access rules for deep packet inspection and application usage analysis. For information on configuring access rules based on web categories and web reputation, see Configuring ACLs on Instant APs for Website Content Classification on page 306.

To configure ACL rules for a user role, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device for which you want to configure the ACL rules.
3. On the navigation pane, click **Security**.
4. Under **Roles**, select the role for which you want to configure access rules.
5. Under **Access Rules For Selected Roles**, click **(+)** to add a new rule. The new rule window is displayed.
6. Under **Rule Type**, select **Access Control.**
7. To configure access to applications or application categories, select a service category from the following list:
   - Network
   - Application Category
   - Application
   - Web Category
   - Web Reputation
8. Based on the selected service category, configure the following parameters:

Table 88: *Access Rule Configuration Parameters*

Service category	Description
Application 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	Application throttling allows you to set a bandwidth limit for an application and application categories. For example, you can limit the bandwidth rate for video streaming applications such as YouTube or Netflix, or assign a low bandwidth to high risk sites. To specify a bandwidth limit: 1. Select the **Application Throttling** check box. 2. Specify the **Downstream** and **Upstream** rates in Kbps per user.
Action	Select one of the following actions: ■ Select **Allow** to allow access users based on the access rule. ■ Select **Deny** to deny access to users based on the access rule.
Destination	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. ■ **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

Table 88: *Access Rule Configuration Parameters*

Service category	Description
	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 Instant AP is allowed, After selecting this option, specify the domain name in the **IP** text box. ■ **To AP Network—**Traffic to the specified Instant 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 Instant 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. Aruba Central supports firewall based logging. Firewall logs on the Instant APs are generated as security logs.
Blacklist	Select the **Blacklist** check box to blacklist the client when this rule is triggered. The blacklisting lasts for the duration specified as **Auth failure blacklist time** on the Blacklisting tab of the **Security** window. For more information, see Blacklisting Instant AP Clients on page 311.
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 on page 281.
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.
802.1 priority	Select this check box to enable 802.1 priority. 802.1p 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 Time-Based Services for Wireless Network Profiles on page 275.

3. Click **Save**.

Configuring ACLs on Instant 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:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device for which you want to configure web policy enforcement rules.
3. On the navigation pane, click **Security**.

4. Under **Roles**, select the role to modify.
5. Under **Access Rules For Selected Roles**, click **(+)** to add a new rule. The new rule window is displayed.
6. Under **Rule Type**, select **Access Control.**
7. 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**.
8. 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.

9. 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.
10. If required, select the following check boxes:

- **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 Instant APs are generated as security logs.
- **Blacklist** — Select this check box to blacklist the client when this rule is triggered. The blacklisting lasts for the duration specified as **Auth Failure Blacklist Time** on the **Blacklisting** pane of the **Security** window. For more information, see Blacklisting Instant AP Clients on page 311.
- **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 on page 281.
- **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.
- **802.1 priority**—Select this check box to enable 802.1 priority. 802.1p 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.

11. Click **Save** to save the rules.
12. Click **Save Settings** in the **Roles** pane to save the changes to the role for which you defined ACL rules.

Configuring Custom Redirection URLs for Instant 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.

Creating a List of Error Page URLs

To create a list of error page URLs, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the navigation pane, click **Security**.
4. Under **Custom Blocked Page URL**, click **+** and enter the URL to block.
5. Repeat the procedure to add more URLs. You can add up to 8 URLs to the list of blocked web pages.
6. Click **OK**.

Configuring ACL Rules to Redirect Users to a Specific URL

To configure ACL rules to redirect users to a specific URL:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device for which you want to configure the ACL rules.
3. On the navigation pane, click **Security**.
4. Under **Roles**, select the role for which you want to configure access rules.
5. Click **+** in the Access Rules section. The **New Rule window** opens.
6. Select the rule type as **Blocked Page URL**.
7. Select the URLs from the existing list of custom redirect URLs. To add a new URL, click **+**.
8. Save the changes.

Configuring Firewall Parameters for Inbound Traffic

Instant APs support an enhanced inbound firewall for the traffic that flows into the network through the uplink ports of an Instant AP. You can configure firewall rules for the inbound traffic in the **Wireless Management** > **Security** > **Inbound Firewall** section.

To configure the firewall rules, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Security**. The **Security** page opens.
4. Click **Inbound Firewall**.
5. In the **Access Rule** section, click the **+** icon. The **Inbound Firewall** page opens.
6. Perform the following in the **Inbound Firewall** page:

Table 89: *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: ■ **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: ■ 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: ■ **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	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. ■ **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 Instant AP is allowed, After selecting this option, specify the domain name in the **IP** text box. ■ **To AP Network—**Traffic to the specified Instant 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 Instant AP or virtual controller is allowed. After selecting this option, specify the domain name in

Parameter	Description
	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.
Blacklist	Select the **Blacklist** check box to blacklist the client when this rule is triggered. The blacklisting lasts for the duration specified in the **Auth failure blacklist time** on the **Blacklisting** 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.

7. Click **Ok**.
8. Click **Save Settings**.

For all subnets, a deny rule is created by default as the last rule. If at least one rule is configured, the deny all rule is applied to the upstream traffic by default..

The inbound firewall is not applied to traffic coming through the GRE tunnel.

Configuring Management Subnets

You can configure subnets to ensure that the Instant 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. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Security**. The **Security** page opens.
4. Click **Firewall Settings**.
5. To add a new management subnet, complete the following steps:
   - Enter the subnet address in **Subnet**.
   - Enter the subnet mask in **Mask.**
   - Click **Add**.
6. To add multiple subnets, repeat step 2.
7. 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 Instant AP is allowed irrespective of the inbound firewall rule.
The inbound firewall is not applied to traffic coming through the GRE tunnel.

Configuring Restricted Access to Corporate Network

You can configure restricted corporate access to block unauthorized users from accessing the corporate network. When restricted corporate access is enabled, corporate access is blocked from the uplink port of master Instant AP, including clients connected to a slave Instant AP.

To configure restricted corporate access, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Security**. The **Security** page opens.
4. Click **Firewall Settings**
5. Enable **Restrict Corporate Access**.
6. Click **Save Settings**.

Enabling ALG Protocols on Instant APs

To configure protocols for ALG, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Security**. The **Security** page opens.
4. Click **Firewall Settings**
5. Under **Application Layer Gateway (ALG) Algorithms**, select **Enabled** against the corresponding protocol to enable SIP, VOCERA, ALCATEL NOE, and CISCO SKINNY protocols.
6. 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 Instant AP and the client, or wait a few minutes for changes to take effect.

Blacklisting Instant AP Clients

The client blacklisting denies connection to the blacklisted clients. When a client is blacklisted, it is not allowed to associate with an Instant AP in the network. If a client is connected to the network when it is blacklisted, a deauthentication message is sent to force client disconnection.

Blacklisting Clients Manually

Manual blacklisting adds the MAC address of a client to the blacklist. These clients are added into a permanent blacklist. These clients are not allowed to connect to the network unless they are removed from the blacklist.

To add a client to the blacklist manually:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Security**. The **Security** page opens.
4. Click **Blacklisting**.

5. Click + and enter the MAC address of the client to be blacklisted in **Enter A New MAC Address**.
6. Click **Ok**. The **Blacklisted Since** field displays the time at which the current blacklisting has started for the client.

For the blacklisting to take effect, you must enable the blacklisting option when you create or edit the WLAN SSID profile. Go to **Wireless Management** > **Wireless SSIDs** > **Security** > **Advanced Settings** and enable the **Blacklisting** option. For more information, see Configuring Wireless Network Profiles on Instant APs.

To delete a client from the manual blacklist, select the MAC Address of the client under the **Manual Blacklisting**, and then click **Delete**.

Blacklisting Clients Dynamically

The clients can be blacklisted dynamically when they exceed the authentication failure threshold or when a blacklisting 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 blacklisted by an Instant AP.

In session firewall based blacklisting, an ACL rule automates blacklisting. When the ACL rule is triggered, it sends out blacklist information and the client is blacklisted.

To configure the blacklisting duration:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Security**. The **Security** page opens.
4. Click **Blacklisting**
5. Under **Dynamic Blacklisting**:

   a. For **Auth Failure Blacklist Time**, enter the duration after which the clients that exceed the authentication failure threshold must be blacklisted.

   b. For **PEF Rule Blacklisted Time**, enter the duration after which the clients can be blacklisted due to an ACL rule trigger.

You can configure a maximum number of authentication failures by the clients, after which a client must be blacklisted. For more information on configuring maximum authentication failure attempts, see Configuring Security Settings for a Wireless Network on page 247.

To enable session-firewall-based blacklisting, select the **Blacklist** check box in the **Access Rule** page during the WLAN SSID profile creation. For more information, see Configuring Network Service ACLs.

Configuring Instant APs for VPN Services

This section describes the following VPN configuration procedures:

Instant AP VPN Overview

As Instant APs use a Virtual Controller architecture, the Instant 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 Instant AP networks at branch locations or data centers, where the Aruba controller acts as a VPN Concentrator.

When the VPN is configured, the Instant AP acting as the Virtual Controller creates a VPN tunnel to Aruba Mobility Controller in your corporate office. The controller acts as a VPN endpoint and does not supply the Instant 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

Instant APs support the following VPN protocols for remote access:

Table 90: *VPN Protocols*

VPN Protocol	Description
Aruba IPsec	IPsec is a protocol suite that secures IP communications by authenticating and encrypting each IP packet of a communication session. 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. When IPsec is configured, ensure that you add the Instant AP MAC addresses to the whitelist database stored on the controller or an external server. IPsec supports Local, L2, and L3 modes of IAP-VPN operations. **NOTE:** The Instant APs support IPsec only with Aruba Controllers.
Layer-2 (L2) GRE	GRE is a tunnel protocol for encapsulating multicast, broadcast, and L2 packets between a GRE-capable device and an endpoint. Instant APs support the configuration of L2 GRE (Ethernet over GRE) tunnel with an Aruba Controller to encapsulate the packets sent and received by the Instant AP. You can use the GRE configuration for L2 deployments when there is no encryption requirement between the Instant AP and controller for client traffic. Instant APs support two types of GRE configuration: ■ **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 Instant 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 Instant AP MAC addresses to the whitelist 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. **NOTE:** Instant APs support manual and Aruba GRE configuration only for L2 mode of operations. Aruba GRE configuration is supported only with Aruba Controllers.
L2TP	The L2TP version 3 feature allows Instant 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 Instant 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 Instant APs for VPN Tunnel Creation

Instant AP supports the configuration of tunneling protocols such as GRE, IPsec, and L2TPv3. This section describes the procedure for configuring VPN host settings on an Instant AP to enable communication with a controller in a remote location:

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 a tunnel using the IPsec Protocol, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **VPN**.
4. Click **Controller**.
5. Select **Aruba IPSec** from the **Protocol** drop-down list.
6. Enter the IP address or FQDN for the main VPN/IPsec endpoint in the **Primary host** field.
7. Enter the IP address or FQDN for the backup VPN/IPsec endpoint in the **Backup host** field. This entry is optional. When you specify the primary and backup host details, the other fields are displayed.
8. 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.

   b. 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.

   c. To allow the Instant 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 Instant AP can switch the data stream to the backup tunnel. This reduces the total failover time to less than one minute.

   d. Specify a value in seconds for **Secs between test packets**. Based on the configured frequency, the Instant AP can verify if an active VPN connection is available. The default value is 5 seconds, which means that the Instant AP sends one packet to the controller every 5 seconds.

   e. Enter a value for **Max allowed test packet loss**, to define a number for lost packets, after which the Instant AP can determine that the VPN connection is unavailable. The default value is 2.

   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** check box.

   g. 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.
9. When the IPsec tunnel configuration is completed, the packets that are sent from and received by an Instant AP are encrypted.

Configuring Automatic GRE VPN Tunnel

You can configure an Instant AP to automatically set up a GRE tunnel from the Instant AP to controller in Aruba Central.

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **VPN**.
4. Click **Controller**.
5. Select **Aruba GRE** from the **Protocol** drop-down list.
6. Enter the IP address or FQDN for the main VPN/IPsec endpoint in the **Primary host** field.
7. Enter the IP address or FQDN for the backup VPN/IPsec endpoint in the **Backup host** field. This entry is optional. When you enter the primary host IP address and backup host IP address, other fields are displayed.
8. 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.

   b. 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.

   c. To allow the Instant 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. If the primary tunnel fails, the Instant AP can switch the data stream to the backup tunnel. This reduces the total failover time to less than one minute.

   d. 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**.

   e. 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 the range of 30—900 seconds. By default, the reconnection duration is set to 60 seconds.

   f. Specify a value in seconds for **Secs between test packets**. Based on the configured frequency, the Instant AP can verify if an active VPN connection is available. The default value is 5 seconds, which means that the Instant AP sends one packet to the controller every 5 seconds.

   g. Enter a value for **Max allowed test packet loss**, to define a number for lost packets, after which the Instant AP can determine that the VPN connection is unavailable. The default value is 2.

   h. Select the **Per-AP tunnel** check box. The administrator can enable this option to create a GRE tunnel from each Instant AP to the VPN/GRE Endpoint rather than the tunnels created just from the master Instant AP. When enabled, the traffic to the corporate network is sent through a Layer-2 GRE tunnel from the Instant AP itself and need not be forwarded through the master Instant AP.
9. Click **Next** to continue.

Configuring a GRE VPN Tunnel

You can also manually configure a GRE tunnel by configuring the GRE tunnel parameters on the Instant 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 Instant AP IP to create the GRE tunnel at the controller side depending upon the following Instant 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 Instant AP IP is used to create the GRE tunnel.

To configure the GRE tunnel manually, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **VPN**.
4. Click **Controller**.
5. Select **Manual GRE** from the **Protocol** drop-down list.
6. Specify the following parameters:

   a. **Host**—Enter the IPv4 or IPv6 address or FQDN for the main VPN/GRE tunnel.

   b. **Backup Host**—(Optional) Enter the IPv4 or IPv6 address or FQDN for the backup VPN/GRE tunnel. You can edit this field only after you enter the IP address or FQDN in the **Host** field.

   c. **Reconnect User On Failover**—When you enter the host IP address and backup host IP address, this field appears. Select this check box to disconnect all wired and wireless users when the system switches during VPN tunnel transition from primary to backup and backup to primary.

   d. **Reconnect Time On Failover**—If you select the **Reconnect User On Failover** check box, this field appears. To configure an interval for which wired and wireless users must be disconnected during a VPN tunnel switch, specify a value within a range of 30-900 seconds. By default, the reconnection duration is set to 60 seconds.

   e. **GRE Type**—Enter a value for the parameter.

   f. **GRE MTU**—Specify a size for the **GRE MTU** within the range of 1024–1500. After GRE encapsulation, if packet length exceeds the configured MTU, IP fragmentation occurs. The default MTU size is 1300.

   g. **Per-AP-Tunnel**—The administrator can enable this option to create a GRE tunnel from each Instant AP to the VPN/GRE endpoint rather than the tunnels created just from the master Instant AP. When enabled, the traffic to the corporate network is sent through a Layer-2 GRE tunnel from the Instant AP itself and need not be forwarded through the master Instant AP.

By default, the **Per-AP tunnel** option is disabled.

   h. 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**.

   i. 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 the range of 30—90 seconds. By default, the reconnection duration is set to 60 seconds.

7. When the GRE tunnel configuration is completed on both the Instant AP and Controller, the packets sent from and received by an Instant AP are encapsulated, but not encrypted.

Configuring an L2TPv3 VPN Tunnel

The Layer 2 Tunneling Protocol version 3 (L2TPv3) feature allows Instant 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 Instant 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. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.

3. On the left navigation pane, click **VPN**.
4. Click **Controller**.
5. Select **L2TPv3** from the Protocol drop-down list.
6. To configure a tunnel profile:
   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**.
7. To configure a session profile:
   a. Turn on the **Enable Tunnel Profile** toggle switch.
   b. Enter the session profile name.
   c. Enter the tunnel profile name where the session will be associated.
   d. Configure the tunnel IP address with the corresponding network mask and VLAN ID. This is required to reach an AP from a corporate network. For example, SNMP polling.
   e. Select the cookie length and enter a cookie value corresponding to the length. By default, the cookie length is not set.
   f. Click **Save**.

Configuring Routing Profiles for Instant AP VPN

Aruba Central can terminate a single VPN connection on Aruba Mobility Controller. The routing profile defines the corporate subnets which need to be tunneled through IPsec.

You can configure routing profiles to specify a policy based on routing into the VPN tunnel.

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **VPN**.

4. Click **Routing**.
5. Click **New**. The route parameters to configure are displayed.
6. 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. This IP address must be the controller IP address on which the VPN connection is 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.
7. Click **OK**.
8. Click **Finish**.

Configuring DHCP Pools and Client IP Assignment Modes on Instant APs

This section provides the following information:

- Configuring DHCP Scopes on Instant APs on page 318
- Configuring DHCP Server for Assigning IP Addresses to Instant AP Clients on page 323

Configuring DHCP Scopes on Instant APs

The VC supports the following types different modes of DHCP address assignment:

- Configuring Distributed DHCP Scopes on page 318
- Configuring a Centralized DHCP Scope on page 320
- Configuring Local DHCP Scopes on page 322

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.

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.

3. On the left navigation pane, click **DHCP**.
4. To configure a distributed DHCP mode, click + under **Distributed DHCP Scopes**. The **New DHCP Scope** pane is displayed.
5. Based on the type of distributed DHCP scope, configure the following parameters:

Table 91: *Distributed DHCP scope configuration parameters*

Data pane item	Description
Name	Enter a name for the DHCP scope.
Type	Select any of the following options: ■ **Distributed, L2**— On selecting **Distributed, L2**, the VC acts as the DHCP Server but the default gateway is in the data center. Traffic is bridged into VPN tunnel. ■ **Distributed, L3**— On selecting **Distributed, L3**, the VC acts as both DHCP Server and default gateway. Traffic is routed into the VPN tunnel.
VLAN	Specify a VLAN ID. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile.
Netmask	If **Distributed, L2** is selected for type of DHCP scope, specify the subnet mask. The subnet mask and the network determine the size of subnet.
Default Router	If **Distributed, L2** is selected for type of DHCP scope, specify the IP address of the default router.
DNS Server	If required, specify the IP address of a DNS server.
Domain Name	If required, specify the domain name.
Lease Time	Specify a lease time for the client in minutes.
IP Address Range	Specify a range of IP addresses to use. To add another range, click the + icon. You can specify up to four different ranges of IP addresses. ■ 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 discontiguous IP ranges. The configured IP range is divided into multiple IP subnets that are sufficient to accommodate the configured client count. **NOTE:** You can allocate multiple branch IDs (BID) per subnet. The Instant 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.
DHCP Reservation	Displays the total number of DHCP reservations. Click the number to view the list of DHCP reservations. **NOTE:** You can configure DHCP reservation only on virtual controllers. From the filter bar, select a virtual controller and click the + icon to configure DHCP reservation. Specify the following details: ■ **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. **NOTE:** Aruba Central allows you to configure a maximum of 32 DHCP reservations. To delete a DHCP reservation, click the delete icon.
Option	Specify the type and a value for the DHCP option. You can configure the organization-specific DHCP options supported by the DHCP server. For example, 176, 242, 161, and so on. To add multiple DHCP options, click the + icon. You can add up to eight DHCP options.

6. Click **Next**.
7. 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 Instant 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.
8. Click **Next**. The **Static IP** tab is displayed. Specify the number of first and last IP addresses to reserve in the subnet.
9. 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:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **DHCP**.
4. To configure **Centralized** DHCP scopes, click + under **Centralized DHCP Scopes**. The **New DHCP Scope** data pane is displayed.
5. Based on type of DHCP scope, configure the following parameters:

Table 92: *DHCP mode configuration parameters*

Data pane item	Description
Name	Enter a name for the DHCP scope.
Type	Select one of the following options: ■ Centralized ,Layer-2 ■ Centralized ,Layer-3
VLAN	Specify a VLAN ID. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile.
Split Tunnel	Enable the split tunnel function if you want allow a VPN user to access a public network and a local LAN or

Table 92: *DHCP mode configuration parameters*

Data pane item	Description
	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. 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. 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.
DHCP Relay	Select **Enabled** to allow the Instant 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	Select one of the following options: ■ **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: ● 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. For information related to XML files, see DHCP Option 82 XML on page 238.

6. Click **OK**.

The following table describes the behavior of the DHCP Relay Agent and Option 82 in the Instant AP.

Table 93: *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 Instant 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 Instant 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 Instant 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 Instant 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. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **DHCP**.
4. Click **Local DHCP Scopes**.
5. Click + to add new local DHCP scope. The **New DHCP Scope** pane opens.
6. Based on type of DHCP scope, configure the following parameters:

Table 94: *Local DHCP configuration parameters*

Data pane item	Description
Name	Enter a name for the DHCP scope.
Type	Select any of the following options: ■ **Local**— On selecting **Local**, the DHCP server for local branch network is used for keeping the scope of the subnet local to the Instant 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. **NOTE:** You can configure DHCP reservation only on virtual controllers. From the filter bar, select a virtual controller and click the + icon to configure DHCP reservation. Specify the following details: ■ **MAC**—Specify the MAC address of the device for which the IP address has to be reserved.

Table 94: *Local DHCP configuration parameters*

Data pane item	Description
	■ **IP**—Specify the IP address that has to be reserved for the MAC address. The IP address should be in the IP address range. **NOTE:** Aruba Central allows you to configure a maximum of 32 DHCP reservations. To delete a DHCP reservation, click the delete icon.
Default Router	Enter the IP address of the default router.
DNS Server	Enter the IP address of a DNS server.
Domain Name	Enter the domain name.
Lease Time	Enter a lease time for the client in minutes.
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.

7. Click **OK**.

Configuring DHCP Server for Assigning IP Addresses to Instant 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 Instant AP automatically determines a suitable DHCP pool for **Virtual Controller Assigned** networks.

The Instant AP typically selects the 172.31.98.0/23 subnet. If the IP address of the Instant AP is within the 172.31.98.0/23 subnet, the Instant 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.

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **System**. The **System** page for the selected group or device opens.
4. Click **DHCP**.
5. Enter the domain name of the client in **Domain Name**.
6. Enter the IP addresses of the DNS servers in **DNS Server**. To add another DNS server, click the **+** icon.
7. Enter the duration of the DHCP lease in **Lease Time**.
8. Select **Minutes**, **Hours**, or **Days** for the lease time from the list next to **Lease Time**. The default lease time is 0.
9. Enter the network in the **Network** box.

10. Enter the mask in the **Mask** box.

To provide simultaneous access to more than 512 clients, use the Network and Mask fields to specify a larger range. While the network (or prefix) is the common part of the address range, the mask (suffix) specifies how long the variable part of the address range is.

11. Click **Save Settings**.

Configuring Services

This section describes how to configure AirGroup, location services, Lawful Intercept, OpenDNS, and Firewall services.

Configuring AirGroup Services

AirGroup is a zero configuration networking protocol that enables service discovery, address assignment, and name resolution for desktop computers, mobile devices, and network services. It is designed for flat, single-subnet IP networks such as wireless networking at home.

Bonjour can be installed on computers running Microsoft Windows and is supported by the new network-capable printers. Bonjour uses multicast DNS (mDNS) to locate devices and the services offered by these devices. The AirGroup solution supports both wired and wireless devices. Wired devices that support Bonjour services are part of AirGroup when connected to a VLAN that is terminated on the Virtual Controller.

In addition to the mDNS protocol, Instant APs also support UPnP, and DLNA enabled devices. DLNA is a network standard derived from UPnP, which enables devices to discover the services available in a network.

DLNA also provides the ability to share data between the Windows or Android-based multimedia devices. All the features and policies applicable to mDNS are extended to DLNA to ensure full interoperability between compliant devices.

AirGroup Features

AirGroup provides the following features:

- Send unicast responses to mDNS queries and reduces mDNS traffic footprint.
- Ensure cross-VLAN visibility and availability of AirGroup devices and services.
- Allow or block AirGroup services for all users.
- Allow or block AirGroup services based on user roles.
- Allow or block AirGroup services based on VLANs.

For more information on AirGroup solution, see *Aruba Instant User Guide*.

AirGroup Services

Bonjour supports zero-configuration services. The services are pre-configured and are available as part of the factory default configuration. The administrator can also enable or disable any or all services.

The following services are available for Instant AP clients:

- AirPlay — Apple AirPlay allows wireless streaming of music, video, and slide shows from your iOS device to Apple TV and other devices that support the AirPlay feature.
- AirPrint — Apple AirPrint allows you to print from an iPad, iPhone, or iPod Touch directly to any AirPrint compatible printer.
- iTunes— The iTunes service is used by iTunes Wi-Fi sync and iTunes home-sharing applications across all Apple devices.
- RemoteMgmt— Use this service for remote login, remote management, and FTP utilities on Apple devices.
- Sharing— Applications such as disk sharing and file sharing, use the service ID that are part of this service on one or more Apple devices.
- Chat— The iChat® (Instant Messenger) application on Apple devices uses this service.
- ChromeCast—The ChromeCast service allows you to use a ChromeCast device to play audio or video content on a high-definition television by streaming content through Wi-Fi from the Internet or local network.
- DLNA Media—Applications such as Windows Media Player use this service to browse and play content on a remote device.
- DLNA Print—This service is used by printers that support DLNA.

Configuring AirGroup and AirGroup Services

To enable AirGroup and its services:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Services**. The **Services** page opens.
4. Under **AirGroup**, select the **AirGroup** check box. The **AirGroup** configuration parameters are displayed.
5. To allow the users to use AirGroup services enabled in a guest VLAN, select the **Guest Bonjour Multicast** check box. However, the AirGroup devices are visible in the guest VLAN and AirGroup does not discover or enforce policies in the guest VLAN.
6. Select **AirGroup Across Mobility Domains** to enable Inter cluster mobility.
7. Select required services. To allow all services, select **Allow All**.
8. To add a new service, click + Add New Service.
9. Based on the services configured, you can block any user roles and VLAN from accessing a AirGroup service. The user roles and VLANs marked as disallowed are prevented from accessing the corresponding AirGroup service. You can create a list of disallowed user roles and VLANs for all AirGroup services configured on the Instant AP. For example, If the AirPlay service is selected, the **Edit** links for the **AirPlay Disallowed Roles** and **AirPlay Disallowed VLANS** are displayed. Similarly, if sharing service is selected, the **Edit** links for the **Sharing Disallowed Roles** and **Sharing Disallowed VLANS** are displayed.
   - To block user roles from accessing a AirGroup service, click the corresponding **Edit** link and select the user roles for which you want to restrict access. By default, an AirGroup service is accessible by all user roles configured in your Instant AP cluster.

- To select VLANs from allowing access to AirGroup service, click the corresponding **Edit** link and select the VLANs to exclude. By default, the AirGroup services are accessible by users or devices in all VLANs configured in your Instant AP cluster.

10. To enable DLNA support, select the **DLNA** check box and select the DLNA services such as Amazon TV, Google Cast, DLNA print or media. DLNA is a network standard derived from UPnP, which enables devices to discover the services available in a network. DLNA also provides the ability to share data between the Windows or Android-based multimedia devices.
11. Configure **ClearPass Settings** to set up ClearPass Policy Manager server, CoA server, and enforce ClearPass registering.
    - **ClearPass Policy Manager Server 1**—Indicates the ClearPass Policy Manager server information for the AirGroup policy.
    - **Enforce ClearPass registering**—When enabled, only devices registered with ClearPass Policy Manager will be discovered by Bonjour devices, based on the ClearPass Policy Manager policy.
12. Click **Save Settings**.

Configuring an Instant 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. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Services**. The **Services** page opens.
4. Click **Real Time Locating System**.
5. Select **Aruba RTLS** to send the RFID tag information to the Aruba RTLS server.
6. Click **3rd Party** and select **Aeroscout** to send reports on the stations to a third-party server.
7. Specify the IP address and port number of the RTLS server, to which location reports must be sent.
8. If **Aruba RTLS** is selected, enter the passphrase required for connecting to the RTLS server.
9. Select **Include Unassociated Stations** to send reports on the stations that are not associated to any Instant AP.
10. Click **Save Settings**.

Configuring an Instant 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 Instant AP sends client information and all status information to the ALE server.

To integrate Instant AP with ALE, the ALE server address must be configured on an Instant 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 Instant AP

To configure an Instant AP for ALE support:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Services**. The **Services** pane is displayed.
4. Under **Real Time Locating System**, click **Aruba**, and then select **Analytics & Location Engine**.
5. Specify the ALE server name or IP address.
6. Specify the reporting interval within the range of 6–60 seconds. The Instant AP sends messages to the ALE server at the specified interval. The default interval is 30 seconds.
7. Click **OK**.

Managing BLE Beacons

Instant 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 Instant 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

Instant AP assets can be tracked using BLE tags, Instant AP beacons scan the network. When a tag is detected, the Instant 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. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Services**. The **Services** page opens.
4. Click **Real Time Locating System** > **Aruba**.
5. To manage the BLE devices using BMC, select the **Manage BLE Beacons** check box.
6. Enter the 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.
7. In **Endpoint URL**, enter the URL of the server to which the BLE sends the monitoring data.
8. Select any of the following options from **BLE Operation Mode** drop-down list:

Table 95: *BLE Operation Modes*

Mode	Description
beaconing	The built-in BLE chip in the Instant AP functions as an iBeacon combined with the beacon management functionality.
disabled	The built-in BLE chip of the Instant AP is turned off. The BLE operation mode is set to **Disabled** by default.
dynamic-console	The built-in BLE chip of the Instant AP functions in the beaconing mode and dynamically enables access to Instant AP console over BLE when the link to LMS is lost.
persistent-console	The built-in BLE chip of the Instant AP provides access to the Instant AP console over BLE and also operates in the **Beaconing** mode.

9. To configure BLE web socket management server, click **BLE Asset Tag Mgmt** field and enter the URL of BLE web socket management server.
10. To configure BLE HTTPS management server, select the **BLE Asset Tag Mgmt** check box to enter the BLE HTTPS management server URL.
11. Enter the URL of BLE HTTPS management server corresponding to the **Server URL** field.
12. Click **Save Settings**.

Configuring OpenDNS Credentials on Instant APs

Instant APs use the OpenDNS credentials to provide enterprise-level content filtering.

To configure OpenDNS credentials:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Services**. The **Services** page opens.
4. Click **OpenDNS**.
5. Enter the **Username** and **Password**.
6. Click **Save Settings**.

Configuring CALEA Server Support on Instant 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 Instant AP in a hierarchical and flat topology, mesh Instant 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 Instant AP to CALEA server, see *Aruba Instant User Guide*.

To enable an Instant AP to communicate with the CALEA server, complete the following steps:

- Creating a CALEA Profile
- Creating ACLs for CALEA Server Support

Creating a CALEA Profile

To create a CALEA profile, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Services**. The **Services** page opens.
4. Click **CALEA**. The **CALEA** tab details are displayed.
5. 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.
6. Click **OK**.

Creating ACLs for CALEA Server Support

To create an access rule for CALEA, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Security**. The **Security** page opens.
4. Click **Roles**.
5. Under **Access Rules for Selected Roles**, click **New**. The **New Rule** window is displayed.
6. Set the **Rule Type** to **CALEA**.
7. Click **OK**.
8. Create a role assignment rule if required.
9. Click **Finish**.

Configuring Instant APs for Palo Alto Networks Firewall Integration

Instant APs maintains the network (such as mapping IP address) and user information for its clients in the network. To integrate the Instant AP network with a third-party network, you can enable an Instant AP to provide this information to the third-party servers.

To integrate an Instant AP with a third-party network, you must add a global profile. This profile can be configured on an Instant AP with information such as IP address, port, user name, password, firewall enabled or disabled status.

Configuring an Instant AP for Network Integration

To configure an Instant AP for network integration:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Services**. The **Services** page opens.
4. Click **Network Integration**. The PAN firewall configuration options are displayed.
5. Select **Enable** to enable PAN firewall.
6. Specify the **User Name** and **Password**. Ensure that you provide user credentials of the PAN firewall administrator.

7. Enter the PAN firewall **IP Address**.
8. Enter the port number within the range of 1—65535. The default port is 443.
9. Click **Save Settings**.

Configuring XML API Interface

The XML API interface allows Instant APs to communicate with an external server. The communication between Instant 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 Instant 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. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Services**. The **Services** page opens.
4. Go to **Network Integration** > **XML API Server Configuration**.
5. Click + to add a new XML API server.
6. Enter a name for the XML API server in the **Name** text box.
7. Enter the IP address of the XML API server in the **IP Address** text box.
8. Enter the subnet mask of the XML API server in the **Mask** text box.
9. Enter a passcode in the **Passphrase** text box, to enable authorized access to the XML API Server.
10. Re-enter the passcode in the **Retype** box.
11. To add multiple entries, repeat the procedure.
12. Click **OK**.
13. To edit or delete the server entries, use the **Edit** and **Delete** buttons, respectively.

For information on adding an XML API request, see *Aruba Instant User Guide*.

Enabling Application Visibility Service on Instant APs

To view application usage metrics for Instant AP clients, you must enable the Application Visibility feature on Instant APs.

To enable the Application Visibility feature, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Services**. The **Services** page opens.
4. Click **Application Visibility.**
5. 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.

Configuring Uplink Interfaces on Instant APs

This section provides the following information:

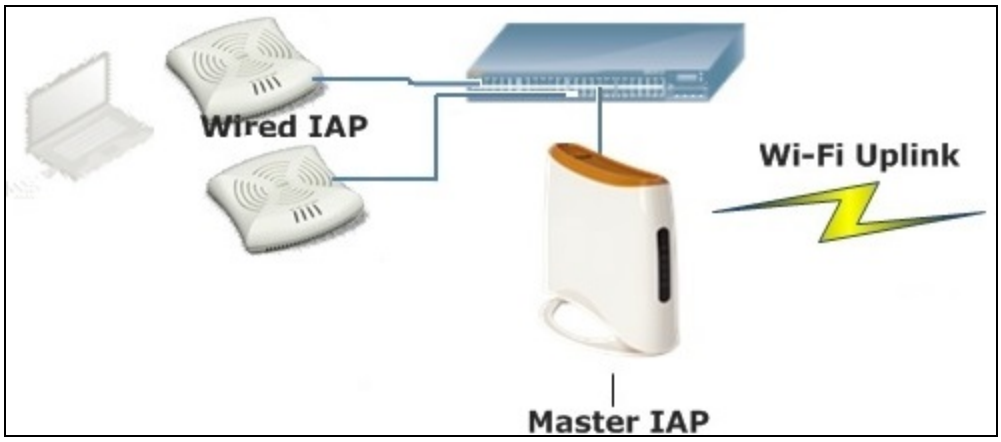
Uplink Interfaces

Aruba Central supports 3G and 4G USB modems, and the Wi-Fi uplink to provide access to the corporate network.

By default, the AP-318, AP-374, AP-375, and AP-377 access points have Eth1 as the uplink port and Eth0 as the downlink port. Aruba recommends you not to upgrade the mentioned access points to 8.5.0.0 and 8.5.0.1 firmware versions as the upgrade process changes the uplink from Eth1 to Eth0 port thereby making the devices non-reachable.

Figure 94 illustrates a scenario in which the Instant APs join the Virtual Controller as slave Instant APs through a wired or mesh Wi-Fi uplink:

Figure 94 *Uplink Types*



The following types of uplinks are supported on Aruba Central:

3G/4G Uplink

Aruba Central supports the use of 3G/4G USB modems to provide the Internet backhaul to Aruba Central. The 3G/4G USB modems can be used to extend client connectivity to places where an Ethernet uplink cannot be configured. This enables the Instant APs to automatically choose the available network in a specific region.

Types of Modems

Aruba Central supports the following three types of 3G modems:

- **True Auto Detect** — Modems of this type can be used only in one country and for a specific ISP. The parameters are configured automatically and hence no configuration is necessary.
- **Auto-detect + ISP/country** — Modems of this type require the user to specify the Country and ISP. The same modem is used for different ISPs with different parameters configured for each of them.
- **No Auto-detect** — Modems of this type are used only if they share the same Device-ID, Country, and ISP details. You need to configure different parameters for each of them. These modems work with Aruba Central when the appropriate parameters are configured.

Table 96: *4G supported modem*

Modem Type	Supported 4G Modem
True Auto Detect	■ Pantech UML290 ■ Ether-lte

When UML290 runs in auto detect mode, the modem can switch from 4G network to 3G network or vice-versa based on the signal strength. To configure the UML290 for the 3G network only, manually set the USB type to **pantech-3g**. To configure the UML290 for the 4G network only, manually set the 4G USB type to **pantech-lte**.

Configuring Cellular Uplink Profiles

You can configure 3G or 4G uplinks using Aruba Central.

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **System**. The **System** page for the selected group or device opens.
4. Click **Uplink** and perform any of the following steps:

- To configure a 3G or 4G uplink automatically, select the **Country** and **ISP**. The parameters are automatically populated.
- To configure a 3G or 4G uplink manually, perform the following steps:

  a. Obtain the modem configuration parameters from the local IT administrator or the modem manufacturer.

  b. Enter the type of the 3G/4G modem driver type:
  - For 3G — Enter the type of 3G modem in the **USB type** text box.
  - For 4G — Enter the type of 4G modem in the **4G USB type** text box.

  c. Enter the device ID of modem in the **USB dev** text box.

  d. Enter the TTY port of the modem in the **USB tty** text box.

  e. Enter the parameter to initialize the modem in the **USB init** text box.

  f. Enter the parameter to dial the cell tower in the **USB dial** text box.

  g. Enter the username used to dial the ISP in the **USB user** text box.

  h. Enter the password used to dial the ISP in the **USB password** text box.

  i. Enter the parameter used to switch a modem from the storage mode to modem mode in the **USB mode switch** text box.

5. To configure 3G/4G switch network, provide the driver type for the 3G modem in the **USB type** text box and the driver type for 4G modem in the **4G USB type** text box.
6. Click **OK**.
7. Reboot the Instant AP for changes to affect.

Ethernet Uplink

The Ethernet 0 port on an Instant AP is enabled as an uplink port by default. The Ethernet uplink supports the following:

- PPPoE
- DHCP
- Static IP

You can use PPPoE for your uplink connectivity in a single AP deployment.

Uplink redundancy with the PPPoE link is not supported.

When the Ethernet link is up, it is used as a PPPoE or DHCP uplink. After the PPPoE settings are configured, PPPoE has the highest priority for the uplink connections. The Instant AP can establish a PPPoE session with a PPPoE server at the ISP and get authenticated using PAP or the CHAP. Depending upon the request from the PPPoE server, either the PAP or the CHAP credentials are used for authentication. After configuring PPPoE, reboot the Instant AP for the configuration to take effect. The PPPoE connection is dialed after the AP comes up. The PPPoE configuration is checked during Instant AP boot and if the configuration is correct, Ethernet is used for the uplink connection.

When PPPoE is used, do not configure Dynamic RADIUS Proxy and IP address of the VC. An SSID created with default VLAN is not supported with PPPoE uplink.

You can also configure an alternate Ethernet uplink to enable uplink failover when an Ethernet port fails.

Configuring PPPoE uplink profile

To configure PPPoE settings:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **System**. The **System** page for the selected group or device opens.
4. Click **Uplink**. Under **PPPoE**, configure the following parameters:
   a. Enter the **PPPoE service name** provided by your service provider in **Service Name**.
   b. In the **Chap Secret** and **Retype CHAP Secret** fields, enter the secret key used for CHAP authentication. You can use a maximum of 34 characters for the CHAP secret key.
   c. Enter the user name for the PPPoE connection in the **USER** field.
   d. In the **Password** and **Retype Password** fields, enter a password for the PPPoE connection and confirm it.
5. To set a local interface for the PPPoE uplink connections, select a value from **Local Interface**. The selected DHCP scope is used as a local interface on the PPPoE interface and the Local, L3 DHCP gateway IP address as its local IP address. When configured, the local interface acts as an unnumbered PPPoE interface and allocated the entire Local, L3 DHCP subnet to the clients.

NOTE

The options in **Local Interface** are displayed only if a Local, L3 DHCP scope is configured on the Instant AP.

6. Click **Save Settings**.
7. Reboot the Instant AP.

Wi-Fi Uplink

The Wi-Fi uplink is supported for all Instant AP models, except 802.11ac APs. Only the master Instant AP uses the Wi-Fi uplink. The Wi-Fi allows uplink to open, PSK-CCMP, and PSK-TKIP SSIDs.

- For single radio Instant APs, the radio serves wireless clients and Wi-Fi uplink.
- For dual radio Instant APs, both radios can be used to serve clients but only one of them can be used for Wi-Fi uplink.

NOTE

When Wi-Fi uplink is in use, the client IP is assigned by the internal DHCP server.

Configuring a Wi-Fi Uplink Profile

The following configuration conditions apply to the Wi-Fi uplink:

- To bind or unbind the Wi-Fi uplink on the 5 GHz band, reboot the Instant AP.
- If Wi-Fi uplink is used on the 5 GHz band, mesh is disabled. The two links are mutually exclusive.

To provision an Instant AP with Wi-Fi Uplink, complete the following steps:

1. If you are configuring a Wi-Fi uplink after restoring factory settings on an Instant AP, connect the Instant AP to an Ethernet cable to allow the Instant AP to get the IP address. Otherwise, go to step 2.
2. From the app selector, click **Wireless Management**.
3. From the group selector, select a group or a device.
4. On the left navigation pane, click **System**. The **System** page for the selected group or device opens.
5. Click **Uplink**, under **WiFi**, enter the name of the wireless network that is used for Wi-Fi uplink in the **Name (SSID)** box.
6. From **Management**, select the type of key for uplink encryption and authentication. If the uplink wireless router uses mixed encryption, WPA-2 is recommended for Wi-Fi uplink.
7. From **Band**, select the band in which the VC currently operates. The following options are available:
   - 2.4 GHz (default)
   - 5 GHz
8. From **Passphrase Format**, select a **Passphrase format**. The following options are available:
   - 8 - 63 alphanumeric characters
   - 64 hexadecimal characters

NOTE

Ensure that the hexadecimal password string is exactly 64 digits in length.

9. Enter a PSK passphrase in **Passphrase** and click **OK**.

Uplink Preferences and Switching

This topic describes the following procedures:

- Enforcing Uplinks on page 335

- Setting an Uplink Priority on page 335
- Enabling Uplink Pre-emption on page 335

By default, the AP-318, AP-374, AP-375, and AP-377 access points have Eth1 as the uplink port and Eth0 as the downlink port. Aruba recommends you not to upgrade the mentioned access points to 8.5.0.0 and 8.5.0.1 firmware versions as the upgrade process changes the uplink from Eth1 to Eth0 port thereby making the devices non-reachable.

Enforcing Uplinks

The following conditions apply to the uplink enforcement:

- When an uplink is enforced, the Instant AP uses the specified uplink regardless of uplink pre-emption configuration and the current uplink status.
- When an uplink is enforced and multiple Ethernet ports are configured and uplink is enabled on the wired profiles, the Instant AP tries to find an alternate Ethernet link based on the priority configured.
- When no uplink is enforced and pre-emption is not enabled, and if the current uplink fails, the Instant AP tries to find an available uplink based on the priority configured.
- When no uplink is enforced and pre-emption is enabled, and if the current uplink fails, the Instant AP tries to find an available uplink based on the priority configured. If current uplink is active, the Instant AP periodically tries to use a higher priority uplink and switches to the higher priority uplink even if the current uplink is active.

To enforce a specific uplink on an Instant AP, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **System**. The **System** page for the selected group or device opens.
4. Click **Uplink**.
5. Under **Management**, select the type of uplink from **Enforce Uplink**. If Ethernet uplink is selected, the **Port** field is displayed.
6. Specify the Ethernet interface port number.
7. Click **OK**. The selected uplink is enforced on the Instant AP.

Setting an Uplink Priority

To set an uplink priority:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **System**. The **System** page for the selected group or device opens.
4. Click **Uplink**.
5. Under **Uplink Priority List**, select the uplink, and increase or decrease the priority. By default, the Eth0 uplink is set as a high priority uplink.
6. Click **OK**. The selected uplink is prioritized over other uplinks.

Enabling Uplink Pre-emption

The following configuration conditions apply to uplink pre-emption:

- Pre-emption can be enabled only when no uplink is enforced.
- When pre-emption is disabled and the current uplink fails, the Instant AP tries to find an available uplink based on the uplink priority configuration.

- When pre-emption is enabled and if the current uplink is active, the Instant AP periodically tries to use a higher priority uplink, and switches to a higher priority uplink even if the current uplink is active.

To enable uplink pre-emption:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **System**. The **System** page for the selected group or device opens.
4. Click **Uplink**.
5. Under **Management**, ensure that the **Enforce Uplink** is set to **None**.
6. Set **Pre-Emption** to **ON**.
7. Click **OK**.

Switching Uplinks based on the Internet Availability

You can configure Aruba Central to switch uplinks based on the Internet availability.

When the uplink switchover based on Internet availability is enabled, the Instant AP continuously sends ICMP packets to some well-known Internet servers. If the request is timed out due to a bad uplink connection or uplink interface failure, and the Internet is not reachable from the current uplink, the Instant AP switches to a different connection.

To configure uplink switching, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **System**. The **System** page for the selected group or device opens.
4. Click **Uplink**.
5. Under **Management**, set **Internet Failover** to **ON**.
6. Specify values for **Failover Internet Packet Send Frequency**, **Failover Internet Packet Lost Count**, and **Internet Check Count**.
7. Click **OK**.

When **Internet failover** is enabled, the Instant AP ignores the VPN status, although uplink switching based on VPN status is enabled.

Mobility and Client Management

This section provides the following information on layer-3 mobility for Instant AP clients:

- Layer-3 Mobility for Instant AP Clients on page 336
- Configuring L3 mobility domain on page 337

Layer-3 Mobility for Instant AP Clients

Instant 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 Instant APs in a given Aruba Central

network can roam to Instant 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 Instant 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 L3 mobility domain, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **System**. The **System** page for the selected group or device opens.
4. Click **L3 Mobility**.
5. From **Home Agent Load Balancing**, select **Enabled**. By default, home agent load balancing is disabled.
6. Click **New** in **Virtual Controller IP Addresses**, add the IP address of a VC that is part of the mobility domain, and click **OK**.
7. Repeat Step 2 to add the IP addresses of all VCs that form the L3 mobility domain.
8. Click **New** in **Subnets** 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.
9. Click **OK**.

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. From the app selector, click **Wireless Management**.

2. From the group selector, select a group or a device.
3. On the left navigation pane, click **System**. The **System** page for the selected group or device opens.
4. Click **Enterprise Domains**.
5. Click **New** and enter a name in the **New Domain Name**.
6. Click **OK**.

To delete e a domain, select the domain and click **Delete**.

Configuring SNMP Parameters

This section provides the following information:

- SNMP Configuration Parameters on page 338
- Configuring Community String for SNMP on page 339
- Configuring SNMP Traps on page 339

SNMP Configuration Parameters

Aruba Central supports SNMPv1, SNMPv2c, and SNMPv3 for reporting purposes only. An Instant AP cannot use SNMP to set values in an Aruba system.

You can configure the following parameters for an Instant AP:

Table 97: *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 Instant 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: ■ **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 using the 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. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **System**. The **System** page for the selected group or device opens.
4. Click **SNMP**.
5. To add a new community string, click + and enter the string in the **New Community String** text box.
6. Click **OK**.
7. To delete a community string, select the string, and click **Delete**.

Creating community strings for SNMPv3 using Aruba Central

To create community strings for SNMPv3, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **System**. The **System** page for the selected group or device opens.
4. Click **SNMP**.
5. Select the type of authentication protocol from the **Auth protocol** drop-down list.
6. Enter the authentication password in the **Password** text box and retype the password in the **Retype** text box.
7. Select the type of privacy protocol from the **Privacy protocol** drop-down list.
8. Enter the privacy protocol password in the **Password** text box and retype the password in the **Retype** text box.
9. Click **OK**.
10. To edit the details for a particular user, select the user and click **Edit**.
11. To delete a particular user, select the user and click **Delete**.

Configuring SNMP Traps

Aruba Central supports the configuration of external trap receivers. Only the Instant AP acting as the VC generates traps. The OID of the traps is 1.3.6.1.4.1.14823.2.3.3.1.200.2.X.

To configure SNMP traps, complete the following steps.

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **System**. The **System** page for the selected group or device opens.
4. Click **SNMP**.
5. Under **SNMP Traps**, enter a name in the **SNMP Engine ID** text box. It indicates the name of the SNMP agent on the access point. The SNMPV3 agent has an engine ID that uniquely identifies the agent in the device and is unique to that internal network.

6. Click **+** and update the following fields:

- **IP Address—** Enter the **IP Address** of the new SNMP Trap receiver.
- **Version**— Select the SNMP version— **v1, v2c, v3** from the drop-down list. The version specifies the format of traps generated by the access point.
- **Community/Username**— Specify the community string for SNMPv1 and SNMPv2c traps and a username for SNMPv3 traps.
- **Port**— Enter the port to which the traps are sent. The default value is 162.
- **Inform**— When enabled, traps are sent as SNMP INFORM messages. It is applicable to SNMPv3 only. The default value is **Yes**.

7. Click **OK** to view the trap receiver information in the **SNMP Trap Receivers** window.

Configuring Syslog and TFTP Servers for Logging Events

This section provides the following information:

- Configuring Syslog Server on Instant APs on page 340
- Configuring TFTP Dump Server Instant APs on page 341

Configuring Syslog Server on Instant APs

To specify a syslog server for sending syslog messages to the external servers:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **System**. The **System** page for the selected group or device opens.
4. Click **Logging**.
5. Under **Servers**, enter the IP address of the server to which you want to send system logs in the **Syslog Server** box.
6. Select the required values to configure Syslog Facility Levels. 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 Instant AP supports the following syslog facilities:

- **AP-Debug**—Detailed log about the AP device.
- **Network**— Log about change of network, for example, when a new Instant 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 98 describes the logging levels in order of severity, from the most severe to the least.

Table 98: *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.

7. Click **Save Settings**.

Configuring TFTP Dump Server Instant APs

To configure a TFTP server for storing core dump files, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **System**. The **System** page for the selected group or device opens.
4. Click **Logging**.
5. Under **Servers**, enter the IP address of the TFTP server in the **TFTP Dump Server** box.
6. Click **Save Settings**.

Resetting an AP

You can reset the system configuration of an Instant AP by erasing the existing configuration on the Instant AP. To erase the existing configuration on an Instant AP, perform any of the following procedures:

Clearing Instant AP Configuration Using Groups

To reset an Instant AP using groups, complete the following steps:

1. Create a new group. Ensure that the group has no additional configuration.
2. Move the Instant AP that you want to reset, under the new group. After the Instant AP is moved to a new group, the configuration on the Instant AP is erased and the default group configuration is pushed to the Instant AP. However, in this procedure, only the system configuration is cleared and the **Per AP Settings** on the Instant AP are retained.

Resetting an AP through the Console

To reset an Instant AP from the console, complete the following steps:

1. Log in to the Instant AP console. To access the Instant AP console:
2. Select **Monitoring & Reporting** app.
3. Click APs and select List from the APs drop-down.
4. Select the AP to reset.
5. From the **Actions** drop-down, click **Console**.
6. Execute the **write erase all** command at the command prompt.
7. Reboot the Instant AP. With this procedure, the complete configuration including the **Per AP Settings** on the Instant AP is reset.

   After the reboot, the Instant AP is moved to default group and will not be present in the group to which it was previously attached.

For information on resetting an Instant AP to factory default configuration by using the reset button on the device, see *Aruba Instant User Guide*.

Rebooting APs

You can reboot an Instant AP or an Instant AP cluster using the Aruba Central UI.

Perform any of the following procedures:

Reboot an Instant AP

To reboot an Instant AP:

1. From the app selector, click **Monitoring & Reports** and go to **Network Overview** > **APs**.
2. Select **List of Up APs**. The **Access Points** table displays a list of Instant APs in the group.
3. In the **Access Points** table, select the Instant AP to reboot.
4. In the **Actions** drop-down list, click **Reboot AP**.
5. In the **Reboot** dialog box, click **Continue**.

Reboot an Instant AP cluster

To reboot an Instant AP cluster:

1. From the app selector, click **Monitoring & Reports** and go to **Network Overview** > **APs**.
2. Select **List of Up APs**. The **Access Points** table displays a list of Instant APs in the group.
3. In the **Access Points** table, select the master Instant AP to reboot.
4. In the **Actions** drop-down list, click **Reboot Swarm**.
5. In the **Reboot** dialog box, click **Continue**.

Mapping Instant AP Certificates

When an Instant AP joins a group that does not have a certificate, the Instant AP's existing certificate is retained. When an Instant AP joins a group that already has a certificate, the Instant AP's certificate is overwritten by the group's certificate.

To map an Instant AP certificate name to a specific certificate type or category, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **Security**. The **Security** page for the selected group or device opens.
4. Click **Certificate**.
5. To map a certificate to a specific certificate category, click **Certificate Usage**.
6. Select the required certificate from the corresponding drop-down list. Aruba Central supports the following types of certificates:
   - Server certificates for RADIUS, Captive Portal, and RadSec (for cloud guest networks) authentication.
   - CA certificates—To validate the identity of a client.
   - Authentication Server—To verify the identity of the server to a client.
   - Captive portal server—To verify the identity of internal captive portal server.
   - RadSec—To verify the identity of the TLS server.
   - RadSec CA—For mutual authentication between the Instant AP and the TLS server.
7. Save the changes. Aruba Central pushes the certificate to all Instant APs in that group.

To enable certificates for the Cloud Guest Service, contact the Aruba Central support team.

For more information on the **Wireless Management** app and Instant AP procedures, see *Wireless Management* in the Aruba Central Help Center.

Configuring HTTP Proxy on Instant AP

If your network requires a proxy server for Internet access, ensure that you configure the HTTP proxy on the Instant AP to download the image from the cloud server. After setting up the HTTP proxy settings, the Instant 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 Instant AP) by providing their host name or IP address under exceptions. Aruba Central allows the user to configuring HTTP proxy on an Instant AP.

To configure HTTP proxy on Instant AP through Aruba Central, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the group selector, select a group or a device.
3. On the left navigation pane, click **System**. The **System** page for the selected group or device opens.
4. Click **Proxy** and specify the following:
   a. Enter the HTTP proxy server IP address in the **Server** box.
   b. Enter the port number in the **Port** box.
5. Click **OK**.

Aruba Central displays the **Username**, **Password,** and **Retype Password** fields under **Wireless Management** > **System** > **Proxy** for Instant AP running Aruba Instant 8.3.0.0. The Instant APs with the Aruba Instant 8.3.0.0 firmware require user credentials for proxy server authentication.

Configuring Instant APs Using Templates

Templates in Aruba Central 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 Instant AP deployments.

To minimize configuration errors and troubleshoot device-specific configuration issues, Aruba recommends that the device administrators familiarize themselves with the CLI configuration commands available on Aruba Instant APs.

Creating a Group for Template-Based Configuration

For template-based provisioning, Instant APs must be assigned to a group with template-based configuration method enabled.

For more information, see Creating a Group on page 76 and Assigning Devices to Groups on page 77.

Creating a Configuration Template

To create a template for the devices in a template group, complete the following steps:

1. From the app selector, click **Wireless Configuration**.
2. Select a template group. The template configuration menu options are displayed.
3. Click **Templates**. The **Templates** page opens.
4. Click **+** to add a new template. The **Add Template** window opens.
5. Add the template name.
6. Set the model and firmware version parameters to **ALL**.
7. Add the CLI script content. Note the following points for adding contents 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 Instant 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.

8. Click **OK**.

The variables configured for the Instant 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 Instant 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%

wlan ssid-profile %ssid_name%
%if disable_ssid=true%
disable-ssid
%endif%
%if ssid_security=wpa2%
opmode wpa2-aes
%else%
opmode opensystem
%endif%

%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%
```

Aruba switches enable secure, role-based network access for wired users and devices, independent of their location or application. With Aruba switches, enterprises can deploy a consistent and secure access to network resources based on the type of users, client devices, and connection methods.

Aruba Central offers a cloud-based management platform for managing your Aruba switch infrastructure. It simplifies switch management with flexible configuration options, monitoring dashboards, and troubleshooting tools.

Provisioning Factory Default Switches

Switches that run default configuration either after shipped from a factory or a factory reset are referred to as factory default switches. This topic describes the steps for provisioning factory default switches in Aruba Central.

Step 1: Onboard the Switch to Aruba Central

To onboard switches to the device inventory in Aruba Central, complete the following steps:

- Log in to Aruba Central
- Add switches to Aruba Central
- Assign Subscriptions

Step 2: Assign the Switch to a Group

Before assigning a group, determine if the switch must be provisioned in a UI or template group. By default, Aruba Central assigns the factory default switches to default group. You can create a new group and assign switch to the new group.

For more information on creating a group, see Creating a Group on page 76.

To assign a device to a group from the **Global Setting** > **Device Inventory** page:

1. Select the device that you want to assign to a group.
2. Click **Assign Group**. The **Assign Group** pop-up window opens.

3. Select the group to which you want to assign.
4. Click **Assign Device(s)**.

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

1. Click **Global Settings** > **Manage Groups**. The **Groups** page opens.
2. From the devices table on the right, select the device that you want to assign to a new group.
3. Drag and drop the device to the group to which you want to assign the device.

Step 3: Connect the Switch to Aruba Central

Switches with factory default configuration have very basic configuration for all ports in VLAN-1 that is required for obtaining an IP address and automatic provisioning (ZTP). For ZTP, switches must have a valid IP address, DNS, and NTP configuration.

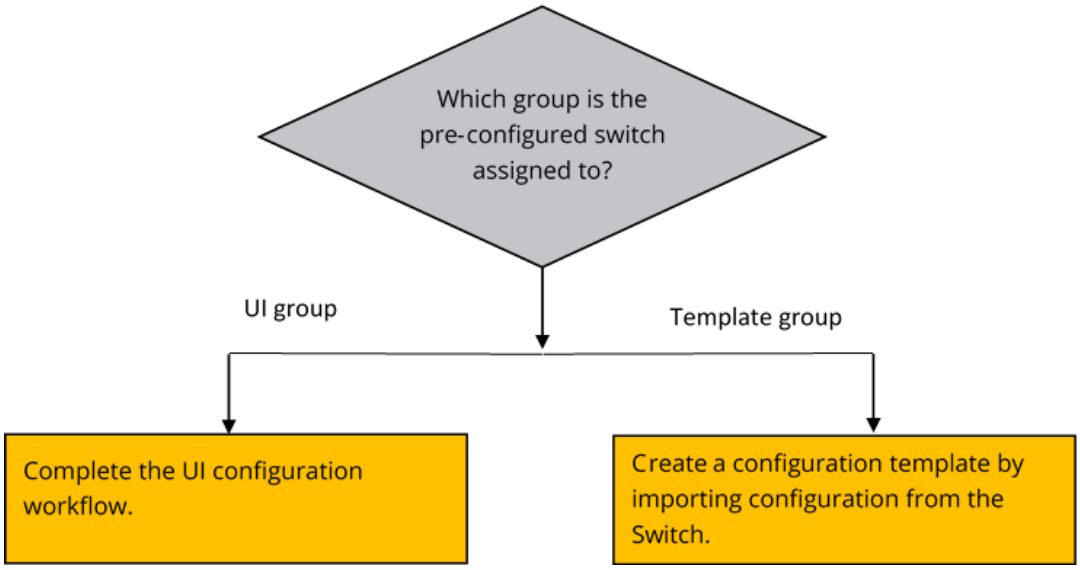
When a factory default switch is powered on and connected to the Internet, it establishes connection with Aruba Activate and downloads the provisioning parameters. If the switch is already added and assigned a subscription, it connects to Aruba Central.

Step 4: Provision the Switch to a Group

When the switch connects to Central, if it is already added to the device inventory and is assigned a subscription in Aruba Central, Aruba Central assigns it to a pre-assigned group. If there is no pre-assigned group, Aruba Central moves the device to **default** group. Based on your configuration requirements, you create a UI group or template group and assign the switch.

The following figure illustrates the provisioning step required for each group type.

Figure 95 *Switch Provisioning Steps Per Group Type*



If the switch is assigned to a new UI group, Aruba Central uses the current configuration of switch as base configuration and applies it to the other switches that join this group later. You can also modify the group configuration using the UI menu options under **Wired Management**. For more information, see Configuring or Viewing Switch Properties in UI Groups.

Provisioning Switches in Template Groups

If you have assigned the switch to a template group, create a new configuration template. To create a configuration template:

1. From the app selector, click **Wired Configuration**.
2. Select a template group. The **Templates** page opens.
3. Click **+** to add a new template. The **Add Template** pop-up window opens.
4. Enter a name for the template.
5. Ensure that **Aruba Switch** is selected as the **Device**.
6. Select the switch model and the software version to which you want to apply the new template. You can specify any of the following combinations:
   - **ALL** for both **Model** and **Version**—To apply the template to all switch models and all supported switch software versions.
   - **ALL** for **Model** and a specific software version for **Version**—To apply the template to all switch models running the specified software version.
   - **ALL** for **Version** and a specific switch model for **Model**—To apply the template to a specific switch model and all software versions supported by the selected switch model.
   - A specific switch model and a software version—To apply the template to a specific switch model and the software version. The template created for a specific switch model and a firmware version takes precedence over the template that is created for all platforms and versions.
7. Enter the manufacturing part number of the switch for **Part Number**. The **Part Number** field is not applicable for switch stacks.
8. Build a new template or import configuration information from a switch that is already provisioned in the template group.
   - To build a new template, add the switch command information in the **Template Text** field. Ensure that the template text adheres to the guidelines listed in Using Configuration Templates for Switch Management on page 356.
   - To import configuration text from a switch that is already provisioned in the template group:
     a. Select the switch from which you want to import the configuration.
     b. Click **Import Template**. The imported configuration is displayed in the **Template** text box.

Importing configuration from an existing device in the template group allows you to quickly create a basic template. However, before applying the template to other switches in the group, ensure that the template text is variabilized as per your deployment requirements. For more information see Managing Variable Files.

9. Click **Save**. After you apply the configuration template, switches reboot and reconnect to Aruba Central with the new configuration.

Step 5: Verify the Configuration Status

To verify the configuration status:

1. From the app selector, click **Wired Management**.
   - To verify the configuration status for a template group, select the template group and click **Configuration Audit**. The **Configuration Audit** dashboard displays the number of devices with template and configuration synchronization errors.

- To view configuration errors for a specific device, select a switch from the filter bar. The **Configuration Audit** dashboard displays the number of template and configuration synchronization errors for the device.

2. To view template errors, click **View Template Errors**.
3. To view configuration synchronization errors, click **Failed Config Difference**.
4. To compare running configuration and pending changes, click **View** under **Config Comparsion Tool**.

Provisioning Pre-Configured Switches

Unlike factory default switches, locally managed switches and the switches with custom configuration require one touch provisioning. These switches do not automatically identify Aruba Central as their management platform, therefore you must manually enable the Aruba Central management service on these switches to allow them to connect to Aruba Central.

To onboard a locally-managed or a pre-configured switch to Aruba Central, follow one of the following options:

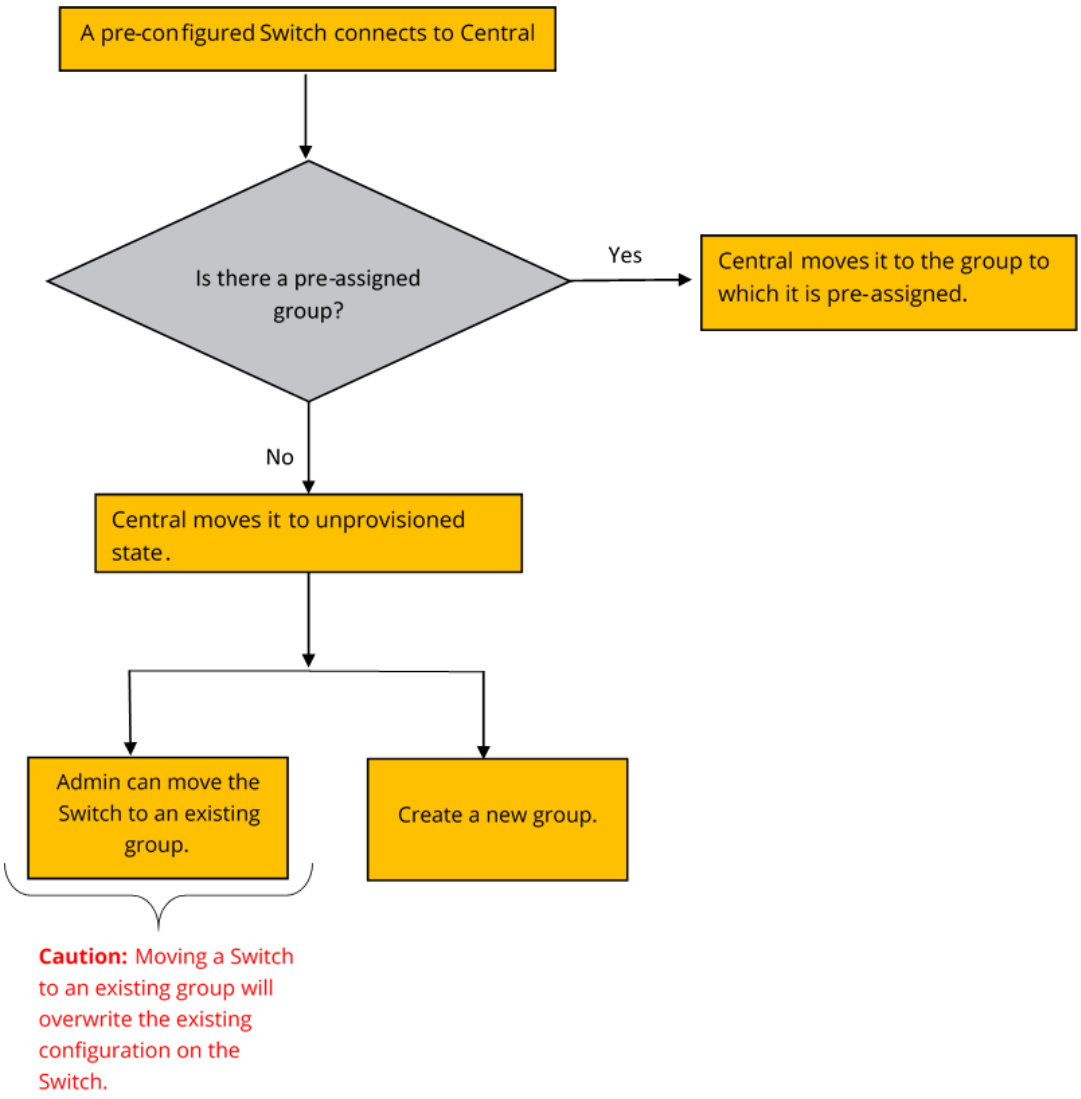
- Manually enable Aruba Central management service on the switch and connect it to Aruba Central. Aruba recommends that you use this option if you want to preserve the current configuration running on the switch. For more information on this procedure, see the workflows described in this topic.
- Reset the switch configuration to factory default and use ZTP to provision the switch. For information on provisioning factory default switches, see Provisioning Factory Default Switches on page 347.

Aruba Central supports provisioning switches using one of the following methods:

- Pre-provisioning—In this workflow, a switch is added to the device inventory and assigned a group in Aruba Central before it connects to Aruba Central.
- Onboarding connected switches—In this workflow, Aruba Central onboards the switch that attempts to connect and then assigns a group.

The following figure illustrates provisioning procedure for a pre-configured switch.

Figure 96 *Provisioning Workflow for Pre-Configured Switches*



Workflow 1—Pre-Provisioning a Switch

The pre-provisioning workflow includes the following steps:

- Step 1: Onboard the Switch to Aruba Central
- Step 2: Assign the Switch to a Group
- Step 3: Enable Aruba Central Management Service on the Switch
- Step 4: Provision the Switch to a Group
- Step 5: Verify the Configuration Status

Step 1: Onboard the Switch to Aruba Central

To onboard switches to the device inventory in Aruba Central, complete the following steps:

- Log in to Aruba Central
- Add switches to Aruba Central

- Assign Subscriptions

Step 2: Assign the Switch to a Group

Before assigning a group, determine if the switch must be provisioned in a UI or template group. If you want to preserve the existing configuration on the switch, Aruba recommends that you create a new group for the switch.

For more information on creating a group, see Creating a Group.

To assign a device to a group from the **Global Setting** > **Device Inventory** page:

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

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

1. Click **Global Settings** > **Manage Groups**. The **Groups** page opens.
2. From the devices table on the right, select the device that you want to assign to a new group.
3. Drag and drop the device to the group to which you want to assign the device.

Step 3: Enable Aruba Central Management Service on the Switch

A locally-managed or pre-configured switch cannot connect to Aruba Central, unless it is configured to identify Aruba Central as its management entity. To manage such a device from Aruba Central, you must manually enable the provisioning and management service on the switch.

1. Verify if the Activate provisioning service is enabled by executing the following command at the switch CLI:

```
switch)# show activate provision
Configuration and Status - Activate Provision Service
Activate Provision Service    : Enabled
Activate Server Address       : device.arubanetworks.com
```

2. If the Activate provision service is not enabled, execute the following command at the switch CLI:

```
(switch)# activate provision enable
```

3. To enable switches to automatically connect to Aruba Central, enforce ZTP on the switch:

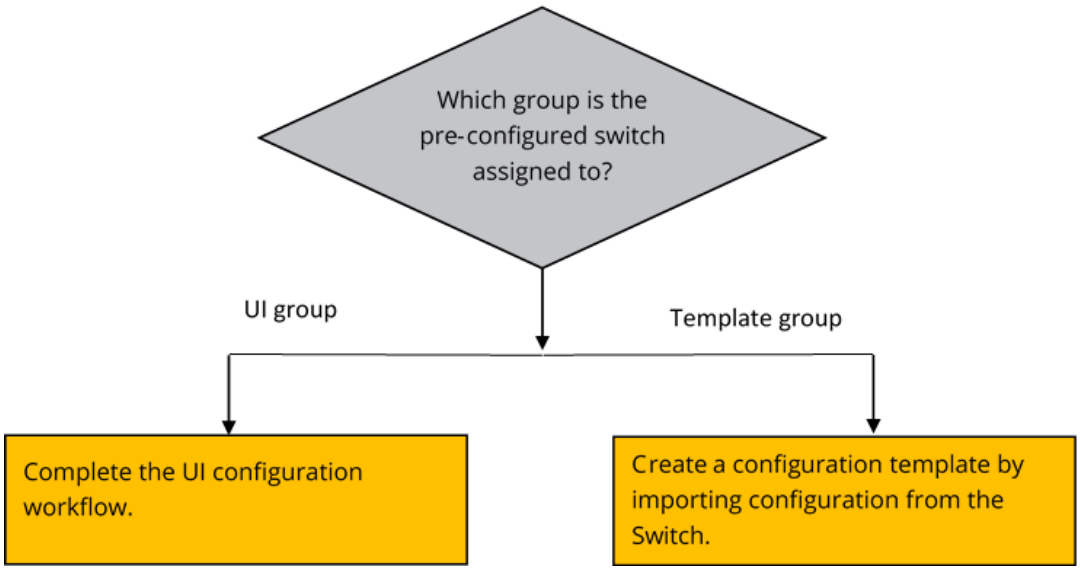
```
(switch)# activate provision force
```

The switch establishes connection with Activate and is directed to Aruba Central. If the switch is already added to the device inventory and is assigned a subscription, Aruba Central assigns it to a pre-assigned group.

Step 4: Provision the Switch to a Group

When the switch connects to Aruba Central, Aruba Central automatically assigns it to the pre-assigned group. The following figure illustrates the provisioning steps for each group type.

Figure 97 *Switch Provisioning Steps Per Group Type*



If the switch is assigned to a new UI group, you can modify the group configuration using the UI menu options under **Wired Management**. For more information, see Configuring or Viewing Switch Properties in UI Groups.

If you have assigned the switch to a template group, you can import the existing configuration to a new configuration template and apply this template to other devices in the group. To create a configuration template using the existing configuration on the switch:

1. From the app selector, click **Wired Configuration**.
2. Select a template group. The **Templates** page opens.
3. Click **+** to add a new template. The **Add Template** pop-up window opens.
4. Enter a name for the template.
5. Ensure that **Aruba Switch** is selected as the **Device**.
6. Select the switch model and the software version to which you want to apply the new template. You can specify any of the following combinations:
   - **ALL** for both **Model** and **Version**—To apply the template to all switch models and all supported switch software versions.
   - **ALL** for **Model** and a specific software version for **Version**—To apply the template to all switch models running the specified software version.
   - **ALL** for **Version** and a specific switch model for **Model**—To apply the template to a specific switch model and all software versions supported by the selected switch model.
   - A specific switch model and a software version—To apply the template to a specific switch model and the software version. The template created for a specific switch model and a firmware version takes precedence over the template that is created for all platforms and versions.
7. Enter the manufacturing part number of the switch for **Part Number**. The **Part Number** field is not applicable for switch stacks.
8. Import configuration from the switch.

Importing configuration from the switch allows you to quickly create a basic configuration template that you can apply for all devices in a template group. Before applying the template to other switches in the group, ensure that the template text is variabilized based on the deployment requirements. For more information on configuration

templates and variable definitions, see Using Configuration Templates for Switch Management and Managing Variable Files.

9. Click **Save**. After you apply the configuration template, switches reboot and reconnect to Aruba Central with the new configuration.

Step 5: Verify the Configuration Status

To verify the configuration status:

1. From the app selector, click **Wired Management**.
   - To verify the configuration status for a template group, select the template group and click **Configuration Audit**. The **Configuration Audit** dashboard displays the number of devices with template and configuration synchronization errors.
   - To view configuration errors for a specific device, select a switch from the filter bar. The **Configuration Audit** dashboard displays the number of template and configuration synchronization errors for the device.
2. To view template errors, click **View Template Errors**.
3. To view configuration synchronization errors, click **Failed Config Difference**.
4. To compare running configuration and pending changes, click **View** under **Config Comparsion Tool**.

Workflow 2—Provisioning a Switch On-Demand

To dynamically provision switches on-demand, complete the following steps:

- Step 3: Enable Aruba Central Management Service on the Switch
- Step 2: Add the Switch to Aruba Central
- Step 3: Assign a Subscription
- Step 4: Provision the Switch to a Group
- Step 5: Verify the Configuration Status

Step 1: Enable Aruba Central Management Service on the Switch

A locally-managed or pre-configured switch cannot connect to Aruba Central, unless it is configured to identify Aruba Central as its management entity. To manage such a device from Aruba Central, you must manually enable the provisioning and management service on the switch.

1. Verify if the Activate provisioning service is enabled by executing the following command at the switch CLI:

```
switch)# show activate provision
Configuration and Status - Activate Provision Service
Activate Provision Service    : Enabled
Activate Server Address       : device.arubanetworks.com
```

2. If the Activate provision service is not enabled, execute the following command at the switch CLI:

```
(switch)# activate provision enable
```

3. To enable switches to automatically connect to Aruba Central, enforce ZTP on the switch:

```
(switch)# activate provision force
```

The switch establishes connection with Activate. Activate directs the switch to Aruba Central.

Step 2: Add the Switch to Aruba Central

Add the switch to the Aruba Central device inventory. For more information, see Onboarding Devices on page 59

Step 3: Assign a Subscription

To allow Aruba Central to manage the switch, ensure that a valid subscription is assigned to the switch. For more information, see Managing Subscriptions on page 63.

Step 4: Provision the Switch to a Group

If the switch has a valid subscription assigned, Aruba Central marks the switch as **unprovisioned**. To preserve the switch configuration, move it to a new group.

To move the device to a UI group:

1. Go to **Global Settings** > **Manage Groups**.
1. On the **Groups** page, select the device.
2. Click **Import Configuration to New Group**. The **Import Configuration** pop-up window opens.
3. Enter a name for the group.
4. Configure a password for the group.
5. Click **Import Configuration**. Aruba Central imports the switch configuration to the new group. You can also modify the group configuration using the UI menu options under **Wired Management**. For more information, see Configuring or Viewing Switch Properties in UI Groups.

To move the device to a template group:

1. Create a template group.
2. On the **Groups** page, select the switch.
3. Drag and drop the switch the new template group that you just created. Aruba Central adds the switch to the new template group.
4. To import switch configuration to a new configuration template:
   a. From the app selector, click **Wired Configuration**.
   b. Select a template group. The **Templates** page opens.
   c. Click **+** to add a new template. The **Add Template** pop-up window opens.
   d. Enter a name for the template.
   e. Select **Aruba Switch** from the **Device** drop-down.
   f. Select the switch model and the software version to which you want to apply the new template. You can specify any of the following combinations:
   - **ALL** for both **Model** and **Version**—To apply the template to all switch models and all supported switch software versions.
   - **ALL** for **Model** and a specific software version for **Version**—To apply the template to all switch models running the specified software version.
   - **ALL** for **Version** and a specific switch model for **Model**—To apply the template to a specific switch model and all software versions supported by the selected switch model.

- A specific switch model and a software version—To apply the template to a specific switch model and the software version. The template created for a specific switch model and a firmware version takes precedence over the template that is created for all platforms and versions.

5. Enter the manufacturing part number of the switch for **Part Number**.
6. Import configuration from the switch.

Importing configuration from the switch allows you to quickly create a basic configuration template that you can apply for all devices in a template group. Before applying the template to other switches in the group, ensure that the template text is variabilized based on the deployment requirements. For more information on configuration templates and variable definitions, see Using Configuration Templates for Switch Management and Managing Variable Files.

7. Click **Save**. After you apply the configuration template, switches reboot and reconnect to Aruba Central with the new configuration.

Step 5: Verify the Configuration Status

To verify the configuration status:

1. From the app selector, click **Wired Management**.
   - To verify the configuration status for a template group, select the template group and click **Configuration Audit**. The **Configuration Audit** dashboard displays the number of devices with template and configuration synchronization errors.
   - To view configuration errors for a specific device, select a switch from the filter bar. The **Configuration Audit** dashboard displays the number of template and configuration synchronization errors for the device.
2. To view template errors, click **View Template Errors**.
3. To view configuration synchronization errors, click **Failed Config Difference**.
4. To compare running configuration and pending changes, click **View** under **Config Comparsion Tool**.

Using Configuration Templates for Switch Management

Templates in Aruba Central refer to a set of configuration commands that can be used by the administrators for provisioning devices in a group. Configuration templates enable administrators to apply a set of configuration parameters simultaneously to multiple switches in a group and thus automate switch deployments.

To minimize configuration errors and troubleshoot device-specific configuration issues, Aruba recommends that the device administrators familiarize themselves with the CLI configuration commands available on Aruba switches.

Creating a Group for Template-Based Configuration

For template-based provisioning, switches must be assigned to a group with template-based configuration method enabled.

For more information, see Creating a Group on page 76 and Assigning Devices to Groups on page 77.

Creating a Configuration Template

To create a configuration template for switches:

1. From the app selector, click **Wired Configuration**.
2. Select a template group. The **Templates** page opens.

3. Click **+** to add a new template. The **Add Template** pop-up window opens.
4. Enter a name for the template.
5. Ensure that **Aruba Switch** is selected in the **Device** drop-down.
6. Select the switch model and the software version. You can specify any of the following combinations:
   - **ALL** for both **Model** and **Version**—To apply the template to all switch models and all supported switch software versions.
   - **ALL** for **Model** and a specific software version for **Version**—To apply the template to all switch models running the specified software version.
   - **ALL** for **Version** and a specific switch model for **Model**—To apply the template to a specific switch model and all software versions supported by the selected switch model.
   - A specific switch model and a software version—To apply the template to a specific switch model and the software version. The template created for a specific switch model and a firmware version takes precedence over the template that is created for all platforms and versions.
7. Enter the manufacturing part number of the switch for **Part Number**. The **Part Number** field is not applicable for switch stacks.
8. Build a new template or import configuration information from a switch that is already provisioned in the template group.
   - To build a new template, add the switch command information in the **Template Text** field. Ensure that the template text adheres to the guidelines listed in the Important Points to Note on page 357.
   - To import configuration text from a switch that is already provisioned in the template group:
     a. Select the switch from which you want to import the configuration.
     b. Click **Import Template**. The imported configuration is displayed in the **Template** text box.
     c. If required, modify the configuration parameters. Ensure that the template text adheres to the guidelines listed in the Important Points to Note on page 357.

Importing configuration from an existing device in the template group allows you to quickly create a basic template. However, before applying the template to other switches in the group, ensure that the template text is variabilized based on the deployment requirements. For more information on template variables, see Managing Variable Files.

9. Click **Save**. After you apply the configuration template, switches reboot and reconnect to Aruba Central with the new configuration.

Important Points to Note

Note the following points when adding configuration text to a template:

- The CLI syntax in the switch template must be accurate. Aruba recommends that you validate the configuration syntax on the switch before adding it to the template text.
- Ensure that the command text indentation matches the indentation in the running configuration.
- The commands in the template are case-sensitive.

  The following example illustrates the case discrepancies that the users must avoid in the template text:

```
trunk E1-E4 trk1 trunk
interface Trk1
  dhcp-snooping trust
  exit

trunk E1-E4 trk1 trunk
switch-interconnect trk1

trunk E5-E6 trk2 trunk
vlan 5
```

```
  name "VLAN5"
  untagged Trk2
  tagged Trk1
  isolate-list Trk1
  ip igmp forcedfastleave Trk1
  ip igmp blocked Trk1
  ip igmp forward Trk1
  forbid Trk1

loop-protect Trk2

trunk E1-E4 trk1 trunk
trunk E4-E5 trk2 trunk
spanning-tree Trk1 priority 4
spanning-tree Trk2 admin-edge-port

trunk A2-A4 trk1 trunk
igmp fastlearn Trk1

trunk E4-E5 trk2 trunk
ip source-binding 2 4.5.6.7 b05ada-96a4a0 Trk2

[no] ip source-binding trap OutOfResources

snmp-server mib hpSwitchAuthMIB ..

snmp-server mib hpicfMACsec unsecured-access ..

[no] lldp config <P-PORT-LIST> dot1TlvEnable ..

[no] lldp config <P-PORT-LIST> medTlvEnable ..

no lldp config <P-PORT-LIST> medPortLocation..

[no] lldp config <P-PORT-LIST> dot3TlvEnable ..

[no] lldp config <P-PORT-LIST> basicTlvEnable ..

[no] lldp config <P-PORT-LIST> ipAddrEnable <lldp-ip>

trunk-load-balance L4-based
trunk-load-balance L3-based
```

Managing Variable Files

Aruba Central allows you to configure multiple devices in bulk using templates. However, in some cases, the configuration parameters may vary per device. To address this, Aruba Central identifies some customizable CLI parameters as variables and allows you to modify the definitions for these variables as per your requirements.

You can download a sample file with variables for a template group or for the devices deployed in a template group, update the variable definitions, upload the file with the customized definitions, and apply these configuration changes in bulk.

Downloading Sample Variables File

The sample variables file includes a set of sample variables that the users can customize. You can download the sample variables file in the JSON or CSV format.

To download a sample variables file:

1. Go to **Variables**.
   - For switches—Go to **Wired Management** > **Variables**.
   - For Instant APs—Go to **Wireless Management** > **Variables**.
   - For Gateways—Go to **Gateway Management** > **Variables**.
2. Download the sample variables file.
   - To download a sample variables file for the device group, select a template group.
   - To download a sample variables file for a device, select the device from the filter bar.
3. Select any of the following format:
   - JSON—shows the file JSON format.
   - CSV—Shows the variables in different columns.
4. Click **Download Sample Variables File**. The sample variables file is saved to your local directory.

Modifying a Variable File

The CSV file includes the following columns for which the variable definitions are mandatory:

- **_sys_serial**—For serial number of the device
- **_sys_lan_mac**—For MAC address of the device
- **modified**—To indicate the modification status of the device. The value for this column is set to N in the sample variables file. When you edit a variable definition, set the **modified** column to **Y** to allow Aruba Central to parse the modified definition.

Predefined Variables

The system defined variables in the sample variables files are indicated with **_sys** prefix.

Table 99shows a list of predefined variables for switches.

Table 99: *Predefined Variables Example*

Variable Name	Description	Variable Value
_sys_gateway	Populates gateway IP address.	10.22.159.1
_sys_hostname	Maintains unique host name.	HP-2920-48G-POEP
_sys_ip_address	Indicates the IP address of the device.	10.22.159.201
_sys_module_command	Populates module lines	module 1 type j9729a
_sys_netmask	Netmask of the device.	255.255.255.0

Variable Name	Description	Variable Value
_sys_oobm_command	Represents Out of Band Management (OOBM) block.	oobm ip address dhcp-bootp exit
_sys_snmpv3_engineid	Populates engine ID.	00:00:00:0b:00:00:5c:b9:01:22:4c:00
_sys_stack_command	Represents stack block	stacking member 1 type "J9729A" mac-address 5cb901-224c00 exit
_sys_template_header	Represents the first two lines of the configuration file. Ensure that this variable is the first line in the template.	; J9729A Configuration Editor; Created on release #WB.16.03.0003+ ; Ver #0f:3f.f3.b8.ee.34.79.3c.29.eb.9f.fc.f3.ff.37.ef:91
_sys_use_dhcp	Indicates DHCP status (true or false) of VLAN 1	0
_sys_vlan_1_untag_command	Indicates untagged ports of VLAN 1	1-28,A1-A2
_sys_vlan_1_tag_command	Indicates tagged ports of VLAN 1	28-48

The **_sys_template_header_** and **_sys_snmpv3 engineid** are mandatory variables that must have the values populated, irrespective of their use in the template. If there is no value set for these variables, Aruba Central re-imports the values for these mandatory variables when it processes the running configuration of the device.

For Instant APs, the sample variables file includes the **_sys_allowed_ap** variable for which you can specify a value to allow new APs to join the Instant AP cluster.

Important Points to Note

The following conditions apply to the variable files:

- The variable names must be on the left side of condition and its value must be defined on the right side. For example, %if var=100% is supported and %if 100=var% is not supported.
- The < or <= or > or >= operators should have only numeric integer value on the right side. The variables used in these 4 operations are compared as integer after flooring. For example, if any float value is set as %if dpi_value > 2.8%, it is converted as %if dpi_value > 2 for comparison.
- The variable names should not include white space, and the **&** and **%** special characters. The variable names must match regular expression [a-zA-Z0-9_]. If the variables values with **%** are defined, ensure that the variable is surrounded by space. For example, *wlan ssid-profile %ssid_name%*.
- The first character of the variable name must be an alphabet. Numeric values are not accepted.
- The values defined for the variable must not include spaces. If quotes are required, they must be included as part of the variable value. For example, if the intended variable name is *wlan ssid-profile "emp ssid"*, then the recommended format for the syntax is "*wlan ssid-profile %ssid_name%*" and variable as *"ssid_name": "\"emp ssid\""*.
- If the configuration text has the percentage sign **%** in it—for example, **"url "/portal/scope.cust-5001098/Splash%20Profile%201/capture"**—Aruba Central treats it as a variable when you save the template. To allow the use of percentage **%** as an escape character, use **\"** in the variable definition as shown in the following example:

Template text

```
wlan external-captive-portal "Splash Profile 1_#guest#_"
server naw1.cloudguest.central.arubanetworks.com
port 443
url %url%
```

Variable

```
"url": "\"/portal/scope.cust-5001098/Splash%20Profile%201/capture\""
```

- Aruba Central supports adding multiple lines of variables in Instant AP configuration templates. If you want to add multiple lines of variables, you must add the `HAS_MULTILINE_VARIABLE` directive at the beginning of the template.

  Example

  ```
  #define HAS_MULTILINE_VARIABLE 1
  %if allowed_aps%
  %allowed_aps%
  %endif%
  ```

  Variable

  ```
  "allowed_aps": "allowed-ap 24:de:c6:cb:76:4e\n allowed-ap ac:a3:1e:c5:db:d8\n allowed-ap
  84:d4:7e:c4:8f:2c"
  ```

For Instant APs, you can configure a variable file with a set of values defined for a master AP in the network. When the variable file is uploaded, the configuration changes are applied to all Instant AP devices in the cluster.

Examples

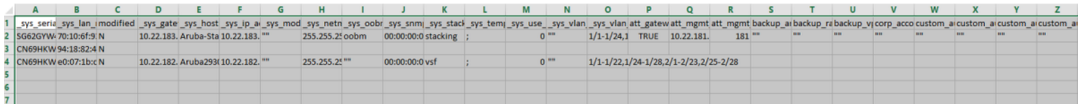
The following example shows the contents of a variable file in the JSON format for Instant APs:

```
{
"CK0036968": {
"_sys_serial": "CK0036968",
"ssid": "s1",
"_sys_lan_mac": "ac:a3:1e:c5:db:7a",
"vc_name": "test_config_CK0036968",
"org": "Uber_org_test",
"vc_dns_ip":"22.22.22.22",
"zonename": "Uber_1",
"uplinkvlan": "0",
"swarmmode": "cluster",
"md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
"hostname": "Uber_1"
},
"CJ0219729": {
"_sys_serial": "CJ0219729",
"ssid": "s1",
"_sys_lan_mac": "ac:a3:1e:cb:04:92",
"vc_name": "test_config_CK0036968",
"org": "Uber_org_test",
"vc_dns_ip":"22.22.22.22",
"zonename": "Uber_1",
"uplinkvlan": "0",
"swarmmode": "cluster",
"md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
"hostname": "Uber_2"
},
"CK0112486": {
"_sys_serial": "CK0112486",
"ssid": "s1",
"_sys_lan_mac": "ac:a3:1e:c8:29:76",
"vc_name": "test_config_CK0036968",
```

```
"org": "Uber_org_test",
"vc_dns_ip":"22.22.22.22",
"zonename": "Uber_1",
"uplinkvlan": "0",
"swarmmode": "cluster",
"md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
"hostname": "Uber_3"
},
"CT0779001": {
"_sys_serial": "CT0779001",
"ssid": "s1",
"_sys_lan_mac": "84:d4:7e:c5:c6:b0",
"vc_name": "test_config_CK0036968",
"org": "Uber_org_test",
"vc_dns_ip":"22.22.22.22",
"zonename": "Uber_1",
"uplinkvlan": "0",
"swarmmode": "cluster",
"md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
"hostname": "Uber_4"
},
"CM0640401": {
"_sys_serial": "CM0640401",
"ssid": "s1",
"_sys_lan_mac": "84:d4:7e:c4:8f:2c",
"vc_name": "test_config_CK0036968",
"org": "Uber_org_test",
"vc_dns_ip":"22.22.22.22",
"zonename": "Uber_1",
"uplinkvlan": "0",
"swarmmode": "cluster",
"md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
"hostname": "Uber_6"
},
"CK0037015": {
"_sys_serial": "CK0037015",
"ssid": "s1",
"_sys_lan_mac": "ac:a3:1e:c5:db:d8",
"vc_name": "test_config_CK0036968",
"org": "Uber_org_test",
"vc_dns_ip":"22.22.22.22",
"zonename": "Uber_1",
"uplinkvlan": "0",
"swarmmode": "cluster",
"md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
"hostname": "Uber_7"
},
"CK0324517": {
"_sys_serial": "CK0324517",
"ssid": "s1",
"_sys_lan_mac": "f0:5c:19:c0:71:24",
"vc_name": "test_config_CK0036968",
"org": "Uber_org_test",
"vc_dns_ip":"22.22.22.22",
"zonename": "Uber_1",
"uplinkvlan": "0",
"swarmmode": "cluster",
"md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
"hostname": "Uber_8"
}
}
```

Figure 98 shows a sample variables file in the CSV format:

Figure 98 *Variables File in the CSV Format*



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	_sys_serial	_sys_lan_mac	modified	_sys_gateway	_sys_hostname	_sys_ip_addr	_sys_mode	_sys_netmask	_sys_oobm	_sys_snmp	_sys_stack	_sys_temp	_sys_user	_sys_vlan	_sys_vlan	att_gateway	att_mgmt	att_mgmt	backup_addr	backup_rad	backup_vpn	corp_access	custom_attr	custom_attr	custom_attr	custom_attr
2	SG62GYW	70:10:6f:9	N	10.22.183.	Aruba-Sta	10.22.183.	""	255.255.2	oobm	00:00:00:0	stacking	;	0	""	1/1-1/24,1	TRUE	10.22.181.	181	""	""	""	""	""	""	""	""
3	CN69HKW	94:18:82:4	N																							
4	CN69HKW	e0:07:1b:c	N	10.22.182.	Aruba293(	10.22.182.	""	255.255.2	""	00:00:00:0	vsf	;	0	""	1/1-1/22,1/24-1/28,2/1-2/23,2/25-2/28											
5																										
6																										
7																										

Uploading Variable Files

To upload a variable file, complete the following steps:

1. Ensure that the **_sys_serial** and **_sys_lan_mac** variables are defined with the serial number and MAC address of the devices, respectively.
2. Navigate to the **Variables** page:
   - For switches—Go to **Wired Management** > **Variables**.
   - For Instant APs—Go to **Wireless Management** > **Variables**.
   - For Gateways—Go to **Gateway Management** > **Variables**.
3. Click **Upload Variables File** and select the variable file to upload.
4. Click **Open**. The content of the variable file is displayed in the **Variables** table.
5. To search for a variable, specify a search term and click the **Search** icon.
6. To download variable file with device-specific definitions, click the download icon in the **Variables** table.

Configuring or Viewing Switch Properties in UI Groups

This section describes the configuration and viewing procedures for the switches in the UI groups.

Aruba Central does not support pre-configured switches in a UI group. If you want to move a switch from a template group to a UI group, you must clear the switch configuration, delete the device from Aruba Central, and then provision the switch as a new device in a UI group.

To configure or view properties of the switches provisioned in UI groups, perform the following procedure:

1. Click **Wired Management**.
2. From the group selector, select a group or a device.

The following table describes the left-navigation menu items and their functions.

For more details on each navigation-menu item, refer to the specific section about the menu item.

Table 100: *Menu Items for Configuring Switches Provisioned in a UI Group*

Menu Item	Function
Switches	Configure or view general switch properties, such as, hostname, type of IP addressing, and so on. See Configuring or Viewing the Switch Properties.
Ports	Assign or view port properties, such as, PoE, access policies, and trunk groups. See Configuring Switch Ports on Mobility Access Switches and Aruba Switches
VLANs	Configure or view VLANs and the associated ports and access policies. See Configuring VLANs on Switches

Menu Item	Function
Port Rate Limit	View or specify bandwidth to be used for inbound or outbound traffic for each port. See Configuring Port Rate Limit on Aruba Switches in UI Groups.
Trunk Groups	Configure or view trunk groups and their associated properties, such as, members of the trunk group, type of trunk group and so on. See Configuring Trunk Groups on Aruba Switches in UI Groups.
Spanning Tree	Configure or view spanning tree protocol and its associated properties. See Enabling Spanning Tree Protocol on Aruba Switches in UI Groups
Loop Protection	Configure or view loop protection and its associated properties. See Configuring Loop Protection on Aruba Switch Ports.
Security	Add or view access policies. See Configuring Security Policies on Aruba Switches.
DHCP Pools	Add or view a DHCP pool and its associated properties. See Configuring DHCP Pools on Aruba Switches.
Routing	Configure or view a specific routing path to a gateway. See Configuring Routing on Aruba Switches.
System	Configure or view the administrator and operator logins. If the switch is configured for static IP, you can also configure the name server. See Configuring System Parameters for a Switch.
Configuration Audit	View configuration sync errors and overrides. See Viewing Configuration Status.

Configuring or Viewing the Switch Properties

When you add a switch to a group, the switch inherits the configuration of the group.

It is not recommended to add a switch with an existing configuration to a group that already has a defined configuration. Aruba Central permits device-level overrides, however the overrides are resolved or preserved based on the requirements.

You can create a new group and add a pre-configured switch to that group so that the group inherits the configuration of the switch. If the switch inherits the group configuration, the configuration parameters are already defined. If required, you can edit these parameters. All factory default switches are provisioned in a new group and these parameters can also be defined at the group level.

To edit the configuration parameters for the switch in an UI group, complete the following steps:

1. From the app selector, click **Wired Management**.
2. From the group selector, select a group or a device.

The **Switches** page opens and displays the following information.

Table 101: *Switches Parameters*

Name	Description	Value
MAC Address	MAC address of the switch.	Property inherited from the switch.
Hostname	Name of the host.	A string.
IP Assignment	Method of IP assignment as static or DHCP.	Static or DHCP.
IP Address	IP address for static IP assignment.	IPv4 address.
Netmask	Netmask for static IP assignment.	Netmask address.
Default Gateway	Default gateway for static IP assignment.	IPv4 address.
Location	Location of the switch.	For example: Portland, Oregon.
Contact	Email address or phone number.	For example: admin@xyzcompany.com.

3. To edit the switch configuration parameters, click the edit icon.
4. Click **OK** to save the changes.

Configuring Switch Ports on Mobility Access Switches and Aruba Switches

To view the port details of a switch, complete the following steps:

1. From the app selector, click **Wired Management**.
2. From the group selector, select a group or a device.
3. Click **Ports**.

The **Ports** page displays the list of ports configured on the switch.

For the Aruba Mobility Access Switches, the **Ports** page displays the following information:

Table 102: *Ports Page—Mobility Access Switches*

Name	Description	Value
Port Number	Indicates the number assigned to the switch port.	Dependent on the type of switch.
Admin Status	Indicates the operational status of the port.	**Up** or **Down**.
Port Mode	Indicates the mode of operation. The port can be configured to function in **Trunk** or **Access** mode.	**Trunk Mode** or **Access Mode**. By default, a port is in **Access** mode and carries traffic only for the VLAN to which it is assigned. In **Trunk** mode, a port can carry traffic for multiple VLANs.
VLAN	Shows the VLAN to which the port is assigned. Based on the port mode, you can assign different types of VLAN.	■ For **Access** mode, an **Access VLAN** can be specified. ■ For **Trunk** mode, the **Native VLAN** and **Allowed VLAN** can be configured.

Name	Description	Value
Power over Ethernet	Displays the enabled or disabled status of PoE.	**Enabled** or **Disabled**.
Auto Negotiation	Indicates the status of the Auto Negotiation.	■ If auto negotiation is enabled, the **Speed** and **Duplex** fields are automatically set to **Auto**. ■ If auto negotiation is disabled, the speed can be set to 10 Mbps, 100 Mbps, or 1 Gbps and the duplex mode can be set to half or full.
Speed/Duplex	Displays the speed and duplex configuration settings for the client traffic.	
Trusted	Indicates if the port is trusted.	

For the other Aruba switches, the **Ports** page displays the following information:

Table 103: *Ports Page—Aruba Switches*

Name	Description	Value
Port Number	Indicates the number assigned to the switch port.	Dependent on the switch type.
Name	A name of the port for easy identification. You can add or edit port names. However, do not delete port names as it may cause config push to fail. The config push failure may also arise if you move a switch from a group configured with port names to a new group. This issue is only applicable to switch firmware versions earlier than 16.08.0002.	For example: UPLINK-SRVR-ROOM.
Admin Status	Allows you set the operational status of the port.	**Up** or **Down**
Power over Ethernet	Allows you to enable or disable PoE.	**Enabled** or **Disabled**.
Speed-Duplex (Mbps)	Allows you to set the maximum bandwidth of the port traffic.	Select from drop-down menu. Default is **Auto**.

Name	Description	Value
Access Policy (In)	Allows you to apply an existing access policy for the inbound traffic on the port.	Select from drop-down menu. See Configuring Security Policies on Aruba Switches.
Access Policy (Out)	Allows you to apply an existing access policy for the outbound traffic on the port.	Select from drop-down menu. See Configuring Security Policies on Aruba Switches.
Trunk Group	Displays the name of the trunk group to which the port is assigned.	To configure a Trunk Group, see Configuring Trunk Groups on Aruba Switches in UI Groups.

4. To edit port details, click **Edit**, and configure the port parameters.
5. Click **Save**.

Configuring VLANs on Switches

The Aruba switches support the following types of VLANs:

- Port-based VLANs — In the case of trusted interfaces, all untagged traffic is assigned a VLAN based on the incoming port.
- Tag-based VLANs — In the case of trusted interfaces, all tagged traffic is assigned a VLAN based on the incoming tag.

The Aruba Mobility Access Switch also supports the following types of VLANs.

- Voice VLANs — You can use voice VLANs to separate voice traffic from data traffic when the voice and data traffic are carried over the same Ethernet link.
- MAC-based VLANs — In the case of untrusted interfaces, you can associate a client to a VLAN based on the source MAC of the packet. Based on the MAC, you can assign a role to the user after authentication.

Adding VLAN Details

By default, all the ports in the Switches are assigned to VLAN 1. However, if the ports are assigned to different VLANs, the VLANs page displays these details.

To add a VLAN, complete the following steps:

1. Click **Wired Management**.
2. From the group selector, select a group or a device.
3. Click **VLANs**.

   The **VLANs** page is displayed with the following parameters:

Table 104: *Configuring and Viewing VLAN Parameters*

Name	Description	Value
Name	MAC address of the switch.	A string.
IP Assignment	Name of the host.	Static or DHCP.
IP Address	Method of IP assignment as static or DHCP.	IPv4 address.
Netmask	Netmask for static IP assignment.	
Tagged Ports	Default gateway for static IP assignment.	A port number or a range of port numbers.
Untagged Ports	Location of the switch.	A port number or a range of port numbers.
Access Policy (In)	Select a security policy that you want to apply for the inbound traffic.	See Configuring Security Policies on Aruba Switches
Access Policy (Out)	Select a security to apply for the outbound traffic.	
VLAN Policy (In)	Select a security policy to apply for the bridged and routed inbound packets on the VLAN.	
VLAN Policy (Out)	Select a security policy to apply for the bridged and routed outbound packets on the VLAN.	

4. Click + to add a VLAN.

The **Add VLAN** window opens.

5. Configure the parameters explained in step 3.
6. To apply a port, complete the following steps:
   a. Select the port number.
   b. Select any of the following port modes:
   - **Tagged Ports**
   - **Untagged Ports**

- To apply the VLAN to a port, select the port from the list of available ports.
- To assign the VLAN to a trunk group, select the trunk group.

7. Click **OK**.

Editing the VLAN Details

To edit the VLAN details, select the VLAN row and click the edit icon.

Deleting VLAN Details

To delete the VLAN details, complete the following steps:

1. Ensure that the VLANs are not tagged to any ports.
2. Click the delete icon for the VLAN you want to delete.

NOTE

VLAN 1 is the primary VLAN and cannot be deleted.

Configuring Trunk Groups on Aruba Switches in UI Groups

If you have switches provisioned in an UI group, Aruba Central enables you to configure port trunking on these switches using the UI workflows. The network administrator can configure a trunk group on switches to create one logical link or a trunk by aggregating multiple links. The trunk link functions as a high-speed link to provide increased bandwidth.

A trunk group is a set of up to eight ports configured as members of the same port trunk.

Table 105: *Trunk Group Configuration Support Per Switch Platform*

Aruba Switch Platform	Valid Trunk Groups
Aruba 2540 Switch Series	Trk1-Trk26
Aruba 2920 Switch Series Aruba 2930F Switch Series Aruba 2930M Switch Series	Trk1-Trk60
Aruba 2530 Switch Series	Trk1-Trk24
Aruba 3810 Switch Series	Trk1-Trk144

The following are some guidelines:

- All ports in the same trunk group must be of the same trunk type (LACP or trunk.)
- The names of the trunk groups include the prefix **Trk** followed by the numbers in a sequential order. For example, Trk1, Trk2 and so on.
- When STP is enabled on the switch, the STP configuration is applied for all ports at the trunk group level. Individual ports cannot be configured for STP or VLAN operation.

To configure a trunk group on switches:

Ensure that the switches are onboarded and provisioned to a UI group in Aruba Central.

1. Click **Wired Management**.
2. From the group selector, select the UI group to which the switches are assigned.
3. Click **Trunk Groups**.

   The **Trunk Group** page opens.
4. Click + to add a trunk group.

   The **Add New Trunk Group** page is displayed with the following parameters:

Table 106: *Ports Page—Aruba Switches*

Name	Description	Value
Name	Indicates the number assigned to the switch port.	String.
Type	A name of the port for easy identification.	**Trunk** or **LACP**.
Untagged VLANs	If the switch ports are untagged, select a VLAN from the Untagged VLAN list.	Select from drop-down menu.
Tagged VLANs	If the switch ports are tagged, select the VLANs from the Tagged VLAN list.	Select from drop-down menu.
Ports	Select the ports for trunking. You can use up to eight ports for link aggregation. The ports in a trunk group need not be consecutive.	Select from drop-down menu.

5. To verify the configuration, click **Configuration Audit**.

Enabling Spanning Tree Protocol on Aruba Switches in UI Groups

This is a beta feature and not recommended for a production environment.

The Spanning Tree Protocol (STP) eliminates Layer 2 loops in networks, by selectively blocking some ports and allowing other ports to forward traffic, based on global (bridge) and local (port) parameters you can configure.

For switches provisioned in UI groups, enable or disable STP on the switch ports or trunks by using the UI menu options available under Wired Management.

STP is always disabled by default on Aruba switches. To configure STP for switches provisioned in the UI groups:

1. Click **Wired Management**.
2. From the group selector, select the UI group to which the switches are assigned.
3. Enable STP if you want to avoid bridge loops between network nodes and to maintain a single active path between the network nodes. STP will be enabled all VLANs assigned to switch ports. If you have a trunk group configured for the switches in the group, STP is enabled at the trunk level.
4. Set the priority of the UI group. Refer to the following tables for configuring the STP parameters for port or trunks of individual switches. To edit a port or a trunk, select the check-mark on the right-most column and then click **Edit**.

Table 107: *Viewing or Configuring Port and Trunk Settings*

Name	Description	Value
Priority	A number used to identify the root bridge in an STP instance. The switch with the lowest value has the highest priority and is the root bridge. A higher numerical value means a lower priority; thus, the highest priority is 0. When the switches in a network select their root bridge, two parameters are considered, the STP priority and the MAC address of the switch. All Aruba switches have a default STP priority of 8. So the switch with the lowest MAC automatically gets selected as a root bridge. This is not a recommended process as it randomizes the selection of the root bridge.	0 – 8 Default: 8
BPDU Protection	A security feature used to protect the active STP topology by preventing spoofed BPDU packets from entering the STP domain. In a typical implementation, BPDU protection is applied to the edge ports and access ports connected to end-user devices that do not run STP. If STP BPDU packets are received on a protected port, the port is disabled and the network manager is alerted via SNMP traps.	**Enable** or **Disable** Default: **Disable**
BPDU Filter	Inables control of STP participation for each port. The feature can be used to exclude specific ports from becoming part of STP operations. A port with the BPDU filter enabled ignores incoming BPDU packets and stays locked in the STP forwarding state. All other ports maintain their role. Recommended ports for BPDU filter: Ports or trunks connected to client devices.	**Enable** or **Disable** Default: **Disable**
Admin-Edge	When set, the port directly goes into forwarding state. This configuration is not recommended for ports which connect to infrastructure devices. A BPDU guard also assists when a port inadvertently goes into a forwarding state.	**Enable** or **Disable** Default: **Disable**
Root Guard	Sets the port to ignore superior BPDUs to prevent the switch from becoming the Root Port.	**Enable** or **Disable** Default: **Disable**
Trunk Group	Sets the trunk group to which the port is assigned.	**Enable** or **Disable** Default: **Disable**

Configuring Security Policies on Aruba Switches

Aruba Central does not support access policy configuration on Aruba Mobility Access Switches.

To restrict certain types of traffic on physical ports of Aruba switches, you can configure ACLs from the Aruba Central UI.

To create an access policy, complete the following steps:

1. Click **Wired Management**.
2. From the group selector, select a group or a device.
3. Click **Security**.

   The **Security** page opens.

4. Click +.

The **New Access Policy** pop-up opens.

5. Enter a name for the policy.
6. Click **Add**.
7. To add a rule to the access policy, click + under **Rules**, and configure the following parameters:

Table 108: *Configuring Rules for Access Policies*

Name	Description	Value
Source	Select a source of the traffic for which you want to an access rule.	■ Any, Network, or Host ■ For Network, specify IP address and mask ■ For Host, specify IP address
Destination	Select a destination.	■ Any, Network, or Host ■ For Network, specify IP address and mask ■ For Host, specify IP address
Protocol	Select the type of protocol. Some protocols also require source and destination port.	Select from drop-down menu.
Action	Allow or deny access as required.	

8. Click **Ok**.

The access policies must be applied to a Switch port and the VLAN assigned to a port. For more information on, access policy assignment to ports and VLANs, see the following topics:

Configuring Switch Ports on Mobility Access Switches and Aruba Switches

Configuring VLANs on Switches

Configuring DHCP Pools on Aruba Switches

To configure a new DHCP pool on a switch, complete the following steps:

1. Click **Wired Management**.
2. From the group selector, select a group or a device.

Aruba 2530 Switch Series do not support DHCP server on the device platform. Hence, Aruba Central pushes the group-level configuration for DHCP to all applicable devices in the group except the Aruba 2530 Switch Series.

If any of the devices is running a lower version, a warning message is displayed, and the DHCP configuration changes are pushed only to the devices that support the DHCP. If the devices are upgraded to a supported version or moved out of the group, the warning message will not be displayed.

3. To activate the DHCP service, move the **Enable DHCP service** toggle switch to the on position. The DHCP service can be enabled only if there is a valid DHCP pool.
4. To add a new DHCP pool, click the + sign, configure the following parameters, and click **Add**:

Table 109: *Configuring a DHCP Pool*

Name	Description	Value
Name	Name of the pool.	A string.
Network	A valid network IP address to assigned to the DHCP pool.	IPv4 address
Netmask	Netmask of the DHCP pool.	Subnet mask
Lease Time	The lease time for the DHCP pool in days-hours-minutes format.	You can set a maximum value of 365 days 23 hours and 59 minutes in the DD-HH-MM format.
Default Router	IP address of the default router in the subnet.	You can add up to 8 IP addresses.
DNS Server	Address of the DNS server. To add multiple DNS servers, click +.	You can add up to 8 DNS servers.
Netbios Server	Address of the Netbios server. The Netbios server address configuration is not required for Mobility Access Switches. To add multiple Netbios servers, click +.	You can add up to 8 Netbios servers. For Mobility Access Switches, an option called WINS Server is available.
IP Address Range	IP address range within the network and network mask combination. To add multiple IP address range, click +.	You can add up to 64 IP address range.
Exclude Address Range	IP address range to exclude. This field is available only for the Mobility Access Switches. To add multiple excluded address range, click +.	You can add up to 64 IP address range.
Option	The code, type, and ASCI or HEX value of the DHCP option to configure. To add multiple options, click +.	You can add up to 8 options. A value within the range of 2-254 with type as hexadecimal and ASCII is valid.

5. To edit the DHCP pool details, click the edit icon.
6. To delete a DHCP pool, click the delete icon. When the **Do you want to delete <DHCP Pool Name>?** pop-up window prompts you, click **Yes**.

Configuring System Parameters for a Switch

The **System** menu under **Switch-MAS** and **Switch-Aruba** allows you to configure administrator credentials and enable mode for the switch users.

Configuring Administrator Credentials for Mobility Access Switch

To configure administrator credentials for a Mobility Access Switch, complete the following steps:

1. From the app selector, click **Wired Management**.
2. From the group selector, select a group or a device.
3. Click **Switch-MAS** > **System**. The **System** page opens.
4. Enter the password for admin in the **Admin Password** text box and confirm the administrator password.

5. Enter the password for enable mode in the **Enable Mode Password** text box and confirm the password.
6. Click **Save Settings**.

Configuring Administrator and Operator Credentials for Other Aruba Switches

To configure administrator credentials for other Aruba switches, complete the following steps:

1. From the app selector, click **Wired Management**.
2. From the group selector, select a group or a device.
3. Enter the username for the administrator user.
4. Enter the password for admin in the **Admin Password** text box and confirm the administrator password.
5. Enter the password for enable mode in the **Enable Mode Password** text box and confirm the password.
6. To configure the operator user credentials, complete the following steps:
7. Select the **Set Operator Username** check box.
8. Enter a username and password for the operator user.
9. Confirm the password.
10. Click **Save Settings**.

Configuring a Name Server

To set a static IP switches, you must configure a name server. To configure a name server, complete the following steps:

1. From the app selector, click **Wired Management**.
2. From the group selector, select a group or a device. The switch configuration options are displayed.
   - For Aruba Mobility Access Switches, click **Switch-MAS**.
   - To configure other Aruba switches, click **Switch-Aruba**.
3. Enter the IP address of the name server obtained from the DNS server in the **Name Server** text box.
4. Click **Save Settings**.

Aruba Switch Stack

A switch stack is a set of switches that are interconnected through stacking ports. The switches in a stack elect a primary switch called Commander and a backup switch as Standby. The remaining switches become Members of the stack. The following table lists the switches support stacking:

Table 110: *Switch Stacking Support*

Switch Platform	Maximum Number of Stack Members	Minimum Supported Version
Aruba 2920 Switch Series	4	WB.16.04.0008
Aruba 2930M Switch Series	10	WC.16.06.0006
Aruba 5400R Switch Series	2	KB.16.06.0008
Aruba 2930F Switch Series	8	WC.16.07.0002
Aruba 3810 Switch Series	10	KB.16.07.0002

For more information on topology and configuration of switch stacks, see the *HPE ArubaOS-Switch Management and Configuration Guide* for the respective switch series.

Provisioning Switch Stacks in Aruba Central

The switch elected as the commander establishes a WebSocket connection to Aruba Central. The following criteria apply to provisioning and management of switch stacks in Aruba Central:

- Switch stacks can be added only to a template group and cannot be moved to a UI group.
- If the standalone switches in a group join to form a switch stack, the switch is moved to the Unprovisioned state.
- If a switch stack is moved from a pre-provisioned group to an existing group in the UI, it will be moved to Unprovisioned state.
- After forming a switch stack, you can remove a member and erase its stacking configuration. However, the member can join Aruba Central as a standalone switch only after it is deleted from the switch stack.

Assigning Labels and Sites

Aruba Central supports organizing your devices into sites for ease of monitoring. Sites refer to physical locations in which the devices are installed. Administrators can assign switch stacks to a single site for ease of managing installations and monitoring the overall site health. For more information on assigning devices to sites, see Managing Sites on page 69.

Similarly, switch stacks can also be tagged using labels. Labels allow you to identify or tag devices installed in a specific site for ease of monitoring. For more information on assigning labels, see Managing Labels on page 71.

If any one member of the switch stack is assigned to a site, Aruba Central automatically assigns all other members in a switch stack to the same site. Similarly, if a label is assigned to an individual member in a stack, the same label is applied to all other members of the stack.

Because all members of a switch stack must be assigned to the same site and label, Aruba Central automatically corrects the site and label assignment for switch stacks that were earlier assigned to different labels or sites. If you have such switch stacks in your account, you will notice that all stack members are migrated to the same site or label to which the commander was assigned. Aruba recommends that you review the sites and labels assigned by Aruba

Central to verify that the switch stacks in your account are assigned to sites and labels that you intended to use, and if required, assign all members of stack to a common site or label of your choice.

Configuring Switch Stacks

The switch stacks are provisioned under template groups in Aruba Central. The template groups allow you to configure and modify the settings of a switch stack using configuration templates.

When uploading a configuring template, ensure that the variables are uploaded for all the members of the stack. The template is applied with the variables of the member that is elected as the commander.

To create a configuration template for switch stack, complete the following steps:

1. From the app selector, click **Wired Management**.
2. From the group selector, select template group to which the switch stack is assigned. The menu options for configuring devices in the template groups are displayed.
3. Click **Templates**. The **Templates** page opens.
4. Click **+** to create a template for the Aruba switch stack.
5. Specify a name for the template.
6. Select Aruba Switch from the **Device** drop-down list.
7. Select the Aruba Switch model in the **Model** drop-down list.
8. Select the Aruba Switch software version in the **Version** drop-down list.
9. Enter the template text in the **Template** box.
10. Click **Save**.

Aruba Central does not support the use of part number (J-number) in place of Switch model number in configuration templates for the Aruba switch stack.

The following pre-defined variables are refreshed and re-imported from a switch stack when a new stack member is added or removed, or when a failover occurs.

- _sys_template_header
- _sys_module_command
- _sys_stack_command
- _sys_oobm_command
- _sys_vlan_1_untag_command
- _sys_vlan_1_tag_command

Monitoring Switch Stacks

See Monitoring Switches and Switch Stacks on page 130.

Viewing Switch Stacks in Site Topology

See Topology on page 216.

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** menu option is available for all types of device

configuration containers, such as **Wireless Management** for Aruba WLAN APs, **Wired Management** for Aruba Switches, and **Gateway Management** for Aruba Gateways.

Accessing the Configuration Audit Page

To access the **Configuration Audit** page:

- For Instant APs:
  a. Click **Wireless Management**.
  b. From the group selection filter, select a group or device.
  c. Click **Configuration Audit**.
- For Aruba switches:
  a. Click **Wired Management**.
  b. From the group selection filter, select a group or device.
  c. Click **Configuration Audit**.
- For Aruba Gateways:
  a. Click **Gateway Management**.
  b. From the group selection filter, select a group or a device.
  c. Click **Configuration Audit**.

Applying Configuration Changes

Aruba Central now supports a two-staged configuration commit workflow for Instant AP and switches.

The **Auto Commit State** section in the **Configuration Audit** page allows administrators to switch their preference for committing configuration changes to devices.

- When **Auto Commit State** is set to **ON**, the configuration changes are applied instantly to the device.
- When **Auto Commit State** is set to **OFF**, the administrators can build a candidate configuration, save it on cloud, review it, and then push the configuration changes to the managed devices for activation.

When a device is moved from one group to another, Aruba Central resets the **Auto Commit State** for the device. The device inherits the **Auto Commit State** settings of the group to which the device is moved.

Auto Commit Workflow

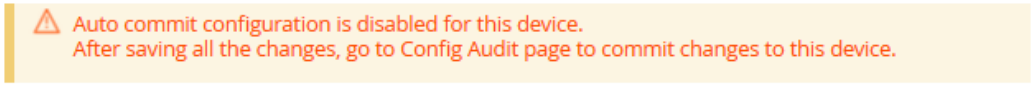
To enable Aruba Central to push configuration changes instantly, complete the following steps:

1. Select a device and navigate to the appropriate configuration app (**Wireless Management** for Instant APs and **Wired Management** for switches).
2. Click **Configuration Audit**.
3. Ensure that the **Auto Commit State** is set to **ON**.
4. 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. Aruba Central automatically pushes the configuration changes to the devices.
5. Go to **Configuration Audit** and click Failed Changes to view configuration errors if any.

Manual Commit Workflow

To build configuration and review it before applying the changes to devices:

1. Select a device and navigate to the appropriate configuration app (**Wireless Management** for Instant APs and **Wired Management** for switches).
2. Click **Configuration Audit**.
3. Ensure that the **Auto Commit State** is set to **OFF**.
4. 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 changes, Aruba Central displays the following message:



5. Go to **Configuration Audit** and click **Failed/PendingChanges**.
6. Click the **Failed Push** tab and review the configuration.
7. Click **Close**.
8. If you want to push the configuration to devices, click **Commit Now**.

Aruba Central does not support the two-staged configuration commit workflow only for 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.

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 page include:

- **Failed/Pending Changes**
  - **Failed Changes**—The devices managed by Aruba Central receive the configuration changes from Aruba Central. Occasionally, a managed device may fail to receive a configuration change from Aruba Central. The **Failed changes** tile allows you to view a list of the configruation push errors.
  - **Pending Changes**—With the Auto Commit feature is disabled, Aruba Central allows you to build your configuration changes, save it, and review it before committing the configuration changes. The **Failed/Pending Changes** tile displays the configuration that is not yet pushed to the devices.
- **Local Overrides**—In Aruba Central, devices are assigned to groups that serve as the primary configuration elements. Occasionally, based on the network provisioning requirements, the administrators may need to modify the configuration of a specific device in a group. As these modifications override the configuration settings that the device has inherited from the group, Aruba Central marks these changes as local overrides.
- **Configuration Conflicts**—For all connected devices in Aruba Central, when a new feature is introduced and applied to the device, one of two subsequent scenarios might ensue. The new feature might not cause any conflict with the existing configuration and no further action is required from the administrator. However, if the new feature causes a conflict with the existing configuration in the device, the feature is disabled automatically and no further configuration is pushed for that device. The **Configuration Audit** page displays a configuration conflict error. For each device under conflict, click the **Manage Configuration Conflict** link. In the subsequent **Configuration Conflict** page, enable the checkbox against each conflict and type REMOVE to remove the conflict. After you resolve all conflicts, you are able to push group configuration to the device.
- **Template Errors**—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 devices fails. Aruba

Central records such failed instances as template errors and displays these errors on the **Configuration Audit** page.

- **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)

On selecting a template group from the filter bar, the **Configuration Audit** page displays the options listed in Table 111:

Table 111: *Configuration Audit Status for a Template Group*

Data Pane Content	Description
Template Errors	Displays the number of template errors for the selected template group. 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 To view a complete list of errors, click **View Template Errors**. The **Template Errors** pop-up window allows you to view and resolve the template errors issues if any.
Failed/Pending Changes	Displays the number configuration sync errors for the selected template group. To view and resolve the configuration sync errors, click the **Failed Config Difference** link.
Configuration Backup and Restore	Allows you to create a backup of templates and variables applied to the devices in the template group. For more information, see Viewing Configuration Status.
All Devices	The **All Devices** table provides the following device information for the selected group: ■ **Name**—The name of the device. ■ **Type**—The type of the device. ■ **Auto Commit**—Enabled or disabled status of the **Auto Commit** feature. ■ **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)

On selecting a device that is provisioned in a template group, the **Configuration Audit** page displays the options listed in Table 111:

Table 112: *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**.
Failed Changes	Displays configuration sync errors for the selected device. To view and resolve the configuration sync errors, click the **Failed/Pending Config Changes** link.
Config Comparison Tool	Allows you to view the difference between the current configuration and the configuration that is yet to be pushed to the device (pending configuration). To view the current and pending configuration changes side by side, click **View**.

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

On selecting a UI group, the **Configuration Audit** page displays the options listed in Table 111.

Table 113: *Configuration Audit Status for a UI Group*

Data Pane Content	Description
Failed Changes	Displays the number of devices with configuration sync errors for the selected UI group. To view and resolve the configuration sync errors, click the **Failed Config Difference** link.
Local Overrides	Displays the number of devices with local overrides. To view a complete list of overrides, click the **Manage Local Overrides** link. The **Local Overrides** pop-up window opens. ■ To preserve the overrides, click **Close**. ■ To remove the overrides, select the group name with local override, click **Remove** and click **OK**.
All Devices	The **All Devices** table provides the following device information for the selected group: ■ **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. ■ **Config Sync** / **Config Status**—Indicator showing configuration sync errors. ■ **Local Override**—Indicator showing configuration overrides for the devices deployed in UI groups. **NOTE:** The **MAC Address**, **IP Address**, **Config Status**, **Site**, and **Type** columns are available only for groups in which Aruba Gateways are provisioned (**Gateway Management** > **Configuration Audit**).

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

On selecting a device assigned to a UI group, the **Configuration Audit** page displays the options listed in Table 111.

Table 114: *Configuration Audit Status for a Device Assigned to a UI Group*

Data Pane Content	Description
Failed Changes	Displays the number of devices with configuration sync errors for the selected device. To view and resolve the configuration sync errors, click the **Failed Config Difference** link.
Local Overrides	Displays the number of local overrides. To view a complete list of overrides, click the **Manage Local Overrides** link. The **Local Overrides** pop-up window opens. ■ To preserve the overrides, click **Close**. ■ To remove the overrides, click **Remove**, and click **OK**.

Backing up and Restoring Configuration Templates

Aruba Central allows you to back up configuration templates assigned to the devices deployed in a template group. The **Configuration Audit** pages for Instant AP, Switch, and Gateway configuration containers allow you to create and manage backed up files and restore these files when required. For more information, see Backing Up and Restoring Configuration Templates.

The Aruba SD-WAN Gateways are the most important components of the Aruba SD-Branch Solution. Aruba's SD Branch provides a software overlay to centralize network controls in the public or private cloud. It allows robust management, configuration, and automation of the WAN processes. The solution supports SD-WAN, which is a specific application of the Software-Defined Networking (SDN) technology applied to WAN connections for enterprise networks, including branch offices and data centers, spread across different geographic locations.

The SD-WAN Gateway portfolio includes Aruba 7000 Series and Aruba 7200 Series Mobility Controllers that function as Branch Gateways and VPN Concentrators respectively.

To obtain access to SD-WAN solution in your deployments, please contact your Aruba Sales Specialist.

For more information about SD Branch and SD-WAN configuration, look up *SD-WAN Solution* or see the *Aruba SD-WAN Solution Guide* in *Aruba Central Help Center*.

Aruba Central supports a robust set of REST APIs to enable users to build custom applications and integrate the APIs with their applications. The Aruba Central API framework uses OAuth protocol to authenticate and authorize third-party applications, and allows them to obtain secure and limited access to an Aruba Central service.

API Gateway and NB APIs

The **API Gateway** feature in Aruba Central supports the REST API for all Aruba Central services. This feature allows Aruba Central users to write custom applications, embed, or integrate the APIs with their own applications. The REST APIs support HTTP GET and POST operations by providing a specific URL for each query. The output for these operations is returned in the JSON format.

For secure access to the APIs, the Aruba Central API Framework plug-in supports OAuth protocol for authentication and authorization. The access tokens provide a temporary and secure access to the APIs. The access tokens have a limited lifetime for security reasons and the applications should use the refresh API to obtain new tokens periodically (every 2 hours).

List of Supported APIs

Aruba Central supports the following APIs for the managed devices.

Table 115: *APIs and Description*

API	Description
Monitoring	Gets network, client, and event details. It also allows you to manage labels and switches.
Configuration	Allows you to configure and retrieve the following: ■ Groups ■ Templates ■ Devices
AppRF	Gets Top N AppRF statistics.
Guest	Gets visitor and session details of the portal.
MSP	Allows you to manage and retrieve the following: ■ Customers ■ Users ■ Resources ■ Devices Aruba has enforced a request limit for the following APIs: ■ **GET /msp_api/v1/customers** ■ **GET /msp_api/v1/customers/{customer_id}/devices** ■ **GET /msp_api/v1/devices** ■ **PUT /msp_api/v1/customers/{customer_id}/devices** The maximum limit is set to 50 per API call. If you exceed this limit, the API call returns the HTTP error code 400 and the following error message: **LIMIT_REQUEST_EXCEEDED**.

Table 115: *APIs and Description*

API	Description
User Management	Allows you to manage users and also allows you to configure various types of users with a specific level of access control.
Audit Event Logs	Gets a list of audit events and the details of an audit event.
Device Inventory	Gets device details and device statistics.
Licensing	Allows you to manage and retrieve subscription keys.
Presence Analytics	Allows you to configure the Presence Analytics application. It also retrieves site and loyalty data.
Device Management	Allows you to manage devices.
Firmware	Allows you to manage firmware.
Troubleshooting	Gets a list of troubleshooting commands for a specific type of device.
Notification	Gets notification alerts generated for events pertaining to device provisioning, configuration, and user management.
Clarity	Allows you to retrieve the status of the wireless connection for the devices added in Aruba Central and troubleshoot issues detected in the network.
Unified Communications	Retrieves data for all sessions for a specific period of time. It also retrieves the total number of clients who made calls in the given time range and gets the Lync/Skype for Business URL for the Aruba Central cluster that you are using.
Refresh API Token	Allows you to refresh the API token.
Reporting	Gets the list of configured reports for the given customer ID.
WAN Health	Allows you to the following: ■ Get list of configured WAN health policies. ■ Create a new WAN health policy. ■ Delete an existing WAN health policy. ■ Get the details of any specific WAN health policy. ■ Update an existing WAN health policy. ■ Delete recurring WAN health check policies on all the sites where it was configured. ■ Get policy schedule details. ■ Create a schedule for a WAN health policy. ■ Get statistics for WAN health cookie generated for a site. ■ Get WAN health test results. ■ Get WAN health test results for a specific site.
Network Health	Allows you to get data for all the labels and sites.
Webhook	Allows you to add, or delete Webhooks, and get or refresh Webhook tokens. See Webhooks on page 393 for further details on Webhook.
VisualRF	Allows you retrieve information on floor plans, location of APs, clients and rogue devices.
DPS Monitoring	Gets DPS compliance and session statistics for all the links of a device belonging to a specific policy.

Accessing API Gateway

To access API Gateway:

1. From the app selector, click **Maintenance**.
2. Click the **API Gateway** menu option. The **API Gateway** page is opens. The **API Gateway** page allows you to get new tokens and refresh the old tokens. To obtain a new token application, you must set authentication parameters for a user session.

The admin user profile of MSP has **System Apps & Tokens** tab which displays all the apps and tokens generated locally in the admin user profile. This tab also displays all the apps created in the non-admin user profiles. Clicking these apps lists out all the associated tokens created for the non-admin user profile.

For enabling API Gateway license, contact your Aruba sales representative.

Domain URLs

Table 116 shows the region-specific domain URLs for accessing API Gateway:

Table 116: *Domain URLs for API Gateway Access*

Region	Domain Name
US-West-A (US-1 cluster zone)	app1-apigw.central.arubanetworks.com
US-West-B (US-2 cluster zone)	apigw-prod2.central.arubanetworks.com
Europe	eu-apigw.central.arubanetworks.com
APAC	api-ap.central.arubanetworks.com
China	apigw.central.arubanetworks.com.cn
Canada	apigw-ca.central.arubanetworks.com

The procedures described in this article use app1-apigw.central.arubanetworks.com as an example. Ensure that you use the appropriate domain URL when accessing API Gateway or generating tokens.

Using OAuth 2.0 to Access API

For secure access to the APIs, the Aruba Central API Framework plug-in supports OAuth protocol for authentication and authorization. OAuth 2.0 is a simple and secure authorization framework. It allows applications to acquire an access token for Aruba Central through a variety of work flows supported within the OAuth2 specification.

All OAuth2 requests must use the SSL endpoint available at https://app1-apigw.central.arubanetworks.com.

Access and Refresh Tokens

The access token is a string that identifies a user, app, or web page and is used by the app to access an API. The access tokens provide a temporary and secure access to the APIs.

The access tokens have a limited lifetime. If the application uses web server or user-agent OAuth authentication flows, a refresh token is provided during authorization that can be used to get a new access token.

If you are writing a long running applications (web app) or native mobile application you should refresh the token periodically. For more information, see Refreshing a Token on page 389.

Creating an Application

To create an application, complete the following steps:

1. From the app selector, click **Maintenance**.
2. Click the **API Gateway** menu option. The **API Gateway** page is displayed.
3. Click **My Apps & Tokens**.

The admin user will be able to create new apps for all the non-admin user by clicking **+ Add Apps & Tokens** in the **System Apps & Tokens** tab.

4. Click **+ Add Apps & Tokens**.
5. Enter a name for the application and the redirect URI in the **Application Name** and **Redirect URI** fields, respectively, and click **Generate**. A new application is created and added to the **My Apps & Tokens** table. The **My Apps & Tokens** table displays the following:

- Name—Name of the application. In non-admin user profile, the **Application Name** field contains the logged-in user name and is non-editable**.** Any new tokens generated in non- admin user profile will be associated with the same application name.
- Client ID—Unique ID for each application.
- Client Secret—Unique secret ID for each application.
- Tokens—An application can have multiple tokens. Click **View Tokens** to view the list of tokens.
- Created At—Date on which the application was created.
- Actions—Click the **Delete** icon on the row corresponding to an application and click **Yes** to delete that application.

After an application is created, go to the **My Apps & Tokens** page and click **View Tokens**. In the **Token List** pop-up window, you can view the user ID(s) associated to the application in the User Name column. An application can be associated to multiple users.

Only admin users will be able to generate tokens with multiple application names. In non-admin user profile, the **Application Name** field contains the user name and is non-editable**.** Any new tokens generated in non- admin user profile will be associated with the same application name. However, all the multiple application names and the associated tokens in non-admin user profiles from the earlier versions will still be retained in the **Token List** pop-up window.

After an application is created for a non-admin user in the admin user mode, go to the **System Apps & Tokens** page and click **View Tokens**. In the **Token List** pop-up window, you can view the user IDs associated to the application in the **User Name** column. An application can be associated to multiple users.

Obtaining Tokens

The users can generate the OAuth token using one of the following methods:

- Offline token download
- Authorization code grant

Offline Token Mechanism

To obtain tokens using the offline token method, complete the following steps:

1. From the app selector, click **Maintenance**.
2. Click the **API Gateway** menu option. The **API Gateway** page is displayed.
3. Click **My Apps & Tokens**.

In the MSP mode, the admin user profile has **System Apps & Tokens** tab which displays all the apps and tokens generated in all the non-admin user profiles in addition to the apps and tokens created in the admin user profile.

4. Click **+ Add Apps & Tokens**.
5. Click **View Tokens** to view the tokens associated to a specific application. The **Token List** pop-up window opens and displays the following:
   - Token ID—Token ID of the application.
   - User Name—Name of the user to whom this token is associated to. An application can be associated to multiple users.
   - Generated At—Date on which the token was generated.
   - Revoke Token—Click **Revoke Token** and click **Yes** to revoke the token associated to a particular user. For example, if two users are associated to an application and if you want to remove access to a particular user, revoke the token associated to that user.
   - Download Token—Click **Download Token** to download the token.

Authorization Code Grant

The following section describes the procedure for obtaining the access token and refresh token using the authorization code grant mechanism:

Step 1: Create an Application

Create an application in Aruba Central. For more information, see Creating an Application on page 386.

Make a note of the following:

- Client ID
- Client Secret

Step 2: Identify the Base URL

The following example shows the base URL:

https://app1-apigw.central.arubanetworks.com

Step 3: Generating Client Credentials

To generate client credentials, use the following URI and the request method:

Request Method—POST

URI—https://app1-apigw.central.arubanetworks.coms/oauth2/authorize/central/api/client_credentials?client_id=<msp_client_id>

POST Request Body(JSON):

```
{
"customer_id": "<tenant_id>"
}
```

RequestHeader: (Values from login API request)

```
Set-Cookie: csrftoken=xxxx;session=xxxx;
```

Response Body(JSON):

```
{
"client_id": "<new-client-id>",
"client_secret": <new-client-secret>"
}
```

Step 4: Log in and Authenticate Using Your Aruba Central Credentials

Append the base URL with the following:

/oauth2/authorize/central/api/login

URL:https://app1-apigw.central.arubanetworks.com/oauth2/authorize/central/api/login

This endpoint is accessible over SSL. The HTTP (non-SSL) connections are redirected to the SSL port. The endpoint validates the user session. For Aruba Central, the SSO authentication page is presented. After successful authentication, a consent page is shown requesting the resource owner (the customer who has logged in) to give access to the APIs.

Request: Craft an HTTP POST request containing the username, password, and client ID of the application.

Response: The response contains the Cross-Site Request Forgery (CSRF) token and session key that are necessary for obtaining the authorization code.

Step 5: Obtain an Authentication Code

Append the base URL with the following:

/oauth2/authorize/central/api

URL:https://app1-apigw.central.arubanetworks.com/oauth2/authorize/central/api

This endpoint is accessible over SSL. The HTTP (non-SSL) connections are redirected to the SSL port. This endpoint is a POST call to get an authorization code.

Request: Craft an HTTP POST request containing the customer ID, client ID, CSRF token, and session key.

Response: The response contains the authorization code that is necessary for obtaining the access token and refresh token.

Step 6: Exchange the Authentication Code for the Access and Refresh Tokens

Append the base URL with the following:

/oauth2/token

URL:https://app1-apigw.central.arubanetworks.com/oauth2/token

This endpoint is accessible over SSL. The HTTP (non-SSL) connections are redirected to the SSL port. The endpoint is a POST call to get the access token and refresh token using the authorization code obtained from the server. This exchange must be done within 300 seconds of obtaining the authorization code from step 4. Otherwise, the API returns an error.

Request: Craft an HTTP POST request containing the client ID, client secret, and authentication code.

Response: The response contains the access token and refresh token. The access token will expire in 2 hours.

Refreshing a Token

To refresh the access token, access the following URL:

https://app1-apigw.central.arubanetworks.com/oauth2/token

This endpoint is accessible over SSL. The HTTP (non-SSL) connections are redirected to SSL port.

Table 117: *Refresh Tokens*

URL	Description
https://app1-apigw.central.arubanetworks.com/oauth2/token	The endpoint is a POST call to refresh the access token using the refresh token obtained from the step 2.

The query parameters for the API are as follows:

Table 118: *Query Parameters for Refresh Tokens*

Parameter	values	Description
`client_id`	A unique hexadecimal string	A unique identifier that identifies the caller. The application developers can request a client ID and client secret key by registering with the Aruba Technical Support.
`client_secret`	A unique hexadecimal string	The client secret is a unique identifier provided to each developer at the time of registration. The application developers can request a client ID and client secret by registering with the Aruba Technical Support.
`grant_type`	refresh_ token	The *grant_type* must be *refresh_token* to refresh the token.
`refresh_token`	refresh_ token received from step 2	A string representing the authorization granted to the client by the resource owner.

A JSON dictionary with the following values is returned as a response.

Parameter	values	Description
token_type	bearer	Identifies the token type. Only the bearer token type is supported. For more information, see https://tools.ietf.org/html/rfc6750.
refresh_token	string	Refresh tokens are credentials used to renew or refresh the access_token when it expires without going through the complete authorization flow. A refresh token is a string representing the authorization granted to the client by the resource owner.
expires_in	seconds	The expiration duration of the access tokens in seconds.
access_token	string	Access tokens are credentials used to access the protected resources. An access token is a string representing an authorization issued to the client.

Example

Method:POST

https://app1-apigw.central.arubanetworks.com/oauth2/token?client_id=98273576d558401581c425d5bd9df213&grant_type=refresh_token&refresh_token=1272ddc5f4c94683b7ac3080f39503f9&client_secret=e20f3fad10dc4c41bf291a49e85a3b29

Response

```
{
"access_token": "xyz",
"customer_id": "bearer",
"access_token": "889479cac74e4b299723cc9a6f8f9d08",
"expires_in": 7200
}
```

Deleting a Token

To delete the access token, access the following URL:

https://app1-apigw.central.arubanetworks.com/oauth2/token

This endpoint is accessible over SSL. The HTTP (non-SSL) connections are redirected to SSL port. Customer ID is a string.

Example

Method: DELETE

URL: https://app1-apigw.central.arubanetworks.com/oauth2/api/tokens

JSON Body:

```
{
"access_token": "<access_token_to_be_deleted>",
"customer_id": "<customer_id_to_whom_token_belongs_to>"
}
```

Headers:

Content-Type: application/json

X-CSRF-Token: <CSRF_token_obatained_from_login_API>

Cookie: "session=<session_obatained_from_login_API>"

Accessing APIs

To access the API, use the following URL:

https://app1-apigw.central.arubanetworks.com/.

This endpoint is accessible over SSL and the HTTP (non-SSL) connections are redirected to the SSL port.

Table 119: *Accessing the API*

URL	Description
https://app1-apigw.central.arubanetworks.com/	The API gateway URL. All APIs can be accessed from this URL by providing a correct access token.

The query parameters for the API are as follows:

Table 120: *Query Parameters for the API*

Parameter	values	Description
`request_path`	URL Path	UTL path of an API, for example, to access monitoring APIs, use the path */monitoring/v1/aps*.
`access_token`	access_ token	Pass the token string in URL parameter that is obtained in step 2.

Example

Request: (Method=Get)

https://app1-apigw.central.arubanetworks.com/monitoring/v1/aps?access_token=e325c0fb3f1547b5b735de3221690c2f

Response:


```
{
"aps": [
{
"firmware_version": "6.4.4.4-4.2.3.1_54637",
"group_name": "00TestVRK",
"ip_address": "10.29.18.195",
"labels": [
"Filter_242",
"Ziaomof",
"roster",
"242455",
"Diegso"
],
"macaddr": "6c:f3:7f:c3:5d:92",
"model": "AP-134",
"name": "6c:f3:7f:c3:5d:92",
"radios": [
{
"band": 0,
"index": 1,
"macaddr": "6c:f3:7f:b5:d9:20",
"status": "Down"
},
{
```

```
"band": 1,
"index": 0,
"macaddr": "6c:f3:7f:b5:d9:30",
"status": "Down"
}
],
"serial": "AX0140586",
"status": "Down",
"swarm_id": "e3bf1ba201a6f85f4b5eaedeead5e502d85a9aef58d8e1d8a0",
"swarm_master": true
}
],
"count": 1
}
```


Viewing APIs

To view the APIs managed through Aruba Central, complete the following steps:

1. From the app selector, click **Maintenance**.
2. Click the **API Gateway** menu option. The **API Gateway** page with the list of published APIs is displayed.
3. To view the details of an API, click **Details**.
4. To view the API documentation, click the link in the **Documentation** column next to the specific published API name. The documentation is displayed in a new window.

Viewing Tokens

To view tokens, complete the following steps:

1. From the app selector, click **Maintenance**.
2. Click the **API Gateway** menu option. The **API Gateway** page is displayed.
3. Click **My Apps & Tokens.**
4. To view tokens, click the **View Tokens** link for the specific App & Token name. The **Token List** pop-up window opens.

In MSP, the admin user profile has **System Apps & Tokens** tab which displays all the apps and tokens generated in all the non-admin user profiles in addition to the apps and tokens created in the admin user profile. To view all the tokens of admin and non-admin user, go to **Maintenance > API Gateway > System Apps & Tokens.**

Revoking Tokens

To revoke tokens, complete the following steps:

1. From the app selector, click **Maintenance**.
2. Click the **API Gateway** menu option. The **API Gateway** page is displayed.
3. Click **My Apps & Tokens**.
4. o view tokens, click the **View Tokens** link for the specific App & Token name. The **Token List** pop-up window opens.
5. To revoke tokens, click **Revoke Token** in the **Token List** window.

Adding a New Token

To add a new token, complete the following steps:

1. From the app selector, click **Maintenance**.
2. Click the **API Gateway** menu option. The **API Gateway** page is displayed.
3. Click **My Apps & Tokens**.

The admin user will be able to create new tokens for all the non-admin user by clicking **+ Add Apps & Tokens** in the **System Apps & Tokens** tab.

4. Click **+ Add Apps & Tokens** to add a new token.
5. Enter the application name in the **Application Name** box and then click **Generate**.

If you have registered a custom URI when creating a new app under **System Apps and Tokens**, the **Redirect URI** option is disabled for you in the **My Apps and Tokens** tab **> Add Apps and Tokens > New Token** . In such cases, the **Redirect URI** option in **Add Apps and Tokens > New Token** under **My Apps and Tokens** populates your already registered URI.

Only admin users can generate tokens with multiple application names. In a non-admin user profile, the **Application Name** field contains the username and is non-editable. Any new tokens generated in the non- admin user profile will be associated with the same application name.

After an application is created for a non-admin user, go to the **System Apps & Tokens** page and click **View Tokens**. In the **Token List** pop-up window, you can view the user IDs associated to the application in the **User Name** column.

API Documentation

For a complete list of APIs and the corresponding documentation, see https://app1-apigw.central.arubanetworks.com/swagger/central.

Webhooks

Webhooks allow you to implement event reactions by providing real-time information or notifications to other applications. Aruba Central allows you to create Webhooks and select Webhooks as the notification delivery option for all alerts.

Using Aruba Central, you can integrate Webhooks with other third-party applications such as ServiceNow, Zapier, IFTTT, and so on.

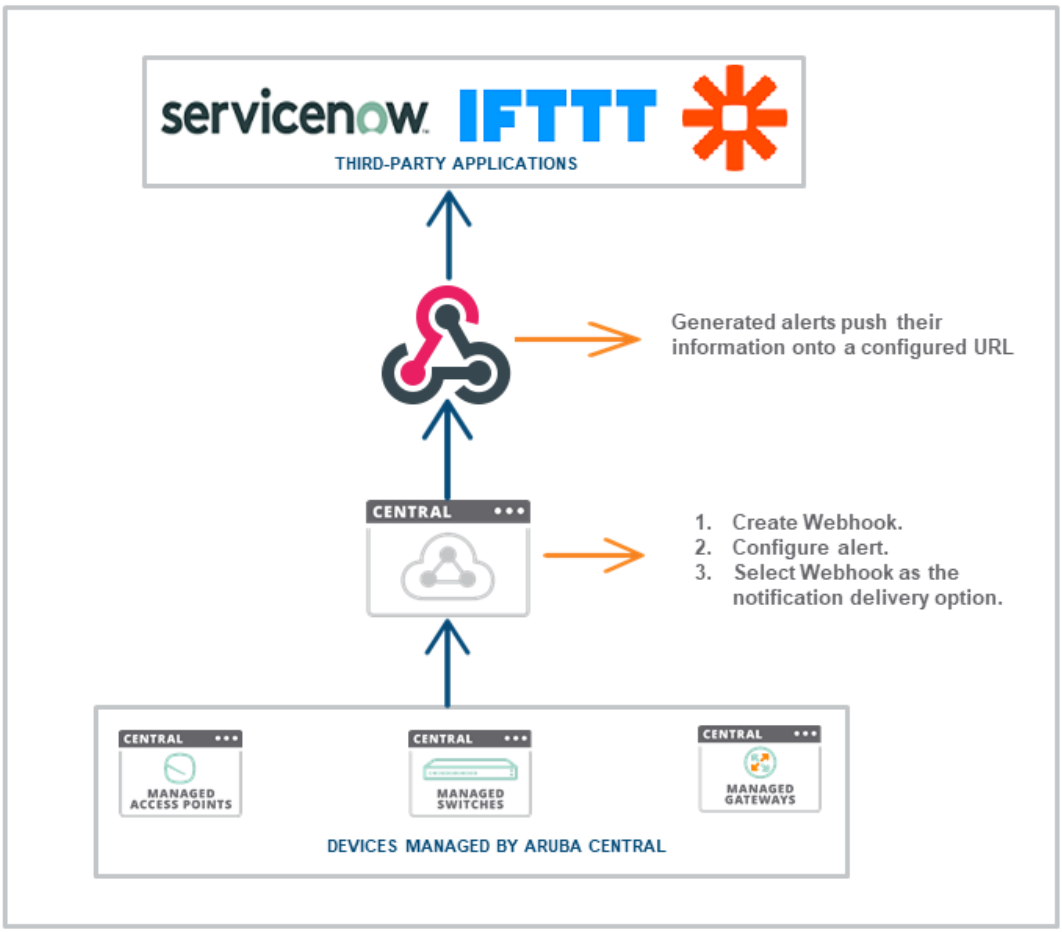
You can access the Webhooks service either through the Aruba Central UI or API Gateway. Aruba Central supports creating up to 10 Webhooks. To enable redundancy, Aruba Central allows you to add up to three URLs per Webhook.

From Aruba Central, you can add, list, or delete Webhooks; get or refresh Webhooks token; get or update Webhooks settings for a specific item; and test Webhooks notification.

Use the **Webhook** check box in the **Monitoring & Reports** > **Alerts** > **Configure Alerts** page to select Webhooks as the notification delivery option.

The following figure illustrates how Aruba Central integrates with third-party applications using Webhooks.

Figure 99 *Webhooks Integration*



This section includes the following topics:

Creating and Updating Webhooks Through the UI

To access the Webhooks service from the UI:

1. Go to **Maintenance** > **API Gateway**.
2. In the **Webhook** tab, click **+Webhook**.
   a. **Webhook Name**—Enter a name for the Webhook
   b. **URLs**—Enter the URL. Click + to enter another URL. You can add up to three URLs.
3. Click **Save**. The Webhooks is created and listed in the **Webhook** table.

The **Webhook** table displays the following information and also allows you to edit or delete Webhooks:

- **Name**—Name of the Webhooks.
- **Number of URL Entries**—Number of URLs in Webhooks. Click the number to view the list of URLs.

- **Updated At**—Date and time at which Webhooks was updated.
- **Webhook ID**—Webhooks ID.
- **Token**—Webhooks token. Webhooks token enables header authentication and the third-party receiving service must validate the token to ensure authenticity.
- **Edit**—Click the **Edit** icon in the last column to edit the Webhook. You can refresh the token and add URLs. Click **Save** to save the changes.
- **Delete**—Click the **Delete** icon in the last column and click **Yes** to delete the Webhook.

Refreshing Webhooks Token Through the UI

To refresh Webhooks token through the UI:

1. Go to **Maintenance** > **API Gateway** > **Webhook** tab.
2. In the **Webhook** table, click the edit icon in the **Token** column.
3. In the pop-up window, click the refresh icon next to the token. The token is refreshed.

Creating and Updating Webhooks Through the API Gateway

The following HTTP methods are defined for Aruba Central API Webhooks resource:

- **GET**
- **POST**
- **PUT**
- **DELETE**

You can perform CRUD operation on the Webhooks URL configuration. The key configuration elements that are required to use API Webhooks service are Webhooks URL and a shared secret.

A shared secret token is generated for the Webhooks URL when you register for Webhooks. A hash key is generated using SHA256 algorithm by using the payload and the shared secret token. The API required to refresh the shared secret token is provided for a specific Webhooks configuration. You can choose the frequency at which you want to refresh the secret token.

To access and use the API Webhooks service:

1. Go to **Maintenance** > **API Gateway**.
2. In the **APIs** tab, click the **Swagger** link under the **Documentation** header. The Swagger website opens.
3. In the Swagger website, select **Webhook** from the **URL** drop-down list. All available Webhooks APIs are listed under **API Reference**.

For more information on Webhooks APIs, refer to https://app1-apigw.central.arubanetworks.com/swagger/central.

List of Webhooks APIs

Aruba Central supports the following Webhooks APIs:

- **GET /central/v1/webhooks**—Gets a list of Webhooks.

  The following is a sample response:

```
{
  "count": 1,
  "settings": [
    {
      "wid": "e26450be-4dac-435b-ac01-15d8f9667eb8",
      "name": "AAA",
      "updated_ts": 1523956927,
      "urls": [
```

```
        "https://example.org/webhook1",
        "https://example.org/webhook1"
      ],
      "secure_token": "KEu5ZPTi44UO4MnMiOqz"
    }
  ]
}
```

- **POST /central/v1/webhooks**—Creates Webhooks.

  The following is a sample response:

```
{
  "name": "AAA",
  "wid": "e829a0f6-1e36-42fe-bafd-631443cbd581"
}
```

- **DELETE /central/v1/webhooks/{wid}**—Deletes Webhooks.

  The following is a sample response:

```
{
  "wid": "e26450be-4dac-435b-ac01-15d8f9667eb8"
}
```

- **GET /central/v1/webhooks/{wid}**—Gets Webhooks settings for a specific item.

  The following is a sample response:

```
{
  "wid": "e26450be-4dac-435b-ac01-15d8f9667eb8",
  "name": "AAA",
  "updated_ts": 1523956927,
  "urls": [
    "https://example.org/webhook1",
    "https://example.org/webhook1"
  ],
  "secure_token": "KEu5ZPTi44UO4MnMiOqz"
}
```

- **PUT /central/v1/webhooks/{wid}**—Updates Webhooks settings for a specific item.

  The following is a sample response:

```
{
  "name": "AAA",
  "wid": "e829a0f6-1e36-42fe-bafd-631443cbd581"
}
```

- **GET /central/v1/webhooks/{wid}/token**—Gets the Webhooks token for the Webhooks ID.

  The following is a sample response:

```
{
  "name": "AAA",
  "secure_token": "[{\"token\": \"zSMrzuYrblgBfByy2JrM\", \"ts\": 1523957233}]"
}
```

- **PUT /central/v1/webhooks/{wid}/token**—Refreshes the Webhooks token for the Webhooks ID.

  The following is a sample response:

```
{
  "name": "AAA",
  "secure_token": "[{\"token\": \"zSMrzuYrblgBfByy2JrM\", \"ts\": 1523957233}]"
}
```

- **GET /central/v1/webhooks/{wid}/ping**—Tests the Webhooks notification and returns whether success or failure.

  The following is a sample response:

  ```
  "Ping Response [{'url': 'https://example.org', 'status': 404}]"
  ```

Sample Webhooks Format for a New Alert Generation

```
URL POST <webhook-url>
```

Custom Headers

```
Content-Type: application/json
X-Central-Service: Alerts
X-Central-Event: Radio-Channel-Utilization
X-Central-Delivery-ID: 72d3162e-cc78-11e3-81ab-4c9367dc0958
X-Central-Delivery-Timestamp: 2016-07-12T13:14:19-07:00
X-Central-Customer-ID: <########>
```

Body

```
{
   "id": "AV6fTbgEG8ncx_zH2-g-",
   "type": "RADIO_NOISE_FLOOR”,
   "setting_id”: "128000236-1253",
   "device_id": "NPAE000001",
   "timestamp": 1505914259,
   "operation": "create",
   "state": "open",
   "severity": "critical",
   "extra": {
   "_band": "5 GHz",
   "duration": "5",
   "name": "NPAE000001",
}
```

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.

For more information, see the following topics:

- Guest Access Dashboard on page 398
- Creating Apps for Social Login on page 399
- Configuring a Cloud Guest Splash Page Profile on page 402
- Configuring Visitor Accounts on page 411

Guest Access Dashboard

The **Overview** page in the **Guest Access** application provides a dashboard displaying the number of guests, guest SSID, client count, type of clients, application usage, and guest connection for the selected group.

Table 121 describes the contents of the **Guest Access Overview** page:

Table 121: *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.

Data Pane Item	Description
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.
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.
Application Usage	The application usage by the guest clients connected to the Instant APs on which the Deep Packet Inspection feature is enabled.

Creating Apps for Social Login

The following topics describe the procedures for creating applications to enable the social login feature:

- Creating a Facebook App on page 399
- Creating a Google App on page 400
- Creating a Twitter App on page 401
- Creating a LinkedIn App on page 401

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. Access the Google Developer site at https://code.google.com/apis/console.

2. To select an existing project, click **Select a project** and select the desired project.

3. If the project is not created, click **Create a project**, enter the project name and click **Create**.

4. Click **Enable APIs and Services**.

5. Navigate to **Social** category, and then click **Google+ API**. The **Google+ API** window opens.

6. To enable the API, click **Enable**.

7. Click **Create Credentials**. If the credentials are already created, click **Go to credentials**.

8. 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**.

9. Under **Create an OAuth 2.0 client ID**. Enter the **OAuth 2.0 Client ID Name**.

10. 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%/.

11. 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.examplenetworks.com/oauth/reply.

12. Click **Create Client ID**.
13. 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.
14. Click **Done**. A page showing the OAuth Client IDs opens.
15. 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 accosunt.

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

This topic describes the following procedures:

Adding a Cloud Guest Splash Page Profile

To create a splash page profile:

1. From the app selector, click **Guest Access**. The guest access configuration and management menu options are displayed.
2. Click **Splash Page**. The **Splash Page** pane is displayed.
3. Select a group from the group selector. You can create splash page profiles only for the individual groups. The splash page creation function is not available if the page view is set to **All Devices**.
4. To create a new Splash page, Click the + icon. The **New Splash Page** pane is displayed.
5. On the **Configuration** tab, configure the parameters described in the following table:

Table 122: *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. ■ **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 122: *Splash Page Configuration*

Data Pane Content	Description
Username/Password	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. To allow the guest users to register by themselves: 1. Enable **Self-Registration**. 2. Set the **Verification Required** to **ON** if the guest user account must be verified. 3. Specify a verification criteria to allow the self-registered users to verify through email or phone. ■ 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**. 4. 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. 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.
Social Login	**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. ■ **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 . 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: ■ https://apps.google.com/intx/en_in/ ■ https://domains.google.com/about/ 3. Specify a text for the Sign-In button. ■ **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.

Table 122: *Splash Page Configuration*

Data Pane Content	Description
Facebook Wi-Fi	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. 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.
Facebook Wifi Configuration	After selecting the Facebook Wi-Fi option, complete the following steps to continue with the Facebook Wi-Fi configuration. 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. **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 *Aruba Instant User Guide*.
Allow Internet In Failure	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.
Override Common Name	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. 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: 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	To set password for anonymous users, enable the Guest Key and enter a password.
Sponsored Guest	Enable the **Sponsored Guest** option if you (network administrator) want to give the authorization control to a guest sponsor to allow or deny a guest from accessing the network.
Allowed Sponsor Domains	This is a mandatory field. Enter accepted company domain names. The domain name must match the suffix of the sponsor's email address. The domain names must be company names and not any public domain names such as gmail, yahoomail, and so on. To add more domain names, click the add icon and enter the domain name.
Allowed Sponsor Emails	Optional field to enter allowed email addresses. If you leave this field empty, all emails that correspond to the allowed domains list are permitted to sponsor guests. To add more sponsor emails, click the add icon and enter the sponsor's email address.
Authentication Success Behavior	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:

Table 122: *Splash Page Configuration*

Data Pane Content	Description
	■ **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.
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.
Simultaneous Login Limit	Specify the maximum number of devices that a user can use to access an account at a given time. For example, if you set the login limit as three, a user can simultaneously log in to an account using three different devices.
Daily Usage Limit	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. To set a daily usage limit, use one of the following options: ■ **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 timezone. ■ **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. ● **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. **Important Points to Note** ■ 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.
Whitelist URL	To allow a URL, click + and add the URL to the whitelist. For example, if the terms and conditions configured for the guest portal include URLs, you can add these URLs to the whitelist, so that the users can access the required web pages.

5. Click **Next**. The **Customization** pane appears. Customizing a Splash Page Design on page 406.

You can edit or delete a splash page profile by clicking the respective icons in the **Splash Page Profile** pane.

Customizing a Splash Page Design

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 123: *Splash page customization*

Data Pane Content	Description
Background color	To change the color of the splash page, select a color from the **Background Color** palette.
Button title	Specify a title for the sign in button.
Button color	To change the color of the sign in button, select a color from the **Button Color** palette.
Header fill color	Select the fill color for the splash page header from the **Header fill color** palette.
Page font color	To change the font color of the text on the splash page, select a color from the **Page font color** palette.
Page font Color	Select the font color of the splash page from the palette.
Logo	To upload a logo, click **Browse**, and browse the image file. Ensure that the image file size does not exceed 256 KB.
Background Image	Click **Browse** to upload a background image. Ensure that the background image file size does not exceed 512 KB.
Page Title	Add a suitable title for the splash page.
Welcome Text	Enter the welcome text to be displayed on the splash page. Ensure that the welcome text does not exceed 20,000 characters.
Terms & Conditions	Enter the terms and conditions to be displayed on the splash page. Ensure that the terms and conditions text does not exceed 20000 characters. 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 HTML tag. Specify an acceptance criteria for terms and condition by selecting any of the following options from the **Display "I Accept" Checkbox**: ■ **No, Accept by default** ■ **Yes, Display Checkbox** If the **I ACCEPT** check box must be displayed on the Splash page, select the display format for terms and conditions. Ensure that **Display Option For Terms & Conditions** has the Inline Text option auto-selected and displayed as an uneditable text.
Ad Settings	If you want to display advertisements on the splash page, enter the URL in the **Advertisement URL**. For **Advertisement Image**, click **Browse** and upload the image.

6. Click **Preview** to preview the customized splash page or click **Finish**.

Previewing and Modifying a Splash Page Profile

To preview a splash page profile, complete the following steps:

1. From the app selector, click **Guest Access**.
2. Click the **Splash Page** menu option. A list of splash Page profiles is displayed.

3. Ensure that the pop-up blocker on your browser window is disabled.

4. Click the preview icon next to the profile you want to preview. 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 next 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.

Localizing a Cloud Guest Portal

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 124: *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** lable.	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

Table 124: *Cloud Guest Portal Localization*

Data Pane Content	Description	Allowed Length of Text
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
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 toshow 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

Table 124: *Cloud Guest Portal Localization*

Data Pane Content	Description	Allowed Length of Text
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
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
Sponsored Guest Section		
Sponsor approval granted title	Enter a custom title for the sponsor's **Approval Granted** page.	1–255 characters

Table 124: *Cloud Guest Portal Localization*

Data Pane Content	Description	Allowed Length of Text
Sponsor approval pending title	Enter a custom title for the sponsor's **Approval Pending** page.	1–255 characters
Sponsor approve button title	Enter a custom title for the sponsor's **Approve** button.	1–255 characters
Sponsor approve title	Enter a custom title for the sponsor's **Approve** page.	1–255 characters
Sponsor approved title	Enter a custom title to be shown on the **Approved** page.	1–255 characters
Sponsor label	Enter a custom text for the **Sponsor** label.	1–255 characters
Sponsor placeholder	Enter a custom placeholder text for sponsor input control.	1–255 characters
Sponsor approval granted message	Enter a custom message to show in the **Approval Granted** page when the guest sponsor had grented approval for the guest to access the network.	Up to 20000 characters
Sponsor approval mail message	Enter an optional alternative email message to send when a guest requests for a Wi-Fi access. Ensure that the email inlcudes the [account:username] and [account:sponsor-approval-url] tokens. To customize the contents of email message, or to change the email message to a local language: 1. Click **Customize Sponsor Approval Mail**. 2. Edit the email message. 3. Click **Save**.	N/A
Sponsor approval pending message	Enter a custom message to show in the **Approval Pending** page when the guest sponsor is yet to approve or deny the guest from accessing the network.	Up to 20000 characters
Sponsor approve message	Enter a custom message to show in the **Approve** page.	Up to 20000 characters
Sponsor approved message	Enter a custom message to show in the **Approved** page when the guest sponsor had approved the guest to access the network.	Up to 20000 characters
Sponsor message	Enter a custom message to show in the **Registration** page for the guest to know that sponsor's approval is required.	Up to 20000 characters

4. Click **Preview** to preview the localized cloud guest portal page or click **Finish**.

Associating a Splash Page Profile to an SSID

To associate a splash page profile with an SSID, complete the following steps:

1. Select **Configuration > Access Points > Networks** and then click **Create New**. The **Create a New Network** pane is displayed.
2. For **Type**, select **Wireless**.
3. Enter a name that is used to identify the network in the **Name(SSID)** box.
4. For **Primary Usage**, select **Guest** and click **Next**.
5. In the **VLANs** tab, if required, configure a VLAN assignment mode, and then click **Next**.
6. In 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 click **Next**.

If the user configures the default Aruba certificate, the **You are using Aruba default certificate. You shall configure new certificate** alert message is displayed for the user to configure a new certificate.

   c. To enable encryption, set **Encryption** to **Enabled** and configure encryption parameters.
   d. To exclude uplink, select an uplink from **Disable If Uplink Type Is**.
   e. Click **Next**.
7. In the **Access** tab, if required, modify and create access rules set the configuration if required, and then click **Finish**.

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. From the app selector, click the **Guest Access** application.
3. Click the **Visitors** menu option, and then click **Add Visitor**. The **Add Visitor** pane is displayed.
4. Configure the parameters described in the following table:

Table 125: *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	■ 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**.
	Select this check box to activate the user account.

5. Click **Save**.
6. Click **Save and Print** to print the details of the visitor.

To view the guest or visitor sessions:

1. From the MSP view, drill down to a customer account.
2. From the app selector, click the **Guest Access** application.
3. Click the **Visitors** menu option. The **Guest Access > Visitors** page is displayed.
4. From the **Show visitors for network** drop-down list, select a network.

The following table displays the session details of the visitor:

Table 126: *Visitor Sessions Pane*

Parameter	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 127: *Visitor Accounts Pane*

Parameter	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.
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.

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 List**.

The Presence Analytics service available on Aruba Central enables businesses to collect and analyze user presence data in public venues, enterprise environments, and retail hubs. The Presence Analytics service enables businesses to collect real-time data on user footprints within the wireless network range of Aruba Instant APs that are managed using Aruba Central. Using the Presence Analytics statistics, businesses can analyze user behavior and improve customer engagement, and thus maximize revenue opportunities, optimize workspace, and increase market presence.

NOTE

Aruba Central supports Presence Analytics only on the APs running Aruba Instant 6.4.4.4-4.2.3.0 or a later version.

Enabling Presence Analytics Service

The Presence Analytics application is available only if the Presence Analytics service is enabled on an Instant AP. To start using the Presence Analytics service, contact the Aruba Central Sales team and obtain a subscription.

If you have a valid subscription, enable the **Presence Analytics** service on your APs using the following steps:

1. From the app selector, click the **Global Settings** app.
2. Click **Subscription Assignment**.
3. Select the device from the devices table.
4. From the list of subscriptions, select the devices that requires the Presence Analytics service subscription.
5. Drag and drop the device to the Presence Analytics service in the subscriptions table.
6. Click **Yes** to confirm the subscription assignment.

NOTE

If the Presence Analytics service subscription is enabled on one Instant AP in the cluster, the other Instant APs in the cluster inherit the Presence Analytics configuration settings, and send the RSSI feeds to Aruba Central. However, the Presence and Loyalty statistics are displayed only for the Instant APs on which the Presence Analytics feature is enabled.

Using the Presence Analytics App

The Presence Analytics application displays data either for all sites or per site. A site in Aruba Central represents a physical location such as a venue or store. If your account does not have any sites configured, ensure that you create a site. For more information on creating sites and adding devices, see Managing Sites on page 69.

The **Presence Analytics** application page displays the following menu options are displayed:

- **Activity**—A dashboard that shows the client presence details, loyalty metrics, and connected client metrics.
- **Settings**—The configuration page in which the RSSI threshold and dwell time for the clients can be set

Activity Dashboard

The Activity dashboard displays the following details:

- Presence metrics for passerby clients and visitors
- Loyalty metrics for visitors
- Connected-client device metrics on Guest and Employee networks

Presence Details

Based on the proximity of the client device to a specific site, the Wi-Fi signal strength, and the time spent at the sites, the clients are classified as follows:

- Passersby—An associated or unassociated client who is in the vicinity of a specific site and has an RSSI value greater than -90 dBm. You can customize the RSSI value for Passerby on the **Presence Analytics** > **Settings** page.
- Visitors—The passerby clients who spend more than 5 minutes at the site and have an RSSI value greater than -65 dBm. You can customize dwell time and RSSI values on the **Presence Analytics** > **Settings** page.

If a client is idle for more than 30 minutes, Aruba Central removes the presence instance for that client. When the client reappears, Aruba Central creates a new instance for that client and applies the same presence classification criteria.

The **Presence** graphs on the dashboard provide statistical analysis of the aggregate count of passerby clients, the dwell time of these clients at the sites, the rate at which the passerby clients converted to visitors, and the aggregate count of visitors over a specific duration.

Loyalty Metrics

Based on the engagement pattern and the time spent by the clients at the site, Aruba Central classifies clients as visitors. It also maintains a record of the number of repeat visits made by these clients over a specific duration. Based on these records, it plots the frequency at which the visitors return to the sites, and classifies these repeat visitors as loyal visitors.

The **Loyalty** graphs on the dashboard provide a statistical analysis of the clients classified as unique, new, and loyal visitors for a given time range.

Wi-Fi Connected Devices

The dashboard includes the Wi-Fi Connected Clients as listed below:

- **Connected Devices**—A Wi-Fi client associated to a Guest or Employee network on the device.
- **Guest Devices**—A Wi-Fi client associated to the Guest networks on the device.
- **Employee Devices**—A Wi-Fi client associated to the Employee or Voice network on the device.

The Wi-Fi Connected Clients graphs on the dashboard provide statistical analysis of the aggregate count of associated clients over a specific duration.

Viewing Dashboard Contents

By default, the **Activity** page displays data for all sites for a time range of 3 hours.

See Table 128 for general guidelines on filtering content and analyzing data:

Table 128: *Presence Analytics Data Metrics and Filters*

Dashboard View	Description
Temporal Filter	You can view the clients' presence data for the following time ranges: ■ **3 Hours**— Data for the last 3 hours, with the current time taken as the basis for calculation. ■ **1 Day**—Data for the last 24 hours, with the current time taken as the basis for calculation. ■ **1 Week**— Data for the last 1 week, with 00:00 hour of the current week taken as the basis for calculation. ■ **1 Month**— Data for the last one month, wit 00:00 hour of the current month taken as basis for calculation. The granularity of data points for activity trends is as follows: ■ 5 minutes for a time range of 3 hours ■ 1 hour for a time range of 1 day ■ 1 day for a time range of 1 week and 1 month
Baseline and Change Metrics	The **Baseline** and **Change** metrics are shown for most of the graphs displayed on the **Activity** page. The baseline metric for presence data is calculated for each time range in the following way: ■ **3 Hours**—The baseline metric is not applicable. ■ **1 Day**—The baseline value is derived from the average of the presence data collected in the last 30 days. ■ **1 Week and 1 Month**—The baseline value is derived from the presence data collected in the last 6 months.
Baseline Versus Aggregate trends	Displays the aggregate or average values across the selected time range in comparison to the baseline value.

The **Activity** page allows you to set your dashboard view so as to show a quick summary or detailed information. To view more details about presence, Wi-Fi-connected clients, or loyalty metrics, enable the **Advanced** mode. See Table 129 for information on default and advanced views of the **Activity** dashboard.

Table 129: *Activity Dashboard*

Dashboard Content	Description	Default View	Advanced View
Presence			
Presence	The **Presence** graphs display presence metrics for passerby clients and visitors. The following graphs with presence metrics are displayed for all sites or a specific site. ■ **Passersby**—Shows the aggregate count of passerby clients for the selected time range. The graph also shows the following details: ● Baseline value for the passerby clients based on the selected time range ● Percentage of change in the count of passerby clients in comparison to the baseline value ■ **Visitors**—Shows the aggregate count of visitors.The graph also shows the following data: ● Baseline value for the visitors trend based on the selected time range ● Percentage of change in the count of visitors in comparison to the baseline value ■ **Draw Rate**—Refers to the percentage of passerby clients that is converted to visitors for a specific time duration. The **Draw Rate** graph shows average draw rate. It also shows the following data: ● Baseline value for the draw rate metric based on the time range selection ● Percentage of change in draw rate compared to the baseline value ■ **Dwell Time**—Refers to the average time spent by visitors at a site at a given point in time. This graph shows the average dwell time of the visitors for all sites or a specific site. It also shows the following data: ● Baseline value for the dwell time metric based on the time range selection ● Percentage of change in the dwell time compared to the baseline value To view detailed presence information along with baseline change percentage graph, switch to the **Advanced** mode.	Yes	Yes
Passersby & Draw Rate Graphs	■ The **Passersby** chart plots the passerby clients' trend for the selected time range. For example, if the time range is set to 3 hours, it shows the passerby clients' count for every 5 minutes for the last 3 hours. Similarly, when the time range is set to 1 day, the count is displayed for every one hour. ■ The **Draw Rate** shows the rate of conversion of passerby clients to visitors for the selected time range. For example, if the time range is set to 3 hours, it shows the conversion count for every 5 minutes for the last 3 hours. Similarly, when the time range is set to 1 day, the count is displayed for every one hour. ● **5th Percentile**—The 5th percentile is the value of draw rate below which 5% of the sites could be found. The graph plots the draw rate trend at 5th percentile. ● **95th Percentile**—The 95th percentile is the value of draw rate below which 95% of the sites may be found. The graph plots draw rate trend at the 95th percentile.	No	Yes
Top & Bottom 5	Displays the top 5 and bottom 5 sites and plots trends for these sites for categories such as the following categories: ■ Passersby ■ Visitors ■ Draw Rate	No	Yes

Table 129: *Activity Dashboard*

Dashboard Content	Description	Default View	Advanced View
	■ Dwell Time The graph also shows the median that is derived based on the values. This information is gathered based on the trends observed for a selected metric across all sites for the selected time period. **NOTE:** If the number of sites is less than 10, the graph does not show the bottom 5 trends.		
View Presence Data	Displays the presence data for all sites. The **All Sites** table shows the passerby clients' count, visitors' count, draw rate, and dwell time metrics. Click the **Download All Sites Data** icon to download the presence data for all sites for a given time range.	Yes	Yes
Loyalty			
Loyalty	The **Loyalty** area displays the following graphs with loyalty metrics for visitors: ■ **Unique Visitors**—Shows the unique visitors' count, which is the sum of new and loyal visitors for the selected time range. Rephrase this sentence to make this as list items-- The graph also shows the following data: ● Baseline metric calculated for a given time range ● Percentage of change in the unique visitors' count in relation to the baseline metric. ■ **New Visitors**—Shows the aggregate count of the new visitors. Visitors who have visited only once in the last 1 month are referred to as the new visitors. The graph also shows the following data: ● Baseline metric calculated for a given time range ● Percentage of change in the new visitors' count in relation to the baseline metric ■ **Loyal Visitors**—Shows the aggregate count of the visitors categorized as loyal. Visitors who have visited a site more than once in the last 1 month are referred to as loyal visitors. The graph also shows the following information: ● Baseline metric calculated for a given time range ● Percentage of change in the loyal visitors' count in relation to the baseline metric To view the detailed loyalty information along with the baseline change percentage graph, switch to the **Advanced** mode.	Yes	Yes
Visitor Loyalty Composition	Shows the number of visitors categorized as new and loyal visitors for a specific time range.	No	Yes
Loyal Visitors – Visits in the last 3 months	Shows the number of visits the loyal visitors made to a site in the last three months.	No	Yes
Top & Bottom 5	Shows the top 5 sites and bottom 5 sites for: ■ New visitors ■ Unique visitors ■ Loyal visitors The graph also shows the following: ■ Trends for the top and bottom sites for the selected category.	No	Yes

Table 129: *Activity Dashboard*

Dashboard Content	Description	Default View	Advanced View
	■ Median derived based on the values gathered from the trends observed for a selected metric across all sites for the selected time period. **NOTE:** If the number of sites is less than 10, the graph does not show the bottom 5 trends.		
View Loyalty Data	Displays the loyalty metrics for all sites. The **All Sites** table shows unique visitors, new visitors, and loyal visitors. Click the **Download All Sites Data** icon to download the loyalty metrics for all sites for a given time range.	Yes	Yes
Wi-Fi Connected Devices			
Wi-Fi Connected Devices	Displays the following graphs for Wi-Fi connected devices: ■ **Connected Devices**—Displays the aggregate count of associated clients for the selected time range. The graph also shows the baseline value for the associated clients based on the selected time range, and the percentage of change in the count of the associated clients in comparison to the baseline value. ■ **Guest Devices**—Displays the aggregate count of associated clients on Guest Networks for the selected time range. The graph also shows the baseline value for the associated clients on Guest Networks based on the selected time range, and the percentage of change in the count of the associated clients on Guest Networks in comparison to the baseline value. ■ **Employee Devices**—Displays the average count of associated clients on Employee Networks for the selected time range. The graph also shows the baseline value for the associated clients on Employee Networks based on the selected time range, and the percentage of change in the count of the associated clients on Employee Networks in comparison to the baseline value. To view detailed Wi-Fi connected device information along with baseline change percentage graph, switch to the **Advanced** mode.	Yes	Yes
Connected Devices Vs Visitors	Displays the total count of client devices categorized as Employee, Guest and Visitor devices. This includes both associated and unassociated client devices.	No	Yes
Top and Bottom 5 Connected Devices	Displays the top 5 and bottom 5 sites and plots trends for these sites for the following categories: ■ Connected Devices ■ Guest Devices ■ Employee Devices The graph also shows the following: ■ Trends for the top and bottom sites for the selected category. ■ Median derived based on the values gathered from the trends observed for a selected metric across all sites for the selected time period. **NOTE:** If number of sites is 10 or lower than 10, the graph does not show the bottom 5 trends.	No	Yes
View Wi-Fi Connected Devices Data	Displays Wi-Fi connected devices data for all sites. The **All Sites** table shows the metrics for Connected devices, Guest devices, and Employee devices for all the sites. Click the **Download All Sites Data** icon to download the connected clients data for all sites for a given time range.	Yes	Yes

Setting RSSI Threshold and Dwell Time

The RSSI and dwell time configuration allows the administrators to perform the following actions:

- Classify the type of client.
- Analyze presence patterns.
- Determine if the usage has increased over a period of time.

To modify the default RSSI and dwell time configuration parameters, complete the following steps:

1. From the app selector, click **Presence Analytics**.
2. Click **Settings**.
3. Under **Passersby**, specify the value for **RSSI threshold**. By default, the RSSI threshold value is set to -90 dBm. You can specify a value within the range of -100 to 0.
4. Under **Passersby to Visitor**, specify the values for **RSSI threshold** and **Dwell Time** parameters. By default, the RSSI threshold is set to -65 dBm and the dwell time is set to 5 minutes.
5. Click **Save Settings**.

This section provides an overview of Clarity application, and descriptions for all its features.

Clarity Application Overview

The Aruba Clarity solution is an application(app) that allows you to monitor deployments and proactively detect network performance issues during the deployment. The administrators can use data from the Clarity app to analyze all the devices in the network thereby monitoring the network performance, and plan for corrective actions to resolve the onboarding issues detected in the network.

The Clarity app in Aruba Central allows you to monitor non-RF and connectivity issues that impact the wireless user experience. With Clarity app, administrators can proactively monitor the client data flow, client association, authentication, DHCP, and DNS service response times in real time within 10-15 minutes.

Using the Clarity analytics dashboard, the administrators can view the status of the wireless connection for the devices added in Aruba Central, and troubleshoot issues detected in the network.

Aruba Central supports the infrastructure for Clarity app. To view the network performance data using the Clarity app, ensure that the AP devices in your network are running the firmware version 6.5.1.0-4.3.1.0 or later.

The Clarity app filters network performance data based on the labels and sites to which the devices are assigned in your network. Ensure that the devices that support Clarity are assigned to labels and sites. For more information, see Managing Labels and Managing Sites.

Enabling Clarity Service

To access the Clarity app, you must obtain a valid subscription and enable the **Clarity** service on your devices. To obtain subscription for the Clarity app, contact the Aruba Central Sales team.

If you have a valid subscription, enable the **Clarity** service on your APs using the following steps:

1. From the app selector, click the **Global Settings** app.
2. Click **Subscription Assignment**.
3. Select the device from the devices table.
4. From the list of subscriptions, select the devices that requires the Clarity service subscription.
5. Drag and drop the device to the Clarity app in the subscriptions table.
6. Click **Yes** to confirm the subscription assignment.

Clarity Monitoring Dashboard

To view the Clarity monitoring dashboard, from the app selector, click **Clarity**. You can use labels and sites as filters to view data for the devices assigned a site or label.

Activity

The **Activity** dashboard displays graphs for connectivity health, latency, performance of the network and the device, and the association and authentication transactions between the client device and the network. This dashboard also displays the causes for network and transaction failures detected in the network.

Table 130: *Activity Monitoring Dashboard*

Dashboard View	Description
Time range	Allows you to view the charts and graphs in any of the following time ranges: ■ **3 Hours**—Displays data from the current time to last 3 hours. This is the default time range for which the data is displayed. When the time range is set to 3 hours, the graphs display the aggregate data points for every 10 minutes. ■ **1 day**—Displays data from the current time to last 1 day. When the time range is set to 1 day, the graphs display the aggregate data points for every two hours. ■ **1 week**—Displays data from the current day to last 1 week. When the time range is set to 1 week, the graphs display the aggregate data points for every week. ■ **1 month**—Displays data from the current day to last 1 month. If the time range is set to 1 month, the graphs display the aggregate data points for every two days.
Search and data display criteria	Allows you to specify a criterion based on the SSIDs on which the clients are connected, and the label, or site to which the AP devices are assigned. You can filter the monitoring data based on the following criteria. ■ **All Devices**—Displays data for all devices in the network. This option also displays the monitoring data for all the SSIDs enabled on the devices. ■ **Label**—Displays data for all the SSIDs enabled on the devices assigned to a specific label. You can select a label from the filter bar on the header pane. ■ **Site**—Displays data for all the SSIDs enabled on the devices assigned to a specific site. You can select a site from the filter bar on the header pane. ■ **SSID**—Displays data for a specific SSID enabled on the devices attached to a specific label or site.
Connectivity Health	Displays a cumulative score that is computed based on the onboarding performance of the network. The data is presented in the following colors to indicate the connectivity health score ranges: ■ Green—100-85 ■ Orange—84-70 ■ Red—69-0 The connectivity health index is calculated based on the following parameters: ■ **Attempts**—The number of attempts made by the client devices to connect to the network. ■ **Success Rate**—The percentage of successful onboarding of the client devices in the network. ■ **Timely**—The number of client connections that were established on time, without any failure or delay. ■ **Delayed**—The number of delayed events detected in client connections and associations to the Instant APs that are provisioned in your network. ■ **Failed**—The number of unsuccessful attempts made by client devices to connect to the network.
Connectivity Performance	Displays a graph that summarizes the connectivity performance of the network for the selected time range. The graph plots the following data points: ■ Number of timely and successful onboarding events for client devices. ■ Number of delays observed when onboarding a client device. ■ Number of failed attempts when onboarding a client device. ■ The connectivity health score for the network.
Stage-wise Performance	Displays the connectivity health index for each category of network performance based on parameters such as timeliness, delays, and failed attempts detected when onboarding client devices.

Dashboard View	Description
	■ **Association**—Number of successful, timely, delayed, and failed association attempts made by the client devices to connect to the network. ■ **Authentication**—Number of successful, timely, delayed, and failed authentication attempts made by the client devices to connect to the network. ■ **DHCP**—Number of successful, timely, delayed, and failed DHCP requests and responses detected when onboarding the client devices. ■ **Captive Portal**—Number of successful, timely, delayed, and failed attempts made by the client devices to connect to the guest SSIDs in the network. ■ **DNS**—Number of successful, timely, delayed, or failed attempts in DNS resolutions detected when client devices connect to the network. The DNS chart is displayed only when the dashboard view is set to display the aggregate connectivity and network performance data for all labels and SSIDs defined in the network.
Delay-Causes	Displays a pie chart that provides a summary of the causes for the delays. The delays that are detected are categorized in one of the following stages in the network: ■ Client association ■ 802.1X authentication ■ MAC authentication ■ Key-Exchange ■ Captivate portal authentication ■ DHCP services
Failure-Causes	Displays a pie chart that provides a summary of the causes for the failed attempts. The causes for failed attempts are categorized in one of the following stages in the network: ■ Client association ■ 802.1X authentication ■ MAC authentication ■ Key-Exchange ■ Captivate portal authentication ■ DHCP services
Device Performance	Displays a chart that shows the types of client devices that attempt to establish connection with the network.
Authentication Performance	Displays a chart that provides a summary of the connectivity health. It is based on the type of authentication methods used by client devices to establish connection with the network.

Insights

The **Insights** dashboard displays the most relevant issues that are detected during the onboarding of client devices. The **Insights** page segregates these issues based on their impact on the onboarding performance of the network.

Cumulative Issue Impact Chart

The chart on the **Insights** page displays a cumulative impact of the issues on the onboarding performance of the network.

The color codes in the chart indicate the following:

- Dark blue—Indicates more number of insights
- Light blue—Indicates less number of insights
- White—No insights

The insights include the following information:

- Failure instances
- Number of devices impacted
- Time stamp of the event
- Associated labels and SSIDs
- Impacted APs and client devices

Filtering Content for Insights Display

The **Insights** page allows you to view insights for all devices and filter insights for a specific label or site. You can also filter the insights for an onboarding stage, or an SSID.

- To view insights for a specific onboarding stage, select one or several stages from the **Select Stage** drop-down list as required.
- To view insights for a specific SSID, select the SSID from the **Select SSID** drop-down list.

Dynamic Range Selection

The chart on the **Insights** page allows you to dynamically select the time range and view insights specific to that time range.

To view insights for a specific time range, use the slider and select the desired time period.

Performance Summary

The **Insights** page also lists the alerts based on the onboarding experience of client devices. The insights can be drilled down to view details such as time stamps of events, and causes for the delayed or failed onboarding of client devices. Using these insights, you can analyze the performance of the network and proactively plan corrective actions to restore and enhance the wireless user experience.

Exporting Insights

To export the insights analytics data, complete the following steps:

1. Select the duration for which you want to view the Insights.
2. Click **Export Insights** (CSV). The insights information is exported in the CSV format.

Troubleshooting

The **Troubleshooting** page allows you to view details such as failure or delay in onboarding a specific client device.

To view a log of the onboarding events associated with a client device, enter the MAC address of the client device or the username, and then click the search icon. The search function on the **Troubleshooting** page also supports partial MAC address and username in the search text.

The event log for client devices displays the following information:

- **Timestamp**—Time stamp of the onboarding event.
- **Stage**—The stage of onboarding such as association with the AP, authentication, and DHCP status.
- **SSID**—The SSID to which the client device attempts to establish a connection.
- **AP MAC**—The MAC address of the AP.
- **Status**—The onboarding status of the client device.
- **Reason**—The reason for the delayed or failed onboarding.

The growing use of Wi-Fi and the proliferation of mobile tablet and smartphone clients cause control and visibility challenges for communication and collaboration applications such as Lync/Skype for Business. To overcome these challenges, Aruba offers the Unified Communications application service to manage your enterprise communication ecosystem.

Overview

The Unified Communications application on Aruba devices provides a seamless user experience for voice, video calls, and application sharing when using Microsoft® Lync/Skype for Business. The application actively monitors and provides visibility into Lync/Skype for Business traffic and allows you to prioritize sessions. The Unified Communications application also leverages the functions of the Service Engine on the cloud platform and provides rich visual metrics for analytical purpose.

The Unified Communications application supports the following functions based on the type of device used in the solution:

- Session prioritization—Based on the type of device provisioned in your network, the Aruba Central server receives call control information from devices such as Instant APs and switches. The Unified Communications application uses this data to detect and classify the traffic type, and dynamically prioritize voice and video over data traffic. Based on the type of device, the following information sources are used for session prioritization.
  - The Lync/Skype for Business SDN API—The SDN API provides an interface for the Aruba devices to access diagnostic information for a comprehensive and a real-time view of applications, users, devices, the Wi-Fi, and the LAN network infrastructure. The Unified Communications application uses this data to prioritize voice and video traffic. The SDN API can be installed on a Lync 2010, Lync 2013, or Skype for Business 2015 server.
  - Heuristics—A built-in method that detects the Lync/Skype for Business traffic and works with all on-premises and Skype for Business online (Office 365) deployments. The heuristics data detection and classification method is used to identify clients in the call, and classify and prioritize media packets. Aruba switches do not support heuristics-based prioritization. The session prioritization for Aruba switches is based on the data from the Skype server through OpenFlow.
- Session visibility—The application also provides call session visibility correlated across the Skype server and mobility network to simplify operations for the network administrator. The administrators can monitor wireless and wired network connectivity health on a per-session basis and analyze the quality of experience.

Enabling Unified Communications Service

To access the Unified Communications application, you must obtain a valid subscription and enable the **Unified Communications** service on your devices. To obtain subscription for the **Unified Communications** application, contact the Aruba Central Sales team.

If you have a valid subscription, enable the **Unified Communications** service on your APs as given in the following steps:

1. From the app selector, click the **Global Settings** app.
2. Click **Subscription Assignment**.

3. From the list of subscriptions, select **UCC**.
4. Select the device from the **Devices** table.
5. Drag and drop the device to the **Subscriptions** table.
6. Click **Yes** to confirm the subscription assignment.

Supported Devices

The Unified Communications application functions in both wired and wireless environments with Aruba devices such as Instant APs and switches.

Table 131 shows the list of supported devices:

Table 131: *Unified Communications Device Support Matrix*

Device Model	Firmware Version	Session Prioritization		Session Visibility
		Heuristics	SDN API	
Aruba 2920 Switch Series	WB.16.03.0000 or later	No	Yes	No
Aruba 2930F Switch Series	WB.16.03.0000 or later			
Aruba 3810 Switch Series	KB.16.03.0000 or later			
Instant APs	6.5.4.0 or later	Yes	Yes	No

Table 132 shows the feature support for Aruba devices:

Table 132: *Unified Communications Feature Matrix*

Feature	Prioritization	Visibility	Supported Devices
Skype	Yes	Yes	Instant APs running 6.5.4.0 or later

Configuring Devices for Session Prioritization

Based on the ArubaOS software version, controllers support session prioritization using both SDN API and heuristics as the source for information. If both methods are enabled, the SDN API-based Skype for Business classification takes precedence.

OpenFlow Configuration

For both SDN API and heuristics-based classification and prioritization, OpenFlow configuration is required.

- In the SDN API-based Skype for Business classification method, the Unified Communications application receives the media identification data from the SDN Manager and call quality report from the devices through OpenFlow.
- In heuristics-based media classification method, the Unified Communications application receives media identification and the call quality reports from the devices through OpenFlow.

Enable OpenFlow on Switches

To enable OpenFlow on Aruba switches, complete the following steps:

1. Configure OpenFlow controller details on the switch.

```
(host)# configure terminal
(host)(config)# openflow
(host)(openflow)# controller-id <number> ip <ip-addr-of-OFC> port <OFC-TCP-port>
controller-interface vlan <vlan-id-used-to-connect-to-OFC>
(host)(openflow)# write memory
(host)(openflow)# exit
```

2. Configure OpenFlow instance details by executing the following commands:

```
(host)# configure terminal
(host)(config)# openflow
(host)(openflow)# instance <instance-name>
(host)(openflow)# member vlan <vlan-id-of-the-member>
(host)(openflow)# controller-id <same as the number given for controller-id in the OFC
details>
(host)(openflow)# version 1.3
(host)(openflow)# pipeline-model standard-match
(host)(openflow)# exit
```

3. Enable OpenFlow and OpenFlow instance by executing the following commands:

```
(host)(config)# configure terminal
(host)(config)# openflow instance <instance-name> enable
(host)(config)# openflow enable
(host)(config)# exit
```

Aruba switches support only the SDN API source for session prioritization.

For more information about configuration commands, see the *HPE ArubaOS-Switch Management and Configuration Guide*.

Enabling OpenFlow on Instant APs

If the Unified Communications subscription is enabled on the Instant APs, OpenFlow is automatically enabled on the Instant APs. Therefore, no explicit configuration from the user is required for enabling OpenFlow.

SDN API-Based Classification

For the Lync/Skype for Business SDN API to dynamically prioritize traffic at the edge of a network using OpenFlow, the OpenFlow controller and its instances must be configured on switches. For information on configuring OpenFlow instances, see OpenFlow Configuration.

Configuring SDN Manager for SDN API

To enable Skype SDN Manager to send XML messages to the Unified Communications application, complete the following configuration:

1. Log in to the Skype SDN Manager.
2. Ensure that you have the *SDNManager.exe* program installed.
3. Open the command prompt and go to the folder in which the *SDNManager.exe* program is installed.
4. Execute the following command:

```
SDNManager.exe p s <some-string> submituri=[https://<Cluster-IP>/skypeSDN/<customer-id>
```

Use the **GET /v1/SkypeCentralURL** API to get the Lync/Skype for Business URL for the Aruba Central cluster that you are using. See API Gateway on page 383 for detailed information on accessing and using APIs.

HTTPS Connectivity with SDN Manager

The customer premises with the Lync/Skype for Business SDN infrastructure must access Aruba Central through an HTTPS connection only. Aruba Central acts as a server while Lync/Skype for Business SDN Manager acts as a client.

For the client and server mutual authentication and TLS handshake, the client must have a root CA certificate provided by GeoTrust to validate the certificate presented by Aruba Central.

Heuristics Classification

In the heuristics method, Aruba devices such as Instant APs perform deep packet inspection on the Skype for Business traffic to determine Skype for Business voice and video traffic. For the heuristics classification method, no changes or additional components are required on the Skype for Business server.

The heuristics classification method includes the following steps:

- When the Skype for Business calls are established, classify-media in the ACL is triggered and Skype for Business clients are marked as media-capable clients.
- Any subsequent UDP data flow with source/destination port numbers above 1023 from or to media-capable users go through the Skype for Business media DPI.
- If an RTP session is based on DPI, the payload type in the RTP header is used to determine if it is a voice or video session.

Configuring ACLs on Instant APs for Media Classification

To enable classify-media option of ACL on Instant APs, complete the following steps:

1. From the app selector, click **Wireless Management**.
2. From the list of groups, select the group for which you want to classify media.
3. Click **Security**. The **Security** page opens.
4. Click **Roles**.
5. Select a user role and click the **+** icon in the **Access Rules for Selected Roles** pane.
6. Set the rule type to **Access Control**.
7. Set the following parameters for the **Network** service:
   a. **Service type**—SIPS
   b. **Action**—Allow
   c. **Destination**—To all destinations
8. Select **Classify Media**.
9. Click **Save**.
10. Click **+** to add another rule and repeat the steps for the required network services such as HTTPS and enable **Classify Media** for each rule.
11. Save the changes.

Dashboard for Session Analysis

The Unified Communications dashboard provides a view of the voice and video traffic trends along with the desktop sharing sessions, for the devices that are provisioned in Aruba Central. The banner in the header pane shows the following details:

- Audio—Displays the number of audio sessions originated in the last 5 minutes.

- Video—Displays the total number of video sessions in the last 5 minutes.
- Desktop Sharing—Displays the total number of the desktop sharing sessions in the last 5 minutes.

The application consists of the following tabs that provide visibility into the Unified Communications instances detected in the network:

- Activity
- Insights
- Troubleshooting
- Call Detail Records
- Settings

Activity

The **Unified Communications > Activity** page displays a variety of charts that allow you to assess the quality of voice and video traffic on network.

Table 133 describes the contents of the **Activity** page:

Table 133: *Activity Page*

Dashboard View	Description
Temporal Filter	Allows you to view the charts and graphs in any of the following time ranges: ■ **3 Hours**—Data for the last 3 hours, with the current time taken as the basis for calculation. This is the default time range for which the data is presented. When the time range is set to 3 hours, the graphs display the aggregate data points for every 10 minutes. ■ **1 Day**—Data for the last 24 hours, with the current time taken as the basis for calculation. When the time range is set to 1 day, the graphs display the aggregate data points for every two hours. ■ **1 Week**—Data for the last 1 week, with the current day taken as the basis for calculation. When the time range is set to 1 week, the graphs display the aggregate data points for every day. ■ **1 Month**—Data for the last one month, with the current day taken as basis for calculation. If the time range is set to 1 month, the graphs display the aggregate data points for every two days. ■ **3 Month**—Data for the last three months, with the current day taken as basis for calculation. If the time range is set to 3 months, the graphs display the aggregate data points for every two days.
Activity summary	The **Activity** summary area displays the following details: ■ **UC Health**—Health status based on the call quality score. ■ **Total Sessions**—Total number of sessions detected in the network. ■ **Poor Sessions**—Number of sessions with poor quality. ■ **Audio**—Percentage of audio sessions in the network. ■ **Video**—Percentage of video sessions in the network. ■ **Desktop Sharing**—Percentage of desktop sharing sessions in the network. ■ **UC Clients**—Number of clients using Lync/Skype for Business. ■ **Wireless**—The percentage of good-, fair-, and poor-quality calls exchanged between wireless networks. ■ **Wired**—The percentage of good-, fair-, and poor-quality calls exchanged between wired networks. ■ **External**—The percentage of sessions exchanged with clients from external networks.
Session Count by Type	Displays trend for audio, video, and desktop sharing sessions.

Dashboard View	Description
Session Quality by Session Type	Displays a comparison trend for audio, video, and desktop sharing sessions based on the call quality indicators such as good, fair, and poor.
Operating Systems	Displays call data segregated based on the type of OS running on the client devices.
Session Quality by Client Health	Displays a breakup of calls that shows a correlation between the session quality and the client health.
Session Quality by SSID	Provides a detailed view of call distribution and session quality across various SSIDs.

Insights

The **Insights** page displays a summary of the patterns identified for poor quality sessions for each day in the last month. The **Insights** page segregates these issues based on their impact on the quality of sessions detected in the network.

Troubleshooting

The **Troubleshooting** page provides a summary of the client connection details and displays possible causes for the poor-quality session, and lists poor call records. The administrators can use this data to determine behavior of the client, and analyze the delays, jitters, and packet loss in the network.

To view a log of the call events associated with a specific client, enter the Skype URI or the MAC address of the client device, and click the search icon. The search results display details such as the device type, username, and IP address of the device, call sessions, average session duration, most frequently called numbers, the MAC address of the AP to which the device is associated, and the SSID to which the device is connected.

Call Detail Records

The **Call Detail Records** page displays various details about the call. You can use this information for debugging purposes. Click **Export CSV** to export the call detail records to a **.csv** file.

Table 134 describes the parameters of the **Call Detail Records** page:

Table 134: *Call Detail Records*

Parameter	Description
Start Time	Displays the start time of the call or session.
End Time	Displays the end time of the call or session.
Client	Displays the username of the client.
Peer Client	Displays the username of the client being called.

Table 134: *Call Detail Records*

Parameter	Description
Session Type	Displays the type of call or session. Possible values are as follows: ■ Desktop Sharing ■ Video ■ Audio
Client Health	Displays the health of the client. Possible values are as follows: ■ Good ■ Fair ■ Poor
Call Quality	Displays the quality of the call based on the UCC score. Possible values are as follows: ■ Good ■ Fair ■ Poor ■ Unknown
AP Name	Displays the name that uniquely identifies the Instant AP.
Customer ID	Displays the customer ID.
Device Type	Displays the type of device from which the client is connected.
Connectivity Type	Displays the connectivity type.
CDR ID	Displays the call detail record ID.
AP IP	Displays the IP address of the Instant AP.
AP MAC	Displays the MAC address of the Instant AP.
Application	Displays the application using which the client is connected.
BSSID	Displays the BSSID of the Instant AP.
Peer Client IP	Displays the IP address of the peer client.
Client IP	Displays the IP address of the client.
Call State	Displays the state of the call.
Capture Device	Displays the type of video camera device.
Channel	Displays the channel number.
Channel Busy	Displays the channel utilization percentage.
ESSID	Displays the extended SSID that is used across multiple Instant APs.
Interference	Displays the level of interference.
Label ID	Displays the label ID.

Table 134: *Call Detail Records*

Parameter	Description
Render Device	Displays the type of audio device.
Station MAC	Displays the MAC address of the calling station.
UCC MOS	Displays the UCC Mean Opinion Score (MOS).
User Role	Displays the user role assigned to the client.
Wifi Driver Description	Displays the Wi-Fi driver description.
Wifi Driver Version	Displays the Wi-Fi driver version.

Settings

The **Settings** page allows you to configure Skype for Business (audio, video, desktop sharing) protocol priority and Skype for Business server certificate domain name.

Table 135 describes the parameters of the **Settings** page:

Table 135: *Settings page*

Parameter	Description
Protocol Priority	
Skype for Business (Audio)	Enter the protocol priority for audio sessions. Specify a value within 0—63 range. The default value is 46.
Skype for Business (Video)	Enter the protocol priority for video sessions. Specify a value within 0—63 range. The default value is 34.
Skype for Business (Desktop Sharing)	Enter the protocol priority for desktop sharing sessions. Specify a value within 0—63 range. The default value is 34.
Other Settings	
Skype Server Certificate Domain Name	Enter the Skype for Business Server certificate domain name.

Appendix A
Glossary of Terms

The following table provides a brief description of the terminology used in this guide.

3DES

Triple Data Encryption Standard. 3DES is a symmetric-key block cipher that applies the DES cipher algorithm three times to each data block.

3G

Third Generation of Wireless Mobile Telecommunications Technology. See W-CDMA.

3GPP

Third Generation Partnership Project. 3GPP is a collaborative project aimed at developing globally acceptable specifications for third generation mobile systems.

4G

Fourth Generation of Wireless Mobile Telecommunications Technology. See LTE.

802.11

802.11 is an evolving family of specifications for wireless LANs developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). 802.11 standards use the Ethernet protocol and Carrier Sense Multiple Access with collision avoidance (CSMA/CA) for path sharing.

802.11 bSec

802.11 bSec is an alternative to 802.11i. The difference between bSec and standard 802.11i is that bSec implements Suite B algorithms wherever possible. Notably, Advanced Encryption Standard-Counter with CBC-MAC is replaced by Advanced Encryption Standard - Galois/Counter Mode, and the Key Derivation Function (KDF) of 802.11i is upgraded to support SHA-256 and SHA-384.

802.11a

802.11a provides specifications for wireless systems. Networks using 802.11a operate at radio frequencies in the 5 GHz band. The specification uses a modulation scheme known as orthogonal frequency-division multiplexing (OFDM) that is especially well suited to use in office settings. The maximum data transfer rate is 54 Mbps.

802.11ac

802.11ac is a wireless networking standard in the 802.11 family that provides high-throughput WLANs on the 5 GHz band.

802.11b

802.11b is a WLAN standard often called Wi-Fi and is backward compatible with 802.11. Instead of the Phase-Shift Keying (PSK) modulation method used in 802.11 standards, 802.11b uses Complementary Code Keying (CCK) that allows higher data speeds and makes it less susceptible to multipath-propagation interference. 802.11b operates in the 2.4 GHz band and the maximum data transfer rate is 11 Mbps.

802.11d

802.11d is a wireless network communications specification for use in countries where systems using other standards in the 802.11 family are not allowed to operate. Configuration can be fine-tuned at the Media Access Control (MAC) layer level to comply with the rules of the country or district in which the network is to be used. Rules are subject to variation and include allowed frequencies, allowed power levels, and allowed signal bandwidth. 802.11d facilitates global roaming.

802.11e

802.11e is an enhancement to the 802.11a and 802.11b specifications that enhances the 802.11 Media Access Control layer with a coordinated Time Division Multiple Access (TDMA) construct. It adds error-correcting mechanisms for delay-sensitive applications such as voice and video. The 802.11e specification provides seamless interoperability between business, home, and public environments such as airports and hotels, and offers all subscribers high-speed Internet access with full-motion video, high-fidelity audio, and VoIP.

802.11g

802.11g offers transmission over relatively short distances at up to 54 Mbps, compared with the 11 Mbps theoretical maximum of 802.11b standard. 802.11g employs Orthogonal Frequency Division Multiplexing (OFDM), the modulation scheme used in 802.11a, to obtain higher data speed. Computers or terminals set up for 802.11g can fall back to speed of 11 Mbps, so that 802.11b and 802.11g devices can be compatible within a single network.

802.11h

802.11h is intended to resolve interference issues introduced by the use of 802.11a in some locations, particularly with military Radar systems and medical devices. Dynamic Frequency Selection (DFS) detects the presence of other devices on a channel and automatically switches the network to another channel if and when such signals are detected. Transmit Power Control (TPC) reduces the radio frequency (RF) output power of each network transmitter to a level that minimizes the risk of interference.

802.11i

802.11i provides improved encryption for networks that use 802.11a, 802.11b, and 802.11g standards. It requires new encryption key protocols, known as Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES).

802.11j

802.11j is a proposed addition to the 802.11 family of standards that incorporates Japanese regulatory extensions to 802.11a; the main intent is to add channels in the radio frequency (RF) band of 4.9 GHz to 5.0 GHz.

802.11k

802.11k is an IEEE standard that enables APs and client devices to discover the best available radio resources for seamless BSS transition in a WLAN.

802.11m

802.11m is an Initiative to perform editorial maintenance, corrections, improvements, clarifications, and interpretations relevant to documentation for 802.11 family specifications.

802.11n

802.11n is a wireless networking standard to improve network throughput over the two previous standards, 802.11a and 802.11g. With 802.11n, there will be a significant increase in the maximum raw data rate from 54 Mbps to 600 Mbps with the use of four spatial streams at a channel width of 40 MHz.

802.11r

802.11r is an IEEE standard for enabling seamless BSS transitions in a WLAN. 802.11r standard is also referred to as Fast BSS transition.

802.11u

802.11u is an amendment to the IEEE 802.11 WLAN standards for connection to external networks using common wireless devices such as smartphones and tablet PCs. The 802.11u protocol provides wireless clients with a streamlined mechanism to discover and authenticate to suitable networks, and allows mobile users to roam between partner networks without additional authentication. An 802.11u-capable device supports the Passpoint technology from the Wi-Fi Alliance Hotspot 2.0 R2 Specification that simplifies and automates access to public Wi-Fi.

802.11v

802.11v is an IEEE standard that allows client devices to exchange information about the network topology and RF environment. This information is used for assigning best available radio resources for the client devices to provide seamless connectivity.

802.1Q

802.1Q is an IEEE standard that enables the use of VLANs on an Ethernet network. 802.1Q supports VLAN tagging.

802.1X

802.1X is an IEEE standard for port-based network access control designed to enhance 802.11 WLAN security. 802.1X provides an authentication framework that allows a user to be authenticated by a central authority.

802.3af

802.3af is an IEEE standard for Power over Ethernet (PoE) version that supplies up to 15.4W of DC power. See PoE.

802.3at

802.3at is an IEEE standard for PoE version that supplies up to 25.5W of DC power. See PoE+.

A-MPDU

Aggregate MAC Protocol Data Unit. A-MPDU is a method of frame aggregation, where several MPDUs are combined into a single frame for transmission.

A-MSDU

Aggregate MAC Service Data Unit. A-MSDU is a structure containing multiple MSDUs, transported within a single (unfragmented) data MAC MPDU.

AAA

Authentication, Authorization, and Accounting. AAA is a security framework to authenticate users, authorize the type of access based on user credentials, and record authentication events and information about the network access and network resource consumption.

ABR

Area Border Router. ABR is used for establishing connection between the backbone networks and the Open Shortest Path First (OSPF) areas. ABR is located near the border of one or more OSPF areas.

AC

Access Category. As per the IEEE 802.11e standards, AC refers to various levels of traffic prioritization in Enhanced Distributed Channel Access (EDCA) operation mode. The WLAN applications prioritize traffic based on the Background, Best Effort, Video, and Voice access categories. AC can also refer to Alternating Current, a form of electric energy that flows when the appliances are plugged to a wall socket.

ACC

Advanced Cellular Coexistence. The ACC feature in APs enable WLANs to perform at peak efficiency by minimizing interference from 3G/4G/LTE networks, distributed antenna systems, and commercial small cell/femtocell equipment.

Access-Accept

Response from the RADIUS server indicating successful authentication and containing authorization information.

Access-Reject

Response from RADIUS server indicating that a user is not authorized.

Access-Request

RADIUS packet sent to a RADIUS server requesting authorization.

Accounting-Request

RADIUS packet type sent to a RADIUS server containing accounting summary information.

Accounting-Response

RADIUS packet sent by the RADIUS server to acknowledge receipt of an Accounting-Request.

ACE

Access Control Entry. ACE is an element in an ACL that includes access control information.

ACI

Adjacent Channel Interference. ACI refers to interference or interruptions detected on a broadcasting channel, caused by too much power on an adjacent channel in the spectrum.

ACL

Access Control List. ACL is a common way of restricting certain types of traffic on a physical port.

Active Directory

Microsoft Active Directory. The directory server that stores information about a variety of things, such as organizations, sites, systems, users, shares, and other network objects or components. It also provides authentication and authorization mechanisms, and a framework within which related services can be deployed.

ActiveSync

Mobile data synchronization app developed by Microsoft that allows a mobile device to be synchronized with either a desktop or a server running compatible software products.

ad hoc network

An ad hoc network is a network composed of individual devices communicating with each other directly. Many ad hoc networks are Local Area Networks (LANs) where computers or other devices are enabled to send data directly to one another rather than going through a centralized access point.

ADO

Active X Data Objects is a part of Microsoft Data Access Components (MDACs) that enables client applications to access data sources through an (Object Linking and Embedding Database) OLE DB provider. ADO supports key features for building client-server and Web-based applications.

ADP

Aruba Discovery Protocol. ADP is an Aruba proprietary Layer 2 protocol. It is used by the APs to obtain the IP address of the TFTP server from which it downloads the AP boot image.

AES

Advanced Encryption Standard. AES is an encryption standard used for encrypting and protecting electronic data. The AES encrypts and decrypts data in blocks of 128 bits (16 bytes), and can use keys of 128 bits, 192 bits, and 256 bits.

AIFSN

Arbitrary Inter-frame Space Number. AIFSN is set by the AP in beacon frames and probe responses. AIFS is a method of prioritizing a particular category of traffic over the other, for example prioritizing voice or video messages over email.

AirGroup

The application that allows the end users to register their personal mobile devices on a local network and define a group of friends or associates who are allowed to share them. AirGroup is primarily designed for colleges and other institutions. AirGroup uses zero configuration networking to allow Apple mobile devices, such as the AirPrint wireless printer service and the AirPlay mirroring service, to communicate over a complex access network topology.

AirWave Management Client

AirWave Management Client is a Windows software utility that enables client devices (such as a laptop) to act as passive RF sensors and augments the AirWave RAPIDS module.

ALE

Analytics and Location Engine. ALE gives visibility into everything the wireless network knows. This enables customers and partners to gain a wealth of information about the people on their premises. This can be very important for many different verticals and use cases. ALE includes a location engine that calculates associated and unassociated device location periodically using context streams, including RSSI readings, from WLAN controllers or Instant clusters.

ALG

Application Layer Gateway. ALG is a security component that manages application layer protocols such as SIP, FTP and so on.

AM

Air Monitor. AM is a mode of operation supported on wireless APs. When an AP operates in the Air Monitor mode, it enhances the wireless networks by collecting statistics, monitoring traffic, detecting intrusions, enforcing security policies, balancing wireless traffic load, self-healing coverage gaps, and more. However, clients cannot connect to APs operating in the AM mode.

AMON

Advanced Monitoring. AMON is used in Aruba WLAN deployments for improved network management, monitoring and diagnostic capabilities.

AMP

AirWave Management Platform. AMP is a network management system for configuring, monitoring, and upgrading wired and wireless devices on your network.

ANQP

Access Network Query Protocol. ANQP is a query and a response protocol for Wi-Fi hotspot services. ANQP includes information Elements (IEs) that can be sent from the AP to the client to identify the AP network and service provider. The IEs typically include information about the domain name of the AP operator, the IP addresses available at the AP, and information about potential roaming partners accessible through the AP. If the client responds with a request for a specific IE, the AP will send a Generic Advertisement Service (GAS) response frame with the configured ANQP IE information.

ANSI

American National Standards Institute. It refers to the ANSI compliance standards for products, systems, services, and processes.

API

Application Programming Interface. Refers to a set of functions, procedures, protocols, and tools that enable users to build application software.

ARM

Adaptive Radio Management. ARM dynamically monitors and adjusts the network to ensure that all users are allowed ready access. It enables full utilization of the available spectrum to support maximum number of users by intelligently choosing the best RF channel and transmit power for APs in their current RF environment.

ARP

Address Resolution Protocol. ARP is used for mapping IP network address to the hardware MAC address of a device.

Aruba Activate

Aruba Activate is a cloud-based service that helps provision your Aruba devices and maintain your inventory. Activate automates the provisioning process, allowing a single IT technician to easily and rapidly deploy devices throughout a distributed enterprise network.

AS

Autonomous System An autonomous system is a single network or a collection of networks that is under a single administrative control. The routing devices in an Autonomous System generally use a single interior gateway protocol (IGP) for routing information. Routing between two Autonomous Systems is handled by the Exterior Gateway Protocols like BGP.

ASCII

American Standard Code for Information Interchange. An ASCII code is a numerical representation of a character or an action.

ASN

Autonomous System Number ASN is a unique number assigned to an autonomous system. ASN is used for identifying an autonomous system when exchanging exterior routing information with other neighboring autonomous systems.

Autonomous System

Also referred to as AS. An autonomous system is a single network or a collection of networks that is under a single administrative control. The routing devices in an Autonomous System generally use a single interior gateway protocol (IGP) for routing information. Routing between two Autonomous Systems is handled by the Exterior Gateway Protocols like BGP.

B-RAS

Broadband Remote Access Server. A B-RAS is a server that facilitates and converges traffic from multiple Internet traffic resources such as cable, DSL, Ethernet, or Broadband wireless.

band

Band refers to a specified range of frequencies of electromagnetic radiation.

BGP

Border Gateway Protocol. BGP is a routing protocol for exchanging data and information between different host gateways or autonomous systems on the Internet.

BLE

Bluetooth Low Energy. The BLE functionality is offered by Bluetooth® to enable devices to run for long durations with low power consumption.

BMC

Beacon Management Console. BMC manages and monitors beacons from the BLE devices. The BLE devices are used for location tracking and proximity detection.

BPDU

Bridge Protocol Data Unit. A BPDU is a data message transmitted across a local area network to detect loops in network topologies.

BRE

Basic Regular Expression. The BRE syntax standards designed by the IEEE provides extension to the traditional Simple Regular Expressions syntax and allows consistency between utility programs such as grep, sed, and awk.

BSS

Basic Service Set. A BSS is a set of interconnected stations that can communicate with each other. BSS can be an independent BSS or infrastructure BSS. An independent BSS is an ad hoc network that does not include APs, whereas the infrastructure BSS consists of an AP and all its associated clients.

BSSID

Basic Service Set Identifier. The BSSID identifies a particular BSS within an area. In infrastructure BSS networks, the BSSID is the MAC address of the AP. In independent BSS or ad hoc networks, the BSSID is generated randomly.

BYOD

Bring Your Own Device. BYOD refers to the use of personal mobile devices within an enterprise network infrastructure.

CA

Certificate Authority or Certification Authority. Entity in a public key infrastructure system that issues certificates to clients. A certificate signing request received by the CA is converted into a certificate when the CA adds a signature generated with a private key. See digital certificate.

CAC

Call Admission Control. CAC regulates traffic volume in voice communications. CAC can also be used to ensure or maintain a certain level of audio quality in voice communications networks.

CALEA

Communications Assistance for Law Enforcement Act. To comply with the CALEA specifications and to allow lawful interception of Internet traffic by the law enforcement and intelligence agencies, the telecommunications carriers and manufacturers of telecommunications equipment are required to modify and design their equipment, facilities, and services to ensure that they have built-in surveillance capabilities.

Campus AP

Campus APs are used in private networks where APs connect over private links (LAN, WLAN, WAN or MPLS) and terminate directly on controllers. Campus APs are deployed as part of the indoor campus solution in enterprise office buildings, warehouses, hospitals, universities, and so on.

captive portal

A 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.

CCA

Clear Channel Assessment. In wireless networks, the CCA method detects if a channel is occupied or clear, and determines if the channel is available for data transmission.

CDP

Cisco Discovery Protocol. CDP is a proprietary Data Link Layer protocol developed by Cisco Systems. CDP runs on Cisco devices and enables networking applications to learn about the neighboring devices directly connected to the network.

CDR

Call Detail Record. A CDR contains the details of a telephone or VoIP call, such as the origin and destination addresses of the call, the start time and end time of the call, any toll charges that were added through the network or charges for operator services, and so on.

CEF

Common Event Format. The CEF is a standard for the interoperability of event or log-generating devices and applications. The standard syntax for CEF includes a prefix and a variable extension formatted as key-value pairs.

CGI

Common Gateway Interface. CGI is a standard protocol for exchanging data between the web servers and executable programs running on a server to dynamically process web pages.

CHAP

Challenge Handshake Authentication Protocol. CHAP is an authentication scheme used by PPP servers to validate the identity of remote clients.

CIDR

Classless Inter-Domain Routing. CIDR is an IP standard for creating and allocating unique identifiers for networks and devices. The CIDR IP addressing scheme is used as a replacement for the older IP addressing scheme based on classes A, B, and C. With CIDR, a single IP address can be used to designate many unique IP addresses. A CIDR IP address ends with a slash followed by the IP network prefix, for example, 192.0.2.0/24.

ClearPass

ClearPass is an access management system for creating and enforcing policies across a network to all devices and applications. The ClearPass integrated platform includes applications such as Policy Manager, Guest, Onboard, OnGuard, Insight, Profile, QuickConnect, and so on.

ClearPass Guest

ClearPass Guest is a configurable ClearPass application for secure visitor network access management.

ClearPass Policy Manager

ClearPass Policy Manager is a baseline platform for policy management, AAA, profiling, network access control, and reporting. With ClearPass Policy Manager, the network administrators can configure and manage secure network access that accommodates requirements across multiple locations and multivendor networks, regardless of device ownership and connection method.

CN

Common Name. CN is the primary name used to identify a certificate.

CNA

Captive Network Assistant. CNA is a popup page shown when joining a network that has a captive portal.

CoA

Change of Authorization. The RADIUS CoA is used in the AAA service framework to allow dynamic modification of the authenticated, authorized, and active subscriber sessions.

CoS

Class of Service. CoS is used in data and voice protocols for classifying packets into different types of traffic (voice, video, or data) and setting a service priority. For example, voice traffic can be assigned a higher priority over email or HTTP traffic.

CPE

Customer Premises Equipment. It refers to any terminal or equipment located at the customer premises.

CPsec

Control Plane Security. CPsec is a secure form of communication between a controller and APs to protect the control plane communications. This is performed by means of using public-key self-signed certificates created by each master controller.

CPU

Central Processing Unit. A CPU is an electronic circuitry in a computer for processing instructions.

CRC

Cyclic Redundancy Check. CRC is a data verification method for detecting errors in digital data during transmission, storage, or retrieval.

CRL

Certificate Revocation List. CRL is a list of revoked certificates maintained by a certification authority.

cryptobinding

Short for cryptographic binding. A procedure in a tunneled EAP method that binds together the tunnel protocol and the tunneled authentication methods, ensuring the relationship between a collection of data assets. Cryptographic binding focuses on protecting the server; mutual cryptographic binding protects both peer and server.

CSA

Channel Switch Announcement. The CSA element enables an AP to advertise that it is switching to a new channel before it begins transmitting on that channel. This allows the clients, which support CSA, to transition to the new channel with minimal downtime.

CSMA/CA

Carrier Sense Multiple Access / Collision Avoidance. CSMA/CA is a protocol for carrier transmission in networks using the 802.11 standard. CSMA/CA aims to prevent collisions by listening to the broadcasting nodes, and informing devices not to transmit any data until the broadcasting channel is free.

CSR

Certificate Signing Request. In PKI systems, a CSR is a message sent from an applicant to a CA to apply for a digital identity certificate.

CSV

Comma-Separated Values. A file format that stores tabular data in the plain text format separated by commas.

CTS

Clear to Send. The CTS refers to the data transmission and protection mechanism used by the 802.11 wireless networking protocol to prevent frame collision occurrences. See RTS.

CW

Contention Window. In QoS, CW refers to a window set for access categories based on the type of traffic. Based on the type and volume of the traffic, the minimum and maximum values can be calculated to provide a wider window when necessary.

DAI

Dynamic ARP inspection. A security feature that validates ARP packets in a network.

DAS

Distributed Antenna System. DAS is a network of antenna nodes strategically placed around a geographical area or structure for additional cellular coverage.

dB

Decibel. Unit of measure for sound or noise and is the difference or ratio between two signal levels.

dBm

Decibel-Milliwatts. dBm is a logarithmic measurement (integer) that is typically used in place of mW to represent receive-power level. AMP normalizes all signals to dBm, so that it is easy to evaluate performance between various vendors.

DCB

Data Center Bridging. DCB is a collection of standards developed by IEEE for creating a converged data center network using Ethernet.

DCE

Data Communication Equipment. DCE refers to the devices that establish, maintain, and terminate communication network sessions between a data source and its destination.

DCF

Distributed Coordination Function. DCF is a protocol that uses carrier sensing along with a four-way handshake to maximize the throughput while preventing packet collisions.

DDMO

Distributed Dynamic Multicast Optimization. DDMO is similar to Dynamic Multicast Optimization (DMO) where the multicast streams are converted into unicast streams on the AP instead of the controller, to enhance the quality and reliability of streaming videos, while preserving the bandwidth available to non-video clients.

DES

Data Encryption Standard. DES is a common standard for data encryption and a form of secret key cryptography, which uses only one key for encryption and decryption.

designated router

Designated router refers to a router interface that is elected to originate network link advertisements for networks using the OSPF protocol.

destination NAT

Destination Network Address Translation. Destination NAT is a process of translating the destination IP address of an end route packet in a network. Destination NAT is used for redirecting the traffic destined to a virtual host to the real host, where the virtual host is identified by the destination IP address and the real host is identified by the translated IP address.

DFS

Dynamic Frequency Selection. DFS is a mandate for radio systems operating in the 5 GHz band to be equipped with means to identify and avoid interference with Radar systems.

DFT

Discrete Fourier Transform. DFT converts discrete-time data sets into a discrete-frequency representation. See FFT.

DHCP

Dynamic Host Configuration Protocol. A network protocol that enables a server to automatically assign an IP address to an IP-enabled device from a defined range of numbers configured for a given network.

DHCP snooping

DHCP snooping enables the switch to monitor and control DHCP messages received from untrusted devices that are connected to the switch.

digital certificate

A digital certificate is an electronic document that uses a digital signature to bind a public key with an identity—information such as the name of a person or an organization, address, and so forth.

Digital wireless pulse

A wireless technology for transmitting large amounts of digital data over a wide spectrum of frequency bands with very low power for a short distance. Ultra Wideband radio can carry a huge amount of data over a distance up to 230 ft at very low power (less than 0.5 mW), and has the ability to carry signals through doors and other obstacles that tend to reflect signals at more limited bandwidths and a higher power.

Disconnect-Ack

Disconnect-Ack is a NAS response packet to a Disconnect-Request, which indicates that the session was disconnected.

Disconnect-Nak

Disconnect-Nak is NAS response packet to a Disconnect-Request, which indicates that the session was not disconnected.

Disconnect-Request

Disconnect-Request is a RADIUS packet type sent to a NAS requesting that a user or session be disconnected.

distribution certificate

Distribution certificate is used for digitally signing iOS mobile apps to enable enterprise app distribution. It verifies the identity of the app publisher.

DLNA

Digital Living Network Alliance. DLNA is a set of interoperability guidelines for sharing digital media among multimedia devices.

DMO

Dynamic Multicast Optimization. DMO is a process of converting multicast streams into unicast streams over a wireless link to enhance the quality and reliability of streaming videos, while preserving the bandwidth available to non-video clients.

DN

Distinguished Name. A series of fields in a digital certificate that, taken together, constitute the unique identity of the person or device that owns the digital certificate. Common fields in a DN include country, state, locality, organization, organizational unit, and the “common name”, which is the primary name used to identify the certificate.

DNS

Domain Name System. A DNS server functions as a phone book for the intranet and Internet users. It converts human-readable computer host names into IP addresses and IP addresses into host names. It stores several records for a domain name such as an address 'A' record, name server (NS), and mail exchanger (MX) records. The Address 'A' record is the most important record that is stored in a DNS server, because it provides the required IP address for a network peripheral or element.

DOCSIS

Data over Cable Service Interface Specification. A telecommunication standard for Internet access through cable modem.

DoS

Denial of Service. DoS is any type of attack where the attackers send excessive messages to flood traffic and thereby preventing the legitimate users from accessing the service.

DPD

Dead Peer Detection. A method used by the network devices to detect the availability of the peer devices.

DPI

Deep Packet Inspection. DPI is an advanced method of network packet filtering that is used for inspecting data packets exchanged between the devices and systems over a network. DPI functions at the Application layer of the Open Systems Interconnection (OSI) reference model and enables users to identify, categorize, track, reroute, or stop packets passing through a network.

DRT

Downloadable Regulatory Table. The DRT feature allows new regulatory approvals to be distributed for APs without a software upgrade or patch.

DS

Differentiated Services. The DS specification aims to provide uninterrupted quality of service by managing and controlling the network traffic, so that certain types of traffic get precedence.

DSCP

Differentiated Services Code Point. DSCP is a 6-bit packet header value used for traffic classification and priority assignment.

DSL

Digital Subscriber Line. The DSL technology allows the transmission of digital data over telephone lines. A DSL modem is a device used for connecting a computer or router to a telephone line that offers connectivity to the Internet.

DSSS

Direct-Sequence Spread Spectrum. DSSS is a modulation technique used for reducing overall signal interference. This technique multiplies the original data signal with a pseudo random noise spreading code. Spreading of this signal makes the resulting wideband channel more noisy, thereby increasing the resistance to interference. See FHSS.

DST

Daylight Saving Time. DST is also known as summer time that refers to the practice of advancing clocks, so that evenings have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring and are adjusted backward in autumn.

DTE

Data Terminal Equipment. DTE refers to a device that converts user information into signals or re-converts the received signals.

DTIM

Delivery Traffic Indication Message. DTIM is a kind of traffic indication map. A DTIM interval determines when the APs must deliver broadcast and multicast frames to their associated clients in power save mode.

DTLS

Datagram Transport Layer Security. DTLS communications protocol provides communications security for datagram protocols.

dynamic authorization

Dynamic authorization refers to the ability to make changes to a visitor account's session while it is in progress. This might include disconnecting a session or updating some aspect of the authorization for the session.

dynamic NAT

Dynamic Network Address Translation. Dynamic NAT maps multiple public IP addresses and uses these addresses with an internal or private IP address. Dynamic NAT helps to secure a network by masking the internal configuration of a private network.

EAP

Extensible Authentication Protocol. An authentication protocol for wireless networks that extends the methods used by the PPP, a protocol often used when connecting a computer to the Internet. EAP can support multiple authentication mechanisms, such as token cards, smart cards, certificates, one-time passwords, and public key encryption authentication.

EAP-FAST

EAP – Flexible Authentication Secure Tunnel (tunneled).

EAP-GTC

EAP – Generic Token Card. (non-tunneled).

EAP-MD5

EAP – Method Digest 5. (non-tunneled).

EAP-MSCHAP

EAP Microsoft Challenge Handshake Authentication Protocol.

EAP-MSCHAPv2

EAP Microsoft Challenge Handshake Authentication Protocol Version 2.

EAP-PEAP

EAP–Protected EAP. A widely used protocol for securely transporting authentication data across a network (tunneled).

EAP-PWD

EAP-Password. EAP-PWD is an EAP method that uses a shared password for authentication.

EAP-TLS

EAP–Transport Layer Security. EAP-TLS is a certificate-based authentication method supporting mutual authentication, integrity-protected ciphersuite negotiation and key exchange between two endpoints. See RFC 5216.

EAP-TTLS

EAP–Tunneled Transport Layer Security. EAP-TTLS is an EAP method that encapsulates a TLS session, consisting of a handshake phase and a data phase. See RFC 5281.

EAPoL

Extensible Authentication Protocol over LAN. A network port authentication protocol used in IEEE 802.1X standards to provide a generic network sign-on to access network resources.

ECC

Elliptical Curve Cryptography or Error correcting Code memory. Elliptical Curve Cryptography is a public-key encryption technique that is based on elliptic curve theory used for creating faster, smaller, and more efficient cryptographic keys. Error Correcting Code memory is a type of computer data storage that can detect and correct the most common kinds of internal data corruption. ECC memory is used in most computers where data corruption cannot be tolerated under any circumstances, such as for scientific or financial computing.

ECDSA

Elliptic Curve Digital Signature Algorithm. ECDSA is a cryptographic algorithm that supports the use of public or private key pairs for encrypting and decrypting information.

EDCA

Enhanced Distributed Channel Access. The EDCA function in the IEEE 802.11e Quality of Service standard supports differentiated and distributed access to wireless medium based on traffic priority and Access Category types. See WMM and WME.

EIGRP

Enhanced Interior Gateway Routing Protocol. EIGRP is a routing protocol used for automating routing decisions and configuration in a network.

EIRP

Effective Isotropic Radiated Power or Equivalent Isotropic Radiated Power. EIRP refers to the output power generated when a signal is concentrated into a smaller area by the Antenna.

ESI

External Services Interface. ESI provides an open interface for integrating security solutions that solve interior network problems such as viruses, worms, spyware, and corporate compliance.

ESS

Extended Service Set. An ESS is a set of one or more interconnected BSSs that form a single sub network.

ESSID

Extended Service Set Identifier. ESSID refers to the ID used for identifying an extended service set.

Ethernet

Ethernet is a network protocol for data transmission over LAN.

EULA

End User License Agreement. EULA is a legal contract between a software application publisher or author and the users of the application.

FCC

Federal Communications Commission. FCC is a regulatory body that defines standards for the interstate and international communications by radio, television, wire, satellite, and cable.

FFT

Fast Fourier Transform. FFT is a frequency analysis mechanism that aims at faster conversion of a discrete signal in time domain into a discrete frequency domain representation. See also DFT.

FHSS

Frequency Hopping Spread Spectrum. FHSS is transmission technique that allows modulation and transmission of a data signal by rapidly switching a carrier among many frequency channels in a random but predictable sequence. See also DSSS.

FIB

Forwarding Information Base. FIB is a forwarding table that maps MAC addresses to ports. FIB is used in network bridging, routing, and similar functions to identify the appropriate interface for forwarding packets.

FIPS

Federal Information Processing Standards. FIPS refers to a set of standards that describe document processing, encryption algorithms, and other information technology standards for use within non-military government agencies, and by government contractors and vendors who work with these agencies.

firewall

Firewall is a network security system used for preventing unauthorized access to or from a private network.

FQDN

Fully Qualified Domain Name. FQDN is a complete domain name that identifies a computer or host on the Internet.

FQLN

Fully Qualified Location Name. FQLN is a device location identifier in the format: APname.Floor.Building.Campus.

frequency allocation

Use of radio frequency spectrum as regulated by governments.

FSPL

Free Space Path Loss. FSPL refers to the loss in signal strength of an electromagnetic wave that would result from a line-of-sight path through free space (usually air), with no obstacles nearby to cause reflection or

diffraction.

FTP

File Transfer Protocol. A standard network protocol used for transferring files between a client and server on a computer network.

GARP

Generic Attribute Registration Protocol. GVRP is a LAN protocol that allows the network nodes to register and de-register attributes, such as network addresses, with each other.

GAS

Generic Advertisement Service. GAS is a request-response protocol, which provides Layer 2 transport mechanism between a wireless client and a server in the network prior to authentication. It helps in determining a wireless network infrastructure before associating clients, and allows clients to send queries to multiple 802.11 networks in parallel.

Gbps

Gigabits per second.

GBps

Gigabytes per second.

GET

GET refers HTTP request method or an SNMP operation method. The GET HTTP request method submits data to be processed to a specified resource. The GET SNMP operation method obtains information from the Management Information Base (MIB).

GHz

Gigahertz.

GMT

Greenwich Mean Time. GMT refers to the mean solar time at the Royal Observatory in Greenwich, London. GMT is the same as Coordinated Universal Time (UTC) standard, written as an offset of UTC +/- 00:00.

goodput

Goodput is the application level throughput that refers to the ratio of the total bytes transmitted or received in the network to the total air time required for transmitting or receiving the bytes.

GPS

Global Positioning System. A satellite-based global navigation system.

GRE

Generic Routing Encapsulation. GRE is an IP encapsulation protocol that is used to transport packets over a network.

GTC

Generic Token Card. GTC is a protocol that can be used as an alternative to MSCHAPv2 protocol. GTC allows authentication to various authentication databases even in cases where MSCHAPv2 is not supported by the database.

GVRP

GARP VLAN Registration Protocol or Generic VLAN Registration Protocol. GARP is an IEEE 802.1Q-compliant protocol that facilitates VLAN registration and controls VLANs within a larger network.

H2QP

Hotspot 2.0 Query Protocol.

hot zone

Wireless access area created by multiple hotspots that are located in close proximity to one another. Hot zones usually combine public safety APs with public hotspots.

hotspot

Hotspot refers to a WLAN node that provides Internet connection and virtual private network (VPN) access from a given location. A business traveler, for example, with a laptop equipped for Wi-Fi can look up a local hotspot, contact it, and get connected through its network to reach the Internet.

HSPA

High-Speed Packet Access.

HT

High Throughput. IEEE 802.11n is an HT WLAN standard that aims to achieve physical data rates of close to 600 Mbps on the 2.4 GHz and 5 GHz bands.

HTTP

Hypertext Transfer Protocol. The HTTP is an application protocol to transfer data over the web. The HTTP protocol defines how messages are formatted and transmitted, and the actions that the w servers and browsers should take in response to various commands.

HTTPS

Hypertext Transfer Protocol Secure. HTTPS is a variant of the HTTP that adds a layer of security on the data in transit through a secure socket layer or transport layer security protocol connection.

IAS

Internet Authentication Service. IAS is a component of Windows Server operating systems that provides centralized user authentication, authorization, and accounting.

ICMP

Internet Control Message Protocol. ICMP is an error reporting protocol. It is used by network devices such as routers, to send error messages and operational information to the source IP address when network problems prevent delivery of IP packets.

IDS

Intrusion Detection System. IDS monitors a network or systems for malicious activity or policy violations and reports its findings to the management system deployed in the network.

IEEE

Institute of Electrical and Electronics Engineers.

IGMP

Internet Group Management Protocol. Communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships.

IGMP snooping

IGMP snooping prevents multicast flooding on Layer 2 network by treating multicast traffic as broadcast traffic. Without IGMP snooping, all streams could be flooded to all ports on that VLAN. When multicast flooding occurs, end-hosts that happen to be in the same VLAN would receive all the streams only to be discarded without snooping.

IGP

Interior Gateway Protocol. IGP is used for exchanging routing information between gateways within an autonomous system (for example, a system of corporate local area networks).

IGRP

Interior Gateway Routing Protocol. IGRP is a distance vector interior routing protocol used by routers to exchange routing data within an autonomous system.

IKE

Internet Key Exchange. IKE is a key management protocol used with IPsec protocol to establish a secure communication channel. IKE provides additional feature, flexibility, and ease of configuration for IPsec standard.

IKEv1

Internet Key Exchange version 1. IKEv1 establishes a secure authenticated communication channel by using either the pre-shared key (shared secret), digital signatures, or public key encryption. IKEv1 operates in Main and Aggressive modes. See RFC 2409.

IKEv2

Internet Key Exchange version 2. IKEv2 uses the secure channel established in Phase 1 to negotiate Security Associations on behalf of services such as IPsec. IKEv2 uses pre-shared key and Digital Signature for authentication. See RFC 4306.

IoT

Internet of Things. IoT refers to the internetworking of devices that are embedded with electronics, software, sensors, and network connectivity features allowing data exchange over the Internet.

IPM

Intelligent Power Monitoring. IPM is a feature supported on certain APs that actively measures the power utilization of an AP and dynamically adapts to the power resources.

IPS

Intrusion Prevention System. The IPS monitors a network for malicious activities such as security threats or policy violations. The main function of an IPS is to identify suspicious activity, log the information, attempt to block the activity, and report it.

IPsec

Internet Protocol security. IPsec is a protocol suite for secure IP communications that authenticates and encrypts each IP packet in a communication session.

IPSG

Internet Protocol Source Guard. IPSG restricts IP address from untrusted interface by filtering traffic based on list of addresses in the DHCP binding database or manually configured IP source bindings. It prevents IP spoofing attacks.

IrDA

An industry-sponsored organization set up in 1993 to create international standards for the hardware and software used in infrared communication links. In this special form of radio transmission, a focused ray of light in the infrared frequency spectrum, measured in terahertz (THz), or trillions of hertz (cycles per second), is modulated with information and sent from a transmitter to a receiver over a relatively short distance.

ISAKMP

Internet Security Association and Key Management Protocol. ISAKMP is used for establishing Security Associations and cryptographic keys in an Internet environment.

ISP

Internet Service Provider. An ISP is an organization that provides services for accessing and using the Internet.

JSON

JavaScript Object Notation. JSON is an open-standard, language-independent, lightweight data-interchange format used to transmit data objects consisting of attribute–value pairs. JSON uses a "self-describing" text format that is easy for humans to read and write, and that can be used as a data format by any programming language.

Kbps

Kilobits per second.

KBps

Kilobytes per second.

keepalive

Signal sent at periodic intervals from one device to another to verify that the link between the two devices is working. If no reply is received, data will be sent by a different path until the link is restored. A keepalive can also be used to indicate that the connection should be preserved so that the receiving device does not consider it timed out and drop it.

L2TP

Layer-2 Tunneling Protocol. L2TP is a networking protocol used by the ISPs to enable VPN operations.

LACP

Link Aggregation Control Protocol. LACP is used for the collective handling of multiple physical ports that can be seen as a single channel for network traffic purposes.

LAG

Link Aggregation Group . A LAG combines a number of physical ports together to make a single high-bandwidth data path. LAGs can connect two switches to provide a higher-bandwidth connection to a public network.

LAN

Local Area Network. A LAN is a network of connected devices within a distinct geographic area such as an office or a commercial establishment and share a common communications line or wireless link to a server.

LCD

Liquid Crystal Display. LCD is the technology used for displays in notebook and other smaller computers. Like LED and gas-plasma technologies, LCDs allow displays to be much thinner than the cathode ray tube technology.

LDAP

Lightweight Directory Access Protocol. LDAP is a communication protocol that provides the ability to access and maintain distributed directory information services over a network.

LDPC

Low-Density Parity-Check. LDPC is a method of transmitting a message over a noisy transmission channel using a linear error correcting code. An LDPC is constructed using a sparse bipartite graph.

LEAP

Lightweight Extensible Authentication Protocol. LEAP is a Cisco proprietary version of EAP used in wireless networks and Point-to-Point connections.

LED

Light Emitting Diode. LED is a semiconductor light source that emits light when an electric current passes through it.

LEEF

Log Event Extended Format. LEEF is a type of customizable syslog event format. An extended log file contains a sequence of lines containing ASCII characters terminated by either the sequence LF or CRLF.

LI

Lawful Interception. LI refers to the procedure of obtaining communications network data by the Law Enforcement Agencies for the purpose of analysis or evidence.

LLDP

Link Layer Discovery Protocol. LLDP is a vendor-neutral link layer protocol in the Internet Protocol suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, which is principally a wired Ethernet.

LLDP-MED

LLDP–Media Endpoint Discovery. LLDP-MED facilitates information sharing between endpoints and network infrastructure devices.

LMS

Local Management Switch. In multi-controller networks, each controller acts as an LMS and terminates user traffic from the APs, processes, and forwards the traffic to the wired network.

LNS

L2TP Network Server. LNS is an equipment that connects to a carrier and handles the sessions from broadband lines. It is also used for dial-up and mobile links. LNS handles authentication and routing of the IP addresses. It also handles the negotiation of the link with the equipment and establishes a session.

LTE

Long Term Evolution. LTE is a 4G wireless communication standard that provides high-speed wireless communication for mobile phones and data terminals. See 4G.

MAB

MAC Authentication Bypass. Endpoints such as network printers, Ethernet-based sensors, cameras, and wireless phones do not support 802.1X authentication. For such endpoints, MAC Authentication Bypass mechanism is used. In this method, the MAC address of the endpoint is used to authenticate the endpoint.

MAC

Media Access Control. A MAC address is a unique identifier assigned to network interfaces for communications on a network.

MAM

Mobile Application Management. MAM refers to software and services used to secure, manage, and distribute mobile applications used in enterprise settings on mobile devices like smartphones and tablet computers. Mobile Application Management can apply to company-owned mobile devices as well as BYOD.

Mbps

Megabits per second

MBps

Megabytes per second

MCS

Modulation and Coding Scheme. MCS is used as a parameter to determine the data rate of a wireless connection for high throughput.

MD4

Message Digest 4. MD4 is an earlier version of MD5 and is an algorithm used to verify data integrity through the creation of a 128-bit message digest from data input.

MD5

Message Digest 5. The MD5 algorithm is a widely used hash function producing a 128-bit hash value from the data input.

MDAC

Microsoft Data Access Components. MDAC is a framework of interrelated Microsoft technologies that provides a standard database for Windows OS.

MDM

Mobile Device Management. MDM is an administrative software to manage, monitor, and secure mobile devices of the employees in a network.

mDNS

Multicast Domain Name System. mDNS provides the ability to perform DNS-like operations on the local link in the absence of any conventional unicast DNS server. The mDNS protocol uses IP multicast User Datagram Protocol (UDP) packets, and is implemented by the Apple Bonjour and Linux NSS-mDNS services. mDNS works in conjunction with DNS Service Discovery (DNS-SD), a companion zero-configuration technique specified. See RFC 6763.

MFA

Multi-factor Authentication. MFA lets you require multiple factors, or proofs of identity, when authenticating a user. Policy configurations define how often multi-factor authentication will be required, or conditions that will trigger it.

MHz

Megahertz

MIB

Management Information Base. A hierarchical database used by SNMP to manage the devices being monitored.

microwave

Electromagnetic energy with a frequency higher than 1 GHz, corresponding to wavelength shorter than 30 centimeters.

MIMO

Multiple Input Multiple Output. An antenna technology for wireless communications in which multiple antennas are used at both source (transmitter) and destination (receiver). The antennas at each end of the communications circuit are combined to minimize errors and optimize data speed.

MISO

Multiple Input Single Output. An antenna technology for wireless communications in which multiple antennas are used at the source (transmitter). The antennas are combined to minimize errors and optimize

data speed. The destination (receiver) has only one antenna.

MLD

Multicast Listener Discovery. A component of the IPv6 suite. It is used by IPv6 routers for discovering multicast listeners on a directly attached link.

MPDU

MAC Protocol Data Unit. MPDU is a message exchanged between MAC entities in a communication system based on the layered OSI model.

MPLS

Multiprotocol Label Switching. The MPLS protocol speeds up and shapes network traffic flows.

MPPE

Microsoft Point-to-Point Encryption. A method of encrypting data transferred across PPP-based dial-up connections or PPTP-based VPN connections.

MS-CHAP

Microsoft Challenge Handshake Authentication Protocol. MS-CHAP is Password-based, challenge-response, mutual authentication protocol that uses MD4 and DES encryption.

MS-CHAPv1

Microsoft Challenge Handshake Authentication Protocol version 1. MS-CHAPv1 extends the user authentication functionality provided on Windows networks to remote workstations. MS-CHAPv1 supports only one-way authentication.

MS-CHAPv2

Microsoft Challenge Handshake Authentication Protocol version 2. MS-CHAPv2 is an enhanced version of the MS-CHAP protocol that supports mutual authentication.

MSS

Maximum Segment Size. MSS is a parameter of the options field in the TCP header that specifies the largest amount of data, specified in bytes, that a computer or communications device can receive in a single TCP segment.

MSSID

Mesh Service Set Identifier. MSSID is the SSID used by the client to access a wireless mesh network.

MSTP

Multiple Spanning Tree Protocol. MSTP configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each spanning tree.

MTU

Maximum Transmission Unit. MTU is the largest size packet or frame specified in octets (eight-bit bytes) that can be sent in networks such as the Internet.

MU-MIMO

Multi-User Multiple-Input Multiple-Output. MU-MIMO is a set of multiple-input and multiple-output technologies for wireless communication, in which users or wireless terminals with one or more antennas communicate with each other.

MVRP

Multiple VLAN Registration Protocol. MVRP is a Layer 2 network protocol used for automatic configuration of VLAN information on switches.

mW

milliWatts. mW is 1/1000 of a Watt. It is a linear measurement (always positive) that is generally used to represent transmission.

NAC

Network Access Control. NAC is a computer networking solution that uses a set of protocols to define and implement a policy that describes how devices can secure access to network nodes when they initially attempt to connect to a network.

NAD

Network Access Device. NAD is a device that automatically connects the user to the preferred network, for example, an AP or an Ethernet switch.

NAK

Negative Acknowledgement. NAK is a response indicating that a transmitted message was received with errors or it was corrupted, or that the receiving end is not ready to accept transmissions.

NAP

Network Access Protection. The NAP feature in the Windows Server allows network administrators to define specific levels of network access based on identity, groups, and policy compliance. The NAP Agent is a service that collects and manages health information for NAP client computers. If a client is not compliant, NAP provides a mechanism to automatically bring the client back into compliance and then dynamically increase its level of network access.

NAS

Network Access Server. NAS provides network access to users, such as a wireless AP, network switch, or dial-in terminal server.

NAT

Network Address Translation. NAT is a method of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device.

NetBIOS

Network Basic Input/Output System. A program that lets applications on different computers communicate within a LAN.

NFC

Near-Field Communication. NFC is a short-range wireless connectivity standard (ECMA-340, ISO/IEC 18092) that uses magnetic field induction to enable communication between devices when they touch or are brought closer (within a few centimeters of distance). The standard specifies a way for the devices to establish a peer-to-peer (P2P) network to exchange data.

NIC

Network Interface Card. NIC is a hardware component that allows a device to connect to the network.

Nmap

Network Mapper. Nmap is an open-source utility for network discovery and security auditing. Nmap uses IP packets to determine such things as the hosts available on a network and their services, operating systems and versions, types of packet filters/firewalls, and so on.

NMI

Non-Maskable Interrupt. NMI is a hardware interrupt that standard interrupt-masking techniques in the system cannot ignore. It typically occurs to signal attention for non-recoverable hardware errors.

NMS

Network Management System. NMS is a set of hardware and/or software tools that allow an IT professional to supervise the individual components of a network within a larger network management framework.

NOE

New Office Environment. NOE is a proprietary VoIP protocol designed by Alcatel-Lucent Enterprise.

NTP

Network Time Protocol. NTP is a protocol for synchronizing the clocks of computers over a network.

OAuth

Open Standard for Authorization. OAuth is a token-based authorization standard that allows websites or third-party applications to access user information, without exposing the user credentials.

OCSP

Online Certificate Status Protocol. OCSP is used for determining the current status of a digital certificate without requiring a CRL.

OFDM

Orthogonal Frequency Division Multiplexing. OFDM is a scheme for encoding digital data on multiple carrier frequencies.

OID

Object Identifier. An OID is an identifier used to name an object. The OIDs represent nodes or managed objects in a MIB hierarchy. The OIDs are designated by text strings and integer sequences and are formally defined as per the ASN.1 standard.

OKC

Opportunistic Key Caching. OKC is a technique available for authentication between multiple APs in a network where those APs are under common administrative control. Using OKC, a station roaming to any AP in the network will not have to complete a full authentication exchange, but will instead just perform the 4-way handshake to establish transient encryption keys.

OpenFlow

OpenFlow is an open communications interface between control plane and the forwarding layers of a network.

OpenFlow agent

OpenFlow agent. OpenFlow is a software module in Software-Defined Networking (SDN) that allows the abstraction of any legacy network element, so that it can be integrated and managed by the SDN controller. OpenFlow runs on network devices such as switches, routers, wireless controllers, and APs.

Optical wireless

Optical wireless is combined use of conventional radio frequency wireless and optical fiber for telecommunication. Long-range links are provided by using optical fibers; the links from the long-range endpoints to end users are accomplished by RF wireless or laser systems. RF wireless at Ultra High Frequencies and microwave frequencies can carry broadband signals to individual computers at substantial data speeds.

OSI

Open Systems Interconnection. OSI is a reference model that defines a framework for communication between the applications in a network.

OSPF

Open Shortest Path First. OSPF is a link-state routing protocol for IP networks. It uses a link-state routing algorithm and falls into the group of interior routing protocols that operates within a single Autonomous System (AS).

OSPFv2

Open Shortest Path First version 2. OSPFv2 is the version 2 of the link-state routing protocol, OSPF. See RFC 2328.

OUI

Organizationally Unique Identifier. Synonymous with company ID or vendor ID, an OUI is a 24-bit, globally unique assigned number, referenced by various standards. The first half of a MAC address is OUI.

OVA

Open Virtualization Archive. OVA contains a compressed installable version of a virtual machine.

OVF

Open Virtualization Format. OVF is a specification that describes an open-standard, secure, efficient, portable and extensible format for packaging and distributing software for virtual machines.

PAC

Protected Access Credential. PAC is distributed to clients for optimized network authentication. These credentials are used for establishing an authentication tunnel between the client and the authentication server.

PAP

Password Authentication Protocol. PAP validates users by password. PAP does not encrypt passwords for transmission and is thus considered insecure.

PAPI

Process Application Programming Interface. PAPI controls channels for ARM and Wireless Intrusion Detection System (WIDS) communication to the master controller. A separate PAPI control channel connects to the local controller where the SSID tunnels terminate.

PBR

Policy-based Routing. PBR provides a flexible mechanism for forwarding data packets based on polices configured by a network administrator.

PDU

Power Distribution Unit or Protocol Data Unit. Power Distribution Unit is a device that distributes electric power to the networking equipment located within a data center. Protocol Data Unit contains protocol control Information that is delivered as a unit among peer entities of a network.

PEAP

Protected Extensible Authentication Protocol. PEAP is a type of EAP communication that addresses security issues associated with clear text EAP transmissions by creating a secure channel encrypted and protected by TLS.

PEF

Policy Enforcement Firewall. PEF also known as PEFNG provides context-based controls to enforce application-layer security and prioritization. The customers using Aruba mobility controllers can avail PEF features and services by obtaining a PEF license. PEF for VPN users—Customers with PEF for VPN license can apply firewall policies to the user traffic routed to a controller through a VPN tunnel.

PEFNG

Policy Enforcement Firewall. PEF also known as PEFNG provides context-based controls to enforce application-layer security and prioritization. The customers using Aruba mobility controllers can avail PEF features and services by obtaining a PEF license. PEF for VPN users—Customers with PEF for VPN license can apply firewall policies to the user traffic routed to a controller through a VPN tunnel.

PEFV

Policy Enforcement Firewall. PEF also known as PEFNG provides context-based controls to enforce application-layer security and prioritization. The customers using Aruba mobility controllers can avail PEF features and services by obtaining a PEF license. PEF for VPN users—Customers with PEF for VPN license can apply firewall policies to the user traffic routed to a controller through a VPN tunnel.

PFS

Perfect Forward Secrecy. PFS refers to the condition in which a current session key or long-term private key does not compromise the past or subsequent keys.

PHB

Per-hop behavior. PHB is a term used in DS or MPLS. It defines the policy and priority applied to a packet when traversing a hop (such as a router) in a DiffServ network.

PIM

Protocol-Independent Multicast. PIM refers to a family of multicast routing protocols for IP networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN, or the Internet.

PIN

Personal Identification Number. PIN is a numeric password used to authenticate a user to a system.

PKCS#n

Public-key cryptography standard n. PKCS#n refers to a numbered standard related to topics in cryptography, including private keys (PKCS#1), digital certificates (PKCS#7), certificate signing requests (PKCS#10), and secure storage of keys and certificates (PKCS#12).

PKI

Public Key Infrastructure. PKI is a security technology based on digital certificates and the assurances provided by strong cryptography. See also certificate authority, digital certificate, public key, private key.

PLMN

Public Land Mobile Network. PLMS is a network established and operated by an administration or by a Recognized Operating Agency for the specific purpose of providing land mobile telecommunications services to the public.

PMK

Pairwise Master Key. PMK is a shared secret key that is generated after PSK or 802.1X authentication.

PoE

Power over Ethernet. PoE is a technology for wired Ethernet LANs to carry electric power required for the device in the data cables. The IEEE 802.3af PoE standard provides up to 15.4 W of power on each port.

PoE+

Power over Ethernet+. PoE+ is an IEEE 802.3at standard that provides 25.5W power on each port.

POST

The HTTP POST method is used for transferring data from a client (browser) to a server using the HTTP protocol. The POST method is considered a secure way of transferring data from a client as it carries the request parameter in the message body and does not append it in the URL string.

PPP

Point-to-Point Protocol. PPP is a data link (layer 2) protocol used to establish a direct connection between two nodes. It can provide connection authentication, transmission encryption, and compression.

PPPoE

Point-to-Point Protocol over Ethernet. PPPoE is a method of connecting to the Internet, typically used with DSL services, where the client connects to the DSL modem.

PPTP

Point-to-Point Tunneling Protocol. PPTP is a method for implementing virtual private networks. It uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets.

private key

The part of a public-private key pair that is always kept private. The private key encrypts the signature of a message to authenticate the sender. The private key also decrypts a message that was encrypted with the public key of the sender.

PRNG

Pseudo-Random Number Generator. PRNG is an algorithm for generating a sequence of numbers whose properties approximate the properties of sequences of random numbers.

PSK

Pre-shared key. A unique shared secret that was previously shared between two parties by using a secure channel. This is used with WPA security, which requires the owner of a network to provide a passphrase to users for network access.

PSU

Power Supply Unit. PSU is a unit that supplies power to an equipment by converting mains AC to low-voltage regulated DC power.

public key

The part of a public-private key pair that is made public. The public key encrypts a message and the message is decrypted with the private key of the recipient.

PVST

Per-VLAN Spanning Tree. PVST provides load balancing of VLANs across multiple ports resulting in optimal usage of network resources.

PVST+

Per-VLAN Spanning Tree+. PVST+ is an extension of the PVST standard that uses the 802.1Q trunking technology.

QoS

Quality of Service. It refers to the capability of a network to provide better service and performance to a specific network traffic over various technologies.

RA

Router Advertisement. The RA messages are sent by the routers in the network when the hosts send multicast router solicitation to the multicast address of all routers.

Radar

Radio Detection and Ranging. Radar is an object-detection system that uses radio waves to determine the range, angle, or velocity of objects.

RADIUS

Remote Authentication Dial-In User Service. An Industry-standard network access protocol for remote authentication. It allows authentication, authorization, and accounting of remote users who want to access network resources.

RAM

Random Access Memory.

RAPIDS

Rogue Access Point identification and Detection System. An AMP module that is designed to identify and locate wireless threats by making use of all of the information available from your existing infrastructure.

RARP

Reverse Address Resolution Protocol. RARP is a protocol used by a physical machine in a local area network for determining the IP address from the ARP table or cache of the gateway server.

Regex

Regular Expression. Regex refers to a sequence of symbols and characters defining a search pattern.

Registration Authority

Type of Certificate Authority that processes certificate requests. The Registration Authority verifies that requests are valid and comply with certificate policy, and authenticates the user's identity. The Registration Authority then forwards the request to the Certificate Authority to sign and issue the certificate.

Remote AP

Remote APs extend corporate network to the users working from home or at temporary work sites. Remote APs are deplyed at branch office sites and are connected to the central network on a WAN link.

REST

Representational State Transfer. REST is a simple and stateless architecture that the web services use for providing interoperability between computer systems on the Internet. In a RESTful web service, requests made to the URI of a resource will elicit a response that may be in XML, HTML, JSON or some other defined format.

RF

Radio Frequency. RF refers to the electromagnetic wave frequencies within a range of 3 kHz to 300 GHz, including the frequencies used for communications or Radar signals.

RFC

Request For Comments. RFC is a commonly used format for the Internet standards documentss.

RFID

Radio Frequency Identification. RFID uses radio waves to automatically identify and track the information stored on a tag attached to an object.

RIP

Routing Information Protocol. RIP prevents the routing loops by limiting the number of hops allowed in a path from source to destination.

RJ45

Registered Jack 45. RJ45 is a physical connector for network cables.

RMA

Return Merchandise Authorization. RMA is a part of the product returning process that authorizes users to return a product to the manufacturer or distributor for a refund, replacement, or repair. The customers who want to return a product within its Warranty period contact the manufacturer to initiate the product returning process. The manufacturer or the seller generates an authorization number for the RMA, which is used by the customers, when returning a product to the warehouse.

RMON

Remote Monitoring. RMON provides standard information that a network administrator can use to monitor, analyze, and troubleshoot a group of distributed LANs.

RoW

Rest of World. RoW or RW is an operating country code of a device.

RSA

Rivest, Shamir, Adleman. RSA is a cryptosystem for public-key encryption, and is widely used for securing sensitive data, particularly when being sent over an insecure network such as the Internet.

RSSI

Received Signal Strength Indicator. RSSI is a mechanism by which RF energy is measured by the circuitry on a wireless NIC (0-255). The RSSI is not standard across vendors. Each vendor determines its own RSSI scale/values.

RSTP

Rapid Spanning Tree Protocol. RSTP provides significantly faster spanning tree convergence after a topology change, introducing new convergence behaviors and bridge port roles to do this.

RTCP

RTP Control Protocol. RTCP provides out-of-band statistics and control information for an Real-Time Transport Protocol session.

RTLS

Real-Time Location Systems. RTLS automatically identifies and tracks the location of objects or people in real time, usually within a building or other contained area.

RTP

Real-Time Transport Protocol. RTP is a network protocol used for delivering audio and video over IP networks.

RTS

Request to Send. RTS refers to the data transmission and protection mechanism used by the 802.11 wireless networking protocol to prevent frame collision occurrences. See CTS.

RTSP

Real Time Streaming Protocol. RTSP is a network control protocol designed for use in entertainment and communications systems to control streaming media servers.

RVI

Routed VLAN Interface. RVI is a switch interface that forwards packets between VLANs.

RW

Rest of World. RoW or RW is an operating country code of a device.

SA

Security Association. SA is the establishment of shared security attributes between two network entities to support secure communication.

SAML

Security Assertion Markup Language. SAML is an XML-based framework for communicating user authentication, entitlement, and attribute information. SAML enables single sign-on by allowing users to authenticate at an identity provider and then access service providers without additional authentication.

SCEP

Simple Certificate Enrollment Protocol. SCEP is a protocol for requesting and managing digital certificates.

SCP

Secure Copy Protocol. SCP is a network protocol that supports file transfers between hosts on a network.

SCSI

Small Computer System Interface. SCSI refers to a set of interface standards for physical connection and data transfer between a computer and the peripheral devices such as printers, disk drives, CD-ROM, and so on.

SD-WAN

Software-Defined Wide Area Network. SD-WAN is an application for applying SDN technology to WAN connections that connect enterprise networks across disparate geographical locations.

SDN

Software-Defined Networking. SDN is an umbrella term encompassing several kinds of network technology aimed at making the network as agile and flexible as the virtualized server and storage infrastructure of the modern data center.

SDR

Server Derivation Rule. An SDR refers to a role assignment model used by the controllers running ArubaOS to assign roles and VLANs to the WLAN users based on the rules defined under a server group. The SDRs override the default authentication roles and VLANs defined in the AAA and Virtual AP profiles.

SDU

Service Data Unit. SDU is a unit of data that has been passed down from an OSI layer to a lower layer and that has not yet been encapsulated into a PDU by the lower layer.

SFP

The Small Form-factor Pluggable. SFP is a compact, hot-pluggable transceiver that is used for both telecommunication and data communications applications.

SFP+

Small Form-factor Pluggable+. SFP+ supports up to data rates up to 16 Gbps.

SFTP

Secure File Transfer Protocol. SFTP is a network protocol that allows file access, file transfer, and file management functions over a secure connection.

SHA

Secure Hash Algorithm. SHA is a family of cryptographic hash functions. The SHA algorithm includes the SHA, SHA-1, SHA-2 and SHA-3 variants.

SIM

Subscriber Identity Module. SIM is an integrated circuit that is intended to securely store the International Mobile Subscriber Identity (IMSI) number and its related key, which are used for identifying and authenticating subscribers on mobile telephony devices.

SIP

Session Initiation Protocol. SIP is used for signaling and controlling multimedia communication session such as voice and video calls.

SIRT

Security Incident Response Team. SIRT is responsible for reviewing as well as responding to computer security incident reports and activity.

SKU

Stock Keeping Unit. SKU refers to the product and service identification code for the products in the inventory.

SLAAC

Stateless Address Autoconfiguration. SLAAC provides the ability to address a host based on a network prefix that is advertised from a local network router through router advertisements.

SMB

Server Message Block or Small and Medium Business. Server Message Block operates as an application-layer network protocol mainly used for providing shared access to files, printers, serial ports, and for miscellaneous communications between the nodes on a network.

SMS

Short Message Service. SMS refers to short text messages (up to 140 characters) sent and received through mobile phones.

SMTP

Simple Mail Transfer Protocol. SMTP is an Internet standard protocol for electronic mail transmission.

SNIR

Signal-to-Noise-Plus-Interference Ratio. SNIR refers to the power of a central signal of interest divided by the sum of the interference power and the power of the background noise. SINR is defined as the power of a certain signal of interest divided by the sum of the interference power (from all the other interfering signals) and the power of some background noise.

SNMP

Simple Network Management Protocol. SNMP is a TCP/IP standard protocol for managing devices on IP networks. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

SNMPv1

Simple Network Management Protocol version 1. SNMPv1 is a widely used network management protocol.

SNMPv2

Simple Network Management Protocol version 2. SNMPv2 is an enhanced version of SNMPv1, which includes improvements in the areas of performance, security, confidentiality, and manager-to-manager communications.

SNMPv2c

Community-Based Simple Network Management Protocol version 2. SNMPv2C uses the community-based security scheme of SNMPv1 and does not include the SNMPv2 security model.

SNMPv3

Simple Network Management Protocol version 3. SNMPv3 is an enhanced version of SNMP that includes security and remote configuration features.

SNR

Signal-to-Noise Ratio. SNR is used for comparing the level of a desired signal with the level of background noise.

SNTP

Simple Network Time Protocol. SNTP is a less complex implementation of NTP. It uses the same , but does not require the storage of state over extended periods of time.

SOAP

Simple Object Access Protocol. SOAP enables communication between the applications running on different operating systems, with different technologies and programming languages. SOAP is an XML-based messaging protocol for exchanging structured information between the systems that support web services.

SoC

System on a Chip. SoC is an Integrated Circuit that integrates all components of a computer or other electronic system into a single chip.

source NAT

Source NAT changes the source address of the packets passing through the router. Source NAT is typically used when an internal (private) host initiates a session to an external (public) host.

SSH

Secure Shell. SSH is a network protocol that provides secure access to a remote device.

SSID

Service Set Identifier. SSID is a name given to a WLAN and is used by the client to access a WLAN network.

SSL

Secure Sockets Layer. SSL is a computer networking protocol for securing connections between network application clients and servers over the Internet.

SSO

Single Sign-On. SSO is an access-control property that allows the users to log in once to access multiple related, but independent applications or systems to which they have privileges. The process authenticates the user across all allowed resources during their session, eliminating additional login prompts.

STBC

Space-Time Block Coding. STBC is a technique used in wireless communications to transmit multiple copies of a data stream across a number of antennas and to exploit the various received versions of the data to improve the reliability of data transfer.

STM

Station Management. STM is a process that handles AP management and user association.

STP

Spanning Tree Protocol. STP is a network protocol that builds a logical loop-free topology for Ethernet networks.

SU-MIMO

Single-User Multiple-Input Multiple-Output. SU-MIMO allocates the full bandwidth of the AP to a single high-speed device during the allotted time slice.

subnet

Subnet is the logical division of an IP network.

SVP

SpectraLink Voice Priority. SVP is an open, straightforward QoS approach that has been adopted by most leading vendors of WLAN APs. SVP favors isochronous voice packets over asynchronous data packets when contending for the wireless medium and when transmitting packets onto the wired LAN.

SWAN

Structured Wireless-Aware Network. A technology that incorporates a Wireless Local Area Network (WLAN) into a wired Wide Area Network (WAN). SWAN technology can enable an existing wired network to serve hundreds of users, organizations, corporations, or agencies over a large geographic area. SWAN is said to be scalable, secure, and reliable.

TAC

Technical Assistance Center.

TACACS

Terminal Access Controller Access Control System. TACACS is a family of protocols that handles remote authentication and related services for network access control through a centralized server.

TACACS+

Terminal Access Controller Access Control System+. TACACS+ provides separate authentication, authorization, and accounting services. It is derived from, but not backward compatible with, TACACS.

TCP

Transmission Control Protocol. TCP is a communication protocol that defines the standards for establishing and maintaining network connection for applications to exchange data.

TCP/IP

Transmission Control Protocol/ Internet Protocol. TCP/IP is the basic communication language or protocol of the Internet.

TFTP

Trivial File Transfer Protocol. The TFTP is a software utility for transferring files from or to a remote host.

TIM

Traffic Indication Map. TIM is an information element that advertises if any associated stations have buffered unicast frames. APs periodically send the TIM within a beacon to identify the stations that are using power saving mode and the stations that have undelivered data buffered on the AP.

TKIP

Temporal Key Integrity Protocol. A part of the WPA encryption standard for wireless networks. TKIP is the next-generation Wired Equivalent Privacy (WEP) that provides per-packet key mixing to address the flaws encountered in the WEP standard.

TLS

Transport Layer Security. TLS is a cryptographic protocol that provides communication security over the Internet. TLS encrypts the segments of network connections above the Transport Layer by using

asymmetric cryptography for key exchange, symmetric encryption for privacy, and message authentication codes for message integrity.

TLV

Type-length-value or Tag-Length-Value. TLV is an encoding format. It refers to the type of data being processed, the length of the value, and the value for the type of data being processed.

ToS

Type of Service. The ToS field is part of the IPv4 header, which specifies datagrams priority and requests a route for low-delay, high-throughput, or a highly reliable service.

TPC

Transmit Power Control. TPC is a part of the 802.11h amendment. It is used to regulate the power levels used by 802.11a radio cards.

TPM

Trusted Platform Module. TPM is an international standard for a secure cryptoprocessor, which is a dedicated microcontroller designed to secure hardware by integrating cryptographic keys into devices.

TSF

Timing Synchronization Function. TSF is a WLAN function that is used for synchronizing the timers for all the stations in a BSS.

TSPEC

Traffic Specification. TSPEC allows an 802.11e client or a QoS-capable wireless client to signal its traffic requirements to the AP.

TSV

Tab-Separated Values. TSV is a file format that allows the exchange of tabular data between applications that use different internal data formats.

TTL

Time to Live. TTL or hop limit is a mechanism that sets limits for data expiry in a computer or network.

TTY

TeleTypeWriter. TTY-enabled devices allow telephones to transmit text communications for people who are deaf or hard of hearing as well as transmit voice communication.

TXOP

Transmission Opportunity. TXOP is used in wireless networks supporting the IEEE 802.11e Quality of Service (QoS) standard. Used in both EDCA and HCF Controlled Channel Access modes of operation, TXOP is a bounded time interval in which stations supporting QoS are permitted to transfer a series of frames. TXOP is defined by a start time and a maximum duration.

U-APSD

Unscheduled Automatic Power Save Delivery. U-APSD is a part of 802.11e and helps considerably in increasing the battery life of VoWLAN terminals.

UAM

Universal Access Method. UAM allows subscribers to access a wireless network after they successfully log in from a web browser.

UCC

Unified Communications and Collaboration. UCC is a term used to describe the integration of various communications methods with collaboration tools such as virtual whiteboards, real-time audio and video conferencing, and enhanced call control capabilities.

UDID

Unique Device Identifier. UDID is used to identify an iOS device.

UDP

User Datagram Protocol. UDP is a part of the TCP/IP family of protocols used for data transfer. UDP is typically used for streaming media. UDP is a stateless protocol, which means it does not acknowledge that the packets being sent have been received.

UDR

User Derivation Rule. UDR is a role assignment model used by the controllers running ArubaOS to assign roles and VLANs to the WLAN users based on MAC address, BSSID, DHCP-Option, encryption type, SSID, and the location of a user. For example, for an SSID with captive portal in the initial role, a UDR can be configured for scanners to provide a role based on their MAC OUI.

UHF

Ultra high frequency. UHF refers to radio frequencies between the range of 300 MHz and 3 GHz. UHF is also known as the decimeter band as the wavelengths range from one meter to one decimeter.

UMTS

Universal Mobile Telecommunication System. UMTS is a third generation mobile cellular system for networks. See 3G.

UPnP

Universal Plug and Play. UPnp is a set of networking protocols that permits networked devices, such as personal computers, printers, Internet gateways, Wi-Fi APs, and mobile devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing, communications, and entertainment.

URI

Uniform Resource Identifier. URI identifies the name and the location of a resource in a uniform format.

URL

Uniform Resource Locator. URL is a global address used for locating web resources on the Internet.

USB

Universal Serial Bus. USB is a connection standard that offers a common interface for communication between the external devices and a computer. USB is the most common port used in the client devices.

UTC

Coordinated Universal Time. UTC is the primary time standard by which the world regulates clocks and time.

UWB

Ultra-Wideband. UWB is a wireless technology for transmitting large amounts of digital data over a wide spectrum of frequency bands with very low power for a short distance.

VA

Virtual Appliance. VA is a pre-configured virtual machine image, ready to run on a hypervisor.

VBR

Virtual Beacon Report. VBR displays a report with the MAC address details and RSSI information of an AP.

VHT

Very High Throughput. IEEE 802.11ac is an emerging VHT WLAN standard that could achieve physical data rates of close to 7 Gbps for the 5 GHz band.

VIA

Virtual Intranet Access. VIA provides secure remote network connectivity for Android, Apple iOS, Mac OS X, and Windows mobile devices and laptops. It automatically scans and selects the best secure connection to the corporate network.

VLAN

Virtual Local Area Network. In computer networking, a single Layer 2 network may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them through one or more routers; such a domain is referred to as a Virtual Local Area Network, Virtual LAN, or VLAN.

VM

Virtual Machine. A VM is an emulation of a computer system. VMs are based on computer architectures and provide functionality of a physical computer.

VoIP

Voice over IP. VoIP allows transmission of voice and multimedia content over an IP network.

VoWLAN

Voice over WLAN. VoWLAN is a method of routing telephone calls for mobile users over the Internet using the technology specified in IEEE 802.11b. Routing mobile calls over the Internet makes them free, or at least much less expensive than they would be otherwise.

VPN

Virtual Private Network. VPN enables secure access to a corporate network when located remotely. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two.

VRD

Validated Reference Design. VRDs are guides that capture the best practices for a particular technology in field.

VRF

VisualRF. VRF is an AirWave Management Platform (AMP) module that provides a real-time, network-wide views of your entire Radio Frequency environment along with floor plan editing capabilities. VRF also includes overlays on client health to help diagnose issues related to clients, floor plan, or a specific location.

VRF Plan

VisualRF Plan. A stand-alone Windows client used for basic planning procedures such as adding a floor plan, provisioning APs, and generating a Bill of Materials report.

VRRP

Virtual Router Redundancy Protocol. VRRP is an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN.

VSA

Vendor-Specific Attribute. VSA is a method for communicating vendor-specific information between NASs and RADIUS servers.

VTP

VLAN Trunking Protocol. VTP is a Cisco proprietary protocol for propagating VLANs on a LAN.

W-CDMA

Wideband Code-Division Multiple Access. W-CDMA is a third-generation (3G) mobile wireless technology that promises much higher data speeds to mobile and portable wireless devices.

walled garden

Walled garden is a feature that allows blocking of unauthorized users from accessing network resources.

WAN

Wide Area Network. WAN is a telecommunications network or computer network that extends over a large geographical distance.

WASP

Wireless Application Service Provider. WASP provides a web-based access to applications and services that would otherwise have to be stored locally and makes it possible for customers to access the service from a variety of wireless devices, such as a smartphone or Personal Digital Assistant (PDA).

WAX

Wireless abstract XML. WAX is an abstract markup language and a set of tools that is designed to help wireless application development as well as portability. Its tags perform at a higher level of abstraction than that of other wireless markup languages such as HTML, HDML, WML, XSL, and more.

web service

Web services allow businesses to share and process data programmatically. Developers who want to provide integrated applications can use the API to programmatically perform actions that would otherwise require manual operation of the user interface.

WEP

Wired Equivalent Privacy. WEP is a security protocol that is specified in 802.11b and is designed to provide a WLAN with a level of security and privacy comparable to what is usually expected of a wired LAN.

WFA

Wi-Fi Alliance. WFA is a non-profit organization that promotes Wi-Fi technology and certifies Wi-Fi products if they conform to certain standards of interoperability.

Wi-Fi

Wi-Fi is a technology that allows electronic devices to connect to a WLAN network, mainly using the 2.4 GHz and 5 GHz radio bands. Wi-Fi can apply to products that use any 802.11 standard.

WIDS

Wireless Intrusion Detection System. WIDS is an application that detects the attacks on a wireless network or wireless system.

WiMAX

Worldwide Interoperability for Microwave Access. WiMAX refers to the implementation of IEEE 802.16 family of wireless networks standards set by the WiMAX forum.

WIP

Wireless Intrusion Protection. The WIP module provides wired and wireless AP detection, classification, and containment. It detects Denial of Service (DoS) and impersonation attacks, and prevents client and network intrusions.

WIPS

Wireless Intrusion Prevention System. WIPS is a dedicated security device or integrated software application that monitors the radio spectrum of WLAN network for rogue APs and other wireless threats.

WISP

Wireless Internet Service Provider. WISP allows subscribers to connect to a server at designated hotspots using a wireless connection such as Wi-Fi. This type of ISP offers broadband service and allows subscriber computers called stations, to access the Internet and the web from anywhere within the zone of coverage provided by the server antenna, usually a region with a radius of several kilometers.

WISPr

Wireless Internet Service Provider Roaming. The WISPr framework enables the client devices to roam between the wireless hotspots using different ISPs.

WLAN

Wireless Local Area Network. WLAN is a 802.11 standards-based LAN that the users access through a wireless connection.

WME

Wireless Multimedia Extension. WME is a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic QoS features to IEEE 802.11 networks. WMM prioritizes traffic according to four ACs: voice (AC_VO), video (AC_VI), best effort (AC_BE) and background (AC_BK). See WMM.

WMI

Windows Management Instrumentation. WMI consists of a set of extensions to the Windows Driver Model that provides an operating system interface through which instrumented components provide information and notification.

WMM

Wi-Fi Multimedia. WMM is also known as WME. It refers to a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic QoS features to IEEE 802.11 networks. WMM prioritizes traffic according to four ACs: voice (AC_VO), video (AC_VI), best effort (AC_BE), and background (AC_BK).

WPA

Wi-Fi Protected Access. WPA is an interoperable wireless security specification subset of the IEEE 802.11 standard. This standard provides authentication capabilities and uses TKIP for data encryption.

WPA2

Wi-Fi Protected Access 2. WPA2 is a certification program maintained by IEEE that oversees standards for security over wireless networks. WPA2 supports IEEE 802.1X/EAP authentication or PSK technology, but includes advanced encryption mechanism using CCMP that is referred to as AES.

WSDL

Web Service Description Language. WSDL is an XML-based interface definition language used to describe the functionality provided by a web service.

WSP

Wireless Service Provider. The service provider company that offers transmission services to users of wireless devices through Radio Frequency (RF) signals rather than through end-to-end wire communication.

WWW

World Wide Web.

X.509

X.509 is a standard for a public key infrastructure for managing digital certificates and public-key encryption. It is an essential part of the Transport Layer Security protocol used to secure web and email communication.

XAuth

Extended Authentication. XAuth provides a mechanism for requesting individual authentication information from the user, and a local user database or an external authentication server. It provides a method for storing the authentication information centrally in the local network.

XML

Extensible Markup Language. XML is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

XML-RPC

XML Remote Procedure Call. XML-RPC is a protocol that uses XML to encode its calls and HTTP as a transport mechanism. Developers who want to provide integrated applications can use the API to programmatically perform actions that would otherwise require manual operation of the user interface.

ZTP

Zero Touch Provisioning. ZTP is a device provisioning mechanism that allows automatic and quick provisioning of devices with a minimal or at times no manual intervention.