

Aruba Central



a Hewlett Packard
Enterprise company

Getting Started

Copyright Information

© Copyright 2018 Hewlett Packard Enterprise Development LP.

Open Source Code

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

Hewlett Packard Enterprise Company
Attn: General Counsel
3000 Hanover Street
Palo Alto, CA 94304
USA

Contents	1
About this Document	4
Intended Audience	4
Related Documents	4
Conventions	4
Contacting Support	5
About Aruba Central	6
Key Features	6
Operational Modes and Interfaces	7
Supported Devices	7
Supported Instant APs	7
Supported Switch Platforms	9
Supported SD-WAN Gateways	10
Getting Started	12
Setting up Your Accounts and Onboarding Devices	13
Signing Up for a Central Account	13
Accessing Central Portal	14
Central User Interface	14
Left Navigation Pane	15
Filter bar	18
Data Pane	19
Notifications Pane	19
Need Help Bubble	19
Onboarding Devices	19
Adding Devices	19

Quick Reference Illustration	21
Assigning Subscriptions	21
Assigning Device Subscriptions	22
Assigning Service Subscriptions to Devices	22
Assigning Gateway Subscriptions	22
Viewing Subscription Details	23
Organizing, Provisioning, and Managing Your Devices	25
Assigning Devices to Groups	25
Assigning Instant APs to Groups	25
Assigning Switches to Groups	26
Assigning SD-WAN Gateways to Groups	26
Important Points to Note	27
Assigning a SD-WAN Gateway to a Group	27
Connecting Devices to Central	27
Connecting Instant APs to Central	27
Connecting Aruba Switches to Central	28
Connecting SD-WAN Gateways to Central	28
Opening Firewall Ports for Device Communication	29
Managing Labels	30
Device Classification	30
Labels Page	31
Managing Sites	32
Overview	32
Sites Page	34
Creating a Site	34
Add Multiple Sites in Bulk	35
Assigning a Device to a Site	35
Converting Existing Labels to Sites	35
Editing a Site	36

Deleting a Site	36
Managing User Accounts and Roles	36
Role-Based Access	37
Configuring Users	38
Configuring Roles	39
Uploading Certificates	40
Uploading Certificates	40
Managing Software Images	41
Viewing Firmware Details	41
Upgrading a Device	42
Forcing Firmware Upgrade	43
Viewing Audit Trails	43
Viewing Audit Trails in the Standard Enterprise Portal	43
Troubleshooting Devices	44
Troubleshooting a Device	44
Viewing Command Output	47

This document describes how to sign up for Aruba Central subscription, manage your subscriptions, and provision devices such as Aruba Access Points and Switches.

Intended Audience

This guide is intended for customers who use Aruba Central to manage and configure devices.

Related Documents

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

- *Aruba Central User Guide*
- *Aruba Central Online Help*

Conventions

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

Table 1: *Typographical Conventions*

Type Style	Description
<i>Italics</i>	This style is used to emphasize important terms and to mark the titles of books.
<code>System items</code>	This fixed-width font depicts the following: <ul style="list-style-type: none">■ 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: sirt@arubanetworks.com

Aruba Central provides a cloud platform for managing your networks from anywhere. Using 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 6](#)
- [Supported Devices on page 7](#)

Key Features

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. 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 and wireless Infrastructure management—Offers a centralized management interface for managing wireless 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.
- Portal for Managed Service Providers—Offers an additional portal for Managed Service Providers to provision and manage their respective customer accounts. Using the Managed Service Portal, Service provider organizations can administer network infrastructure for multiple organizations in a single interface.
- 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. 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 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.
- **Managed Service mode**—Central offers the Managed Service Portal for managed service providers who need to manage multiple customer networks. With Managed Service Portal, 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.

Browser Compatibility Matrix



To view the 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 5.1.7	Windows
Safari 7 or later	Mac OS

Supported Devices

This section provides the following information:

- [Supported Instant APs](#)
- [Supported Switch Platforms](#)
- [Supported SD-WAN Gateways](#)

Supported Instant APs

This section provides the following information:

Supported Instant AP Platforms

Central supports the following Instant AP platforms:

- AP-344
- AP-345
- AP-374
- AP-375

- AP-377
- AP-318
- AP-303
- AP-303H
- AP-203H
- AP-203R/ AP-203RP
- AP-365
- AP-367
- IAP-304/305
- IAP-207
- IAP-334/335
- IAP-314/315
- IAP-324/325
- IAP-277
- IAP-228
- IAP-205H
- IAP-103
- IAP-114/115
- IAP-204
- IAP-205
- IAP-214/215
- IAP-274/275
- IAP-224/225
- RAP-3WNP
- RAP-108/109
- RAP-155/155P
- IAP-175
- IAP-134/135
- IAP-104
- IAP-105
- IAP-92/93



The minimum Instant AP version for AP-374, AP-375, AP-377, AP-318, AP-303 models of APs is Instant 8.3.0.0.

Supported Instant AP Firmware Versions

The current release of Central supports only the following Instant AP firmware versions:

- 8.3.0.1
- 8.3.0.0
- 6.5.4.8
- 6.5.4.7

- 6.5.4.6
- 6.5.4.5
- 6.5.4.4
- 6.5.4.0
- 6.5.3.7
- 6.5.3.6
- 6.5.3.5
- 6.5.3.4
- 6.5.3.0
- 6.5.2.0
- 6.5.1.5-4.3.1.7
- 6.5.1.0-4.3.1.1
- 6.5.1.0-4.3.1.0
- 6.5.0.0-4.3.0.1
- 6.5.0.0-4.3.0.0
- 6.4.4.8-4.2.4.10
- 6.4.4.8-4.2.4.5
- 6.4.4.8-4.2.4.4
- 6.4.4.6-4.2.4.0
- 6.4.4.4-4.2.3.2
- 6.4.4.4-4.2.3.1
- 6.4.4.4-4.2.3.0
- 6.4.4.3-4.2.2.0
- 6.4.3.4-4.2.1.0
- 6.4.3.1-4.2.0.3
- 6.4.2.3-4.1.2.3
- 6.4.2.0-4.1.1.9 or later



AP-204, AP-205, AP-205H, RAP-108, RAP-109, AP-103, AP-114, and AP-115 Instant APs are no longer supported from Aruba Instant 8.3.0.0 onwards.

Supported Switch Platforms



Central uses the SSL certificate by GeoTrust Certificate Authority for device termination and web services. As the SSL certificate is about to expire, Aruba is replacing it with a new certificate from another trusted Certificate Authority. During the certificate upgrade window, all devices managed by Central will be disconnected. After the upgrade, the devices reconnect to Central and resume their services with Central. However, for Aruba switches to reconnect to Central after the certificate upgrade, you must ensure that the switches are upgraded to the recommended software version listed in [Table 4](#).

[Table 4](#) and [Table 5](#) list the switch platforms, corresponding software versions supported in Central, and switch stacking details.

Table 4: 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.16.05.0008 or later	N/A
Aruba 2540 Switch Series	YC.16.03.0004 or later	YC.16.05.0007 or later	N/A
Aruba 2920 Switch Series	WB.16.03.0004 or later	WB.16.05.0007 or later	Yes Switch Software Dependency: WB.16.04.0008 or later
Aruba 2930F Switch Series	WC.16.03.0004 or later	WC.16.05.0007 or later	No
Aruba 2930M Switch Series	WC.16.04.0008 or later	WC.16.05.0007 or later	Yes Switch Software Dependency: WC.16.06.0006
Aruba 3810 Switch Series	KB.16.03.0004 or later	WC.16.05.0007 or later	No
Aruba 5400R Switch Series	KB.16.04.0008 or later	KB.16.05.0007 or later	No

Table 5: Supported Aruba Mobility Access Switch Series and Software Versions

Mobility Access Switch Series	Supported Software Versions
<ul style="list-style-type: none"> ■ 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 SD-WAN Gateways

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

Branch Gateway

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 Branch Gateway portfolio includes the following Aruba devices:

Table 6: *Supported Branch Gateways*

Platform	Supported Software Version
Aruba 7005 Mobility Controller	ArubaOS_70xx_8.1.0.0-1.0.0.0
Aruba 7008 Mobility Controller	
Aruba 7010 Mobility Controller	
Aruba 7024 Mobility Controller	
Aruba 7030 Mobility Controller	

Headend Gateway or VPN Concentrators

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.

Aruba supports the following devices as Headend Gateways for VPN aggregation and routing functions for corporate data center locations:

Table 7: *Supported Headend Gateways or VPN*

Platform	Supported Software Version
Aruba 7210 Mobility Controller	ArubaOS_72xx_8.1.0.0-1.0.0.0
Aruba 7220 Mobility Controller Aruba 7240 Mobility Controller Aruba 7240XM Mobility Controller	
Aruba 7280 Mobility Controller	
Aruba 7030 Mobility Controller	
Aruba 7010 Mobility Controller	ArubaOS_70xx_8.1.0.0-1.0.0.0
Aruba 7024 Mobility Controller	

Before getting started with Central, browse through the [key features of Aruba Central](#) and [supported devices](#).

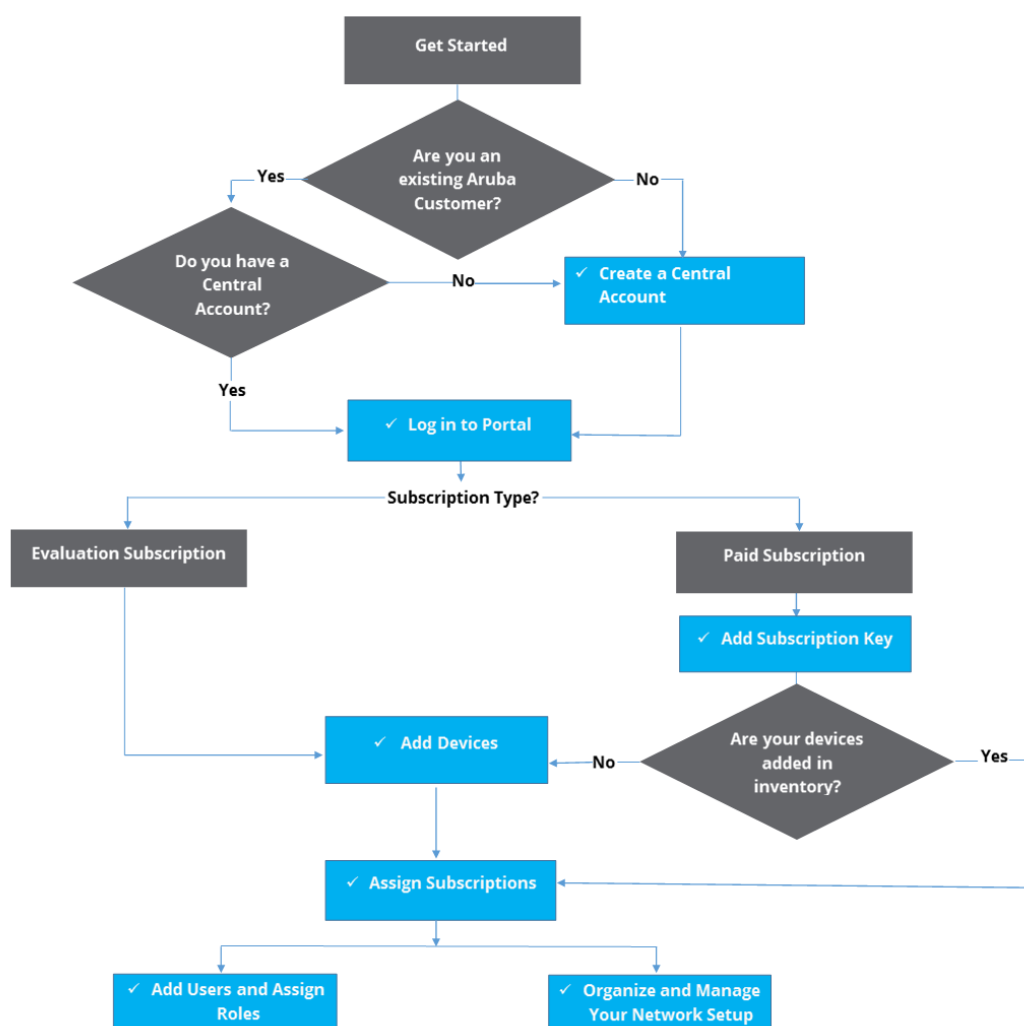
Click the steps below to navigate to the help pages that describe procedures for creating a Central account, onboarding your devices, organizing your devices, configuring, managing, and monitoring your networks.

- [Setting up Your Accounts and Onboarding Devices](#)
- [Signing Up for a Central Account](#)
- [Central User Interface](#)
- [Onboarding Devices](#)
- [Assigning Subscriptions](#)
- [Organizing, Provisioning, and Managing Your Devices](#)
- [Assigning Devices to Groups](#)
- [Connecting Devices to Central](#)
- [Opening Firewall Ports for Device Communication](#)

Setting up Your Accounts and Onboarding Devices

Get started with creating a Central account and onboard your devices. See the illustration below and follow the instructions.

Figure 1 Set up your Account and Onboard Devices



Signing Up for a Central Account

To sign up for a Central account:

1. Go to <http://www.arubanetworks.com/products/sme/eval/>.
2. Click **SIGN UP NOW**. The Registration page opens.
3. To view the Registration page and the Central UI in your preferred language, select the language.
4. Select a zone that is applicable for your region. For example, if you are in the Americas region, you could select a zone that is appropriate for you location.
5. Enter your email address and click **Continue**.
 - If you are signing up for Central for the first time, the Sign Up page is displayed. Complete the registration process (see step 3 through step 8).

- If you are a registered customer of Aruba and you have already verified your email address, the Central login page opens.
 - If your email address already exists in the Central database and you have not verified your email address, click **Resend Verification Email**, and verify your email address by clicking the **Activate Your Account** link.
 - If you are an existing Aruba customer with SSO login credentials and you are signing up for Central for the first time:
 - Validate your account by providing your SSO password. On successful authentication, the registration page is displayed. Complete the registration process to gain access to Central (see step 3 through step 8).
 - If you have forgotten your SSO password, click **Forgot Password** and complete the steps to retrieve your password.
 - To sign up again, click **Try Signing up again** and complete the steps to sign up for a Central account.
6. Enter your first name, last name, and address details. If you are a new user, enter the password. For registered users and those with SSO login credentials, the **Password** field is disabled.
7. Select the **I agree to the Terms and Conditions** check box.
8. Click **Sign Up**. If the registration is successful, a verification email is sent to your email address along with the zone details.
9. Access your email account and click the **Activate Your Account** link. After you verify your email, you can log in to Central.



Central is available as a mobile app for the iOS and Android users. You can download the mobile app from the Apple® App Store or Google® Play Store.

Accessing Central Portal

When you register for a Central account, the Central portal link will be sent to your registered email address. You can use this link to log in to Central.

You can also go to <http://portal.central.arubanetworks.com> to sign into the Central portal. To access the portal:

1. Select the zone to which your Central account is mapped. The zone that you select here shows up in the User Settings menu after you successfully log in to the portal.
2. Enter the email address and click **Continue**.
3. Enter the password and click **Continue**.

After you successfully log in to Central, a welcome message is displayed in the UI. To start using the portal for monitoring and managing your networks, ensure that the devices in the Central's inventory are assigned valid subscriptions.

Central User Interface

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

The main window consists of the following elements:

- [Left Navigation Pane on page 15](#)
- [Filter bar on page 18](#)
- [Data Pane on page 19](#)
- [Notifications Pane on page 19](#)

- [Need Help Bubble on page 19](#)

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 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 any 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 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.
 - **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 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.

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 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 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 in 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 Managed Service Portal 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.

Search bar

The search bar allows portal users to search for devices, clients, or a specific network profile. When you enter a text string in the search box, the search function suggests matching keywords and automatically completes the search text entry. The search bar is available for the following apps only:

- Monitoring & Reports
- Wireless Management
- Wired Management
- Maintenance

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 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.
- The user icon—Displays the user account details such as account name, domain, customer ID, and zone details. It also includes the following options for managing your accounts:
 - **Switch Customer**—Allows you to switch to another customer account.
 - **Change Password**—Allows you to change the password of account.
 - **User Settings**—Displays the date, time and timezone. The administrators can also set a timeout value for inactive user sessions.



The 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. 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.
- **Managed Service Mode**—Enables Managed Service Portal mode and switches the interface to the Managed Service Portal.
- **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.

Onboarding Devices

Central automatically retrieves devices associated to your account if you are a registered user with a paid subscription.

To view the devices, go to **Global Settings > Device Inventory**. If the device inventory does not show up all your devices, click **Sync Now**.

If the devices do not show up in the inventory even after the sync operation, add the devices manually.



Users with an evaluation subscription must manually add the devices to Central's device inventory.

Adding Devices

To manually add the devices, click **Global Settings > Devices Inventory**. On the Device Inventory page, use one of the following device addition options:

Table 8: Device Addition Options

Device Addition Method	Description
Add by MAC/SN	Allows you to add devices using MAC address and serial numbers. You can add up to 32 devices. NOTE: Aruba recommends that the evaluating subscribers use the MAC address and serial number based device addition option to add their devices to the inventory.
Add with Cloud Activation Key	Allows you to add multiple devices from a single purchase order. To add devices using the cloud activation key: <ol style="list-style-type: none">1. Note the Cloud Activation Key and MAC address of the device. To obtain these details, perform the following steps:<ul style="list-style-type: none">• Instant APs—Go to the Maintenance > About page of the Instant UI or execute the show about command at the Instant AP CLI.• Aruba Switches—Run the sh system in Base and sh system in Serial commands at the switch CLI console and note the MAC address and the serial number.• Mobility Access Switches—Run the show inventory include HW and show version commands on the Mobility Access Switch CLI console. You can also view the cloud activation key in the Maintenance > About tab in the switch UI. The activation key is enabled only if the switch has access to the Internet.2. Enter the Cloud Activation Key and MAC address of the device.3. Click Add. NOTE: The cloud activation key based device addition method must be used with caution as it retrieves all devices from a purchase order. If a device belongs to another customer account or is used by other services, Central displays it as a blocked device. As Central does not allow you to add blocked devices, you may have to release the blocked devices before proceeding with the next steps.
Add Using Activate	Allows you to retrieve the devices associated with your Aruba Activate account. To add devices: <ol style="list-style-type: none">1. Enter the username and password of your Aruba Activate account.2. Click Add. All devices associated with the Activate account are retrieved and added to the list of devices displayed on the Device Inventory page. NOTE: Use this option with caution as it synchronizes all devices from your Activate account with the Central device inventory. NOTE: You can use this option only once. After the devices are added, Central does not allow you to modify or re-import the devices using your Aruba Activate credentials.

For Instant APs that dynamically form a cluster, you must add the master Instant AP from the **Device Inventory** page whenever a slave Instant AP joins the cluster, to ensure that the slave Instant AP inherits the configuration from the master Instant AP.

Quick Reference Illustration

See the following figure for an illustration of device addition procedure:

Figure 2 Adding Devices to Inventory

Device Addition Procedure

aruba Central

DEVICE INVENTORY

When you place an order for new devices, those devices will automatically appear in your inventory once the order is processed. If you don't see a purchased device in your inventory, you can manually add it. allows you to add up to 32 devices manually by entering the valid MAC and serial number combination for each device. If you need to add more than 32 devices, you can use the Aruba Cloud Activation Key to do so.

DEVICES

ADD BY MAC/SN ADD WITH CLOUD ACTIVATION KEY ADD USING ACTIVATE

▽ SERIAL # ▽ MAC ▽ IP NAME LAB... MODEL GR... STATUS

Option 1

ADD DEVICES

Central supports adding up to 32 total devices manually.

Enter the serial number and MAC address of the devices. You can add up to 32 total devices.

Option 2

CLOUD ACTIVATION KEY

When you enter a Cloud Activation key, all your devices that were purchased on the same order are added to your Central inventory.

Enter the cloud activation key acquired during the device purchase.

Option 3

ACTIVATE

When you use your Aruba Activate credentials to synchronize your Central account, all devices in your default Activate folder will appear in your Central device inventory.

Enter your Aruba Activate Credentials

Note: Devices can be added to Central without licensing. However, devices can connect to Central only after licensing the devices.


Assigning Subscriptions

Central offers evaluation and paid subscriptions. The users who want to try the Aruba cloud solution can [sign up](#) for a 90-day evaluation subscription. If you are a registered user with a paid subscription, you can [log in](#) to the Central portal.

Aruba Central supports the following types of subscriptions:

- **Device management**—The device management 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 Central. For example, if your account has any Instant APs managed by AirWave, you can assign only service subscription to these devices.
- **Cloud services**—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. Currently, Central offers Clarity, Guest Access, and Presence Analytics service subscriptions.
- **Gateway Subscriptions**—Central supports a separate set of subscriptions for configuring and managing SD-WAN gateways.

The evaluation subscription allows you to add up to 10 Instant APs or 10 Switches, or a combination of 10 Instant APs and Switches.

 The service evaluation subscription allows you to access application services such as Presence Analytics. With this subscription, you can add up to 20 Instant APs.

If you are adding a device and if you get the **Blocked Device** error message, another Central user would have already added the device and assigned a license to this device.

Assigning Device Subscriptions

Central allows you to enable automatic assignment of device subscriptions for the devices joining Central.

Enabling Automatic Assignment of Device Subscriptions

When a subscription assigned to a device expires or is canceled, Central checks the inventory for the available subscription tokens for the device and verifies if the subscription has adequate license tokens. If the subscription has adequate capacity, Central automatically assigns the longest available subscription token to the device. If not, Central ensures that the subscriptions are utilized to the full capacity by assigning as many devices as possible.



In the **Managed Service Mode**, Central does not support automatic assignment of subscriptions. Use the `/licensing/v2/msp/customer/settings/autolicense` API to enable automatic assignment of subscriptions.

To enable automatic assignment of subscriptions:

1. From the app selector, click **Global Settings**.
2. Click **Subscription Assignment**. The **Subscription Assignment** page opens.
3. Under **Device Subscriptions**, click **Auto Subscribe Device Subscription Keys**.

All the devices listed in the **Global Settings > Device Inventory** page are assigned device subscriptions. If you want to specify a set of devices for automatic assignment of device subscriptions, click **Select Devices** and select the devices to which you want assign subscriptions.



If the subscription tokens available are less than the number of devices, no device gets subscribed even after you enable automatic assignment of subscriptions.

Assigning Service Subscriptions to Devices

To manually assign subscription to a device, complete the following steps:

1. From the app selector, click **Global Settings**.
2. Click **Subscription Assignment**. The **Subscription Assignment** page opens.
3. From the table on the right, select the devices to which you want to assign subscriptions.
4. Drag and drop the device to the subscription selected in the table on the left.

Assigning Gateway Subscriptions

After adding gateways to the Central device inventory, you must ensure that the gateway devices are assigned a valid subscription. The gateway subscription allows Aruba Mobility Controllers to function as SD branch devices.

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.

To assign gateway subscription to a device, 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 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 gateway subscription assigned to a device expires, Central automatically assigns a valid subscription from the same subscription category.

Viewing Subscription Details

The **Subscription Assignment** page allows you to view a list of subscriptions and enable automatic assignment of subscriptions to devices.

Table 9: *Subscription Details*

Data Pane Item	Description
Subscriptions	Name of the subscription.
All Devices	Total number of devices provisioned in Central.
No Subscriptions	Total number of devices that do not have a subscription key assigned.
Subscriptions Total	Total number of subscriptions purchased by the customer.
Available	Number subscriptions available for assignment in a customer account.

Unassigning Subscriptions

Central also allows you to unassign subscriptions for the devices connected to Central. Following are the two methods to unassign subscription from a specific device, or multiple devices:

Unassigning Subscription from Specific Device

To unassign subscriptions from a specific device, complete the following steps:

1. On the **Subscription Assignment** page, select a subscription from the table on the left.
2. From the table on the right, select the devices that must be removed from the service.
3. Click the trash icon corresponding to the selected device. The subscription is unassigned for a specific device.

Unassigning Subscription from Multiple Devices

To unassign subscription from multiple devices as a batch, complete the following steps:

1. On the **Subscription Assignment** page, select a subscription from the table on the left.
2. From the table on the right, select the multiple devices to be removed from the service using the **shift+click**, or **ctrl+click** keys.
3. Click **Batch Remove Label**. The subscription is unassigned for the batch of selected devices..



When a license is unassigned from a device, Central now displays a **Confirm Action** pop-up with the **Do you want to modify the subscription for selected devices** message. You must click **Yes** to unassign the license on the device.

Acknowledging Subscription Expiry Notifications

The **Subscription Keys** page displays the subscriptions that are about to expire in 90 days. 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

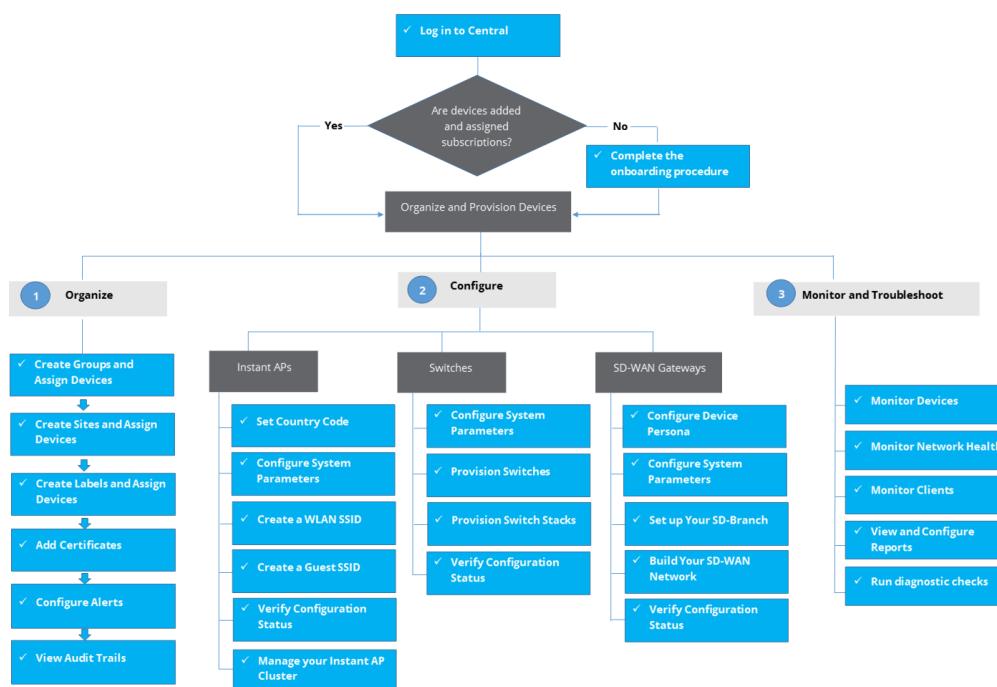
If a subscription has already expired or is about to expire within 24 hours, a subscription expiry notification message is displayed in a pop-up window when the customer logs in to Central.

To prevent Central from generating expiry notifications, click **Acknowledge**. Central does not generate expiry notification messages either in the UI or through email for the acknowledged subscriptions.

Organizing, Provisioning, and Managing Your Devices

Learn how to organize, configure, and manage your devices in Central. See the illustration below and follow the instructions.

Figure 3 *Organize and Provision Devices*



Assigning Devices to Groups

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

Assigning Instant APs to Groups

The Instant AP groups may consist of the configuration elements:

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

[Table 10](#) describes the group assignment criteria for Instant APs:

Table 10: *Instant AP Group Assignment*

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

To manually assign Instant APs to a group:

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

Assigning Switches to Groups

Central allows switches to join groups only if the switches are running factory default configuration. Switches with factory default configuration are automatically assigned to the **default** group.

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



Central does not support provisioning or configuring Aruba 5400R Switch Series and switch stacks through the UI groups. These devices can only be provisioned and configured using templates. By default, these devices are assigned to a template group. You cannot move the Aruba 5400R Switch Series devices from a template group to a UI group. If a Aruba 5400R Switch Series is pre-assigned to a UI group, the device is moved to an unprovisioned group after it joins Central.

To manually assign switches to a group:

1. Go to **Global Settings > Manage Groups**. The **Groups** page opens.
2. To view a list of unassigned devices, click **Unassigned Devices**. A list of unassigned devices is displayed in the devices table.
3. Select the group to which you want to assign the devices.
4. From the devices table on the right, select the switches to assign.
5. Drag and drop the switches to the group that you selected.

Assigning SD-WAN Gateways to Groups

The device groups in Central allow you to:

- 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

Note the following points about groups in Central:

- The groups in 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.
- A device can be part of only one group at any given time.
- Before assigning SD-WAN Gateways to groups, you must set the device persona or role as Branch Gateway or VPN Concentrator.

Assigning a SD-WAN Gateway to a Group

To assign SD-WAN Gateways to a group:

1. Go to **Global Settings > Manage Groups**. The **Groups** page opens.
2. If the group is already available in the list of groups, select the device, and drag and drop the device to the group.
3. If the group is not available in the list, click **New Group** to create a new group, and then drag and drop the SD-WAN Gateways to the group that you just created.

You can also use the **Assign Group** function on the **Global Settings > Device Inventory** page if the SD-WAN Gateways are not yet connected to Central.

Connecting Devices to 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.

For the devices to connect to Activate and the Central management server, ensure that the ports listed in the [Opening Firewall Ports for Device Communication](#) section are open.

Connecting Instant APs to Central

To bring up Instant APs in 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 Central

Note the following points about automatic provisioning of switches:



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.



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

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 Central. For information, on the minimum firmware versions supported on the switches, see [Supported Switch Platforms on page 9](#).

Connecting SD-WAN Gateways to Central

The SD-WAN Gateways have the ability to automatically provision themselves and connect to Central once they are powered on. The SD-WAN 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 SD-WAN Gateways:

1. Connect the devices to the provisioning network.
2. Wait for the device to obtain an IP address through DHCP. When a gateway device is powered on, all ports try to acquire a DHCP IP using the connected uplinks. 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 device identifies Central as its management entity, it automatically connects to 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 11](#) describes the LED behavior.

Table 11: 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 Central, the SD-WAN Gateways download the configuration from Central and reload.



The SD-WAN 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*.

Opening Firewall Ports for Device Communication

Although most of the communication between devices on the remote site and 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.

Table 12: *Domain Names and Ports*

Domain Name	Protocol and port	Description
pool.ntp.org	UDP port 123	To update internal clock on and configure time zone when a factory default device comes up. By default, devices contact pool.ntp.org and use NTP to synchronize their system clocks.
device.arubanetworks.com	TCP port 443	To get provisioning parameters from Aruba Activate. NOTE: Devices must be able to resolve device.arubanetworks.com with a valid DNS server.
activate.arubanetworks.com	TCP port 443	To configure provisioning rules in Activate.
portal.central.arubanetworks.com sso.arubanetworks.com	TCP port 443	To access Central login portal. After a successful authentication, the users are redirected to their respective accounts from which they can manage, configure, and monitor devices.
app1.central.arubanetworks.com for external/prod	TCP port 443	To allow devices to communicate with Central.
internal.central.arubanetworks.com for internal		
app2.central.arubanetworks.com for external/prod	TCP port 443	To allow users to access Central portal.
internal2.central.arubanetworks.com for internal		
naw2.cloudguest.central.arubanetworks.com	TCP port 443, 2083	To allow access to Cloud Guest server from naw3.arubanetworks.com and naw2.arubanetworks.com CDPs.
nae1.cloudguest.central.arubanetworks.com	TCP port 443, 2083	To allow access to Cloud Guest server from nae1.arubanetworks.com .
asw1.cloudguest.central.arubanetworks.com	TCP port 443, 2083	To allow access to Cloud Guest server from asw1.arubanetworks.com
euw1.cloudguest.central.arubanetworks.com	TCP port 443, 2083	To allow access to Cloud Guest server from euw1.arubanetworks.com .

Domain Name	Protocol and port	Description
images.arubanetworks.com	TCP port 80	To access the first server for firmware images to upgrade the devices managed by Central.
http://h30537.www3.hpe.com	TCP port 80	To access firmware images for switches hosted on HPE My Network Portal (MNP).
d2vxf1j0rhr3p0.cloudfront.net	TCP port 80	To access the second server for Instant AP firmware upgrade.
rcs-m.central.arubanetworks.com	TCP port 443	To access an AP console through SSH.
cloud.arubanetworks.com	TCP port 80	To open the Central evaluation sign-up page.
aruba.brightcloud.com	TCP port 443	To access the Brightcloud server for application, application categories, and website content classification.
pqm.arubathena.com pqm.arbunetworks.com	ICMP	To allow Central to probe PQM nodes for the source IP address of the SD-WAN Gateways. To enable PQM nodes to communicate with Central and whitelist IP addresses of the SD-WAN Gateways using the PQM service.



For Branch Gateways to set up IPsec tunnel with the VPN concentrators, the UDP 4500 port must be open. For more information on firewall ports required for communication between the SD-WAN Gateways and other network elements, see *ArubaOS User Guide*.

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 13: *Labels*

Name	Contents of the Table
Labels	<p>This table displays a list of labels configured in Central. It provides the following information:</p> <ul style="list-style-type: none">■ Name of the label■ Number of devices assigned to a label <p>The table also includes the following sorting options to reset the table view on the right:</p> <ul style="list-style-type: none">■ All Devices—Displays all the devices provisioned in Central.■ Unassigned—Displays the list of devices that are not assigned to any label.
Devices	<p>This table displays a list of devices provisioned in Central. It provides the following information about the devices:</p> <ul style="list-style-type: none">■ Name—Name of the device■ Group—Group to which the device is assigned■ Type—Type of the device■ Labels—Number of labels assigned to a device

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**.



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.

Managing Sites

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

Overview

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.

How are sites different from labels?

In the previous versions of Central, the administrators could create the following types of labels:

- Default—Label category for tagging devices
- Sites—Label category used for devices deployed in a specific site. This category was used in data presentation for the Presence Analytics app.

Although labels could be used to provide a location context, a hierarchical distinction of physical sites and specific areas within a site is required for filtering devices for monitoring and reporting purposes.

The **Sites** feature introduced in the current version of Central allows you to explicitly tag devices to a physical location, for example, Campus, Branch, or Venue. You can use sites as a primary navigation element for monitoring and reporting purposes.



Central allows you to assign up to five label tags per device. However, each device can be assigned to only one site.

How do sites work in Central?

Central allows you to create new sites on the **Global Settings > Labels and Sites > Sites** page.

Sites offer the following features and benefits:

- Moving devices from inventory to a specific site based on the device name
- Filtering devices per site for monitoring and viewing reports
- Converting existing labels to sites
- Bulk import of sites from a CSV file

When to use sites?

If your setup requires Central applications to filter devices based on a physical location, use the sites feature. Central allows you to use sites as a primary navigation element and as a filter criterion for the following applications and functions:

- Monitoring
- Reports
- Presence Analytics
- Clarity

What workflows for sites are available in the UI?

The Central UI introduces the following workflows in the user interface:

UI Functions / Applications	Enhancements and Changes
Global Settings > Labels and Sites	The Labels and Sites page offers a separate workflow for labels and sites. To switch between labels and sites, use the toggle switch on the Labels and Sites page. <ul style="list-style-type: none">■ Labels—Allows you to create and assign labels to devices. All new labels are tagged to the Default label category.■ Sites—Allows you to create sites, add devices to a site, and migrate and labels to sites.
Filter bar	The filter bar on the main window displays a list of sites configured in your setup. You can also filter data pane contents per site.
Clarity	The Clarity app now allows you to filter data per site.
Monitoring & Reports	The Monitoring & Reports app now includes the following changes: <ul style="list-style-type: none">■ Label Health—Provides a dashboard view of devices that are tagged to labels.■ Network Overview, Client Overview, AppRF, VisualRF, and Reports—Allow you to filter device details for sites. For example, to view details of the Instant APs provisioned on a specific site, select the site from the filter bar.

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 14: *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 34 .
Sites Table	<p>Displays a list of sites configured in Central. It provides the following information:</p> <ul style="list-style-type: none">■ Site Name—Name of the site.■ Address—Physical address of the site.■ Device Count—Number of devices assigned to a site. <p>The table also includes the following sorting options to reset the table view on the right:</p> <ul style="list-style-type: none">■ All Devices—Displays all the devices provisioned in Central.■ Unassigned—Displays the list of devices that are not assigned to any site. <p>You can also use the filter and sort icons on the Sites and Address columns to filter and sort sites respectively.</p>
New Site	Allows you to create a new site.
Bulk upload	Allows you to add sites in bulk from a CSV file.
Devices Table	<p>Displays a list of devices provisioned in Central. It provides the following information:</p> <ul style="list-style-type: none">■ Name—Name of the device■ Group—Group to which the device is assigned.■ Type—Type of the device.

Creating a Site

To create a site, complete the following steps:

1. 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. 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.

Add 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. On the **Global Settings > Labels and Sites > Sites > (+) Bulk upload** window, 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. 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 **Convert Labels to Sites**. The **Confirm Conversion** pop-up window opens.
5. To download a CSV file with the list of labels configured in your setup, click **Download a File**. A CSV file with a list of all the labels in your setup is downloaded to your local directory.
6. Enter address, city, state, country, and ZIP code details for the labels that you want to convert to sites.



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

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

If the conversion process fails for some labels, 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.



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, Central retains only the historical data for these labels. 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 User Accounts and Roles

The network and organization administrators can create and manage system users in Central. The system users are authenticated either using the Aruba Single Sign On server (public cloud deployments) or LocalDB servers (private cloud deployments).

System users can access both Central UI and API Gateway with their login credentials. User access for system users is determined by the role to which they are mapped.

Role-Based Access

Central supports the following types of roles:

Predefined User Roles

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

User Role	Standard Enterprise Portal	Managed Service Portal
admin	<ul style="list-style-type: none">■ Has full access to all devices.■ Can provision devices and enable access to application services.■ Can create or update users, groups, and labels.	<ul style="list-style-type: none">■ Has full access to tenant accounts■ Can create, modify, provision, and manage customer accounts
readwrite	<ul style="list-style-type: none">■ Has access to the groups and devices assigned in the account.■ Can add, modify, configure, and delete a device in the account.	Can access and modify tenant accounts.
readonly	<ul style="list-style-type: none">■ Can view the groups and devices.■ Can view generated reports.	Can view tenant accounts.
guestoperator	<ul style="list-style-type: none">■ Can access and modify cloud guest splash page profiles.■ Can configure visitor accounts for the cloud guest splash page profiles.	<ul style="list-style-type: none">■ 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, 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 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.

Application Permissions

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.

You can set application permissions for the following application modules:

- **Group management**—Allows you to define user access to device groups.
- **Device inventory**—Allows to define user access for managing devices.
- **Network management**—Allows you to define user access to network monitoring, configuration, and troubleshooting.
- **Guest management**—Allows you to define or block user access to the Guest Access application.
- **Clarity**—Allows you to define or block user access to the Clarity application.

- **Presence Analytics**—Allows you to define or block user access to the Presence Analytics application.
- **VisualRF**—Allows you to define or block user access to the VisualRF application.
- **Unified Communications**—Allows you to define or block user access to the Unified Communications application.
- **Other Applications**—Allows you to define or block access to other applications.

Configuring Users

The **Users & Roles** menu option in the **Global Settings** application allows you to create, modify, and delete users, and view the number of users assigned to user role.

Adding a User

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

1. From the app selector, click **Global Settings** and then click **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 15](#):

Table 15: *User Configuration Attributes*

Parameters	Standard Enterprise Portal	Managed Service Portal
Username —Name of the user. Enter a valid email address.	Yes	Yes
Description —Description of the user role. You can enter upto a maximum of 32 characters including alphabets, numbers, and special characters in the text field.	Yes	Yes
Role —Enter the user role. For more information on user roles, see <i>Role Based User Management in Aruba Central Help Center</i> .	Yes	No
MSP Role —If the user has access to the Managed Service Portal, specify a user role.	No	Yes
Tenant Role —If the user a tenant account user, assign a tenant role. When no tenant role is configured, the user inherits the MSP role configured for the tenant account.	No	Yes
Allowed Groups —Select the groups which the user can access.	Yes	No
Language —Specify a language.	Yes	Yes

5. Click **Save**. An email invite is sent to the user with a registration link.
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. From the app selector, click **Global Settings** and then click **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. From the app selector, click **Global Settings** and then click **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.

Configuring Roles

The **Users & Roles** menu in the **Global Settings** application allows you to create custom roles and configure access rights for these roles.

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.

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.
- **Track Progress**—The link connects to the **Operations Status** page that provides the status such as **in progress** or **failed** for the user account update to the tenant customer.



The **User & Roles** pane also includes the **Support Access** and **Two-factor Authentication (2FA)** options under **Actions**. For more information on two-factor authentication, see [Two-Factor Authentication on page 1](#).

When **Support Access** is enabled, the Aruba support team can access your Central account remotely.

Uploading Certificates

By default, 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 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.

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

Instant APs	Switches
<ul style="list-style-type: none"> ■ AddTrust ■ GeoTrust ■ VeriSign ■ Go Daddy 	<ul style="list-style-type: none"> ■ 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. From the **Type** drop-down list, select **Server Certificate**.
 - 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 Software Images

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 Central:

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

Table 16: *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: <ul style="list-style-type: none">■ Show All■ Need upgrade■ Scheduled■ In progress■ Failed■ Upgrade not required Show All is selected by default.
Virtual Controllers	Displays the following information: <ul style="list-style-type: none">■ 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	Displays the following details about Aruba switches managed through Central: <ul style="list-style-type: none">■ 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.
Switch-Aruba	
Continue	Allows you to continue with firmware upgrade.

Table 16: *Firmware Maintenance*

Data Pane Item	Description
Firmware Compliance Setting	<p>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.</p> <p>To ensure firmware version compliance, complete the following steps in the Firmware Compliance Setting page:</p> <ul style="list-style-type: none"> ■ Groups—Select the group for which the compliance must be set. Select the specific group to set compliance at group level. ■ Device Type—Select the version number from the drop-down list to which the compliance is required to be set. ■ Auto Reboot—Select this check box to reboot Central automatically after the build is downloaded on the device. On reboot, the new build is installed on the device. ■ When—Select one of the following radio buttons to specify if the compliance must be carried out immediately or at a later date and time. <ul style="list-style-type: none"> ● Now— To set the compliance to be carried out immediately ● Later — To set at the later date and time ■ Save and Upgrade—Click this button to save the firmware compliance with the above settings.
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.



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

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



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

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**.

Forcing Firmware Upgrade

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 devices and the firmware versions for upgrade.
6. Select Auto Reboot if you want Central to automatically reboot the device after a successful device upgrade.
7. Click **Save**. 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.

Viewing Audit Trails

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

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 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 17: *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.
Target	The group or device to which the changes were applied.
Details	<p>A short description of the changes such as subscription assignment, firmware upgrade, and configuration updates.</p> <p>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.</p>

Troubleshooting Devices

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

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, 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 18](#) describes the fields and filtering parameters available on the **Troubleshooting** page:

Table 18: *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 18: Contents of the Troubleshooting Page

Data Pane Item	Description
Troubleshooting	<p>Allows you to select one of the following options:</p> <ul style="list-style-type: none"> ■ 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	<p>Allows you to run the following diagnostic tools on the selected devices:</p> <ul style="list-style-type: none"> ■ 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	<p>Category—Allows you to select a category. The troubleshooting commands are segregated under the following categories:</p> <p>Access Points</p> <ul style="list-style-type: none"> ■ Wireless ■ Security ■ Network ■ Airgroup ■ System ■ ARM ■ Datapath ■ Logs ■ Central ■ Cluster Security ■ Speed Test ■ OFC <p>Switch- MAS</p> <ul style="list-style-type: none"> ■ Physical Connection ■ Traffic ■ Configuration ■ Media Access ■ Network <p>Switch - Aruba</p> <ul style="list-style-type: none"> ■ Physical Connection ■ PoE and Media Access ■ L2 Loop Prevention ■ Link Aggregation ■ Loop Detection ■ Network ■ Management ■ Security and Traffic ■ Show Tech ■ Modules ■ Stacking

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, 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