Aruba Central Managed Service Provider

aruba

a Hewlett Packard
Enterprise company

User Guide

Copyright Information

Open Source Code

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

Chapter 1
About This Document

This guide provides an overview of the Managed Service Provider (MSP) mode of the Network Operations app and provides detailed description of the various deployment models supported by Aruba Central.

Intended Audience

This guide is intended for customers who configure and use MSP mode.

Related Documents

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

- *Aruba Central Help Center*
- *Aruba Central User Guide*

Conventions

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

Table 1: *Typographical Conventions*

Type Style	Description
Italics	This style is used to emphasize important terms and to mark the titles of books.
`System items`	This fixed-width font depicts the following: ■ Sample screen output ■ System prompts
Bold	■ Keys that are pressed ■ Text typed into a GUI element ■ GUI elements that are clicked or selected

The following informational icons are used throughout this guide:

NOTE

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

CAUTION

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

WARNING

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	lms.arubanetworks.com
End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team	Site: arubanetworks.com/support-services/security-bulletins/ Email: aruba-sirt@hpe.com

Chapter 2
What is Aruba Central?

Aruba Central offers unified network management, AI-based analytics, and IoT device security for wired, wireless, and SD-WAN networks. All of these capabilities are combined into one easy-to-use platform, which includes the following apps:

- **Network Operations**—Provides unified network management by consolidating wired, wireless, and SD-WAN deployment and management tasks, real-time diagnostics, and live monitoring, for simple and fast problem resolution.
- **ClearPass Device Insight**—Provides a single pane of glass for device visibility employing automated device discovery, machine learning (ML) based fingerprinting and identification. For more information, see Aruba ClearPass Device Insight Information Center.

Key Features

Aruba Central offers the following key features and benefits:

- Streamlined configuration and deployment of devices—Leverages the ZTP capability of Aruba devices to bring up your network in no time. Aruba Central supports group configuration of devices, which allows you to provision and manage multiple devices with similar configuration requirements with less administrative overhead.
- Integrated wired, WAN, and wireless Infrastructure management—Offers a centralized management interface for managing wireless, WAN, and wired networks in distributed environments, and thus help organizations save time and improve efficiency.
- Advanced analytics and assurance—With continuous monitoring, AI-based analytics provide real-time visibility and insight into what's happening in the Wi-Fi network. The insights utilize machine learning that leverage a growing pool of network data and deep domain experience.
- Secure cloud-based platform—Offers a secure cloud platform with HTTPS connection and certificate based authentication.
- Interface for Managed Service Providers—Offers an additional interface for MSPs to provision and manage their respective tenant accounts. Using the MSP mode, service provider organizations can administer network infrastructure for multiple organizations in a single interface.
- SD-Branch Management—Offers a simplified solution for managing and monitoring SD Branch devices such as Branch Gateways, VPN Concentrators, Instant APs, and Aruba Switches. It also provides detailed dashboards showing WAN health and pictorial depictions of the branch setup. The Aruba SD-Branch solution extends the SD-WAN concepts to all elements in a branch setup to deliver a full-stack solution for managing WLAN, LAN and WAN connections. The SD-Branch solution provides a common cloud-management model that simplifies deployment, configuration, and management of all components of a branch setup. The solution leverages the ZTP and cloud management capabilities of Aruba devices to integrate management and infrastructure for WAN, WLAN, and LAN and provide a holistic solution from access network to edge with end-to-end security. It also addresses all communications in distributed deployments, from micro branches to medium or large branches. For more information, see the Aruba SD-Branch Solution.
- Health and usage monitoring—Provides a comprehensive view of your network, device status and health, and application usage. You can monitor, identify, and address issues by using data-driven dashboards, alerts, reports, and troubleshooting workflows. Aruba Central also utilizes the DPI feature of the devices to monitor, analyze and block traffic based on application categories, application type, web categories and

website reputation. Using this data, you can prioritize business critical applications, limit the use of inappropriate content, and enforce access policies on a per user, device or location basis.

- Guest Access—Allows you to manage access for your visitors with a secure guest Wi-Fi experience. You can create guest sponsor roles and social logins for your guest networks. You can also design your guest landing page with custom logos, color, and banner text.
- Presence Analytics—Offers a value added service for Instant AP based networks to get an insight into user presence and loyalty. The Presence Analytics dashboard allows you to view the presence of users at a specific site and the frequency of user visits at a given location or site. Using this data, you can make business decisions to improve customer engagement.

Terminology

Take a few minutes to familiarize yourself with the following key terms:

Term	Description
Standard Enterprise mode	Refers to the Aruba Central deployment mode in which customers manage their respective accounts end-to- end. The Standard Enterprise mode is a single-tenant environment for a single end-customer.
MSP mode	Refers to the Aruba Central deployment mode in which service providers centrally manage and monitor multiple tenant accounts from a single management interface.
Tenant accounts	End-customer accounts created in the MSP mode. Each tenant is an independent instance of Aruba Central.
MSP administrator	Refers to owners of the primary account. These users have administrator privileges to provision, manage, and monitor tenant accounts.
Tenant users	Refers to the owners of an individual tenant account provisioned in the Managed Service Provider mode. The MSP administrator can create a tenant account.

Supported Web Browsers

NOTE

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

Table 3: *Browser Compatibility Matrix*

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

Operational Modes and Interfaces

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

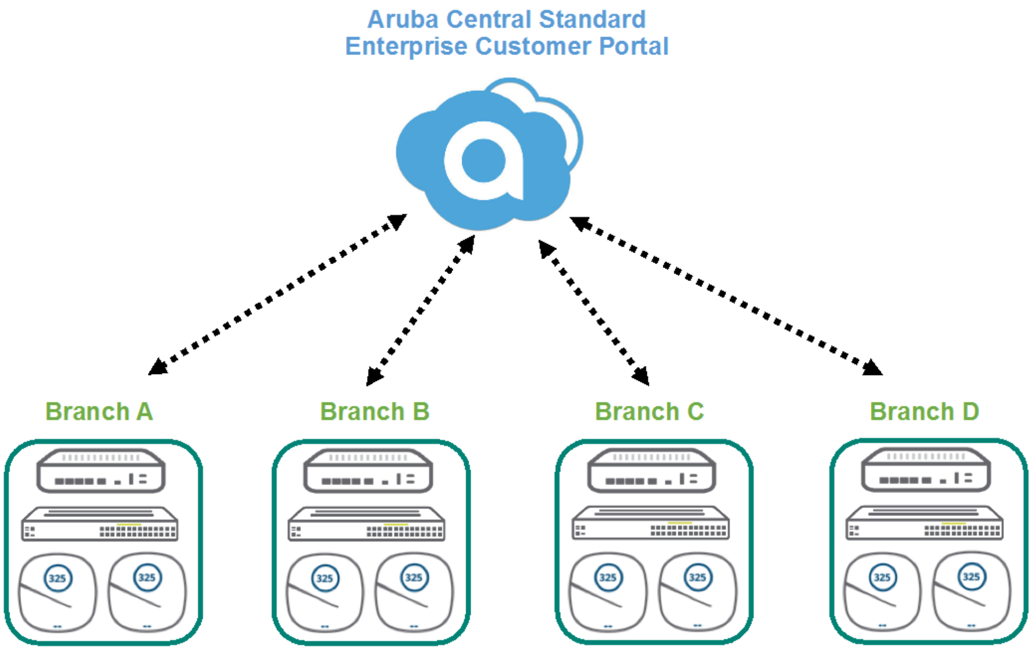
- Standard Enterprise Mode
- Managed Service Provider Mode

Standard Enterprise Mode

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

The following figure illustrates a typical Standard Enterprise mode deployment.

Figure 1 *Standard Enterprise Mode*

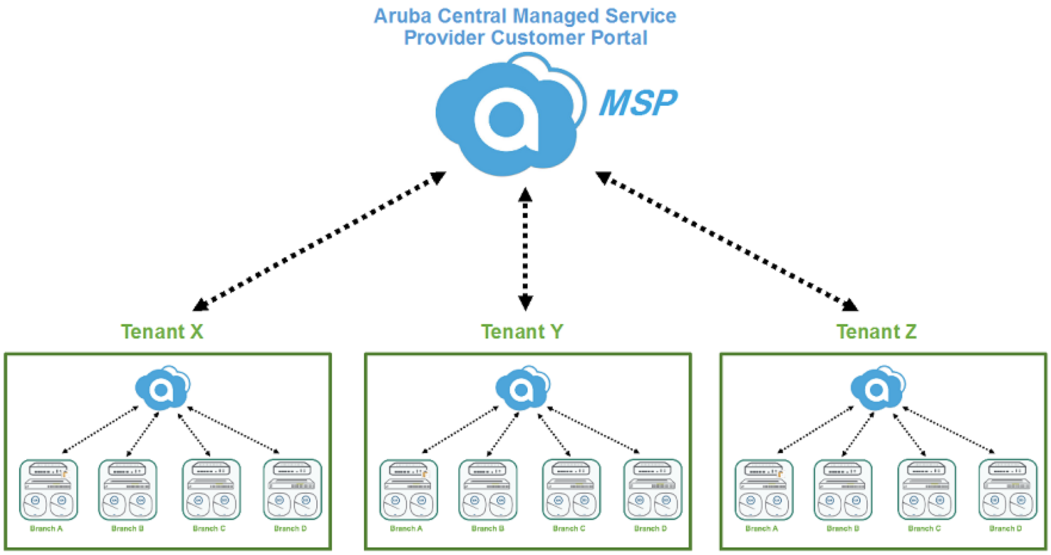


Managed Service Provider Mode

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

The following figure illustrates a typical MSP mode deployment.

Figure 2 *Managed Service Provider Mode*



Supported Devices for MSP

This section provides the following information:

- Supported Instant APs
- Supported Switch Platforms

Supported Instant APs

The following section discusses the supported Instant APs:

Supported Indoor APs

Aruba Central supports the following indoor APs:

- AP-555
- AP-535
- AP-534
- AP-515
- AP-514
- AP-505H
- AP-505
- AP-504
- AP-345
- AP-344
- AP-318
- AP-303
- AP-303P
- AP-303H
- AP-203H
- AP-203R/AP-203RP
- IAP-304/305
- IAP-207
- IAP-334/335
- IAP-314/315
- IAP-324/325
- IAP-228
- IAP-205H
- IAP-103
- IAP-114/115
- IAP-204
- IAP-205
- IAP-214/215

- IAP-224/225
- RAP-3WNP
- RAP-108/109
- RAP-155/155P
- IAP-134/135
- IAP-104
- IAP-105
- IAP-92/93

Supported Outdoor APs

Aruba Central supports the following outdoor APs:

- AP-577EX
- AP-577
- AP-575EX
- AP-575
- AP-574
- AP-518
- AP-387
- AP-377EX
- AP-377
- AP-375EX
- AP-375
- AP-374
- AP-367
- AP-365
- IAP-277
- IAP-274/275
- IAP-175

Supported Instant AP Firmware Versions

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

- 8.7.0.0
- 8.6.0.4
- 8.6.0.3
- 8.6.0.2
- 8.5.0.9
- 8.5.0.8
- 8.5.0.7
- 8.5.0.6
- 8.5.0.5
- 8.4.0.6

- 8.3.0.12
- 8.3.0.11
- 6.5.4.17
- 6.5.4.16
- 6.5.4.15
- 6.5.1.5-4.3.1.9
- 6.4.4.8-4.2.4.16

NOTE

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

By default, AP-318, AP-374, AP-375, and AP-377 access points have Eth1 as the uplink port and Eth0 as the downlink port. Aruba recommends that you not upgrade these access points to 8.5.0.0 or 8.5.0.1 firmware versions as the upgrade process changes the uplink port from Eth1 to Eth0 port thereby making the devices unreachable.

APs Supporting Power Draw

The following APs support Power Draw:

- AP-577EX
- AP-577
- AP-575EX
- AP-575
- AP-574
- AP-518
- AP-515
- AP-514
- AP-505H
- AP-505
- AP-504
- AP-387
- AP-377
- AP-375
- AP-374
- AP-345
- AP-344
- IAP-335
- IAP-334
- AP-318
- IAP-314
- IAP-305
- IAP-304
- AP-303H

NOTE

For more information about Aruba's End-of-life policy and the timelines for hardware and software products at the end of their lives, see: https://www.arubanetworks.com/support-services/end-of-life/.

Data sheets and technical specifications for the supported AP platforms are available at: https://www.arubanetworks.com/products/networking/access-points/.

Supported Switch Platforms

NOTE

To manage your Aruba switches using Aruba Central, ensure that the switch software is upgraded to 16.05.0007 or a later version. However, if you already have switches running lower software versions in your account, you can continue to manage these devices from Aruba Central.

The following tables list the switch platforms, corresponding software versions supported in Aruba Central, and switch stacking details.

Table 4: *Supported Aruba Switch Series, Software Versions, and Switch Stacking*

Switch Platform	Supported Software Versions	Recommended Software Versions	Switch Stacking Support	Supported Stack Type (Frontplane (VSF) / Backplane (BPS))	Supported Configuration Group Type for Stacking (UI / Template)
Aruba 2540 Switch Series	YC.16.03.0004 or later	YC.16.10.0003	N/A	N/A	N/A
Aruba 2920 Switch Series	WB.16.03.0004 or later	WB.16.10.0003	Yes **Switch Software Dependency**: WB.16.04.0008 or later	BPS	UI and Template
Aruba 2930F Switch Series	WC.16.03.0004 or later	WC.16.10.0003	Yes **Switch Software Dependency**: WC.16.07.0002	VSF	UI and Template
Aruba 2930M Switch Series	WC.16.04.0008 or later	WC.16.10.0003	Yes **Switch Software Dependency**: WC.16.06.0006	BPS	UI and Template
Aruba 3810 Switch Series	KB.16.03.0004 or later	KB.16.10.0003	Yes **Switch Software Dependency**: KB.16.07.0002	BPS	UI and Template
Aruba 5400R Switch Series	KB.16.04.0008 or later	KB.16.10.0003	Yes **Switch Software Dependency**: KB.16.06.0008	VSF	Template only

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

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

Chapter 4
About the Managed Service Portal User Interface

NOTE

This topic discusses the Network Operations app in MSP mode. To know more about the Account Home page, see the online Aruba Central documentation.

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

Launching the Network Operations App for MSP

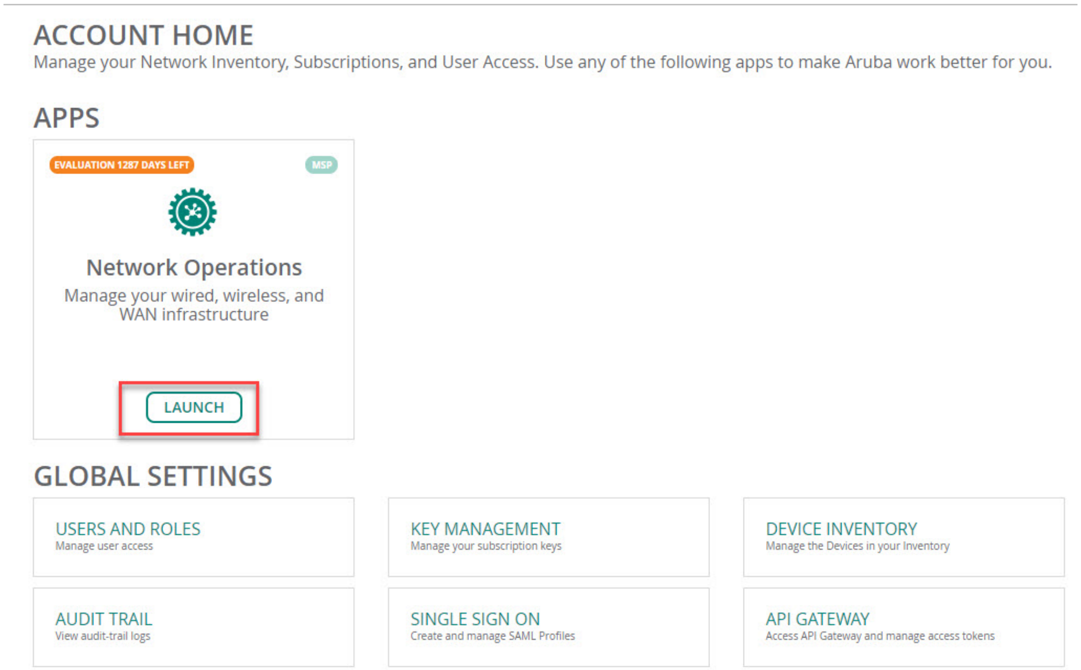
Aruba Central in MSP mode consists of the Network Operations app and the Account Home page.

After you create an Aruba Central account, the link to Aruba Central portal will be sent to your registered email address. You can use this link to log in to Aruba Central. If you are accessing the login URL from the www.arubanetworks.com website, ensure that you select the zone in which your account was created. The Network Operations app is displayed at each user login to Aruba Central.

From the Network Operations app, you can navigate to the Account Home page by clicking the Account Home icon ⁙.

From the Account Home page, you can navigate to the Network Operations app by clicking the Launch button for the Network Operations tile.

Figure 3 *Launching the Network Operations App for MSP from Account Home*



ACCOUNT HOME

Manage your Network Inventory, Subscriptions, and User Access. Use any of the following apps to make Aruba work better for you.

APPS

Network Operations

Manage your wired, wireless, and WAN infrastructure

GLOBAL SETTINGS

USERS AND ROLES
Manage user access

KEY MANAGEMENT
Manage your subscription keys

DEVICE INVENTORY
Manage the Devices in your Inventory

AUDIT TRAIL
View audit-trail logs

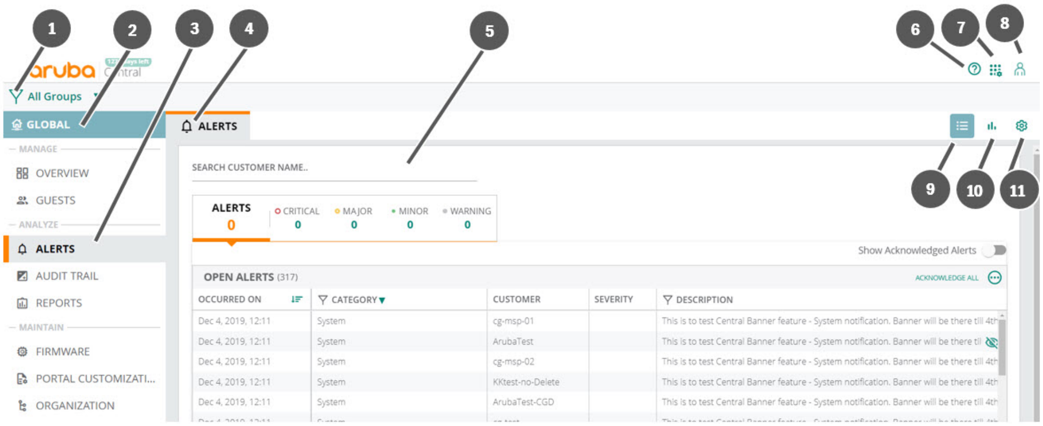
SINGLE SIGN ON
Create and manage SAML Profiles

API GATEWAY
Access API Gateway and manage access tokens

Parts of the Network Operations App for MSP

After you launch the **Network Operations** app, the MSP view opens.

Figure 4 *Parts of the Aruba Central User Interface for MSP*



OCCURRED ON	CATEGORY	CUSTOMER	SEVERITY	DESCRIPTION
Dec 4, 2019, 12:11	System	cg-msp-01		This is to test Central Banner feature - System notification. Banner will be there till 4th
Dec 4, 2019, 12:11	System	ArubaTest		This is to test Central Banner feature - System notification. Banner will be there til
Dec 4, 2019, 12:11	System	cg-msp-02		This is to test Central Banner feature - System notification. Banner will be there till 4th
Dec 4, 2019, 12:11	System	KKtest-no-Delete		This is to test Central Banner feature - System notification. Banner will be there till 4th
Dec 4, 2019, 12:11	System	ArubaTest-CGD		This is to test Central Banner feature - System notification. Banner will be there till 4th

Callout Number	Description
1	Filter to select a group or all groups. For more information, see Filter.
2	Name of the dashboard, here it is set to Global as the filter is set to All Groups.
3	Menu item under left navigation contextual menu. Menu is dependent on the filter selection.
4	First-level tab on dashboard. The dashboard may also have second and third-level tabs dependent on the filter selection.
5	Dashboard for the selected menu item on left navigation pane. For more information, see Launching the MSP Global Dashboard.
6	Help icon. For more information, see Help Icon.
7	Account Home icon. For more information, see Search Bar.
8	User Settings icon. For more information, see User Icon.
9	List view. Click the list icon to view a tabular representation of the data. Only applicable for the global dashboard.
10	Summary view. Click the summary icon to view a graphical representation of the data. Only applicable for the global dashboard.
11	Configuration view. Click the configuration icon to enable configuration mode.

Search Bar

The search bar enables users to search help information.

Help Icon

The help icon contains the following options:

- **Get help on this page**— Selecting this option changes the appearance of some of the text on the UI to green italics. On the UI, when you point to the text in green italics, a dialog box displays the help information for that text. To disable this option, click **Done**.
- **Tutorials**— Displays the Aruba Central product learning center.
- **Feedback**— Allows you to provide feedback on the Aruba Central. You can choose the rating from the range of 1 to 10, where 1 being extremely unlikely and 10 being extremely likely and type your comment into the box and click **Submit** to submit the feedback.
- **Documentation Center**— Directs you to the online help documentation.
- **Airheads Community**— Directs you to the Aruba support forum.
- **View / Update Case**— Enables you to view or edit an existing support ticket in the Aruba Support Portal at https://asp.arubanetworks.com. You must log in to this portal.
- **Open New Case**— Enables you to create a new support ticket in the Aruba Support Portal at https://asp.arubanetworks.com. You must log in to this portal.

Account Home Icon

The Account Home icon enables you to go to the **Account Home** page.

User Icon

The user icon enables you to view user account details such as account name, domain, customer ID, and zone details. It also includes the following options for managing your accounts:

- **Switch Customer**— Enables you to switch to another account. This is especially required during troubleshooting scenarios.
- **Change Password**— Enables you to change the password of the account.
- **User Settings**
  - **Time Zone**— Displays the zone, date, time, and time zone of the region.
  - **Language**— Administrators can set a language preference. The Aruba Central web interface is available in English, French, Spanish, German, Brazilian Portuguese, Chinese, and Japanese languages.
  - **Idle Timeout**— Administrators can set a timeout value for inactive user sessions in the Idle Timeout field. The value is in minutes.
  - **Get system maintenance notification**— Administrators can select the check box to get system maintenance notification.
  - **Get software update notifications**— Administrators can select the check box to get software update notification.
- **Disable MSP**— Disables MSP mode and switches the user interface to the standard enterprise mode. This option changes to Enable MSP when the MSP mode is disabled. You can select **Enable MSP** to switch to the MSP mode. The MSP mode can be disabled only if there is no tenant data. The option is grayed out if there are any active tenant accounts.

- **Terms of Service**— Displays the terms and conditions for using Aruba Central services.
- **Logout**— Enables you to log out of from your account.

Filter

The filter ▽ enables you to select by a group or **All Groups** for performing specific configuration and monitoring tasks. If no filter is applied, by default the filter is set to **All Groups**. When you set the filter to **All Groups**, the Global dashboard is displayed and when you set the filter to a group, the group dashboard is displayed.

Time Range Filter

The time range filter ⟲ enables you to set a time duration for showing monitoring and reports data. This time filter is not displayed when you view the configuration or device details. It is displayed only when you view monitoring data. You can set the filter to any of the following time ranges:

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

Left Navigation Pane

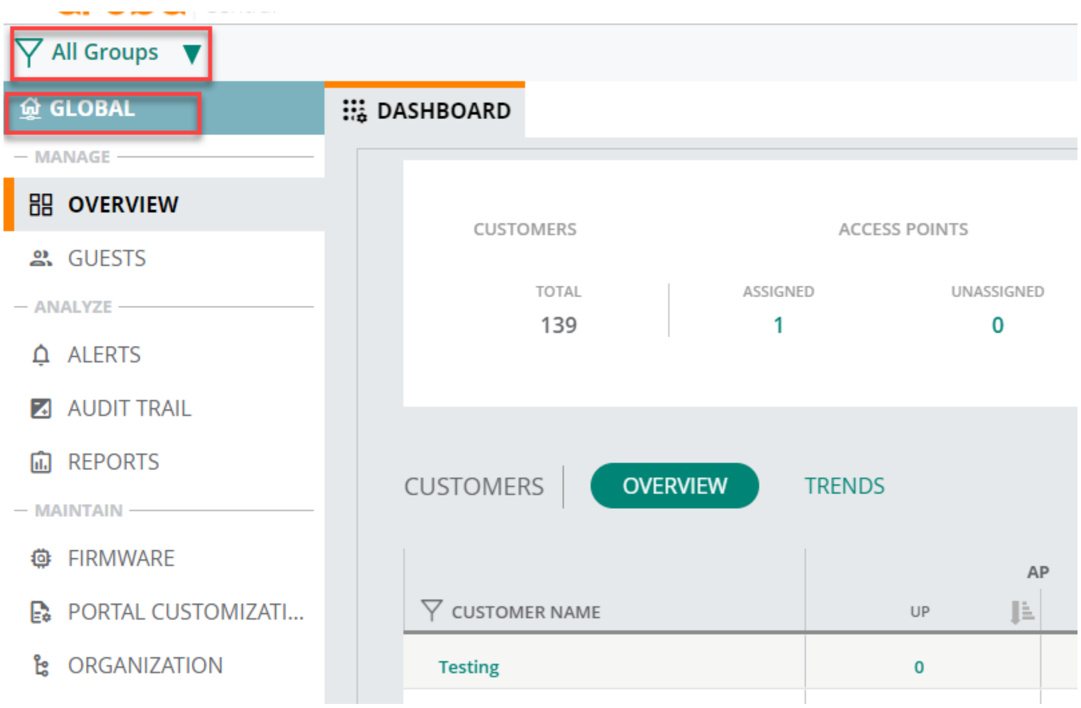
The left navigation pane is a *contextual* menu that displays a number of configuration, monitoring, and troubleshooting options depending on whether you select a group or **All Groups** from the filter.

Launching the MSP Global Dashboard

In the **Network Operations** app in MSP mode, use the filter to select **All Groups**. The Global dashboard is displayed.

In the Global dashboard under the left navigation pane, you can see a number of menu items divided under the following categories: **Manage**, **Analyze**, and **Maintain**.

Figure 5 *Launching the Global Dashboard for MSP*



CUSTOMERS	ACCESS POINTS	
TOTAL	ASSIGNED	UNASSIGNED
139	1	0

CUSTOMER NAME	AP UP
Testing	0

Selecting each menu item in the left navigation pane displays a corresponding dashboard with tabs. Each tab may support all or some of the following functions:

- Summary 📊— Click the summary icon to view a graphical representation of the data. Only applicable for the global dashboard.
- List ☰— Click the list icon to view a tabular representation of the data. Only applicable for the global dashboard.
- Configuration ⚙ — Click the configuration icon to enable configuration mode.

The next sections discuss the left navigation menu items in the Global dashboard.

Manage

The following are included:

- **Overview**— Provides a summary of hardware and subscriptions owned by the MSP and the tenant accounts managed by the MSP. MSP administrators can perform tasks such as drilling down to a tenant account, editing an existing tenant account, and deleting a tenant account.
- **Guests**— Provides a dashboard to view information about cloud guests. Also enables you to create a wired or WLAN guest network based on captive portal authentication for guests, visitors, contractors, and any non-employee users who can use the enterprise Wi-Fi network. Administrators can also create guest accounts and customize the captive portal page with organization-specific logo, terms, and usage policy.

Analyze

The following are included:

- **Alerts**— Displays and configures a list of alerts. This page also enables you to acknowledge these alerts.
- **Audit Trail**— Displays audit trail for the events pertaining to device allocation, configuration, user addition deletion, and firmware upgrade status.

- **Reports**— Enables you to create, view, edit, and download various reports. You can configure the reports to run on demand or periodically. You must have read/write privileges or you must be an Admin user to be able to create reports.

Maintain

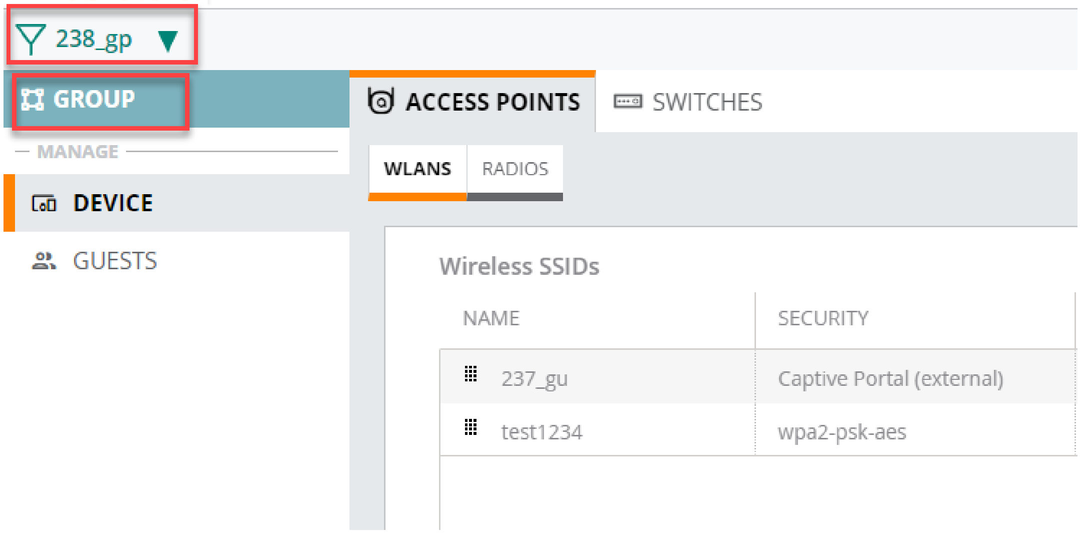
The following are included:

- **Firmware**— Provides an overview of the latest supported version of firmware for the device, details of the device, and the option to upgrade the device. Also enables you to manage firmware compliance for all devices.
- **Portal Customization**— Allows you to customize the look and feel of the user interface and the email notifications sent to the customers and users. For example, you can use your company logo in the user interface and company address in the email notifications sent to the customers or users.
- **Organization**— Enables you to create and manage groups under the **Groups** tab. Under the **Certificates** tab, you can view and add certificates.

Launching the MSP Group Dashboard

In the **Network Operations** app in MSP mode, use the filter to select a group. The group dashboard is displayed.

Figure 6 *Launching the Group Dashboard for MSP*



Wireless SSIDs

NAME	SECURITY
237_gu	Captive Portal (external)
test1234	wpa2-psk-aes

In the group dashboard under the left navigation pane, you can see the **Device** and **Guest** options under **Manage**.

Selecting an option in the left navigation pane displays a corresponding dashboard with tabs. Each tab supports the configuration icon ⚙ that enables the configuration mode. The next sections discuss the left navigation menu items in the group dashboard.

Manage

The following are included:

- **Device**—Enables you to configure APs and Switches for a specific group.
- **Guests**— Enables you to view and configure splash pages for guests.

The MSP mode supports multiple configuration constructs such as UI groups, template groups, local overrides, and so on. This section describes various MSP deployment models using examples. MSP supports the following deployment models:

- MSP Owns Devices and Subscriptions (Deployment Model 1) on page 25.
- End-Customer Owns Both Devices and Subscriptions But MSP Manages (Deployment Model 2) on page 28.
- Hybrid MSP Deployment Model (Deployment Model 3) on page 30.

MSP Owns Devices and Subscriptions (Deployment Model 1)

In this model, the MSP offers Network as a Service (NaaS). The MSP owns both the devices and subscriptions. The MSP acquires end-customers and manages the end-customer's network. The MSP temporarily assigns devices and subscriptions to end-customers for the duration of the managed service contract. Once the contract ends, the devices and the subscriptions are returned back to the MSP's common pool of resources and can be reassigned to another end-customer.

Setup and Provisioning

After the MSP purchases the devices and subscriptions, the MSP administrator has to do the following:

- Set up the Aruba Central account.
- Onboard devices.
- Assign device subscriptions and network services subscriptions.

MSPs can provide Network as a Service to end-customers using Aruba Central MSP mode capabilities. Aruba Central provides simplified provisioning. The **Overview** > **Dashboard** page under **Manage** in the MSP view allows you to add, view, edit, and delete tenant accounts. After adding a device, the MSP administrator must map the device to the tenant account for device management and monitoring operations.

After you create a tenant account, you can map the tenant to a group. The group associated to the tenant account in the MSP mode shows up as the default group for tenant account users. In the MSP mode, all configuration changes made to the group associated to the tenant account are applied to the default group on the tenant account.

For more information, see About Provisioning Tenant Accounts.

Customizing the Portal

MSPs can customize their Aruba Central MSP portal and guest splash pages by uploading their own logo. The **Portal Customization** pane allows you to customize the look and feel of the user interface and the email notifications sent to customers and users. Aruba Central also allows MSPs to localize various pages to support a diverse customer market.

For more information, see Customizing the Portal in MSP Mode.

Monitoring and Reporting

Using the MSP Dashboard, MSPs can monitor and observe trends on end-customer networks.

MSPs can do the following from the MSP Dashboard:

- View total number of tenant accounts and consolidated device inventory and subscription status.

- View graphs representing the devices under management, tenant accounts added, and subscription renewal schedule
- Navigate to each tenant account.

For more information, see MSP Dashboard.

Managing Firmware and Maintenance

MSPs can streamline and automate end-customer's network management while maintaining complete control. MSPs can perform one-click firmware updates or schedule specific updates, manage user accounts across end-customers with different levels of access and tag devices with labels to simplify firmware management and configuration.

For more information, see Firmware Upgrades for MSP Mode.

Example Deployment Scenario

In this scenario, an MSP is offering the following wireless management services:

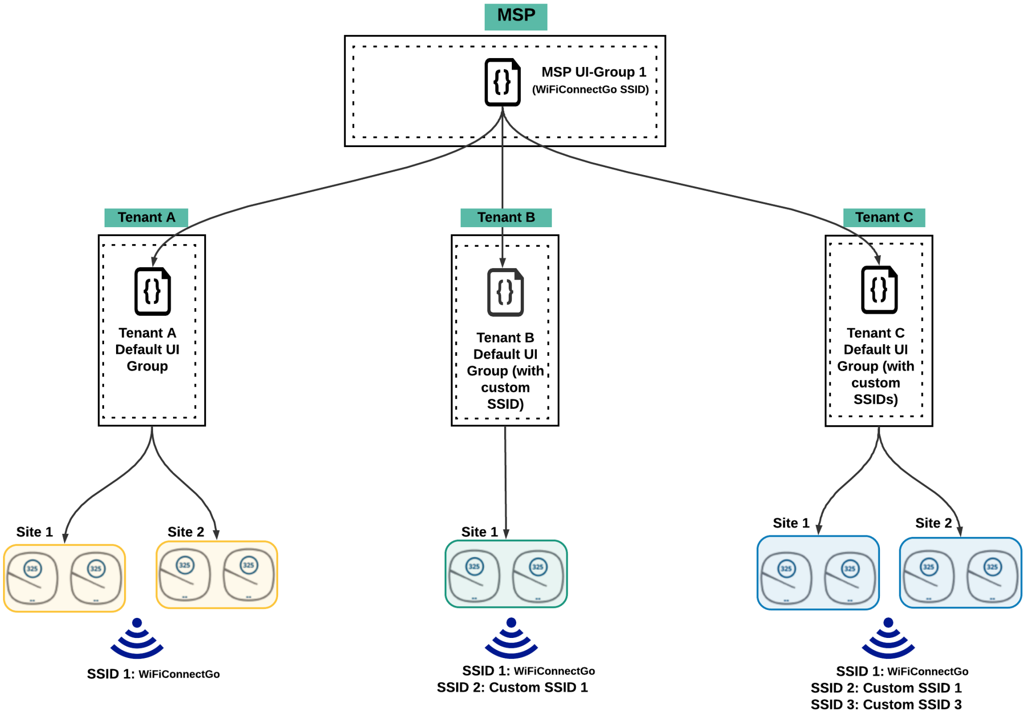
- **WiFiConnectGo**—In this program, for a monthly fee per Instant AP, customers part of this program agree to broadcast MSP's free public WiFi SSID **WiFiConnectGo**. Customers can add up to 15 additional custom SSIDs, including guest, of their own. Tenant account administrators are responsible for configuring any additional SSIDs and ongoing monitoring and maintenance. MSP is responsible for installing and bringing up the Instant AP only.
- **WiFiConnectGo-Plus**—In this program, for an additional monthly fee per Instant AP, customers part of this program need not broadcast the free public WiFi SSID **WiFiConnectGo**. Customers can add up to 15 custom SSIDs, including guest, of their own. MSP is responsible for installing Instant APs, configuring custom SSIDs, and ongoing monitoring and maintenance.

Configuring WiFiConnectGo Using Default UI Groups

Use this deployment model if your customer deployments are identical. UI groups support an inheritance model from MSP to tenant.

As shown in the following figure, MSP uses MSP UI groups to push SSID configuration to the default group in each tenant account. Tenants can choose to add additional custom SSIDs to the default group. All sites are mapped to the same default group.

Figure 7 *MSP Deployment Using Default UI Groups*

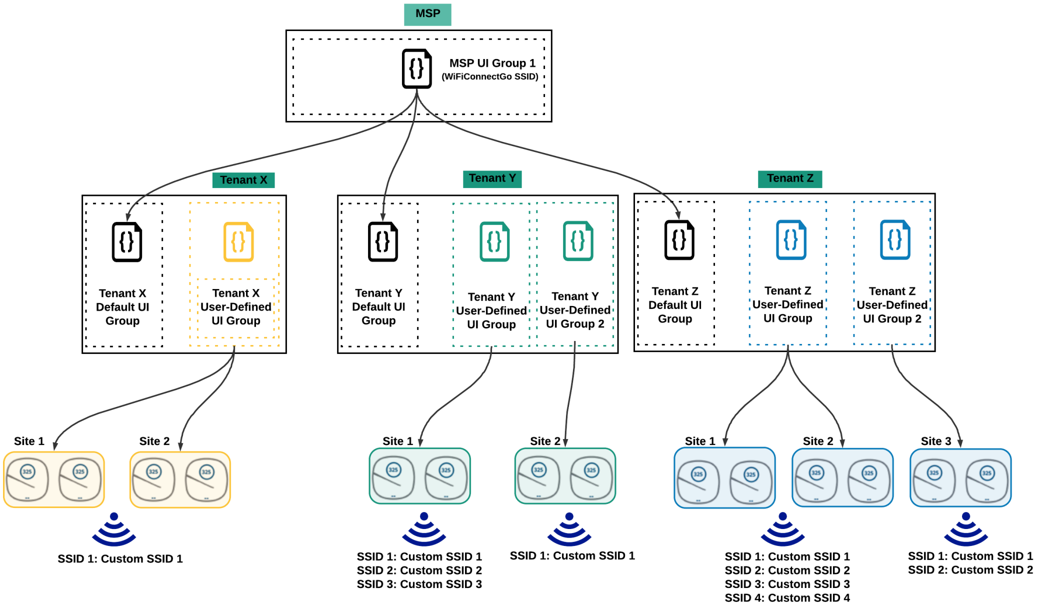


Configuring WiFiConnectGo-Plus Using User-Defined UI Groups

Use this deployment model if your customer deployments are unique and if you wish to use the Aruba Central user interface for configuring. UI groups support an inheritance model from MSP to tenant.

As shown in the following figure, each tenant has their own custom SSID configuration. In this scenario, the MSP administrator can create separate user-defined UI groups for each tenant. Sites with common SSID are mapped to the same UI group. MSP administrators can use the available UI group APIs add, modify, or remove allowed wireless configuration options.

Figure 8 *MSP Deployment Using User-Defined UI Groups*

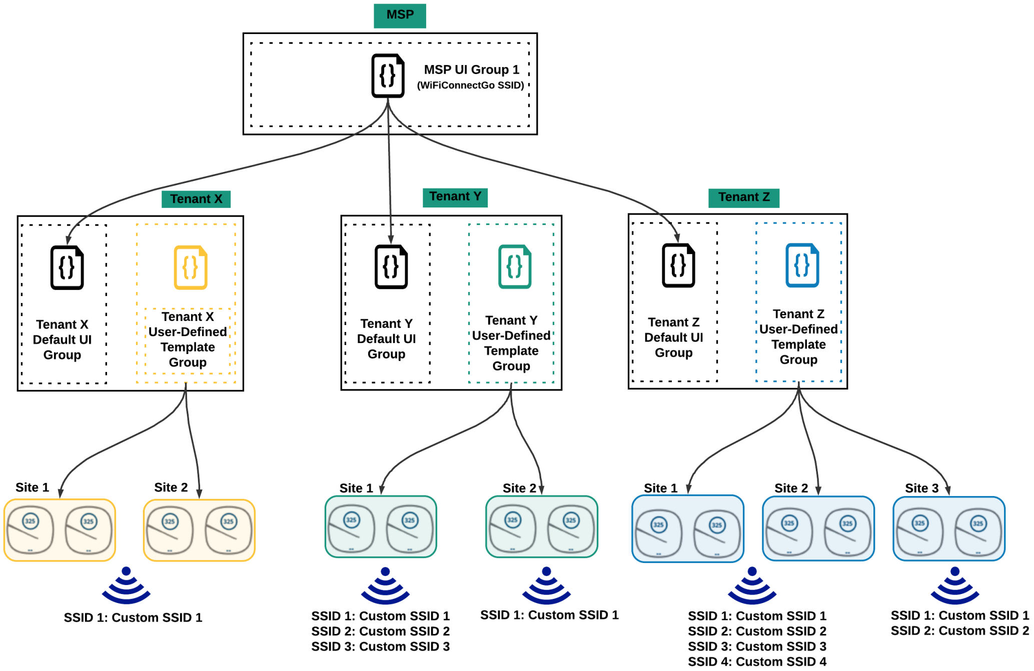


Configuring WiFiConnectGo-Plus Using Template Groups

As shown in the following figure, one template group is defined for each tenant and all devices are associated to the same group. Using the if/else conditional statements, you can push SSIDs to Instant APs selectively. MSP administrators can use the template and variable APIs to add, modify, or remove any wireless configuration.

You can use this deployment model if you wish to automate your customer deployments using Aruba CLIs and Aruba Central APIs.

Figure 9 *MSP Deployment Using Template Groups*



End-Customer Owns Both Devices and Subscriptions But MSP Manages (Deployment Model 2)

In this deployment model, the account type must be Standard Enterprise Mode. Aruba recommends that you contact your Aruba Central sales representative or the Aruba Central Support team if you are an MSP proposing this model to your end-customer.

In this model, the end-customer owns both the devices and subscriptions, but the MSP manages the end-customer's network. The end-customer can be one of the following:

- An existing Aruba customer who owns Aruba devices, but does not have an Aruba Central account.
- An existing Aruba customer who owns Aruba devices and is managing the network using Aruba Central.

In this model, to manage end-customer-owned devices and subscriptions, the MSP can use the Aruba Central Standard Enterprise mode.

The MSP need not create an Aruba Central account of their own, but can instead add their (MSP) administrator to the end-customer's Aruba Central account. The MSP administrator will only have access to each end-customer account.

Setup and Provisioning

The end-customer purchases the devices and subscriptions. The end-customer contacts the MSP to manage the network. As the devices and subscriptions are owned by the end-customer, the MSP uses the Aruba Central Standard Enterprise mode to set up and provision the tenant account.

The MSP has to request the end-customer to add the MSP administrator to their Aruba Central account. The MSP administrator can use the **Switch Customer** option to switch between end-customer accounts. See Using the Switch Customer Option.

Monitoring and Reporting

As the MSP is not using the MSP mode, there is no single pane view of end-customer accounts managed by the MSP. The MSP has to monitor each end-customer individually. The MSP administrator has to use the Aruba Central Standard Enterprise mode to monitor the end-customer network.

Managing Firmware and Maintenance

The MSP has to use the **Firmware** menu under **Maintain** to view the latest supported firmware version of the device, details of the device, and the option to upgrade the device. The MSP administrator has to manage software upgrades for each end-customer individually.

Example Deployment Scenario

In this scenario, an MSP has to configure Instant APs and manage end-customer networks at two different sites. The following are the site details:

Site 1

```
Location: University Ave, Berkeley, CA
SSID Name: "WiFi_CE"
Security: WPA2-PSK
SSID Password: "password@123"
VLAN: 20
```

Site 2

```
Location: University Ave, Berkeley, CA
SSID Name: "WiFi_CE"
Security: WPA2-PSK
SSID Password: "password@123"
VLAN: 40
```

Considering the requirements, each site needs two Instant APs. The only difference between the sites is the VLAN ID.

Deployment Using User-Defined UI Groups

The MSP can configure Instant APs at both sites using user-defined UI groups. As the Wi-Fi configuration per site is different, one UI group must be created for each site.

For each site, the tenant account administrator has to do the following:

1. Create a new UI group for each site.

2. Configure the UI group with Wi-Fi settings specific to each site.

3. Map the Instant APs in each site to the respective UI group.

Point to Note:

- One user-defined UI group is created for each site.
- For any new site with a different VLAN ID, the tenant account administrator must create a new UI group.
- If a configuration change is required at all sites, the tenant account administrator must manually edit each UI group as each group is independent of the other. For example, to change the Wi-Fi SSID name from **WiFi_CE** to **WiFi_Secure_CE**, the tenant account administrator must edit UI group.

Deployment Using Template Groups

The MSP can configure Instant APs at both sites using template groups. The tenant account administrator can create a single template group for both sites with a variable file that differentiates the VLAN setting per device.

NOTE

Template groups are not supported at the MSP level. However, template groups can be defined and managed at each tenant account individually.

For both sites, the tenant account administrator has to do the following:

1. Create one tenant template group.

2. Configure the newly created template group by uploading a base configuration with the **WiFi_CE** setting and a variable for the SSID VLAN.

3. Upload a variable file with unique entries for each Instant AP. For the Instant APs part of **Site 1**, the VLAN variable value is 20. For the Instant APs part of **Site 2**, the VLAN variable value is 40.

4. Map **Site 1** and **Site 2**Instant APs to the common template group.

Points to Note:

- One tenant template group is created for both sites.
- For every additional site with a different VLAN ID, the same template group can be used with a modified variable file.
- If a configuration change is required at all sites, the common template group can be updated and pushed to all sites. For example, to change the Wi-Fi SSID name from **WiFi_CE** to **WiFi_Secure_CE**, the tenant account administrator can edit the common template group and push the configuration changes to all sites.

Hybrid MSP Deployment Model (Deployment Model 3)

In this model, Aruba Central supports a hybrid deployment model for the MSP. The MSP can use the following deployment models in conjunction to manage the end-customers' network:

- MSP Owns Devices and Subscriptions (Deployment Model 1)—The MSP owns both the devices and subscriptions. The MSP acquires the tenants and uses the Aruba Central MSP mode to manage the tenant's network and monitors multiple tenant accounts using the MSP Dashboard.
- End-Customer Owns Both Devices and Subscriptions But MSP Manages (Deployment Model 2)—The MSP manages end-customer's network in which the end-customer owns both the devices and subscriptions. The MSP uses the Aruba Central Standard Enterprise mode to manage the network and the MSP administrator uses the **Switch Customer** option to navigate between different end-customer accounts.

NOTE

In this deployment model if the end customer owns both devices and subscriptions, the account type must be Standard Enterprise Mode. Aruba recommends that you contact your Aruba Central sales representative or the Aruba Central Support team if you are an MSP proposing this model to your end-customer.

Chapter 6
Getting Started with MSP Solution

Before you get started with your onboarding and provisioning operations, we recommend that you browse through the following topics to know the key capabilities of Aruba Central MSP Solution.

- Operational Modes and Interfaces
- About the Managed Service Portal User Interface

Navigate through the following steps to view help pages that describe the onboarding and provisioning procedures for MSP and tenant accounts:

1. Set up your Aruba Central account
2. Accessing Aruba Central Portal
3. Enabling Managed Service Mode
4. Onboard devices
5. Add subscription keys
6. Create groups
7. Provision tenant accounts
8. Assign devices to tenant accounts
9. Assign subscription to devices and services
10. Configure users and roles
11. Customize tenant account view
12. Add Certificates
13. Monitor tenant accounts

Creating an Aruba Central Account

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

Zones and Sign Up URLs

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

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

Table 5: *Sign Up URLs & Apps*

Regional Cluster	Sign Up URL	Available Apps
US-1	https://portal.central.arubanetworks.com/signup	**Network Operations**
US-2	https://portal-prod2.central.arubanetworks.com/signup OR https://signup.central.arubanetworks.com/	■ **Network Operations** ■ **ClearPass Device Insight**
Canada-1	https://portal-ca.central.arubanetworks.com/signup	**Network Operations**
China-1	https://portal.central.arubanetworks.com.cn/signup	**Network Operations**
EU-1	https://portal-eu.central.arubanetworks.com/signup	■ **Network Operations** ■ **ClearPass Device Insight**
APAC-1	https://portal-apac.central.arubanetworks.com/signup	**Network Operations**
APAC-EAST1	https://portal-apaceast.central.arubanetworks.com/signup	**Network Operations**
APAC-SOUTH1	https://portal-apacsouth.central.arubanetworks.com/signup	**Network Operations**

Signing up for an Aruba Central Account

To sign up for an Aruba Central account:

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

Table 6: *Registration Workflow*

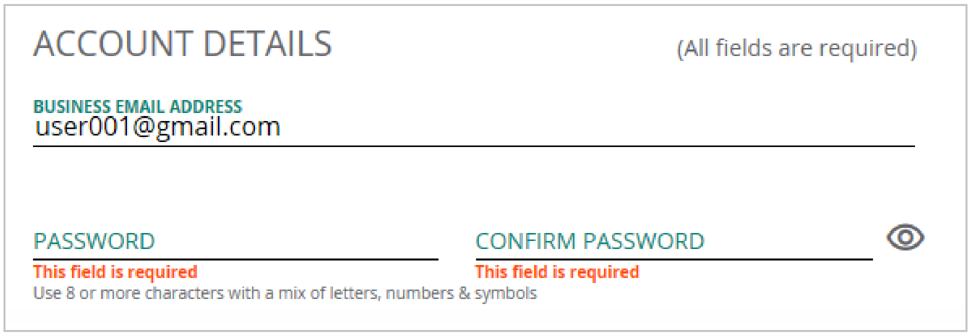
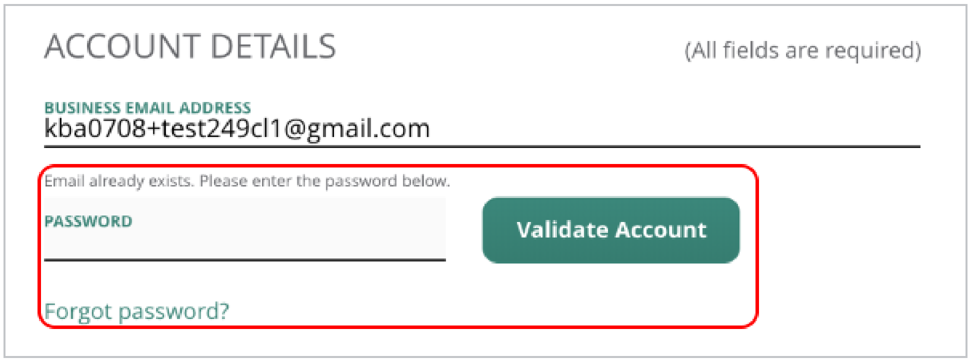
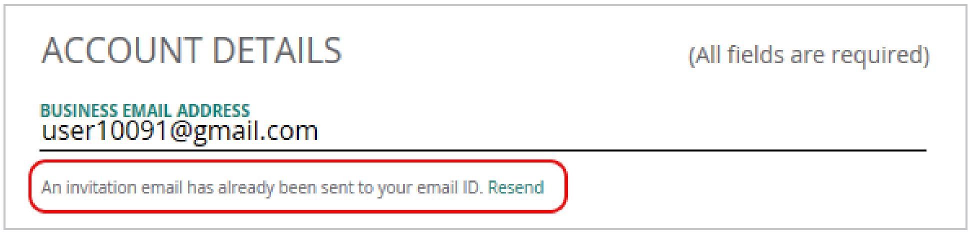
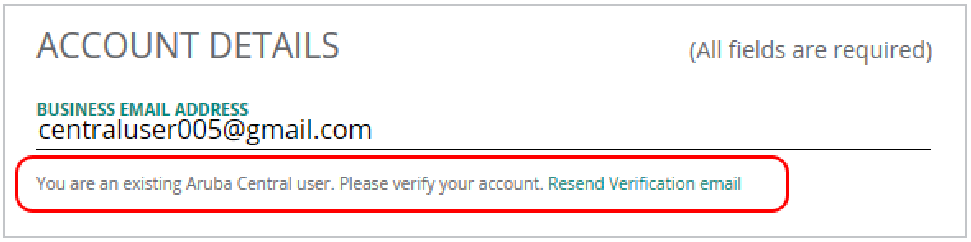
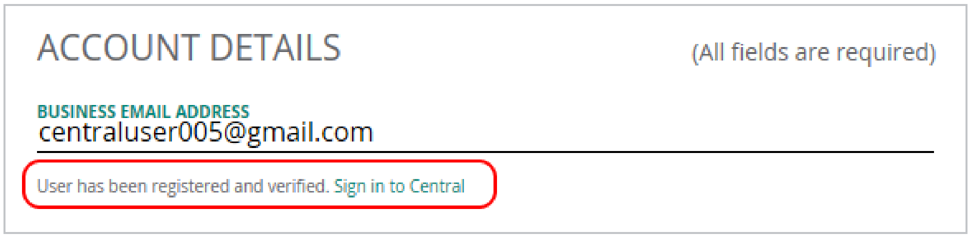
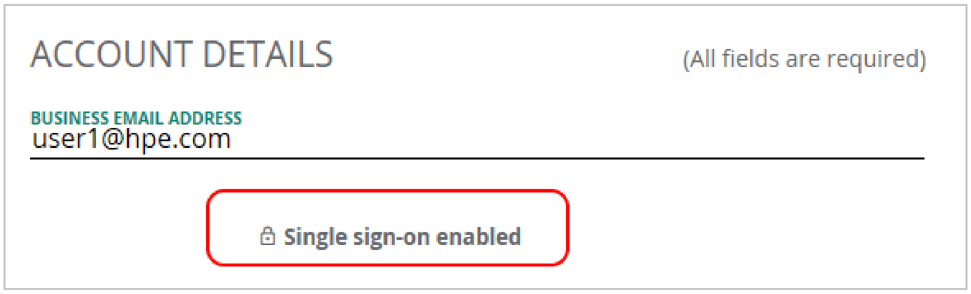
If...	Then...
If you are a new user:	The **Registration** page prompts you to create a password. To continue with the registration, enter a password in the **Password** and **Confirm Password** fields.  ACCOUNT DETAILS (All fields are required) BUSINESS EMAIL ADDRESS user001@gmail.com PASSWORD This field is required CONFIRM PASSWORD This field is required Use 8 or more characters with a mix of letters, numbers & symbols
If you are an existing Aruba customer, but you do not have an Aruba Central account:	The **Registration** page displays the following message: **Email already exists. Please enter the password below**. To continue with registration, validate your account: 1. Enter the password. 2. Click **Validate Account**. **NOTE:** If you do not remember the password, click **Forgot Password** to reset the password.  ACCOUNT DETAILS (All fields are required) BUSINESS EMAIL ADDRESS kba0708+test249cl1@gmail.com Email already exists. Please enter the password below. PASSWORD Validate Account Forgot password?
If your email account is already registered with Aruba, but you do not have an Aruba Central account:	
If you are invited to join as a user in an existing Aruba Central customer account:	The **Registration** page displays the following message: **An invitation email has already been sent to your email ID. Resend**. To continue with the registration: 1. Go to your email box and check if you have received the email invitation. 2. If you have not received the email invitation, go to the **Registration** page and click **Resend**. A registration invitation will be sent your account. 3. Click the registration link. The user account is validated. 4. Complete the registration on the **Sign Up** page to sign in to Aruba Central.  ACCOUNT DETAILS (All fields are required) BUSINESS EMAIL ADDRESS user10091@gmail.com An invitation email has already been sent to your email ID. Resend

Table 6: *Registration Workflow*

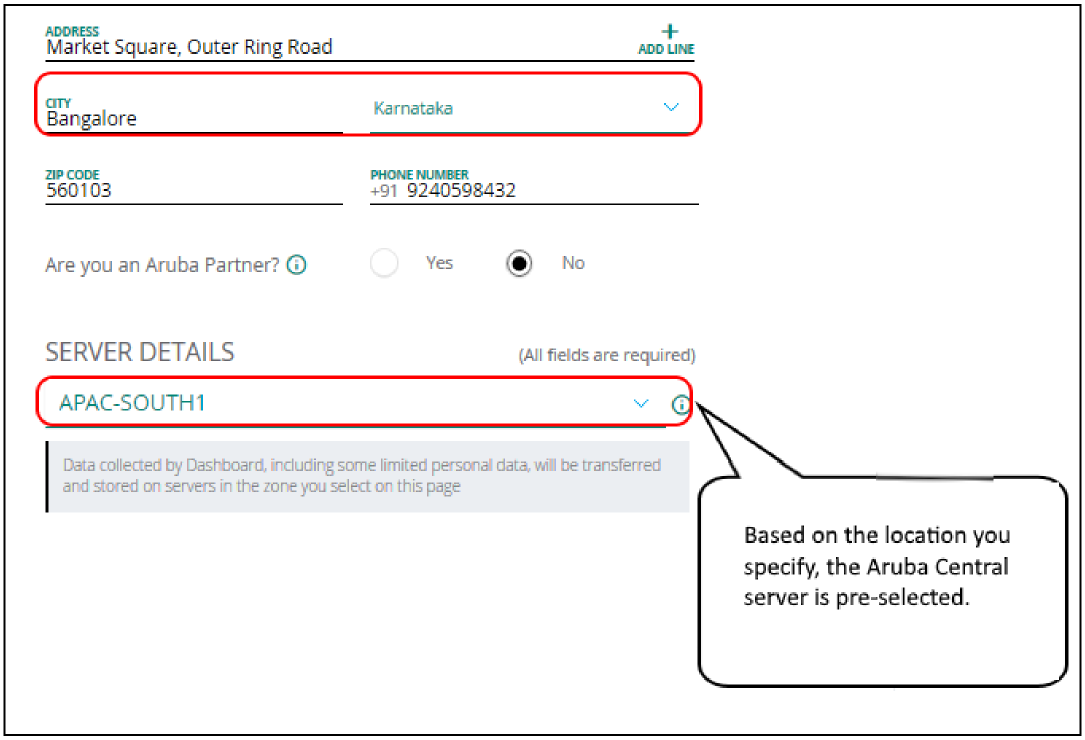
If...	Then...
If you are a registered user of Aruba Central and have not verified your email yet:	The **Registration** page displays the following message: **You are an existing Aruba Central user. Please verify your account. Resend Verification email**. To continue: 1. Go to your email box and check if you have received the email invitation. 2. If you have not received the email invitation, go to the **Registration** page and click **Resend Verification email**. A registration invitation will be sent your account. 3. Click the account activation link. 4. After the email verification is completed successfully, click **Log in** to access Aruba Central.  ACCOUNT DETAILS (All fields are required) BUSINESS EMAIL ADDRESS centraluser005@gmail.com You are an existing Aruba Central user. Please verify your account. Resend Verification email
If you are already a registered user of Aruba Central and have verified your email:	The **Registration** page displays the following message: **User has been registered and verified. Sign in to Central**. Click **Sign in to Central** to skip the registration process and access the Aruba Central portal.  ACCOUNT DETAILS (All fields are required) BUSINESS EMAIL ADDRESS centraluser005@gmail.com User has been registered and verified. Sign in to Central
If your email address is in the **arubanetworks.com** or **hpe.com** domain:	The **Single Sign-On** option is enabled. You can use your respective Aruba or HP Enterprise credentials to log in to your Aruba Central account after the registration.  ACCOUNT DETAILS (All fields are required) BUSINESS EMAIL ADDRESS user1@hpe.com 🔒 Single sign-on enabled

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

6. Specify if you are an Aruba partner.

7. Ensure that you select an appropriate zone. The **Registration** page displays a list of zones in which the Aruba Central servers are available for account creation. Based on the country you select, the Aruba Central

server is automatically selected. If you want your account and Aruba Central data to reside on a server from another zone, you can select an Aruba Central server from the list of available servers.



ADDRESS
Market Square, Outer Ring Road

CITY
Bangalore

Karnataka

ZIP CODE
560103

PHONE NUMBER
+91 9240598432

Are you an Aruba Partner? ○ Yes ● No

SERVER DETAILS (All fields are required)

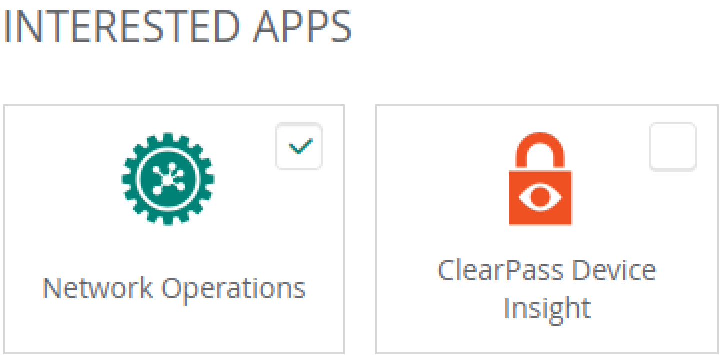
APAC-SOUTH1

Data collected by Dashboard, including some limited personal data, will be transferred and stored on servers in the zone you select on this page

Based on the location you specify, the Aruba Central server is pre-selected.

8. From the **Interested Apps** section, select the app(s) that you want to pre-provision. You must select at least one app to continue:

- **Network Operations**
- **ClearPass Device Insight**



INTERESTED APPS

☑ Network Operations

□ ClearPass Device Insight

See Table 5 for the app(s) available in the zone in which you are signing up.

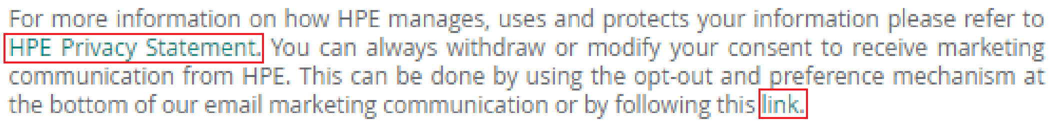
NOTE

If you are interested in evaluating the Aruba Central MSP solution, select only the **Network Operations** app.

9. Select the **I agree to the Terms and Conditions** check box.

10. Set a preferred mode of communication for receiving notifications about Aruba products and services.

11. Optionally, to read about the the privacy statement, click the **HPE Privacy Statement** link. To opt out of marketing communication, you can either click the unsubscribe link available at the bottom of the email or click the link as shown in the following figure:



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

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

Accessing Aruba Central Portal

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

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

Login URLs

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

Table 7: *Cluster Zone— Portal URLs*

Regional Cluster	Sign Up URL
US-1	https://portal.central.arubanetworks.com/signup
US-2	https://portal-prod2.central.arubanetworks.com/signup OR https://signup.central.arubanetworks.com/
Canada-1	https://portal-ca.central.arubanetworks.com/signup
China-1	https://portal.central.arubanetworks.com.cn/signup
EU-1	https://portal-eu.central.arubanetworks.com/signup
APAC-1	https://portal-apac.central.arubanetworks.com/signup
APAC-EAST1	https://portal-apaceast.central.arubanetworks.com/signup
APAC-SOUTH1	https://portal-apacsouth.central.arubanetworks.com/signup

Logging in to Aruba Central

To log in to Aruba Central:

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

NOTE

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

5. Enter the password.

NOTE

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

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

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

Changing Your Password

To change your Aruba Central account:

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

NOTE

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

Logging Out of Aruba Central

To log out of Aruba Central:

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

Enabling Managed Service Mode

The **Enable MSP** option is only available if the following conditions are met:

- You sign into Aruba Central as an administrator.
- The Aruba Central account is only subscribed to the Network Operations app. If the account has multiple subscriptions, such as both Network Operations and ClearPass Device Insight, the **Enable MSP** option is not available.
- You access the **User Settings** icon from the Network Operations app and not the Account Home page.

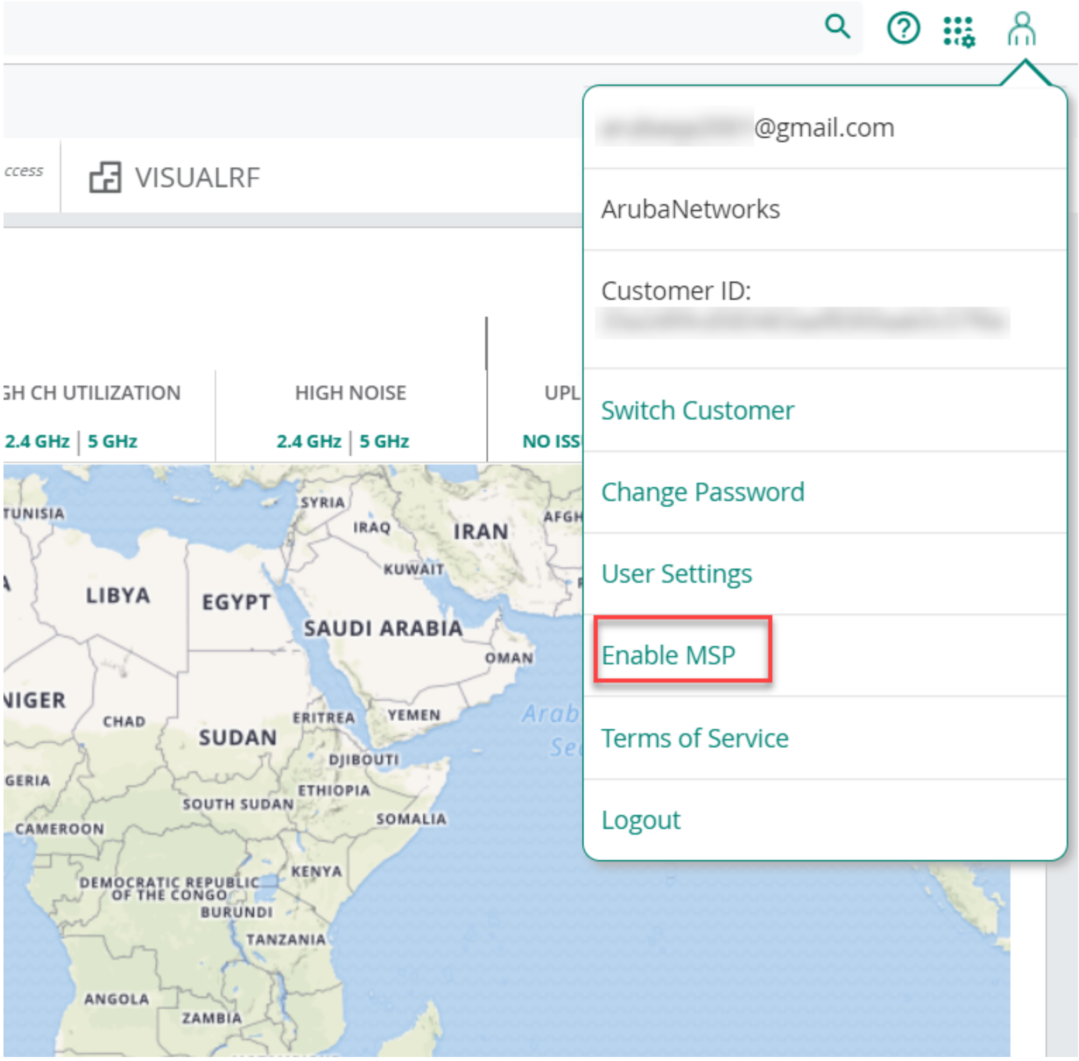
To enable MSP mode, perform the following steps:

1. Log in to your Aruba Central account as an administrator.
2. Launch the **Network Operations** app.

   If you have subscriptions to other apps, enabling MSP mode is not supported, and the **Enable MSP** option is not available. Create a new Aruba Central account with the Networks Operations app and contact Aruba Technical Support to migrate devices and licenses to the new account.

3. Click the user icon 👤.
4. Click **Enable MSP**.

Figure 10 *Click Enable MSP*



5. In the **Managed Service Mode** pop-up window, click **Request Access**.
6. In the **Managed Service Mode** form, enter the details and click **Submit**.
7. In the confirmation pop-up window, click **Close**.

NOTE

After you submit the request and before you get a confirmation from Aruba, clicking the user icon displays the **Enable MSP** option as grayed out. A message is displayed when you hover over the **Enable MSP** option.

8. After you get a confirmation from Aruba that the request to enable MSP mode has been approved, click the user icon and then click **Enable MSP**.
9. In the **Managed Service Mode** pop-up window, click **Enable**.

   The Aruba Central account gets converted into MSP mode. The page is automatically redirected to the MSP Dashboard view.

Disabling the Managed Service Mode

If you do not want to use **Managed Service Mode**, you can switch to the Standard Enterprise mode. Delete all tenant account data before you proceed.

To disable Managed Service mode:

1. Click the user icon .
2. Click **Disable MSP**.

   The option is grayed out if tenant account data exists.
3. In the **Managed Service Mode** pop-up window, click **Disable Managed Service Mode**.

MSP Mode Enablement Scenarios

You can convert the standard enterprise mode in the Network Operations app to MSP mode. Only the Network Operations app supports the MSP mode and it must be the only app running in Aruba Central for enabling the MSP mode. The following is a list of possible scenarios you might encounter while subscribing to the Network Operations app.

- **Scenario 1**: You sign up for an Aruba Central account to evaluate the Network Operations app. After that, you also sign up for evaluating the ClearPass Device Insight app. Subsequently, you wish to enable MSP mode on the Network Operations app. The MSP Mode conversion option is not allowed. As a workaround, create another Aruba Central account with only the ClearPass Device Insight app running to evaluate ClearPass. You can then request for the original Aruba Central account to be converted to MSP mode, provided the only app running in that account is the Network Operations app.
- **Scenario 2**: You sign up for an Aruba Central account to evaluate the ClearPass Device Insight app. After that, you also sign up for evaluating the Network Operations app. Subsequently, you wish to enable MSP mode on the Network Operations app. The MSP Mode conversion option is not allowed. As a workaround, create another Aruba Central account with only the Network Operations app running. You can then request for this account to be converted to MSP mode. You can continue to test both the ClearPass Device Insight app and the Network Operations app in the original Aruba Central account.
- **Scenario 3**: You sign up for an Aruba Central account to evaluate the ClearPass Device Insight app. After that, you also sign up for evaluating the Network Operations app in standard enterprise mode in the same account. This mode of operation is supported.
- **Scenario 4**: You sign up for an Aruba Central account to evaluate the Network Operations app. After that, you also sign up for evaluating the ClearPass Device Insight in the same Aruba Central account. If you are running the Network Operations app in the standard enterprise mode, this mode of operation is supported.

Onboarding Devices

Aruba Central supports the following options for adding devices.

- If you are an evaluating user, you must manually add the serial number and MAC address of the devices that you want to manage from Aruba Central. For more information, see Adding Devices (Evaluation Account) on page 40.
- If you are a paid subscriber, Aruba Central retrieves devices associated with your purchase order from Activate. Set up a sync to import devices from the Activate database, see Adding Devices (Paid Subscription) on page 40.

This section includes the following topics:

- Adding Devices (Evaluation Account)
- Adding Devices (Paid Subscription)
- Manually Adding Devices

Adding Devices (Evaluation Account)

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

Using the Initial Setup Wizard

1. In the **Add Devices** tab of the Initial Setup wizard, click **Add Device**.
2. Enter the serial number of MAC address of your devices.

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

Using the Device Inventory Page

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

   The **Device Inventory** page is displayed.
2. Click **Add Devices**.

   The **Add Devices** pop-up window is displayed.
3. Enter the serial number and the MAC address of each device.

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

Adding Devices (Paid Subscription)

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

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

- In the Initial Setup Wizard
- From the Device Inventory Page

In the Initial Setup Wizard

1. Ensure that you have added a subscription key and click **Next**.
2. In the **Add Devices** tab, enter the serial number and MAC address of one device from your purchase order.

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

From the Device Inventory Page

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

   The **Device Inventory** page is displayed.

NOTE

Aruba Central imports only devices associated with your Central account from Activate.

2. Do one of the following:

- Click **Sync Devices**. Enter the serial number and MAC address and click **Add Device**.
- Click **Add Devices** to manually add devices by entering the MAC address and serial number of each device.
- If you are a paid subscriber, you can add devices using a CSV file. Click **Import Via CSV** and select the CSV file. For a sample CSV file, click **Download sample CSV file**.

NOTE

Manual addition of devices using a CSV file is restricted to 100 devices or to the number of available device management tokens. An error message is displayed if more than 100 devices are imported using the CSV file. You can view the status of the CSV upload in the **Account Home** > **Audit Trail** page.

3. Review the devices in your inventory.
4. Perform the following options:

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

Manually Adding Devices

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

- Adding Devices Using MAC address and Serial Number on page 41
- Adding Devices Using Activate Account on page 42
- Adding Devices Using Cloud Activation Key on page 42

NOTE

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

Adding Devices Using MAC address and Serial Number

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

To add devices using MAC address and serial number, use one of the following methods:

- In the Initial Setup Wizard
- From the Device Inventory Page

In the Initial Setup Wizard

If you are using the Initial Setup wizard:

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

From the Device Inventory Page

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

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

   The **Device Inventory** page is displayed.
2. Do one of the following:
   - Click **Add Devices** to manually add devices by entering the MAC address and serial number of each device.
   - If you are a paid subscriber, you can add devices using a CSV file. Click **Import Via CSV** and select the CSV file. For a sample CSV file, click **Download sample CSV file**.

NOTE

Manual addition of devices using a CSV file is restricted to 100 devices or to the number of available device management tokens. An error message is displayed if more than 100 devices are imported using the CSV file. You can view the status of the CSV upload in the **Account Home** > **Audit Trail** page.

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

NOTE

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

Adding Devices Using Activate Account

NOTE

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

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

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

To add devices from your Activate account:

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

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

Adding Devices Using Cloud Activation Key

NOTE

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

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

Locating Cloud Activation Key and MAC Address

To know the cloud activation key:

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

Adding Devices Using Cloud Activation Key

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

   The **Device Inventory** page is displayed.
2. Click **Advanced** and select **With Cloud Activation Key**. The **Cloud Activation Key** pop-up window opens.
3. Enter the cloud activation key and MAC address of the device.
4. Click **Add**.

NOTE

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

Managing Subscription Keys

The **Key Management** menu option in the **Global Settings** app allows you to view and track subscriptions key.

NOTE

Users having roles with **Modify** permission can add subscription keys or assign licenses. Users having roles with **View Only** permission can only view the Subscription Assignment module.

Viewing Subscription Key Details

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

1. From the **Account Home** page, under **Global Settings**, click **Key Management**.

   The **Key Management** page is displayed.

Table 8 describes the contents of the **Manage Keys** table on the **Key Management** page.

Table 8: *Subscription Key Details*

Data Pane Item	Description
Keys	Subscription key number.
Type	Type of the subscription. Aruba Central supports the following types of subscriptions: ■ Device subscriptions—The device subscription allows you to avail services such as device onboarding, configuration, management, monitoring, and reports. The device subscriptions can be assigned only to the devices managed by Aruba Central. ■ Service subscriptions—Aruba Central supports application services that you can run on the devices provisioned in your setup. For example, if you have Instant APs with 6.4.4.4-4.2.3.0 or later, you can assign a service subscription for Presence Analytics. ■ Gateway Subscriptions—Aruba Central supports a separate set of subscriptions for configuring and managing SD-WAN gateways. The Gateway subscriptions are marked as **Foundation-<device>**; for example, Foundation-70XX. ■ Virtual Gateways—Aruba Central supports a separate set of subscriptions for configuring and managing Virtual Gateways. The Virtual Gateway subscriptions are prefixed with a **VGW-<bandwidth>**; for example, VGW-500MB.
Expiration Date	Expiration date for the subscription key.
Quantity	Number of license tokens available for a subscription. Each Aruba Central subscription holds a specific number of tokens. For example, when a subscription is assigned to a device, Aruba Central binds the device with a token from the existing pool of subscriptions.
Status	Status of the subscription key. For example, if you are a trial user, Aruba Central displays the status of subscription key as **Evaluation**.
Apps	Name of the application.

The **Key Management** page also shows the available and assigned device subscriptions. For the device subscriptions, the page shows the subscriptions per APs, switches, and gateways.

Adding a Subscription Key

To add a subscription key:

1. In the **Account Home** page, under **Global Settings**, click **Key Management**.

   The **Key Management** page is displayed.

2. Enter your subscription key.
3. Click **Add Subscription**. The subscription key is added to Aruba Cloud Platform and the contents of the subscription key are displayed in the **Manage Keys** table.
4. Review the subscription details.

Managing MSP Subscriptions

Aruba Central in MSP mode supports the following types of subscriptions:

- Device Management subscriptions—Allows you to manage and monitor your Access Points and Switches from Aruba Central MSP mode. The device management subscriptions can be assigned only to the devices managed by Aruba Central.

- Services Management subscriptions—Allows you to enable value-added services on the APs managed from Aruba Central MSP mode. For example, if you have APs, you can assign a services management subscription for Presence Analytics.

A subscription key is a 14-character alphanumeric string; for example, **PQREWD6ADWERAS**. Subscription keys allow your devices to be managed by Aruba Central. To use Aruba Central for managing and monitoring your devices and services, you must ensure that you have a valid subscription key. Subscription keys are used to enable managing the devices and network in addition to managing the cloud service application services.

NOTE

The subscription keys are not mapped directly to devices. Before assigning a subscription key to a device, the system only checks whether there are subscriptions available in the pool for the device.

All subscription keys added to the MSP account goes to a subscription pool. Devices are subscribed from this MSP subscription pool. Subscriptions can be assigned to devices, and these devices are mapped to customer accounts. In the MSP mode, all the hardware and subscriptions are owned by the MSP. The MSP temporarily assigns devices and their corresponding subscriptions to customers for the duration of the managed service contract. When the contract ends, the devices and the subscriptions are returned back to the common pool of resources of the MSP and can be reassigned to another customer.

You can either enable automatic assignment of subscriptions or manually assign subscriptions for Access Points and Switches added in Aruba Central MSP mode.

Enabling Automatic Device Management Subscriptions

If you as an MSP administrator want to enable automatic assignment of subscriptions to the devices mapped to your customer accounts, note the following points:

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

To enable automatic assignment of subscriptions from the Initial Setup Wizard:

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

To enable automatic assignment of subscriptions from the Subscription Assignment page:

1. In the **Account Home** page, under **Global Settings**, click **Subscription Assignment**.

   The **Subscription Management** page is displayed.

2. Under **Device Management Subscriptions**, toggle the **Auto Subscribe** slider to ON. All the devices in your inventory are selected for automatic assignment of subscriptions. You can edit the list by clearing the existing selection and re-selecting devices.

NOTE

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

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

Enabling Manual Device Management Subscriptions

You can disable Auto Subscription and manually assign subscriptions to devices. Subscriptions can be assigned only for devices which are mapped to a customer account.

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

1. In the **Account Home** page, under **Global Settings**, click **Subscription Assignment**.

   The **Subscription Management** page is displayed.

2. Ensure that the **Auto Subscribe** toggle is turned off.

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

   - Automatic assignment of subscription for all the existing customers, including the MSP devices, are disabled.
   - All device subscriptions assigned to devices are preserved.
   - Devices must be assigned to customer accounts before assigning a subscription to it. If a subscription is assigned to a device that is not mapped to any specific customer account, Aruba Central displays the following error message: **Please assign this device to a customer before subscribing it. customer assignment can be performed in the Device Inventory page**.

3. Select the devices to which you want to assign subscriptions.
4. Click **Update Subscription**.

Assigning Services Management Subscriptions

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

To assign a services management subscription, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Subscription Assignment**.

   The **Subscription Management** page is displayed.

2. Select the service subscription that you want to enable on a device. The available services are:

   - Cloud Guest
   - Presence Analytics
   - UCC

NOTE

Clarity service is deprecated. Wi-Fi Connectivity dashboard has replaced Clarity. The Wi-Fi Connectivity dashboard displays global connectivity details and insights. You do not require a separate service subscription to view the **Wi-Fi**

Connectivity dashboard.

Although you can assign or unassign **Clarity** service subscription, **Clarity** does not monitor deployments or detect network performance issues.

3. Under **Services Management Subscriptions**, select the AP from the table on the right.
4. Drag and drop the device to the network service selected in the table on the left.

Assigning Subscription to a Device in a Customer Account

You can only assign subscription for devices which have a customer assigned.

1. Go to **Accounts Home**.
2. Under **Global Settings**, click **Subscription Assignment**.

   The **Subscription Assignment** page is displayed. You can see the **Subscribed** status as either **Yes** or **No** for the devices.
3. Enable the checkbox for devices for which you want to enable subscription. Use the filters in the **Customer** column to filter specific customer devices.
4. Specify a set of devices for subscription assignment.
5. Click the select button for the devices to which you want assign subscriptions and click on **Update Subscription**.

   After you are done, the subscription status changes to **Yes**.

Removing or Reassigning a Device Subscription from a Device

1. In the **Account Home** page, under **Global Settings**, click **Subscription Assignment**. Ensure that the **Auto Subscribe** toggle is turned off. The devices that have the subscriptions assigned are selected and highlighted in green.
2. Clear the **Subscribed** check box for the device from which you want to unassign the subscription and click **Update Subscription**. The **Confirm Action** pop-up window with the **Do you want to modify the subscription for selected devices** message opens.
3. Click **Yes** to confirm. The subscription is unassigned and the **Subscribed** status for the device is marked as **No** in the devices table.
4. You can go ahead and assign the device to another customer account.

Removing a Services Management Subscription from a Device

To remove network service subscription from a device:

1. In the **Account Home** page, under **Global Settings**, click **Subscription Assignment**.
2. Under **Services Management Subscriptions**, select a subscription from the table on the left.
3. From the table on the right, select the devices from which you want to unassign the subscription.
4. Click **Batch Remove Subscriptions**. The subscription is unassigned from the selected devices.

Acknowledging Subscription Expiry Notifications

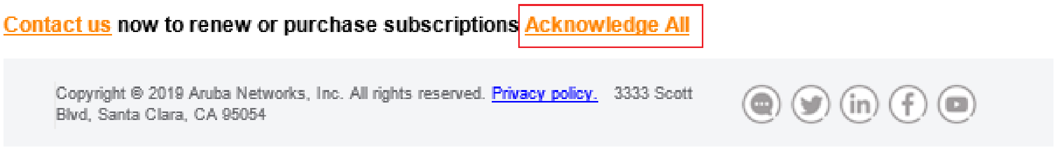
In the **Account Home** page, under **Global Settings**, click **Key Management**. The **Key Management** page displays the expiration date for each subscription.

As the subscriptions expiration date approaches, users receive expiry notifications. The users with evaluation subscription receive subscription expiry notifications on the 30th, 15th and 1 day before the subscription expiry and on day 1 after the subscription expires.

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

Acknowledging Notifications through Email

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



Contact us now to renew or purchase subscriptions Acknowledge All

Copyright © 2019 Aruba Networks, Inc. All rights reserved. Privacy policy. 3333 Scott Blvd, Santa Clara, CA 95054

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 user logs in to Aruba Central.

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

Renewing Subscriptions

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

Groups in the MSP Mode

MSP groups are UI groups mapped to the default UI groups in the tenant account. If a tenant account is associated to a specific group in the MSP mode, the configuration changes to the devices associated with this tenant account are pushed only to the **default** group in the tenant account view. However, MSP administrators can create more groups for a specific tenant by drilling down to a tenant account.

NOTE

Template groups are not supported in the MSP mode. However, template groups can be defined and managed at each tenant account individually.

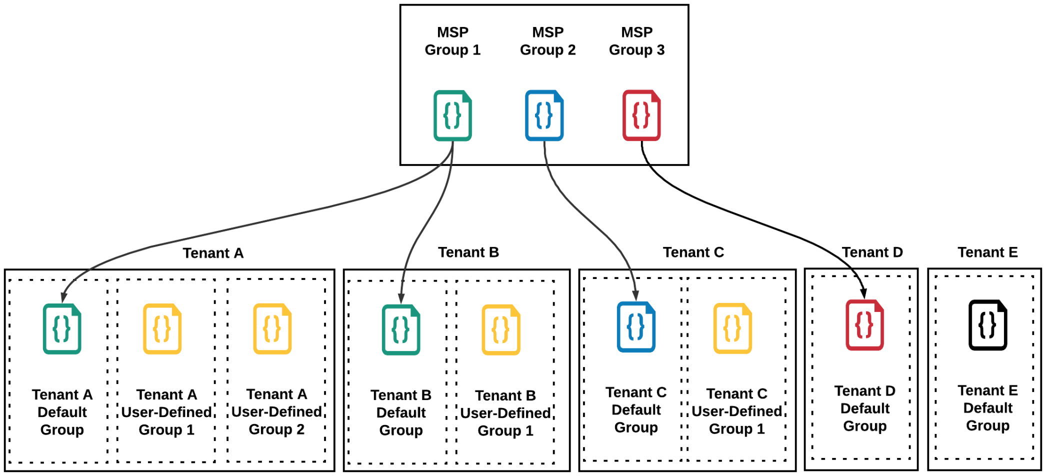
MSP Group Illustration

As shown in the following figure, tenant A and tenant B are mapped to MSP group 1. The default group configuration for these tenants is inherited from MSP group 1 configuration. Tenant A has two additional user-defined groups that are independent of MSP group 1 configuration. Tenant B has one additional user-defined group that is independent of MSP group 1 configuration.

Tenant C is mapped to MSP group 2 configuration. Its default group configuration is inherited from MSP group 2. It also has one additional user-defined group that is independent of MSP group 2 configuration.

Tenant D has only one default group and its configuration is inherited from MSP group 3. Tenant E is not mapped to any MSP group. Its default group configuration is independent of any MSP group configuration. It can have additional user-defined groups as well, if required.

Figure 11 *MSP Groups*



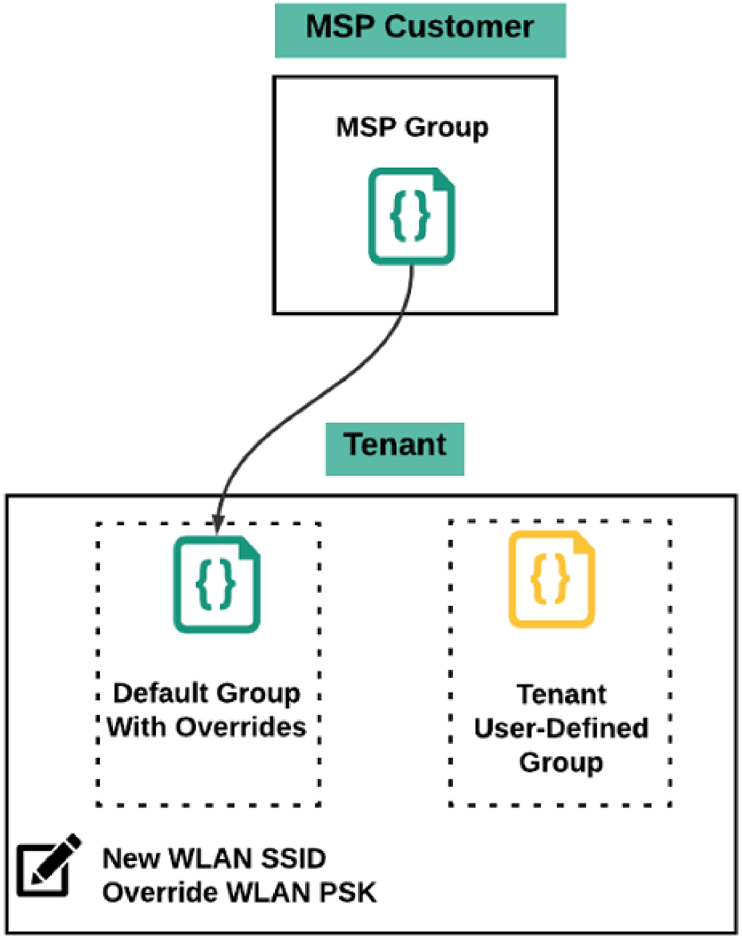
Tenant Default Group Overrides

If a tenant is mapped to an MSP group, the configuration of its default group is inherited from the MSP group it is mapped to. Once mapped, except for any newly created WLAN SSID and WLAN PSK, other configurations are overridden.

As shown in the following figure, the mentioned configuration options are allowed on a tenant default group that is mapped to an MSP group:

- Creating a new WLAN SSID.
- Overriding the WLAN PSK for a WLAN inherited from an MSP group.

Figure 12 *Default Group Overrides*



Creating an MSP UI Group

To manage device configuration using UI configuration containers in Aruba Central, you can create a UI group and assign devices.

To create an MSP UI group:

1. From the **Network Operations** app, filter **All Groups**.
2. Under **Maintain**, click **Organization** to display the **Groups** dashboard.
3. To create a new group, click **New Group**.

   The **Create New Group** pane is displayed.
4. Enter a name for the group.
5. Configure a password to restrict group access to authorized users only.
6. Click **Add Group**.

About Provisioning Tenant or Customer Accounts

After adding a device in the MSP mode, the device must be mapped to a tenant account for device management and monitoring operations.

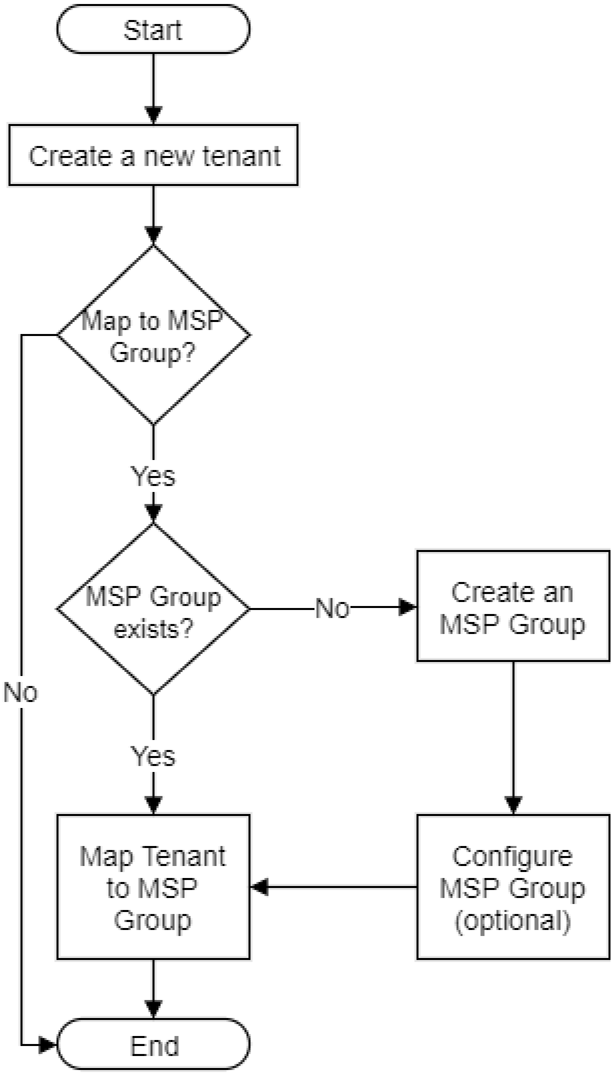
With MSP mode enabled, the MSP administrator manages the creation and deletion of tenant accounts. After a tenant account is created, the MSP administrator can add tenant users to the account. To create a tenant user, the MSP administrator must provide a valid email address for the user. A verification email is sent to this email address. Tenant users have access to their individual tenant account only. Tenant users do not have access to other tenant accounts managed by the MSP.

The group associated to the tenant account in the MSP mode shows up as the default group for tenant account users. In the MSP mode, all configuration changes made to the group associated to the tenant account are applied to the default group on the tenant account.

Flowchart for Tenant Account Mapping in MSP

The following flowchart displays a visual representation of how you can create a tenant account and map it to an MSP group.

Figure 13 *Tenant Account Mapping to an MSP Group*



Creating a Tenant Account and Mapping to an MSP Group

To add a tenant account, complete the following steps:

1. From the **Network Operations** app, filter **All Groups**.
2. Under **Manage**, click **Overview**.

   The **Dashboard** is displayed.
3. Click **Add New Customer**.

   The **Add Customer** page is displayed.
4. Enter the name of the tenant in the **Customer Name** text box. The MSP customer name can be a maximum of 70 single byte characters. All special characters, ASCII, and Unicode are allowed.
5. Enter the description of the tenant in the **Description** text box. The MSP customer description field can be a maximum of 32 single byte characters. All special characters, ASCII, and Unicode are allowed.
6. If you want to associate the tenant to a group, click the **Add to group** toggle switch.
7. From the **Group** drop-down list, select a group to which you want to assign the tenant.

NOTE

The group associated to the tenant account in the MSP mode shows up as the default group for tenant account users. In the MSP mode, all configuration changes made to the group associated to the tenant account are applied to the default group on the tenant account.

8. If you want to prevent the users of the tenant account from modifying SSID settings of the device group, select the **Lock SSID** check box.
9. Click **Save**.

NOTE

For a visual representation of the procedure, click here.

Usage Guidelines for Creating Tenant Account

- If the tenant account provisioning fails, the task is marked as **Provision Failed** in the UI and **PROVISION_FAILED** in the **[GET] /msp/v1/customers** API response. To view the task status in the UI, under **Manage**, click **Overview** to display the **Dashboard** page. Click the **Customers** tab. If the provisioning fails, you can delete the tenant account and try again.
- Tenant account users can only view reports generated for the default group. The administrators of a specific tenant account can drill down to the tenant account and generate reports for the default group.
- If cloud guest provisioning fails, cloud guest features for the tenant may get impacted. In such instances, contact Aruba Central Technical Support.

Viewing Tenant Account Details

To view the tenant account details, perform the following steps:

1. From the **Network Operations** app, filter **All Groups**.
2. Under **Manage**, click **Overview** to display the **Dashboard** page.
3. Click the **Customers** tab.
4. Hover over the tenant account and click **expand**.

Figure 13 describes the contents of the window.

Table 9: *Tenant Account Details*

Data Pane Item	Description
Customer ID	Unique ID of the tenant account. The ID can be in one of the following formats: ■ Numerical format ■ UUID format
Customer Created	Date and time at which the tenant account was created.
MSP Group	The group assigned to the tenant account.
Customer Name	Name of the tenant account.
Description	Description of the tenant account.
Devices	Graphical representation of the devices assigned to the tenant account.
Subscriptions	Graphical representation of the network service and gateway subscriptions assigned to the tenant account.

NOTE

For a visual representation of the procedure, click here.

Editing a Tenant Account

When editing the group associated with the MSP customer or tenant, the default group configuration of the tenant account is also impacted. To edit a tenant account, complete the following steps:

1. From the **Network Operations** app, filter **All Groups**.
2. Under **Manage**, click **Overview**.

   The **Dashboard** is displayed.
3. Hover over the tenant account that you want to edit and click **edit**.
4. Modify the account details.

NOTE

If you want to associate the tenant account to a different group, turn on the **Add to group** toggle switch and select a group.

5. Click **Save**.

NOTE

For a visual representation of the procedure, click here.

Deleting a Tenant Account

To delete a tenant account, complete the following steps:

1. From the **Network Operations** app, filter **All Groups**.
2. Under **Manage**, click **Overview**.

   The **Dashboard** is displayed.
3. Hover over the tenant account that you want to delete and click **delete**.
4. Click **Yes** to confirm the action.

If the tenant account deletion fails, the provisioning status is marked as **Delete Failed** in the UI and **DELETE_FAILED** in the **[GET] /msp/v1/customers/{customer_id}** API response. To view the task status in the UI, go to **Monitoring & Reports** > **Customers** table.

For a visual representation of the procedure, click here.

Assigning Devices to Tenant Accounts

To assign devices to tenant accounts, complete the following steps:

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

   A list of devices provisioned in the MSP mode is displayed.
2. Select one or several devices from the table. To select multiple devices, press and hold the **Ctrl** key and select the devices.

   The **Assign Customer** button is displayed under the table.
3. Click **Assign Customer**.

   A window showing a list of tenant accounts provisioned in the MSP mode is displayed.
4. Select the tenant account to which you want to assign the device.

   The groups associated with the tenant accounts are displayed.
5. Click **Assign Device (s)**.
6. Click **Yes** when prompted for confirmation.

System Users and User Roles in MSP Mode

The **Users and Roles** page under **Global Settings** enables you to view, create, and modify users and roles. The **Users and Roles** page has two tabs: **Users** and **Roles**.

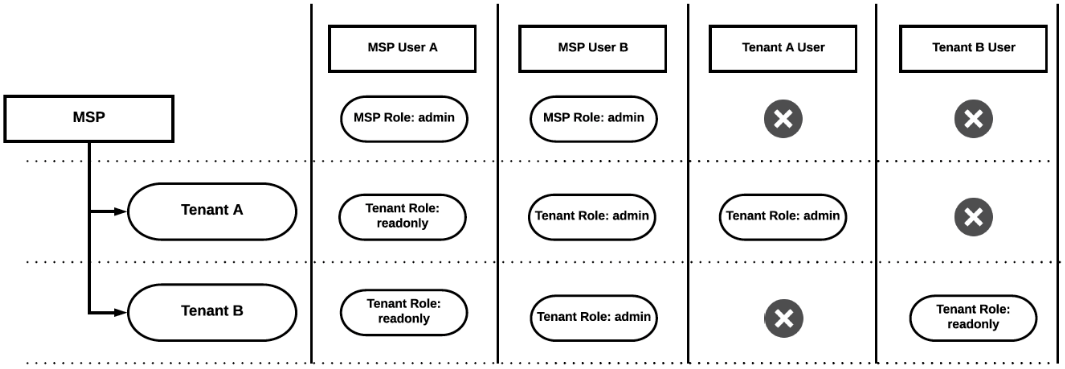
About the Roles Tab in MSP Account Home

Aruba Central MSP mode supports role-based access control. Aruba Central allows you to create predefined user roles and custom roles.

As shown in the following figure, MSP user A is mapped to two roles. MSP role **admin** gives the user administrator access to all MSP applications and the tenant role **readonly** gives the user read-only access to all tenant accounts. MSP user B is tied to MSP role **admin** and tenant role **admin**. The tenant administrator role provides the user administrator access to all tenant accounts.

Tenant user A is mapped to the **admin** role. This role gives the user administrator access to all tenant A applications. Tenant user B is mapped to the **readonly** role. This role gives the user read-only access to tenant B applications. Tenant user A and tenant user B can access only their respective accounts.

Figure 14 *MSP Role-Based Access Control*



The **Roles** tab has the following predefined roles.

Table 10: *Predefined User Roles*

Application	User Role	Privilege
Account Home	**admin**	Administrator for the **Account Home** page.
	readwrite	Can view and modify settings in the **Account Home** page and all **Global Settings** pages.
	readonly	Can view the **Account Home** page and all **Global Settings** pages.
Network Operations	**admin**	Administrator for the **Network Operations** application. Has access to **Account Home** > **Global Settings**.
	deny-access	Cannot view the **Network Operations** application.
	guestoperator	Has guest operator access for the **Network Operations** application. User does not have access to **Account Home** > **Global Settings**.
	readonly	Has read-only access to **Account Home** > **Global Settings** and the **Network Operations** application.
	readwrite	Has read-write access to **Account Home** > **Global Settings** and the **Network Operations** application. Has access to view and modify data using the Aruba Central UI or APIs. However, the user cannot execute APIs to: ■ Enable or disable MSP mode. ■ Perform operations in the following pages: **Account Home** > **Users and Roles** and **Network Operations** > **Organization** > **Labels and Sites**

Adding a Custom Role in MSP Account Home

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

With custom roles, you can configure access control at the application level and specify access rights to view or modify specific application services or modules.

NOTE

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

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

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

To add a custom role, complete the following steps:

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

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

    a. Click **Customize**.

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

    - **View Only**
    - **Modify**
    - **Block**
7. Click **Save**.
8. Assign the role to a user account as required.

Module Permissions in MSP Account Home

Aruba Central allows you to define user roles with **view** or **modify** permissions. You can also block user access to some modules. For example, if the **Guest Management** module is blocked for a specific user role, the corresponding pages are not displayed in the UI.

Aruba Central supports setting permissions for the following modules:

Table 11: *Permissions*

Application	Module	Description
Account Home	**Devices and Subscription**	Allows users to add devices and assign keys and subscriptions to devices.
Network Operations	**MSP**	Allows users with administrator role and privileges to define user access to MSP modules such as Customer Management and Portal Customization. The MSP tenant account user does not have access to the **MSP** application. Even if a tenant account user is assigned a custom role having **MSP** application privileges: ■ Tenant account user does have access to the **MSP** application. ■ **MSP** will not appear in the **Account Home** > **Global Settings** > **Users and Roles** > **Roles** > **Allowed Applications** list.
	Group Management	Allows users to create, view, modify, and delete groups and assign devices to groups.

Application	Module	Description
	Devices and Subscription	Allows users to add devices and assign subscriptions to devices.
	Network Management	Allows users to configure, troubleshoot, and monitor Aruba Central-managed networks.
	Guest Management	Allows users to configure cloud guest splash page profiles.
	AirGroup	Allows users to define or block user access to the AirGroup pages.
	Presence Analytics	Allows users to access the Presence Analytics app and analyze user presence data.
	VisualRF	Allows user to access VisualRF and RF heatmaps.
	Unified Communications	Allows users to access the Unified Communications pages.
	Install Manager	Allows users to manage installer profiles and site installations.
	Reports	Allows users to view and create reports.
	Other Applications	Allows users to access other applications modules such as notifications and Virtual Gateway deployment service.

Viewing User Role Details in MSP Account Home

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

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**.
2. Click the **Roles** tab. The **Roles** tab displays the following information:

- **Role Name**—Name of the user role.
- **Allowed Applications**—The applications to which the users have access.
- **Assigned Users**—Number of users assigned to a role.

Editing a User Role in MSP Account Home

To edit a user role, complete the following steps:

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

Deleting a User Role in MSP Account Home

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

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

About the System User Tab in MSP Account Home

In the **Account Home** page, under **Global Settings**, click **Users and Roles**. The **Users** tab is displayed. The **List of Users** table displays the following information:

- Email ID of the user.
- Type of user. The user can be system user or external user.
- Description of the user.
- MSP role
- Tenant role
- Account Home role
- Allowed groups for the user.
- Last active time of the user. If the last active time cell is blank, the user has not logged in after the product upgrade.

The **Actions** link offers the following options:

- **Resend invitation to users**—If any user has not received the email invite, you can use this link to resend invitations
- **Two-Factor Authentication (2FA)**—Enables Two-factor authentication.
- **Support Access**—Enables you to generate a new password of a specified validity to give access to a support person from Aruba.

Adding a User in MSP Account Home

To add a user, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**.

   The **Users and Roles** page is displayed.
2. Click **Add User**.

   The **New User** window is displayed.
3. Configure the following parameters:
   - **Username**—Email ID of the user. Enter a valid email address.
   - **Description**—Description of the user role. You can enter up to a maximum of 32 characters including alphabets, numbers, and special characters in the text field.
   - **Language**—Select a language. The Aruba Central web interface is available in English, French, Spanish, German, Brazilian Portuguese, Chinese, and Japanese languages.
   - **Account Home**—Select a user role for the **Account Home** page.
   - **Network Operations**—Select an MSP role and Tenant role for the **Network Operations** application.
4. Click **Save**. An email invite is sent to the user with a registration link. Users can use this link to access Aruba Central.

NOTE

The registration link in the email invite is valid for 15 days.

Track Progress

Click the **Track Progress** link to open the **Operations Status** page that provides the user account creation or modification status. The status can be in progress or failed. No status is displayed if the user account is successfully created.

Editing a User in MSP Account Home

To edit a user account, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**.

   The **Users** tab opens.
2. In the **List of Users** table, select the user and click the edit icon.
3. In the **Edit User <"Username">** window, modify description, role, or allowed groups.
4. Click **Save**.

Deleting a User in MSP Account Home

To delete a user account:

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**.

   The **Users** tab opens.
2. In the **List of Users** table, select the user and click the delete icon.
3. Confirm user deletion in the **Confirm Action** dialog box.

Viewing Audit Trail Logs for Users

Audit logs are generated when a new user is created and an existing user is modified or deleted from the Aruba Central account. It also records the login and logout activities of users.

To view audit logs for Aruba Central users:

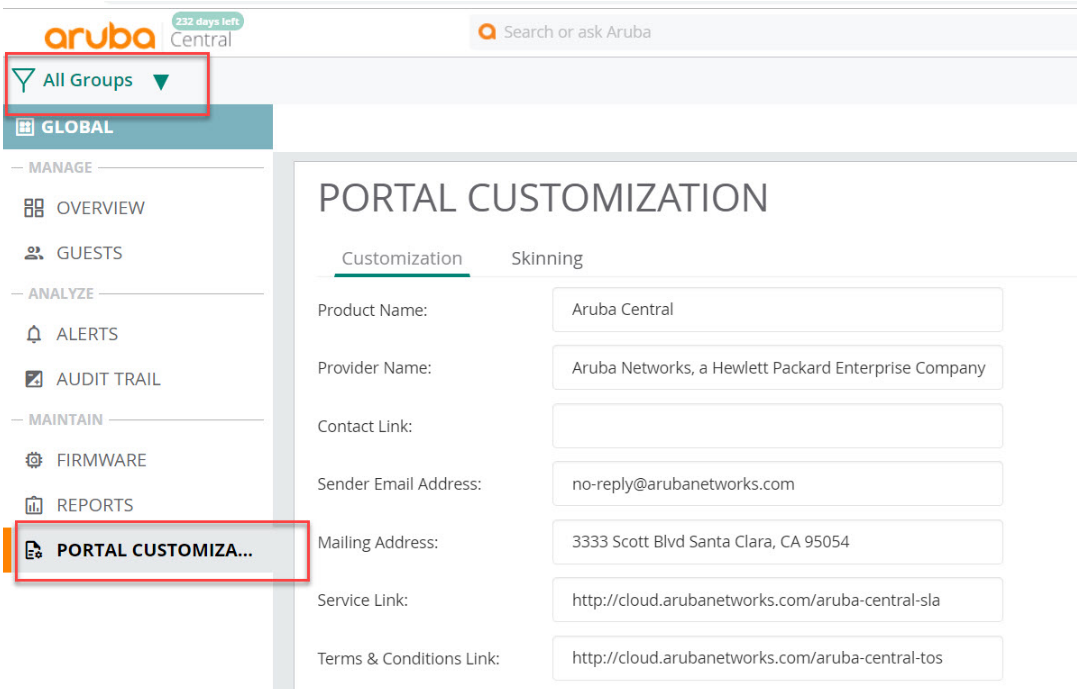
1. In the **Account Home** page, under **Global Settings**, click **Audit Trail**.

   The **Audit Trail** page is displayed.
2. To view audit logs for user addition, modification, or deletion, click the filter in the **Classification** column, and select **User Management**.
3. To filter audit logs about user activity, click the filter in the **Classification** column, and select **User Activity**.

Customizing the Portal in MSP Mode

The **Portal Customization** page enables you to customize the look and feel of the user interface and the email notifications sent to the customers and users. For example, you can use your company logo in the user interface and company address in the email notifications sent to the customers or users.

Figure 15 *Customizing the Portal in the Network Operations App*



Product Name: Aruba Central

Provider Name: Aruba Networks, a Hewlett Packard Enterprise Company

Contact Link:

Sender Email Address: no-reply@arubanetworks.com

Mailing Address: 3333 Scott Blvd Santa Clara, CA 95054

Service Link: http://cloud.arubanetworks.com/aruba-central-sla

Terms & Conditions Link: http://cloud.arubanetworks.com/aruba-central-tos

To customize the look and feel of the portal, complete the following steps:

1. In the **Network Operations** app, set the filter bar to **All Groups**.
2. Under **Maintain**, click **Portal Customization**.
3. The **Portal Customization** page is displayed.
4. Under **Customization**, configure the following information:

- **Product Name**—Name of the product.
- **Provider Name**—Name of the company.
- **Contact Link**—The URL to the company website that shows the contact address of the company.
- **Sender Email Address**—The email address from which the notifications are sent.
- **Mailing Address**—The postal address of the company.
- **Service Link**—The URL to the company website showing the service related information.
- **Terms and Conditions Link**—The URL to the company website listing the terms and conditions.

5. If you want customize the logo of your portal, click **Skinning**.
6. Browse to your local directory and upload the logo image.
7. Click **Save Settings**.

   The customized logo is displayed in the following pages:

- Tenant account—All the apps and pages applicable to the tenant. For more information about tenant accounts, see MSP Dashboard.
- Email invite—Email invite sent while adding a new user. The email contains the registration link. For more information about adding a new user, see System Users and User Roles in MSP Mode.

MSP Certificates

You can view and add certificates in MSP.

Viewing Certificates in MSP Mode

1. In the **Network Operations** app, use the filter to select **All Groups**.
2. Under **Maintain**, click **Organization**.
3. Click the **Certificates** tab.
4. The **Certificate Store** displays the following information:

Table 12: *Certificate Store Parameters*

Date Pane Item	Description
Certificate Name	Name of the certificate.
Status	Status of the certificate as either **Active** or **Expired**.
Expiry Date	Date of expiry for the certificate.
Type	Type of certificate. For example, a server certificate.
MD5 Checksum	The Message Digest 5 (MD5) algorithm is a widely used hash function producing a 128-bit hash value from the data input. Checksum value of the certificate.
SHA-1 Checksum	The Secure Hash Algorithm 1 (SHA-1) is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value. Checksum value of the certificate.

Uploading Certificates in the MSP Mode

MSP administrators can upload certificates to Aruba Central certificate store. They can also map the certificate usage for server and user authentication for the groups associated to a tenant account.

To upload certificates to the certificate store:

1. In the **Network Operations** app, use the filter to select **All Groups**.
2. Under **Maintain**, click **Organization**.
3. Click the **Certificates** tab.
4. To add a new certificate to the **Certificate Store**, click the + sign.

   The **Add Certificate** dialog box is displayed.
5. Enter the certificate name in the **Name** text box.
6. Select the certificate type from the **Type** list.
7. Select the certificate format from the **Format** drop-down.

   The supported certificate formats are PEM, DER, and PKCS12.
8. For server certificates, enter and then retype the passphrase.
9. Click **Choose File** to browse to your local directory and select the certificate to upload.
10. Click **Add**.

NOTE

Aruba Central allows percolation of certificates that are mapped to the MSP group, to the tenant account.

NOTE

When a certificate is removed from the **Device>Access Points> WLANs>Show Advanced >Security> Certificate Usage** section in Group dashboard in MSP, the respective certificate is also removed from the tenant's **Certificates Store**, if the certificate is mapped to the tenant's default group and is no longer used by the tenant. If the certificate is used by any of the tenant's non-default groups, the certificate is retained in the tenant's certificate store, even if the certificate is removed from the MSP. The **Device>Access Points> WLANs>Show Advanced >Security> Certificate Usage** menu is displayed only when you select a group from the filter.

See Mapping Cloud Guest Certificates for information about mapping Cloud Guest certificates.

Chapter 7
Configuring Instant APs

Instant APs offer an enterprise-grade networking solution with a simple setup. The WLAN solution with Instant APs supports simplified deployment, configuration, and management of Wi-Fi networks.

Instant APs run the Aruba Instant software that virtualizes Aruba Mobility Controller capabilities on 802.11 APs and offers a feature-rich enterprise-grade Wi-Fi solution. Instant APs are often deployed as a cluster. An Instant AP cluster includes a master AP and set of other APs that act as slave APs.

In an Instant deployment scenario, only the first AP or the master AP that is connected to a provisioning network is configured. All other Instant APs in the same VLAN join the master AP inherit the configuration changes. The Instant AP clusters are configured through a common interface called Virtual Controller. A Virtual Controller represents the combined intelligence of the Instant APs in a cluster.

The following is a list of configuration guidelines:

- Both the users with administrator and read/write privileges can configure SSIDs for a group or device.
- The changes configured for a group in the MSP are applied to the default group in the tenant's account.

For more information on configuring APs, see the *Aruba Central Online Help*.

Chapter 8
Configuring Switches

Aruba switches enable secure, role-based network access for wired users and devices, independent of their location or application. With Aruba switches, enterprises can deploy a consistent and secure access to network resources based on the type of users, client devices, and connection methods.

Aruba Central offers a cloud-based management platform for managing Aruba switch infrastructure. It simplifies switch management with flexible configuration options, monitoring dashboards, and troubleshooting tools.

For more information on configuring switches, see the *Aruba Central Online Help*.

Chapter 9
Configuring Gateways

The Aruba SD-WAN Gateways are the most important components of the Aruba SD-Branch Solution. Aruba's SD Branch provides a software overlay to centralize network controls in the public or private cloud. It allows robust management, configuration, and automation of the WAN processes. The solution supports SD-WANSoftware-Defined Wide Area Network. SD-WAN applies SDN technology to WAN connections that connect enterprise networks distributed across different locations., which is a specific application of the Software-Defined Networking (SDN) technology applied to WAN connections for enterprise networks, including branch offices and data centers, spread across different geographic locations.

In MSP mode, gateways are not configured in the Network Operations app, they are configurable at the tenant level. For more information on configuring gateways, see the *Aruba Central Online Help*.

The MSP Dashboard provides a summary of hardware and subscriptions owned by the MSP and the tenant accounts managed by the MSP.

Viewing the MSP Dashboard

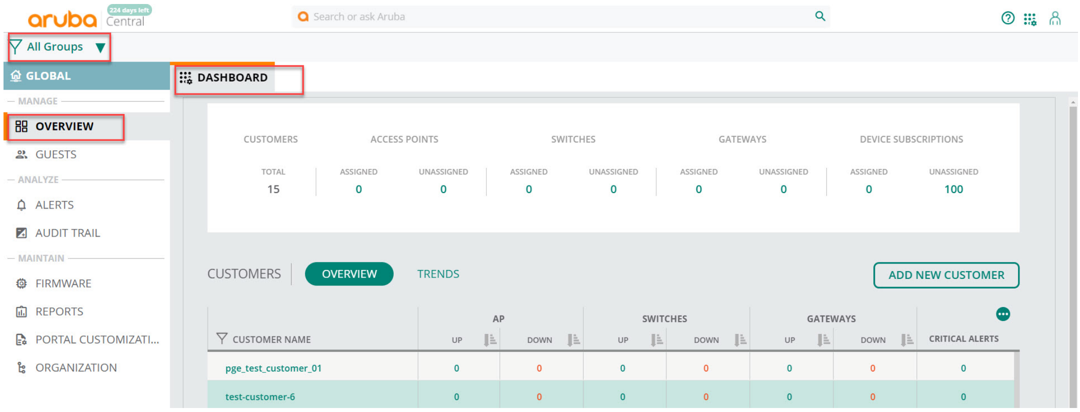
To view the MSP Dashboard, perform the following steps:

1. In the **Network Operations** app, set the filter to **All Groups**.
2. Under **Manage**, click **Overview** to display the **Dashboard**.

   The **Dashboard** page includes the following sections:

- Dashboard summary bar
- Overview and trends for customers

Figure 16 *Viewing the MSP Dashboard*



CUSTOMERS	ACCESS POINTS		SWITCHES		GATEWAYS		DEVICE SUBSCRIPTIONS	
TOTAL	ASSIGNED	UNASSIGNED	ASSIGNED	UNASSIGNED	ASSIGNED	UNASSIGNED	ASSIGNED	UNASSIGNED
15	0	0	0	0	0	0	0	100

	AP		SWITCHES		GATEWAYS		
CUSTOMER NAME	UP	DOWN	UP	DOWN	UP	DOWN	CRITICAL ALERTS
pge_test_customer_01	0	0	0	0	0	0	0
test-customer-6	0	0	0	0	0	0	0

Dashboard Summary

The **Dashboard Summary** bar displays the total number of tenant accounts and the MSP device inventory and device subscription status.

Table 13 describes the contents of the **Dashboard Summary** bar.

Table 13: *Dashboard Summary Bar*

Data Pane Item	Description
Customers	Total number of tenant accounts provisioned.
Access Points	■ **Assigned**—Number of Instant APs assigned to tenant accounts. Click the number to view the list of Instant APs in **Subscribed** state. ■ **Unassigned**—Number of Instant APs available for provisioning. Click the number to view the list of Instant APs in **Unsubscribed** state.
Switches	■ **Assigned**—Number of switches assigned to tenant accounts. Click the number to view the list of switches in **Subscribed** state. ■ **Unassigned**—Number of switches available for provisioning. Click the number to view the list of switches in **Unsubscribed** state.

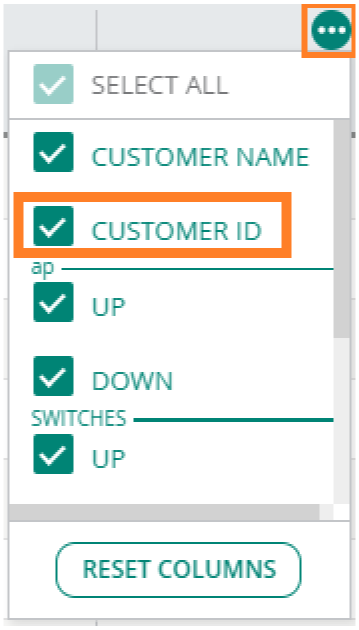
Data Pane Item	Description
Gateways	■ **Assigned**—Number of gateways assigned to tenant accounts. Click the number to view the list of gateways in **Subscribed** state. ■ **Unassigned**—Number of gateways available for provisioning. Click the number to view the list of gateways in **Unsubscribed** state.
Device Subscriptions	■ **Assigned**—Number of device subscriptions assigned to tenant accounts. Click the number to view the list of devices in **Subscribed** state. ■ **Unassigned**—Number of device subscriptions available for provisioning. Click the number to view the list of devices in **Unsubscribed** state.

Customer | Overview

By default, the **Customers** | **Overview** table is displayed. The table provides an overview of tenant accounts. MSP administrators can perform tasks such as drilling down to a tenant account, editing an existing tenant account, and deleting a tenant account.

Table 14 describes the contents of the table.

Table 14: *Customers Table*

Column	Description
Customer Name	Name of the tenant account. Hover over the tenant account name to view the following options: ■ **expand**—Opens a new pop-up window showing the tenant account details. For more information, see Viewing Tenant Account Details on page 52. ■ **edit**—Opens the **Edit Customer** pop-up window. For more information, see Editing a Tenant Account on page 53. ■ **delete**—Opens the confirmation dialog box. ■ For more information, see Deleting a Tenant Account on page 53. Hover over the icon next to the tenant account name to view the provisioning status. The status can be one of the following: ■ In Progress ■ Provision Failed **NOTE:** Use the filter icon on the column header to filter by tenant account name.
Customer ID	Unique ID of the tenant account. The ID can be in one of the following formats: ■ Numerical format ■ UUID format Use the column filter to search for a particular customer ID. Note that you must enter the full customer ID. The **Customer ID** column is not displayed in the default view. Use the column selector and select the **Customer ID** check box to add the column to the table.  SELECT ALL CUSTOMER NAME CUSTOMER ID ap UP DOWN SWITCHES UP RESET COLUMNS
AP	■ **Up**—Total number of online Instant APs. Click the number to view the list of online Instant APs. ■ **Down**—Total number of offline Instant APs. Click the number to view the list of offline Instant APs. **NOTE:** Click the sort icon to sort the column in ascending or descending order.

Column	Description
Switches	■ **Up**—Total number of online switches . Click the number to view the list of online switches. ■ **Down**—Total number of offline switches. Click the number to view the list of offline switches. **NOTE:** Click the sort icon to sort the column in ascending or descending order.
Gateways	■ **Up**—Total number of online Aruba Gateways. Click the number to view the list of online Aruba Gateways. ■ **Down**—Total number of offline Aruba Gateways. Click the number to view the list of offline Aruba Gateways. **NOTE:** Click the sort icon to sort the column in ascending or descending order.
Critical Alerts	Total number of critical alerts for the tenant account. Click the number to navigate to the **Alerts** page of the tenant account. For more information, see MSP Alerts on page 73.

Customers | Trends

Go to **Customers** | **Trends** to view the following graphs:

- **Device Subscription Renewal Schedule** graph—Displays the subscription renewal schedule for the next 12 months. The graph plots the total count of subscriptions that are due for renewal for each month.
- **Device Under Management** graph—Displays the count of devices that are managed in the network over a period of time.
- **Customers** graph—Displays the total number of tenants added to Aruba Central over a period of time.

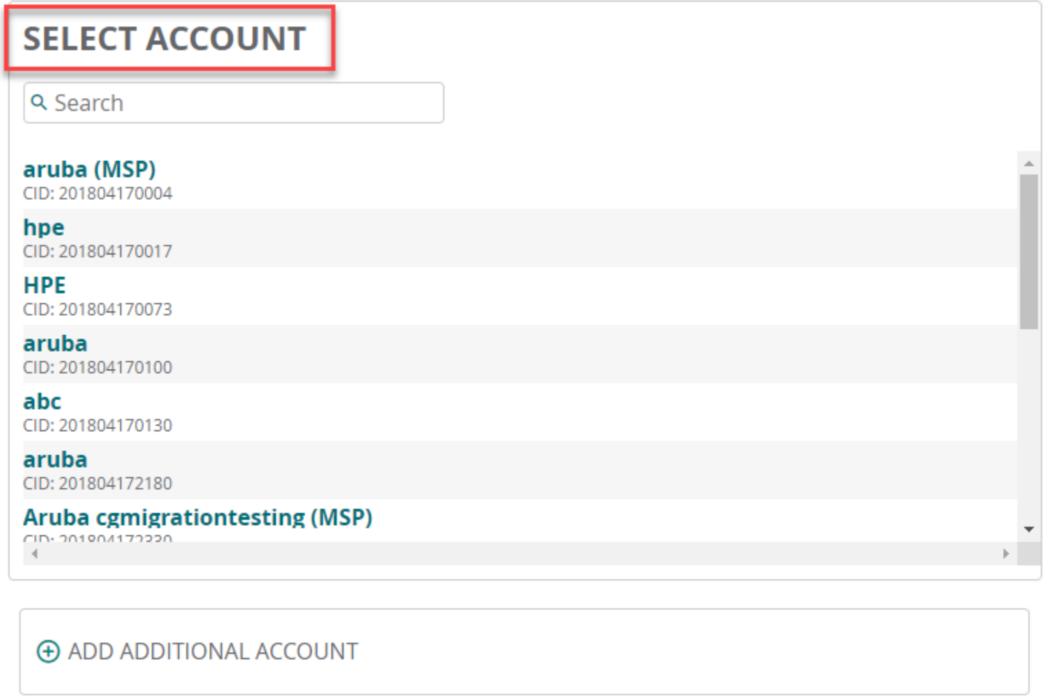
Adding a New Customer

Perform the steps detailed in About Provisioning Tenant or Customer Accounts.

Using the Switch Customer Option

If you are an MSP administrator and if your user ID has been added to multiple tenant accounts, after you log in to Aruba Central, you must select the tenant account that you want to access.

Figure 17 *Select Account*



SELECT ACCOUNT

Search

aruba (MSP)
CID: 201804170004

hpe
CID: 201804170017

HPE
CID: 201804170073

aruba
CID: 201804170100

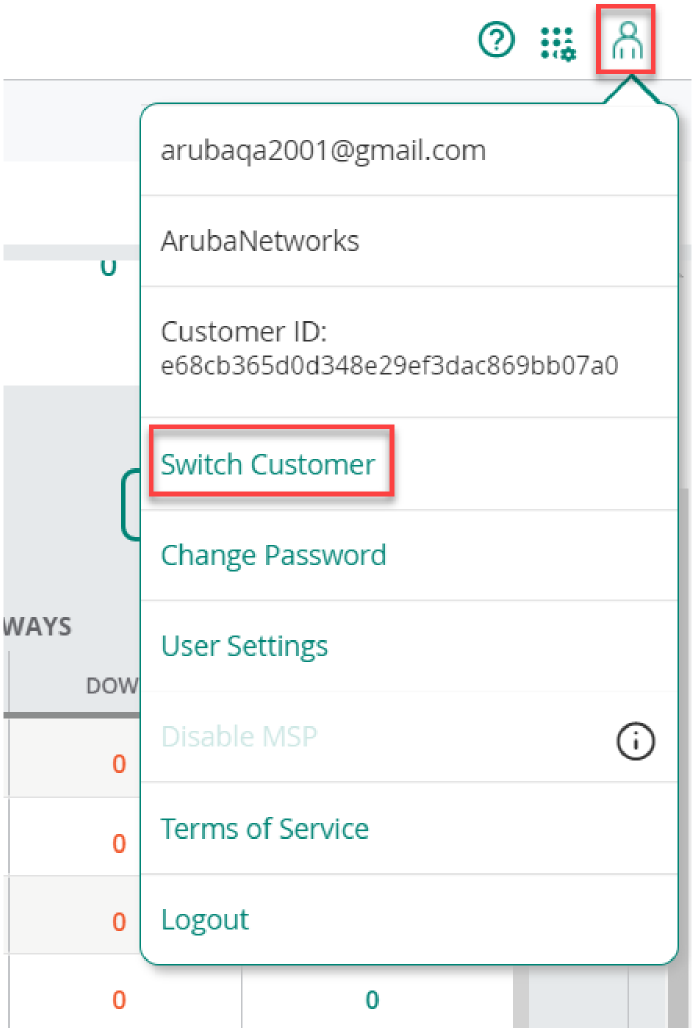
abc
CID: 201804170130

aruba
CID: 201804172180

Aruba cgmigrationtesting (MSP)
CID: 201804172330

To select a different tenant account, click the **User** icon 👤, select **Switch Customer**, and then select the tenant account that you want to access.

Figure 18 *Switch Customer*



Navigating to the Tenant Account

MSP users with administrative privileges to tenant accounts can drill down to tenant accounts.

To drill down to a specific tenant account:

1. In the **Network Operations** app, set the filter to **All Groups**.
2. Under **Manage**, click **Overview** to display the **Dashboard**.

   The **Dashboard** page includes the following sections:

- Dashboard summary bar
- Overview and trends for customers

3. In the **Customers | Overview** table, click the tenant account name and click **Expand**.

   The tenant account details window is displayed. Close the window.
4. To go to the tenant account, click on the tenant account name.

   The tenant account is displayed in Standard Enterprise Mode.

NOTE

To return to the MSP view, click **Return to MSP View**. Aruba recommends that you not use the **Back** button of the web browser to go back to the MSP view.

For a visual representation of the procedure, click here.

Points to Note:

- The group attached to tenant account in the MSP mode shows up as a default group for the users of the tenant account.
- Configuration changes to the group attached to a tenant account in the MSP mode are applied to the default group in the interface displayed for the tenant accounts.
- The administrators can add users to a tenant account using the **Users & Roles** menu in the **Global Settings** app.
- Tenant account administrators can allow or prevent user access to specific groups by configuring custom roles.

Chapter 11
Analyzing and Maintaining MSP Tenant Accounts

In the **Network Operations** app for MSP mode, when you set the filter to **All Groups**, the following left-navigation menu items are displayed for analyzing and maintaining tenant accounts:

- Under **Analyze**:
  - **Alerts**—Aruba Central MSP mode enables administrators to trigger alerts when tenant provisioning, network, device, or user management events occur. An MSP administrator can configure alerts at the MSP level which percolate down to all tenant accounts managed by the MSP. For more information, see MSP Alerts.
  - **Audit Trail**—The **Audit Trail** page shows the logs for all the device management, configuration, and user management events triggered in Aruba Central. For more information, see Viewing Audit Trails.
- Under **Maintain**:
  - **Firmware**—The **Firmware** menu displays the **Access Points**, **Switch-MAS**, **Switch-Aruba**, and **Gateways** tabs that list all the tenants with firmware and compliance status for each of the device types. For more information, see Firmware Upgrades for MSP Mode.
  - **Reports**—The MSP **Reports** dashboard enables you to create reports. You can configure these reports to run on demand or periodically. You must have read and write privileges or you must be an Admin user to create reports. For more information, see MSP Reports.
  - **Portal Customization**—The **Portal Customization** page enables you to customize the look and feel of the user interface and the email notifications sent to the customers and users. For example, you can use your company logo in the user interface and company address in the email notifications sent to the customers or users. For more information, see Customizing the Portal in MSP Mode.
  - **Organization**—Displays the Groups and Certificates tabs.
    - MSP groups are UI groups mapped to the default UI groups in the tenant account. If a tenant account is associated to a specific group in the MSP mode, the configuration changes to the devices associated with this tenant account are pushed only to the **default** group in the tenant account view. However, MSP administrators can create more groups for a specific tenant by drilling down to a tenant account. For more information, see Groups in the MSP Mode.
    - MSP administrators can upload certificates to Aruba Central certificate store. They can also map the certificate usage for server and user authentication for the groups associated to a tenant account. For more information, see MSP Certificates.

MSP Alerts

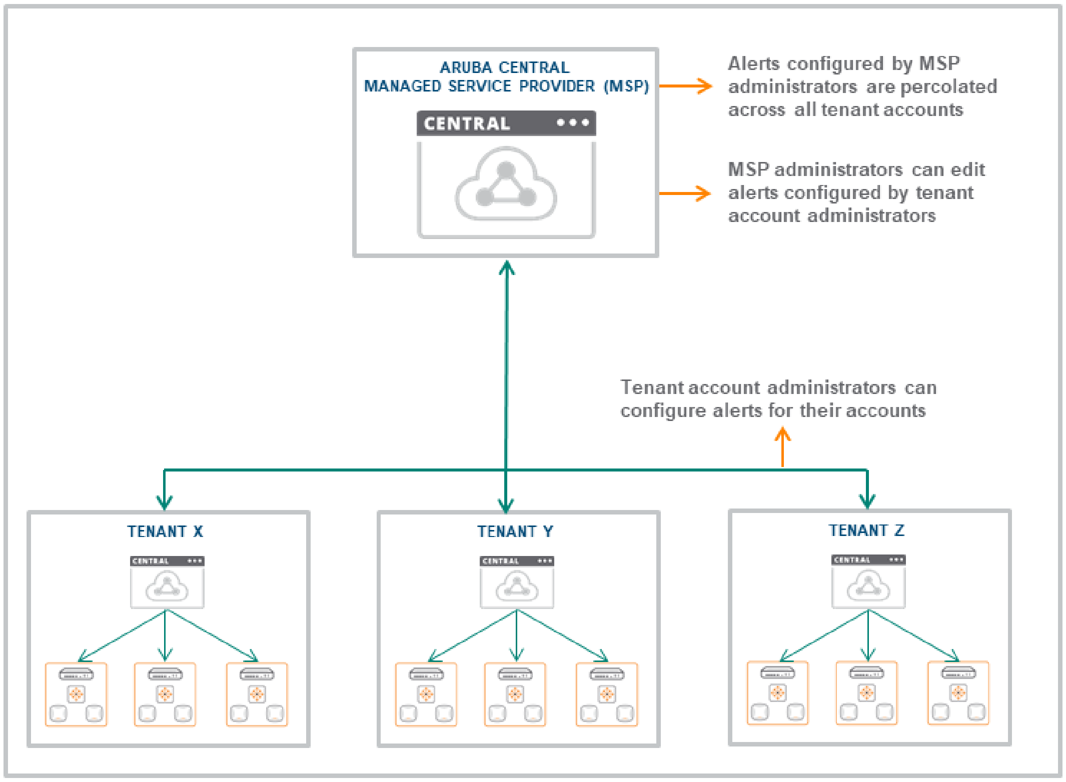
Aruba Central MSP mode enables administrators to trigger alerts when tenant provisioning, network, device, or user management events occur. An MSP administrator can configure alerts at the MSP level which percolate down to all tenant accounts managed by the MSP. For example, if the MSP administrator has configured an alert to be triggered when an AP is disconnected, the MSP is notified when an AP is disconnected in any of the tenant networks managed by the MSP. This allows for faster reactive support and makes monitoring and troubleshooting easy across multiple tenant accounts.

The MSP administrator can configure additional alerts at the tenant account level. At the tenant account level, alerts can be configured based on groups, labels, sites, or devices. Tenant account administrators can also configure additional alerts for their account. In this case, the alert is triggered only for the corresponding tenant account.

The MSP administrator can edit an alert configured by the tenant account administrator. However, the tenant account administrator cannot edit an alert created by the MSP administrator.

MSP level and tenant level alert configurations are managed separately. For example, if an alert is configured and enabled at both the MSP level and tenant level, two separate notifications are triggered for the event.

Figure 19 *MSP Alerts*


ARUBA CENTRAL
MANAGED SERVICE PROVIDER (MSP)
CENTRAL
Alerts configured by MSP administrators are percolated across all tenant accounts
MSP administrators can edit alerts configured by tenant account administrators
Tenant account administrators can configure alerts for their accounts
TENANT X
TENANT Y
TENANT Z

This section includes the following topics:

- Viewing MSP Alerts Dashboard
- Alert Notification Delivery Options
- Configuring Alerts at the MSP Level
- Configuring Alerts at the Tenant Account Level
- Viewing Enabled Alerts

Viewing MSP Alerts Dashboard

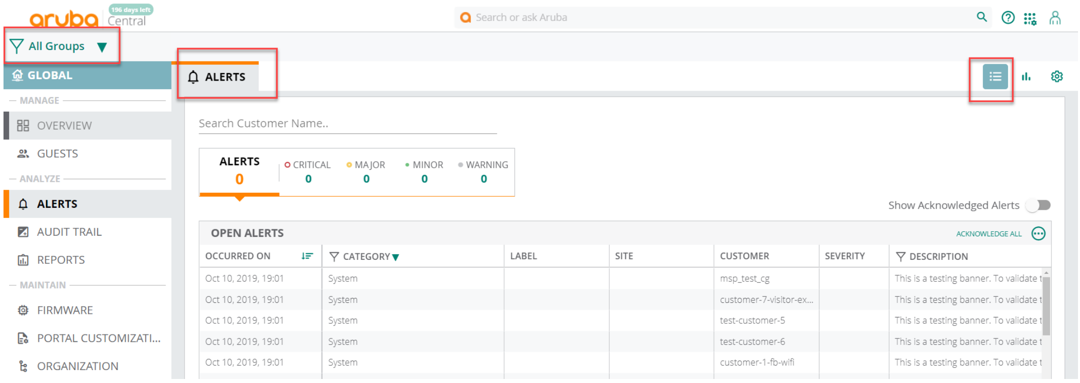
1. In the **Network Operations** app, filter **All Groups**.
2. Under **Analyze**, click **Alerts** to display the **Alerts** dashboard.

   The **Alerts** dashboard enables you to configure, view, and acknowledge alerts.
3. To view detailed graphs about the alerts, click the chart icon 📊.
4. Select each tab, **All**, **Access Points**, **Switches**, or **Gateways** to view the graphs pertaining to each device type.
5. To view the list of alerts, click the ☰ list icon. The list view displays the number of alerts in the following categories:
   - **Critical**
   - **Major**

- **Minor**
- **Warning**

6. Click **Acknowledge All** to acknowledge all the alerts at once.
7. Enable the **Show Acknowledged Alerts** button to display the list of acknowledged alerts.
8. Clicking ⊙ icon enables you to customize the **Alerts** table columns or set it to the default view.
9. The **Search** bar allows you to search for alerts by tenant account. Enter the name of the tenant account and select the tenant account from the list.

Figure 20 *Using the List View for MSP Alerts*



OCCURRED ON	CATEGORY	LABEL	SITE	CUSTOMER	SEVERITY	DESCRIPTION
Oct 10, 2019, 19:01	System			msp_test_cg		This is a testing banner. To validate t
Oct 10, 2019, 19:01	System			customer-7-visitor-ex...		This is a testing banner. To validate t
Oct 10, 2019, 19:01	System			test-customer-5		This is a testing banner. To validate t
Oct 10, 2019, 19:01	System			test-customer-6		This is a testing banner. To validate t
Oct 10, 2019, 19:01	System			customer-1-fb-wifi		This is a testing banner. To validate t

All the alerts are displayed in a tabular format and displays the following information:

Table 15: *Viewing the MSP Alerts pane*

Data Pane Content	Description
Occurred On	Timestamp of the alert. Use the sort option to sort the alerts by date and time.
Category	Displays the category of the alert. Use the filter option to filter the alert by category.
Label	Displays the label name of the alert.
Site	Displays the site name of the alert.
Customer	Displays the customer name of the alert.
Group	Displays the group name of the alert.
Severity	Displays the severity level of the alert. The severity can be Critical, Major, Minor, or Warning.
Description	Displays a description of the alert. Use the search option in filter bar to filter the alert based on description.

Alert Notification Delivery Options

When you configure an alert, you can select how you want to be notified when an alert is generated. Aruba Central supports the following notification types:

- **Email**—Select the **Email** check box and enter an email address to receive notifications when an alert is generated. You can enter multiple email addresses; separate each value with a comma.

- **Webhook**—Select the **Webhook** check box and select the desired Webhooks from the drop-down list. Before you select this option, you must create Webhooks. For more information about creating and modifying Webhooks, see the Aruba Central Online documentation.

Configuring Alerts at the MSP Level

To configure alerts at the MSP level, complete the following steps:

1. In the **Network Operations** app, filter **All Groups**.
2. Under **Analyze**, click **Alerts** to display the **Alerts** dashboard.
3. Click the settings icon ⚙.

NOTE

At the MSP level, you cannot configure alerts based on groups, labels, sites, or devices.

4. Use the tabs to navigate between the alert categories. Select an alert and click **+** to enable the alert with default settings. To configure alert parameters, click on the alert tile (anywhere within the rectangular box) and do the following:

   a. **Severity**—Set the severity. The available options are Critical, Major, Minor, and Warning. By default, the following alerts are enabled and the severity is **Major**:

   - Virtual Controller Disconnected
   - Rogue AP Detected
   - New User Account Added
   - Switch Detected
   - Switch Disconnected

   b. **Notification Options**—See Alert Notification Delivery Options.

   - Click **Save**.
   - **Add Rule**—(Optional) For a few alerts, the **Add Rule** option appears. For such alerts, you can add additional rule(s).

Configuring Alerts at the Tenant Account Level

To configure alerts at the tenant account level, complete the following steps:

1. Navigate to the tenant account. See Navigating to the Tenant Account.
2. In the **Network Operations** app, use the filter bar to select a group or a device.
3. To configure alerts, click the ⚙ settings icon under **Analyze** > **Alerts & Events**. By default, the **Alerts & Events** > **User** category is displayed.
4. Use the tabs to navigate between the alert categories. Select an alert and click **+** to enable the alert with default settings. To configure alert parameters, click on the alert tile (anywhere within the rectangular box) and do the following:

   a. **Severity**—Set the severity. The available options are Critical, Major, Minor, and Warning. By default, the following alerts are enabled and the severity is **Major**:

   - Virtual Controller Disconnected
   - Rogue AP Detected
   - New User Account Added
   - Switch Detected
   - Switch Disconnected

> NOTE
>
> For a few alerts, you can configure threshold value for one or more alert severities. To set the threshold value, select the alert and in the **exceeds** text box, enter the value. The alert is triggered when one of the threshold values exceed the duration.

b. **Duration**—Enter the duration in minutes.

c. **Device Filter Options**—(Optional) You can restrict the scope of an alert by setting one or more of the following parameters:

- **Group**—Select a group to limit the alert to a specific group.
- **Label**—Select a label to limit the alert to a specific label.
- **Device**—Select a device to limit the alert to a specific device.
- **Sites**—Select a site to limit the alert to a specific site.

d. **Notification Options**

- **Email**—Select the **Email** check box and enter an email address to receive notifications when an alert is generated. You can enter multiple email addresses, separate each value with a comma.
- **Webhook**—Select the **Webhook** check box and select the Webhook from the drop-down list.

e. Click **Save**.

f. **Add Rule**—(Optional) For a few alerts, the **Add Rule** option appears. For such alerts, you can add additional rule(s). The rule summaries appear at the top of the pag

Viewing Enabled Alerts

To view alerts enabled at the MSP level or tenant account level, do the following:

1. In the **Network Operations** app, filter **All Groups**.
2. Under **Analyze**, click **Alerts** to display the **Alerts** dashboard.
3. On the **Alerts** page, click **Enabled**.

The **Enabled** tab lists the alerts that you have enabled. Click the tabs to see enabled alerts for each category.

Firmware Upgrades for MSP Mode

The **Firmware** menu under **Maintenance** displays a list of tenant accounts and the status of the devices assigned to the tenant accounts.

Viewing the Firmware Dashboard

1. In the **Network Operations** app, use the filter to select **All Groups**.
2. Under **Maintain**, click **Firmware**.
3. Select one of the following tabs: **Access Points**, **Switch-MAS**, **Switch-Aruba**, or **Gateways**

The **Firmware** menu displays the **Access Points**, **Switch-MAS**, **Switch-Aruba**, and **Gateways** tabs that list all the tenants with firmware and compliance status for each of the device types.

The following table displays the Firmware dashboard for **Access Points**, the table for the other tabs are similar:

Table 16: *Firmware Dashboard Parameters for APs Tab*

Date Pane Item	Description
Customer Name	Name of the customer.
Upgrade Status	Status of the devices associated with the tenant account. This column displays one of the following: ■ Upgrading ■ Scheduling in progress ■ Downloading firmware ■ Upgrade successful, ready for reboot ■ Upgrade successful and rebooting AP ■ Upgrade in process ■ Firmware upgrade failed. Please try again. ■ Rebooting ■ Live upgrade initiating ■ Live upgrade initiated
Compliance Status	Status of compliance for the tenant. This column indicates the compliance status such as **Set**, **Not Set**, or **Compliance scheduled on <date and time>** for a specific tenant.
Manage Firmware Compliance	Enables you to plan upgrades. See Managing Firmware Compliance Based on Tenant Account.

Managing Firmware Compliance Based on Device Tabs

1. In the **Network Operations** app, use the filter to select **All Groups**.
2. Under **Maintain**, click **Firmware**.
3. Select one of the following tabs: **Access Points**, **Switch-MAS**, **Switch-Aruba**, or **Gateways**
4. Click **Manage Firmware Compliance** at the top right.

   The **Manage Firmware Compliance** window opens.
5. Select the firmware version and the time for upgrade.
6. Select **Auto Reboot** if you want Aruba Central to automatically reboot the device after a successful device upgrade. The **Auto Reboot** option is not available for **Access Points**.
7. Select one of the following as required

- Select **Now** to set the compliance to be carried out immediately.
- Select **Later Date** to set the compliance at the later date and time.

8. Click **Save and Upgrade**.
9. MSP 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.

Managing Firmware Compliance Based on Tenant Account

1. In the **Network Operations** app, use the filter to select **All Groups**.
2. Under **Maintain**, click **Firmware**.

3. Select one of the following tabs: **Access Points**, **Switch-MAS**, **Switch-Aruba**, or **Gateways**
4. From the dashboard, select one or more customer name and click **Continue**.
5. The **Upgrade <Device Type> Firmware** page is displayed.

NOTE

You can click the check box on the table heading of tenant details table to include all the tenants for the firmware upgrade listed in the current page. To manually upgrade firmware for specific tenants, select the check box corresponding to the tenant that requires a manual firmware upgrade in the tenant details table. Clicking the **Continue** button displays the **Upgrade <Device Type> Firmware** page.

The **Filter by upgrade status** drop-down list disappears when the **Update All** button is clicked.

6. Perform the following actions:

Table 17: *Upgrade <Device Type> Firmware*

Component	Description
Firmware Version	The firmware version to which the tenant is required to be upgraded. Aruba Central considers the recommended firmware version as the default if no version is specified in the field.
Auto Reboot	Select this check box to reboot the device automatically after the download of the new version. **NOTE:** The **Auto Reboot** option is not applicable for Instant APs.
Schedule	Select one of the following radio buttons to specify if the compliance must be carried out immediately or at a later date and time. ■ **Now**—To set the firmware upgrade to be carried out immediately. ■ **Later Date**—To set the firmware upgrade to take place at a later date and time. Click the **Upgrade** button to upgrade the firmware.
Cancel	Click this button to cancel the settings and go back to the **Maintenance > Firmware** page.

7. The **Firmware** page also displays the **Cancel All** button. Click **Cancel All** button to cancel the manual firmware upgrade for all the tenants in the MSP mode.

NOTE

The compliance upgrade settings for the tenants and the tenant devices takes precedence over the manual firmware upgrade. The scheduled manual firmware upgrade becomes invalid when you set or schedule the compliance upgrade.

Firmware Upgrade in MSP Through NB API

Aruba Central provides an option to upgrade firmware for all the tenants mapped to the MSP through APIs in **Maintenance > API Gateway**.

To set or get the country code at group level through API:

1. In the **Account Home** page, click **API Gateway**.
2. Click **System Apps & Tokens** tab and generate a token key.
3. Download and copy the generated token.
4. Click the link displayed in the **APIs** tab of the **API Gateway**. The **Central Network Management APIs** page opens.
5. On the left navigation pane, select **Firmware** from the **URL** drop-down list.
6. Paste the token key in the **Token** field and press enter.
7. In **Firmware Management,** the following options are displayed**:**

- **[POST] /firmware/v1/msp/upgrade**—Upgrades firmware at the MSP level. To configure the firmware upgrade for all the tenants of a specific device type, enter the following inputs in the corresponding labels of the script { "firmware_scheduled_at": 0, "device_type": "string", "firmware_version": "string", "reboot": true, "exclude_groups": "string", "exclude_customers": "string" }:

Table 18: *Firmware Upgrade at MSP level*

Label	Description
Firmware_ scheduled_ at	The time at which the firmware upgrade must be initiated. The value entered in this field is the count in seconds from the current time.
Device_ type	The type of device for which the firmware upgrade must be initiated.
Firmware_ version	The firmware version to which the device is required to be upgraded. Aruba Central takes the recommended firmware version as the default version if no version is specified in the field.
Reboot	True or false value to enable or disable the reboot of device once the firmware upgrade build is downloaded. **NOTE:** The **Reboot** option is not applicable for Instant APs.
Exclude-groups	The list of groups to be excluded from firmware upgrade.
Exclude_ customers	The list of tenants to be excluded from firmware upgrade.

- **[POST] /firmware/v1/msp/upgrade/customers/{customer_id}**—Upgrades firmware at the tenant level. To configure the firmware upgrade for a specific tenant of a specific device type, enter the following inputs in the corresponding labels of the script{ "firmware_scheduled_at": 0, "device_type": "string", "firmware_version": "string", "reboot": true, "exclude_groups": "string" }.

Table 19: *Firmware Upgrade at the Tenant level*

Label	Description
Firmware_ scheduled_ at	The time at which the firmware upgrade must be initiated. The value entered in this field is the count in seconds from the current time.
Device_ type	The type of device for which the firmware upgrade must be initiated.
Firmware_ version	The firmware version to which the device is required to be upgraded. Aruba Central takes the recommended firmware version as the default version if no version is specified in the field.
Reboot	True or false value to enable or disable the reboot of device once the firmware upgrade build is downloaded. **NOTE:** The **Reboot** option is not applicable for Instant APs.
Exclude-groups	List of groups to be excluded from firmware upgrade.

- **[POST] /firmware/v2/msp/upgrade/cancel**—Cancels a scheduled upgrade firmware of devices specified by device_type. Enter the following inputs in the corresponding labels of the script{ "device_type": "string", "exclude_groups": "string", "exclude_customers": "string" }.

Table 20: *Cancel Scheduled Upgrade at MSP Level*

Label	Description
Device_type	The type of device for which the firmware upgrade schedule must be canceled.
Exclude-groups	List of groups to be excluded while canceling scheduled upgrade.
Exclude_customers	List of customer IDs to be excluded while canceling scheduled upgrade.

- **[POST] /firmware/v2/msp/upgrade/customers/{customer_id}/cancel**—Cancels a scheduled upgrade firmware of devices specified by device_type for a tenant. Enter the following inputs in the corresponding labels of the script{ "device_type": "string", "exclude_groups": "string" }.

Table 21: *Cancel Scheduled Upgrade at the Tenant Level*

Label	Description
Device_type	The type of device for which the firmware schedule must be canceled.
Exclude-groups	List of groups to be excluded while canceling scheduled upgrade.

The following APIs that include **v1** version will be deprecated from API Gateway and is replaced with **v2** version:

- **[POST] /firmware/v1/msp/upgrade/cancel**
- **[POST] /firmware/v1/msp/upgrade/customers/{customer_id}/cancel**

Order of Precedence For Compliance

The devices in the MSP mode inherits the compliance set in the following order of precedence from highest to lowest:

- Group level
- Tenant level
- MSP level

The devices in MSP mode exhibits the following behavior related to compliance settings:

- The compliance set at the group level overrides the compliance set at the tenant level or MSP level. If there is no compliance at the group level, the devices in the group inherits the compliance configured at the tenant level.
- The compliance set at the tenant level overrides the compliance set at the MSP level. If there is no compliance at the tenant level and group level, the tenant devices inherit the compliance configured at the MSP level.

MSP Reports

The MSP **Reports** dashboard enables you to create reports. You can configure these reports to run on demand or periodically. You must have read and write privileges or you must be an Admin user to create reports.

NOTE

MSP reports are generated at the end of day, so the current day data is not available in the report. MSP reports data is supported from version 2.5.0 onwards, the data is available only after an upgrade to version 2.5.0 or later. Data prior to the 2.5.0 upgrade is not available in the report.

The **Reports** dashboard has the following sections:

- **Create**—Creates a report that can be run instantly or periodically.
- **Manage**—Edit or delete scheduled reports.
- **Browse**—Explore, email, download, or delete Generated reports.

Types of Reports

Currently, only **Device and Subscription Inventory** reports are supported in MSP.

To access the **Reports** dashboard, from the **Network Operations** app, under **Analyze**, click **Reports**. Reports that are already run are listed under **Browse** > **Generated Reports**. If any report is yet to run, that report is available under **Browse** > **Scheduled Reports**.

The following table explains the parameters available in **Generated Reports** .

Table 22: *Generated Reports* *Description*

Parameter	Description
Title	Name of the report.
Date Run	Time when the report was last run. For **Scheduled Reports**, this is replaced by Next Run which indicates the time when the report will run in the future.
Scope	List of devices or subscription for which the report was run.
Report Type	Type of report, currently the only supported value is MSP Inventory.
Created by	Email address of the user who created the report.

The following table explains the parameters available in **Scheduled Reports**

Table 23: *Scheduled Reports* *Description*

Parameter	Description
Title	Name of the report.
Next Run	Time when the report will run in the future.
Status	Status of the report, whether **scheduled**, **failed**, **running**, **rerun**, or **waiting**.
Scope	List of devices or subscription for which the report was run.
Report Type	Type of report, currently the only supported value is MSP Inventory.
Recurrence	Time period of the scheduled report.
Created by	Email address of the user who created the report.

Creating a Report

To create a report, complete the following procedure:

1. From the **Network Operations** app, under **Analyze**, click **Reports**.

   The **Reports** dashboard is displayed.

2. Click **Create**.

   The **Infrastructure** page is displayed.

3. Under **Infrastructure**, click **Device and Subscription Inventory** and then click **Next**.

4. Under **Scope**, select **All** or a combination of the other choices and then click **Next**:

- **All**—Generates a report for all access points, gateways, switches, and subscriptions.
- **Access Points**—Generates a report only for access points.
- **Gateways**—Generates a report only for gateways.
- **Switches**—Generates a report only for switches.
- **Subscriptions**—Generates a report only for subscriptions.

5. Under **Report period**, select one of the following options and then click **Next**:

- **Last Month**
- **Last 3 Months**
- **Last 6 Months**
- **Custom Range**

6. Select one of the recurrent options:

- **One Time (now)**
- **One Time (later)**
- **Every day**
- **Every week**
- **Every month**

7. For **Report Information**, enter the title of the report and an email address where the report will be delivered.

8. Select the format as either **PDF** or **CSV**.

9. Click **Generate**.

10. If you select **One Time** as an option in step 6, the report is available under **Generated Reports**. If the report is yet to run, the report is available under **Scheduled Reports**.

Editing a Report

To edit a report, complete the following procedure:

1. From the Network Operations app, under **Analyze**, click **Reports**.

   The **Reports** dashboard is displayed.

2. Click **Manage**.

3. Under **Scheduled Reports**, select the report you want to edit and then click the edit icon.

   The **Infrastructure** page is displayed.

4. Under **Scope**, select one or a combination of the following choices and then click **Next**:

- **All**—Generates a report for all access points, gateways, switches, and subscriptions.
- **Access Points**—Generates a report only for access points.
- **Gateways**—Generates a report only for gateways.
- **Switches**—Generates a report only for switches.
- **Subscriptions**—Generates a report only for subscriptions.

5. Under **Report period**, select one of the following options and then click **Next**

- **Last Month**
- **Last 3 Months**
- **Last 6 Months**
- **Custom Range**

6. Select one of the recurrent options:

- **One Time (now)**
- **One Time (later)**
- **Every day**
- **Every week**
- **Every month**

7. For **Report Information**, enter the title of the report and an email address where the report will be delivered.

8. Select the format as either **PDF** or **CSV**.

9. Click **Generate**.

10. If you select **One Time** as an option, the report is available under **Generated Reports**. If the report is yet to run, the report is available under **Scheduled Reports**.

Viewing or Downloading a Report

To view or download a report, complete the following procedure:

1. From the **Network Operations** app, under **Analyze**, click **Reports**.

   The Reports dashboard is displayed.
2. Click **Browse**. Reports that are already run are listed under **Generated Reports**.
3. Under **Generated Reports**, select the report you want to view or download.

   To view the report online, click the report name.

   To download the report, click the report and then click the download icon for either the CSV or PDF file.

The following table explains the parameters available in the **Device and Subscription Inventory** report.

Table 24: ***Device and Subscription Inventory*** *Report Description*

Parameter	Description
AP Inventory	The **AP inventory** page lists the following options both in table and graph form: ■ **Opening**—Total number of unassigned APs in the beginning of the time period. ■ **Purchased**—Number of APs purchased during the time period. ■ **Returned**—Number of APs returned by the tenants to the customer during the time period. ■ **Assigned**—Number of APs assigned to the tenants during the time period. ■ **Closing Stock**—Total of (Opening + Purchased + Returned - Assigned)
Device Management License	The **Device Management License** page lists the following options both in table and graph form: ■ **Opening**—Total number of licenses available in the beginning of the time period. ■ **Purchased**—Number of licenses purchased during the time period. ■ **Returned**—Number of licenses returned by the tenants to the customer during the time period. ■ **Assigned**—Number of licenses assigned to the tenants during the time period. ■ **Expired**—Number of licenses that expired during the time period. ■ **Closing Stock**—Total of (Opening + Purchased + Returned - Assigned - Expired)
Gateway Advanced License	The **Gateway Advanced License** page lists the following options both in table and graph form: ■ **Opening**—Total number of licenses in the beginning of the time period. ■ **Purchased**—Number of licenses purchased during the time period. ■ **Returned**—Number of licenses returned by the tenants to the customer during the time period. ■ **Assigned**—Number of licenses assigned to the tenants during the time period. ■ **Expired**—Number of licenses that expired during the time period. ■ **Closing Stock**—Total of (Opening + Purchased + Returned - Assigned - Expired)
Gateway Base License	The **Gateway Base License** page lists the following options both in table and graph form: ■ **Opening**—Total number of licenses in the beginning of the time period. ■ **Purchased**—Number of licenses purchased during the time period. ■ **Returned**—Number of licenses returned by the tenants to the customer during the time period. ■ **Assigned**—Number of licenses assigned to the tenants during the time period. ■ **Expired**—Number of licenses that expired during the time period. ■ **Closing Stock**—Total of (Opening + Purchased + Returned - Assigned - Expired)
Gateway Foundation License	The **Gateway Foundation License** page lists the following options both in table and graph form: ■ **Opening**—Total number of licenses in the beginning of the time period. ■ **Purchased**—Number of licenses purchased during the time period. ■ **Returned**—Number of licenses returned by the tenants to the customer during the time period. ■ **Assigned**—Number of licenses assigned to the tenants during the time period. ■ **Expired**—Number of licenses that expired during the time period. ■ **Closing Stock**—Total of (Opening + Purchased + Returned - Assigned -

Parameter	Description
	Expired)
Gateway Inventory	The **Gateway Inventory** page lists the following options both in table and graph form: ■ **Opening**—Total number of unassigned gateways in the beginning of the time period. ■ **Purchased**—Number of gateways purchased during the time period. ■ **Returned**—Number of gateways returned by the tenants to the customer during the time period. ■ **Assigned**—Number of gateways assigned to the tenants during the time period. ■ **Closing Stock**—Total of (Opening + Purchased + Returned - Assigned)
Service Token License	The **Service Token License** page lists the following options both in table and graph form: ■ **Opening**—Total number of licenses in the beginning of the time period. ■ **Purchased**—Number of licenses purchased during the time period. ■ **Returned**—Number of licenses returned by the tenants to the customer during the time period. ■ **Assigned**—Number of licenses assigned to the tenants during the time period. ■ **Expired**—Number of licenses that expired during the time period. ■ **Closing Stock**—Total of (Opening + Purchased + Returned - Assigned - Expired)
Switch Inventory	The **Switch Inventory** page lists the following options both in table and graph form: ■ **Opening**—Total number of unassigned switches in the beginning of the time period. ■ **Purchased**—Number of switches purchased during the time period. ■ **Returned**—Number of switches returned by the tenants to the customer during the time period. ■ **Assigned**—Number of switches assigned to the tenants during the time period. ■ **Closing Stock**—Total of (Opening + Purchased + Returned - Assigned)

Deleting a Report

To delete a report, complete the following procedure:

1. From the **Network Operations** app, under **Analyze**, click **Reports**.

   The Reports dashboard is displayed.

2. Click **Browse**.

   Reports that are already run are listed under **Generated Reports**. If any report is yet to run, that report is available under **Scheduled Reports**.

3. Select the report you want to delete and then click the delete icon.

Viewing Audit Trails in the MSP Mode

The **Audit Trail** page shows the logs for all the device management, configuration, and user management events triggered in Aruba Central. You can search or filter the audit trail records based on any of the following columns:

- Occurred on (Custom Range)
- Username

- IP Address
- Category
- Description
- Target
- Source

To view the audit trail log details in Aruba Central MSP mode:

1. From the **Network Operations** app, filter **All Groups**.
2. Under **Analyze**, click **Audit Trail**.
3. Adjust the time filter 🕒 to get the display for the required time range.

The **Audit Trail** logs are displayed for the following types of operations in the MSP:

- Addition, modification, and deletion of tenant accounts
- Addition, modification and deletion of users associated with a tenant account
- Subscription assignment to devices
- Modification of groups associated with a tenant account
- Configuration push, override , and updates for the devices associated with a tenant account
- Addition, modification, and deletion of MSP admin users
- License reconciliation

The **Audit Trail** page in the MSP mode displays the following information:

Table 25: *Audit Trail Pane in the MSP Mode*

Data Pane Content	Description
Occurred On	Time stamp of the events for which the audit trails are shown. Use the filter option to select a specific time range to display the events.
Username	The username of the admin user who applied the changes.
IP Address	IP address of the client device.
Category	Type of modification and the affected device management category. See Classification of Audit Trails.
Target	The group, device, or tenant account to which the changes were applied.
Source	The tenant account in which the changes occurred.
Description	A short description of the changes such as subscription assignment, firmware upgrade, and configuration updates. Click ⋮ to view the complete details of the event. For example, if an event was not successful, clicking the ellipsis displays the reason for the failure.

Classification of Audit Trails

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

- Alert Configuration
- API Gateway
- Configuration

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

Chapter 12
Guest Access

The guest management feature allows guest users to connect to the network and at the same time, allows the administrator to control guest user access to the network.

Aruba Central allows administrators to create a splash page profile for guest users. Guest users can access the Internet by providing either the credentials configured by the guest operators or their respective social networking login credentials. For example, you can create a splash page that displays a corporate logo, color scheme and the terms of service, and enable logging in from a social networking service such as Facebook, Google, Twitter, and LinkedIn.

Businesses can also pair their network with the Facebook Wi-Fi service, so that the users logging into Wi-Fi hotspots are presented with a business page, before gaining access to the network.

To enable logging using Facebook, Google, Twitter, and LinkedIn credentials, ensure that you create an application (app) on the social networking service provider site and enable authentication for that app. The social networking service provider will then issue a client ID and client secret key that are required for configuring guest profiles based on social logins.

Guest operators can also create guest user accounts. For example, a network administrator can create a guest operator account for a receptionist. The receptionist creates user accounts for guests who require temporary access to the wireless network. Guest operators can create and set an expiration time for user accounts. For example, the expiration time can be set to 1 day.

For more information, see the following topics:

- Guest Access Dashboard on page 89
- Creating Apps for Social Login on page 91
- Configuring a Cloud Guest Splash Page Profile on page 94

Guest Access Dashboard

The 📊 **Summary** page in the **Manage > Guest Access** application provides a dashboard displaying the number of guests, guest SSID, client count, type of clients, and guest connection for the selected group.

Table 26 describes the contents of the **Guest Access Overview** page:

Table 26: *Guest Access Overview Page*

Data Pane Item	Description
Time Range	Time range for the graphs and charts displayed on the **Overview** pane. You can choose to view graphs for a time period of 1 day, 1 week, and 1 month.
Guests	Number of guests connected to the SSIDs with Cloud Guest splash page profiles.
Guest SSID	Number of guest SSIDs that are configured to use the Cloud Guest splash page profiles.
Avg. Duration	The average duration of client connection on the SSIDs with Cloud Guest splash page profiles.

Data Pane Item	Description
Max Concurrent Connections	Maximum number of client devices connected concurrently on the guest SSIDs.
Guest Connection (graph)	Time stamp for the client connections on the cloud guest for the selected time range.
Guest Count by Authentication	Number of client devices based on the authentication type configured on the cloud guest SSIDs.
Guest Count by SSID	Number of guest connections per SSID.
Client Type	Type of the client devices connected on the guest SSIDs.

Mapping Cloud Guest Certificates

NOTE

To enable certificates for the Cloud Guest Service, contact the Aruba Central support team.

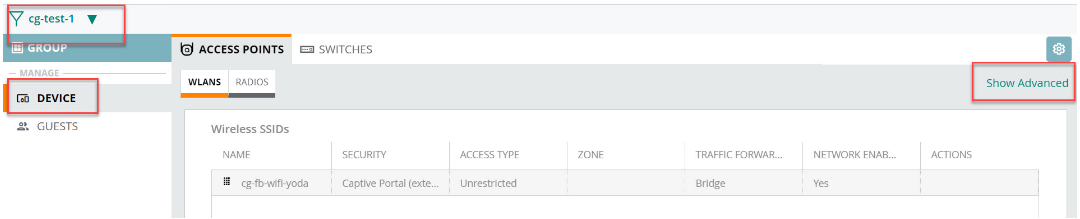
A MSP administrator can upload a new Cloud Guest certificate in the certificate store and map it to Captive Portal for guest user authentication.

To map the cloud guest certificate to Captive Portal:

1. In the **Network Operations** app, use the filter to select **All Groups**.
2. Under **Maintain**, click **Organization**.
3. Click the **Certificates** tab.
4. Click the + sign to upload a certificate to the **Certificate Store**.
5. Use the filter to select the group to which you want to assign the certificate.

   For example, in the following image, a group called **cg-test-1** is selected.
6. Under **Manage**, click **Device** and then click **Show Advanced** > **Security**.

Figure 21 *Click Show Advanced*

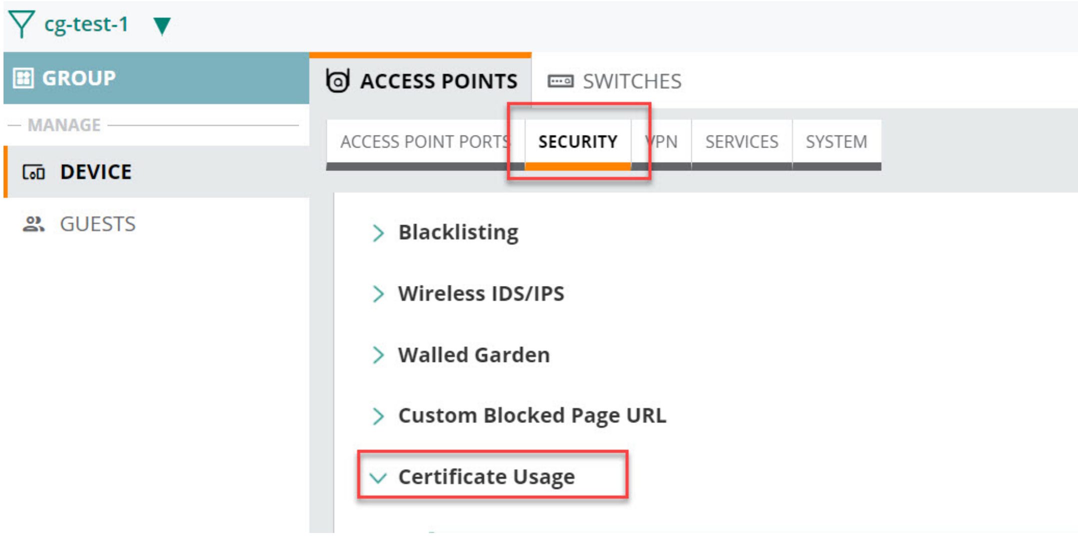


Wireless SSIDs

NAME	SECURITY	ACCESS TYPE	ZONE	TRAFFIC FORWAR...	NETWORK ENAB...	ACTIONS
cg-fb-wifi-yoda	Captive Portal (exte...	Unrestricted		Bridge	Yes	

7. Expand the **Certificate Usage** accordion.

Figure 22 *Click Security and then Expand the Certificate Usage Accordion*



8. Select the required certificate from the **Captive Portal** drop-down list.
9. Click **Save Settings**.

Creating Apps for Social Login

The following topics describe the procedures for creating applications to enable the social login feature:

- Creating a Facebook App
- Creating a Google App
- Creating a Twitter App
- Creating a LinkedIn App

Creating a Facebook App

Before creating a Facebook app, ensure that you have a valid Facebook account and you are registered as a Facebook developer with that account.

To create a Facebook app, complete the following steps:

1. Visit the Facebook app setup URL at https://developers.facebook.com/apps.
2. From **My Apps**, select **Add a New App**.
3. Enter the app name and your email address in the **Display Name** and **Contact Email** text boxes, respectively.
4. Click **Create App ID**.
5. Hover the mouse on **Facebook Login** and select **Setup**.
6. Click **Web** (that is, the WWW platform).
7. Enter the website URL in the **Site URL** box.

   This URL is the same as the server URL mapped in the splash page configuration.
8. Click **Save**.
9. Read through the Next Steps section for further information on including Login Dialog, Access Tokens, Permissions, and App Review.
10. Go to **PRODUCTS** > **Facebook Login** > **Settings** from the left navigation menu.
11. Click the **Client OAuth Login** toggle switch to turn to **Yes**.

12. Enter the OAuth URI in the **Valid OAuth redirect URIs** box.

    The URI is the server URL mapped in the splash configuration with **/oauth/reply** appended to it. To get the valid Oauth redirect URL, go to the **Guest Access > Splash Pages** path and click the eye (◎) icon available against the specific splash page name in the **Splash Pages** table.

NOTE

Ensure that the URL is an HTTPS URL with a domain name and not the IP address. For example, https://example1.cloudguest.arubanetworks.com/oauth/reply.

13. From the left navigation menu, select **App Review**.
14. Select the **Make <App Name> Public** toggle switch to make your app available to public.
15. Click **Category**.
16. In the **Choose a Category** pop-up window, select a category.
17. Click **Confirm**.
18. Select other extra permissions you want to provide for the users of your app.

    There are 41 permissions available for you to select from.
19. Click **Add xx Items**, where x represents the number of permissions you selected.
20. Enter the reason for providing specific permissions and click **Save**.
21. Click **Submit for Review**.
22. On the left navigation pane, click the **Settings** icon.

    Note the app ID and app secret key. Use the app ID and secret key when configuring Facebook login in the Aruba Central UI.
23. Under **App Domains**, enter the server URL.

Creating a Google App

Before creating a an app for Google based login, ensure that you have a valid Google account.

To create a Google app, complete the following steps:

1. Access the Google Developer site at https://code.google.com/apis/console.
2. To select an existing project, click **Select a project** and select the desired project.
3. If the project is not created, click **Create a project**, enter the project name and click **Create**.
4. Click **Enable APIs and Services**.
5. Navigate to **Social** category, and then click **Google API**. The **Google API** window opens.
6. To enable the API, click **Enable**.
7. Click **Create Credentials**. If the credentials are already created, click **Go to credentials**.
8. In the **Credentials** pane, perform the following actions:

- Under the **Where will you be calling the API from** section, select **Web Browser**.
- Under the **What data you will be accessing** section, select **User Data**.
- Click **What Credentials do I need**.

9. Under **Create an OAuth 2.0 client ID**. Enter the **OAuth 2.0 Client ID Name**.
10. Under **Authorized JavaScript Origins**, enter the base URL with FQDN of the cloud guest instance that will be hosting the captive portal. For example, https://%hostname%/.
11. Under **Authorized Redirect URIs**, enter the cloud server OAuth reply URL that includes the FQDN of the cloud server instance with /oauth/reply appended at the end of the URL.

NOTE

Ensure that the URL is an HTTPS URL with a domain name and not the IP address. For example, https://example1.cloudguest.examplenetworks.com/oauth/reply.

12. Click **Create Client ID**.

    Under **Set up the OAuth 2.0 consent screen**, provide your **Email Address** and product name, and then click **Continue**. The client ID is displayed.

13. Click **Done**. A page showing the OAuth Client IDs opens.

14. Click the **Oauth client ID** to view the client ID and client secret key.

    Use this client ID and client secret key when configuring Google login in the Aruba Central UI.

Creating a Twitter App

Before creating a Twitter app, ensure that you have a valid Twitter accosunt.

To create a Twitter app, complete the following steps:

1. Visit the Twitter app setup URL at https://apps.twitter.com.
2. Click **Create New App**. The **Create an application** web page is displayed.
3. Enter the application name and description.
4. For OAuth 2.0 Redirect URLs, enter the HTTPS URL of the cloud guest server to which you want to connect this social authentication source, and append /oauth/reply at the end of the URL.

Ensure that the URL is an HTTPS URL with a domain name and not the IP address. For example, https://exa.example.com/oauth/reply.

5. Select **Yes, I agree** to accept the Developer Agreement terms.
6. Click **Create a Twitter application**.
7. Click **Manage Keys and Access Tokens**.

   The **Keys and Access Tokens** tab opens. The consumer key (API key) and consumer secret (API key) are displayed.

8. Note the ID and the secret key. The consumer key and consumer secret key when configuring Twitter login in Aruba Central UI.

Creating a LinkedIn App

Before creating a LinkedIn app, ensure that you have a valid LinkedIn account.

To create a LinkedIn app, complete the following steps:

1. Visit the LinkedIn app setup URL at https://developer.linkedin.com.
2. Click **My Apps**. You will be redirected to https://www.linkedin.com/secure/developer/apps.
3. Click **Create Application**. The **Create a New Application** web page is displayed.
4. Enter your company name, application name, description, website URL, application logo with the specification mentioned, application use, and contact information.
5. Click **Submit**. The **Authentication** page is displayed.
6. Note the client ID and client secret key displayed on the **Authentication** page.
7. For **OAuth 2.0 Redirect URLs**, enter the HTTPS URL of the cloud guest server to which you want to connect this social authentication source and append /oauth/reply at the end of the URL.
8. Click **Add** and then click **Update**. The API and secret keys are displayed.
9. Note the API and secret key details. Use the API ID and secret key when configuring LinkedIn login in the Aruba Central UI.

Configuring a Cloud Guest Splash Page Profile

The Guest Access app allows MSP administrators to configure Splash Page profiles for tenant accounts. If the tenant account is mapped to a group and the Guest Access service is enabled on the tenant account, the tenant account users inherit the splash page profiles configured in the MSP. If the group associated to a tenant account is locked for editing on the MSP mode, the tenant account users cannot edit the Splash Page profiles inherited from the MSP.

MSP administrator users can delete only those Splash Pages that are not linked to any tenant account.

This topic describes the following procedures:

- Adding a Cloud Guest Splash Page Profile
- Customizing a Splash Page Design
- Configuring a Cloud Guest Splash Page Profile
- Localizing a Cloud Guest Portal
- Associating a Splash Page Profile to an SSID

Adding a Cloud Guest Splash Page Profile

To create a splash page profile:

1. From the **Network Operations** app, filter a group.
2. Under **Manage**, click **Guests** to display the **Splash Page**.

   You can create splash page profiles only for the individual groups.
3. To create a new Splash page, click the + icon.

   The **New Splash Page** pane is displayed.
4. On the **Configuration** tab, configure the parameters described in the following table:

Table 27: *Splash Page Configuration*

Data Pane Content	Description
Name	Enter a unique name to identify the splash profile. **NOTE:** If you attempt to enter an existing splash profile's name, Aruba Central displays a message stating that **Splash page with this name already exists**.
Type	Configure any of the following authentication methods to provide a secure network access to the guest users and visitors. ■ **Anonymous** ■ **Authenticated** ■ **Facebook Wi-Fi**
Anonymous	Configure the **Anonymous** login method if you want to allow guest users to log in to the Splash page without providing any credentials. For anonymous user authentication, you can also enable a pre-shared key to allow access. To enable a pre-shared key based authentication, set the **Guest Key** to ON and specify a password.
Authenticated	Configure authentication and authorization attributes, and login credentials that enable users to access the Internet as guests. You can configure an authentication method based on sponsored access and social networking login profiles. The authenticated options available for configuring the cloud guest splash page are described in the following rows.

Table 27: *Splash Page Configuration*

Data Pane Content	Description
Username/Password	The **Username/Password** based authentication method allows pre-configured visitors to obtain access to wireless connection and the Internet. The visitors or guest users can register themselves by using the splash page when trying to access the network. The password is delivered to the users through print, SMS or email depending on the options selected during registration. To allow the guest users to register by themselves: 1. Enable **Self-Registration**. 2. Set the **Verification Required** to **ON** if the guest user account must be verified. 3. Specify a verification criteria to allow the self-registered users to verify through email or phone. - If email-based verification is enabled and the **Send Verification Link** is selected, a verification link is sent to the email address of the user. The guest users can click the link to obtain access to the Internet. - If phone-based verification is enabled, the guest users will receive an SMS. The administrators can also customize the content of the SMS by clicking on **Customize SMS**. 4. Specify the duration within the range of 1-60 minutes, during which the users can access free Wi-Fi to verify the link. The users can log in to the network for the specified duration and click the verification link to obtain access to the Internet. By default, the expiration date for the accounts of self-registered guest users is set to infinite during registration. The administrator or the guest operator can set the expiration date after registration.
Social Login	**Social Login**—Enable this option to allow guest users to use their existing login credentials from social networking profiles such as Facebook, Twitter, Google, or LinkedIn and sign into a third-party website. When a social login based profile is configured, a new login account to access the guest network or third-party websites is not required. - **Facebook**— Allows guest users to use their Facebook credentials to log in to the splash page. To enable Facebook integration, you must create a Facebook app and obtain the app ID and secret key. For more information on app creation, see Creating a Facebook App. Enter the app ID and secret key for client ID and client Secret respectively to complete the integration. - **Twitter**—Allows guest users to use their Twitter credentials to log in to the splash page. To enable Twitter integration, you must create a Twitter app and obtain the app ID and secret key. For more information, see Creating a Twitter App. Enter the app ID and secret key for client ID and client secret respectively to complete the integration. - **Google**—Allows guest users to use their Google credentials to log in to the splash page. To enable Google integration, you must create a Google app and obtain the app ID and secret key. For more information, see Creating a Twitter App . 1. Enter the app ID and secret key for client ID and client secret respectively. 2. To restrict authentication attempts to only the members of a Google hosted domain, enter the domain name in the **Gmail for Work Domain** text box. Ensure that you have a valid domain account licensed by Google Domains or Google Apps. For more information see: - https://apps.google.com/intx/en_in/ - https://domains.google.com/about/ 3. Specify a text for the Sign-In button. - **LinkedIn**—Allows guest user to use their LinkedIn credentials to log in to the splash page. To enable LinkedIn integration, you must create a LinkedIn app and obtain the app ID and secret key. For more information, see Creating a LinkedIn App. Enter the app ID and secret key for client ID and client secret respectively to complete the integration.

Table 27: *Splash Page Configuration*

Data Pane Content	Description
Facebook Wi-Fi	If you want to enable network access through the free Wi-Fi service offered by Facebook. Select the **Facebook Wi-Fi** option. The Facebook Wi-Fi feature allows you to pair your network with a Facebook business page, thereby allowing the guest users to log in from Wi-Fi hotspots using their Facebook credentials. If the Facebook Wi-Fi business page is set up, when the users try to access the Internet, the browser redirects the user to the Facebook page. The user can log in with their Facebook account credentials and can either check in to access free Internet or skip checking in and then continue.
Facebook Wifi Configuration	After selecting the Facebook Wi-Fi option, complete the following steps to continue with the Facebook Wi-Fi configuration. 1. Click the **Configure Now** link. 2. Sign in to your Facebook account. 3. If you do not have a business page, click **Create Page**. For more information on setting Facebook Wi-Fi service, see **Setting up Facebook Wi-Fi for Your Business** at https://www.facebook.com/help/126760650808045. **NOTE:** Instant AP devices support Facebook Wi-Fi services on their own, without Aruba Central. However, for enabling social login based authentication, the guest splash pages must be configured in Aruba Central. For more information on Facebook Wi-Fi configuration on an Instant AP, see the *Aruba Instant User Guide*.
Allow Internet In Failure	To allow users access the Internet when the external captive portal server is not available, click the **Allow Internet In Failure** toggle switch. By default, this option is disabled.
Override Common Name	To override the default common name, click the **Override Common Name** toggle switch and specify a common name. The common name is the web page URL of the guest access portal. By default, the common name is set to **securelogin.arubanetworks.com**. The guest users can override this default name by adding their own common name. If your devices are managed by AirWave and you want to use your own certificate for the captive portal service, ensure that the captive portal certificate is pushed to the Instant AP from the AirWave management system. When the appropriate certificate is loaded on the AP, perform the following actions: 1. Run the **show captive-portal-domains** command at the Instant AP command prompt. 2. Note the common name or the internal captive portal domain name. 3. Add this domain name in the **Override Common Name** field on the **Splash Page** configuration page. 4. Save the changes.
Guest Key	To set password for anonymous users, enable the Guest Key and enter a password.
Sponsored Guest	Enable the **Sponsored Guest** option to provide authorization control to a guest sponsor for allowing and denying a guest from accessing the network.
Allowed Sponsor Domains	Enter accepted company domain names. The domain name must match the suffix of the sponsor's email address. The domain names must be company names and not any public domain names such as gmail, yahoomail, and so on. To add more domain names, click the add icon and enter the domain name. This is a mandatory field.
Allowed Sponsor Emails	Enter the allowed email addresses. If you leave this field empty, all emails that correspond to the allowed domains list are permitted to sponsor guests. To add more sponsor emails, click the add icon and enter the sponsor's email address. This is an optional field.
Authentication Success Behavior	If **Anonymous** or **Authenticated** option is selected as the guest user authentication method, specify a method for redirecting the users after a successful authentication. Select one of the following options:

Table 27: *Splash Page Configuration*

Data Pane Content	Description
	■ **Redirect to Original URL**— When selected, upon successful authentication, the user is redirected to the URL that was originally requested. ■ **Redirect URL**— Specify a redirect URL if you want to override the original request of users and redirect them to another URL.
Authentication Failure Message	If the **Authenticated** option is selected as the guest user authentication method, enter the authentication failure message text string returned by the server when the user authentication fails.
Session Timeout	Enter the maximum time in Day(s): Hour(s): Minute(s) format for which a client session remains active. The default value is 0:8:00. When the session expires, the users must re-authenticate. If MAC caching is enabled, the users are allowed or denied access based on the MAC address of the connective device.
Share This Profile	Select this check box if you want to allow the users to share the Splash Page profile. The Splash Page profiles under All Devices can be shared across all the groups.
Daily Usage Limit	Use this option to set a data usage limit for authenticated guest users, anonymous profiles, and Facebook Wi-Fi logins. By default, no daily usage limit is applied. To set a daily usage limit, use one of the following options: ■ **By Time**— Specify the time limit in hours and minutes for data usage during a day. When a user exceeds the configured time limit, the device is disconnected from the network until the next day begins; that is, until 00.00 hours in the specified timezone. ■ **By Data**— Specify a limit for data usage in MB. You can set this limit to either **Per User**, **Per Session**, or **Per Device**. When the data usage exceeds the configured limit, the user device is disconnected from the network until the next day begins; that is, until 00.00 hours in the specified time zone. ● **Per User**— This option applies the data usage limit based on authenticated user credentials. ● **Per Session**—This option applies the data usage limit based on user sessions. ● **Per Device**—This option applies the data usage limit based on the MAC address of the client device connected to the network. **Important Points to Note** ■ The values configured for this feature do not serve as hard limits. There might be a slight delay in enforcing daily usage limits due to the time required for processing information. ■ For anonymous and Facebook Wi-Fi logins, the daily usage limit is applied per MAC address of the client device connected to the network.
Whitelist URL	To allow a URL, click + and add the URL to the whitelist. For example, if the terms and conditions configured for the guest portal include URLs, you can add these URLs to the whitelist, so that the users can access the required web pages.

Customizing a Splash Page Design

1. From the **Network Operations** app, filter a group.
2. Under **Manage**, click **Guests** to display the **Splash Page**.

   You can create splash page profiles only for the individual groups.
3. To create a new splash page, click the + icon.

   The **New Splash Page** pane is displayed.

To customize a splash page design, on the **Guest Access > Splash Page > New Splash Page > Customization** pane, configure the parameters described in the following table:

Table 28: *Splash page customization*

Data Pane Content	Description
Background color	To change the color of the splash page, select a color from the **Background Color** palette.
Button color	To change the color of the sign in button, select a color from the **Button Color** palette.
Header fill color	Select the fill color for the splash page header from the **Header fill color** palette.
Page font color	To change the font color of the text on the splash page, select a color from the **Page font color** palette.
Page font Color	Select the font color of the splash page from the palette.
Logo	To upload a logo, click **Browse**, and browse the image file. Ensure that the image file size does not exceed 256 KB.
Background Image	Click **Browse** to upload a background image. Ensure that the background image file size does not exceed 512 KB.
Page Title	Add a suitable title for the splash page.
Welcome Text	Enter the welcome text to be displayed on the splash page. Ensure that the welcome text does not exceed 20,000 characters.
Terms & Conditions	Enter the terms and conditions to be displayed on the splash page. Ensure that the terms and conditions text does not exceed 20000 characters. The text box also allows you to use HTML tags for formatting text. For example, to highlight text with italics, you can wrap the text with the <i> </i> HTML tag. Specify an acceptance criteria for terms and condition by selecting any of the following options from the **Display "I Accept" Checkbox**: ■ **No, Accept by default** ■ **Yes, Display Checkbox** If the **I ACCEPT** check box must be displayed on the Splash page, select the display format for terms and conditions. Ensure that **Display Option For Terms & Conditions** has the Inline Text option auto-selected and displayed as an uneditable text.
Ad Settings	If you want to display advertisements on the splash page, enter the URL in the **Advertisement URL**. For **Advertisement Image**, click **Browse** and upload the image.

Localizing a Cloud Guest Portal

1. From the **Network Operations** app, filter a group.
2. Under **Manage**, click **Guests** to display the **Splash Page**.

   You can create splash page profiles only for the individual groups.
3. To create a new splash page, click the + icon.

   The **New Splash Page** pane is displayed.

To localize or translate the Cloud Guest portal content, on the **Guest Access > Splash Page > New Splash Page > Localization** pane, configure the parameters described in the following table:

NOTE

These are optional settings unless specified as a required parameter explicitly.

Table 29: *Cloud Guest Portal Localization*

Data Pane Content	Description	Allowed Length of Text
Login Section		
Login button title	Enter the custom label text to be localized for the **Login** button.	1–255 characters
Network login title	Enter the custom title text that you want to localize for the **Network Login** page.	1–255 characters
Login page title	Enter the custom text for title in the **Login** page.	1–255 characters
Access denied page title	Enter the custom title text for the **Access Denied** page.	1–255 characters
Logged in title	Enter the custom **Logged in** title text for the page that allows access.	1–255 characters
Username label	Enter the custom text for **Username** lable.	1–255 characters
Username placeholder	Enter the custom text to show in in the **Username** placeholder.	1–255 characters
Password placeholder	Enter the custom text to show in in the **Password** placeholder.	1–255 characters
Email address placeholder	Enter the custom text to show in in the **Email Address** placeholder.	1–255 characters
Register button title	Enter the custom title text for **Register** button.	1–255 characters
Network login button title	Enter the custom title text for **Network Login** button.	1–255 characters
Terms and Conditions title	Enter the custom text to show in the **Terms and Conditions** title.	1–255 characters
'I accept the Terms and Conditions' text	Enter the custom text to show for the **'I accept the Terms and Conditions'** text adjacent to the check box.	Up to 20000 characters
Welcome Text	Enter a custom Welcome text to the cloud guest portal user.	Up to 20000 characters
Login failed message	Enter a custom text to show for the **Login Failed** message when a user's login attempt gets denied or fails.	Up to 20000 characters
Logged in message	Enter a custom text to show for the **Logged in** message in the access allowed page.	Up to 20000 characters
Register Section		

Table 29: *Cloud Guest Portal Localization*

Data Pane Content	Description	Allowed Length of Text
Phone help message	Enter a custom help message to show for the **Phone** help field.	Up to 20000 characters
Phone number placeholder	Enter the custom placeholder text for the **Phone Number** input UI control.	1–255 characters
'Back' button text	Enter the custom text label to show for the **Back** button control.	1–255 characters
'Continue' button text	Enter the custom text label toshow for the **Continue** button control.	1–255 characters
Email radio button	Enter a custom text label for the **Email** option.	—
Phone radio button	Enter a custom label text for the **Phone** option.	—
Register page title	Enter a custom title text for the **Register** page.	1–255 characters
Accept button title	Enter a custom title text for the **Accept** button.	1–255 characters
Register Page instructions	Enter a custom message to show in the **Register** page.	Up to 20000 characters
Verification Section		
Verification code label	Enter a custom text to show for the **Verification code** label.	1–255 characters
Verification code placeholder	Enter a custom text to show for the **Verification code** placeholder.	1–255 characters
Verification email check message	Enter a custom text for the **Verification Email Check** message. This is shown in the verification pending page.	Up to 20000 characters
Verification email notice message	Enter a custom text for the **Verification Email Notice** message. This is the message notifying the user when the email will be sent.	Up to 20000 characters
Verification email sent message	Enter a custom text for the **Verification Email Sent** message.	Up to 20000 characters
Verification phone notice message	Enter a custom text for the **Verification Phone Notice** message. This is the message notifying the user that an SMS has been sent.	Up to 20000 characters
Verified account message	Enter a custom text for the **Verified Account** message. This is the message that will be shown in the Verified page.	Up to 20000 characters
Verify account message	Enter a custom text for the **Verify Account** message. This is the message that will be shown in the Verify page.	Up to 20000 characters

Table 29: *Cloud Guest Portal Localization*

Data Pane Content	Description	Allowed Length of Text
Verify button title	Enter a custom label text for the **Verify** button.	1–255 characters
Verify title	Enter a custom text for **Verify** title.	1–255 characters
Network login message	Enter a custom text message to show in the **Network Login** page.	Up to 20000 characters

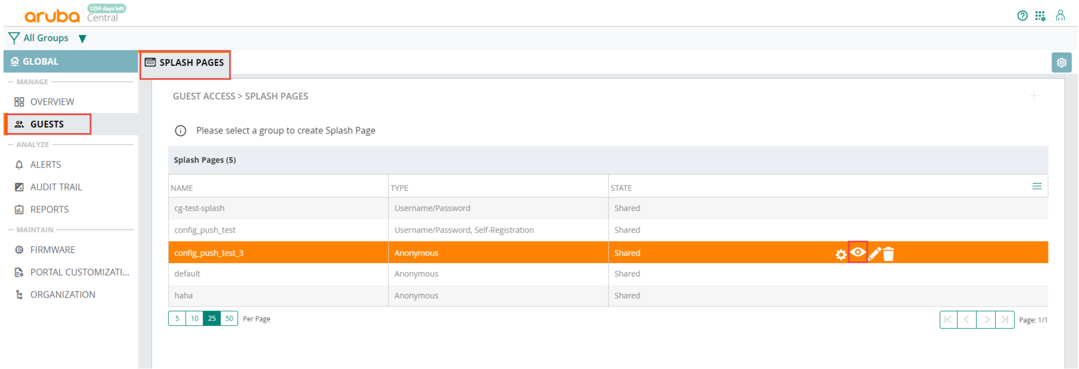
4. Click **Preview** to preview the localized cloud guest portal page or click **Finish**.

Previewing and Modifying a Splash Page Profile

To preview a splash page profile, complete the following steps:

1. From the **Network Operations** app, filter a group.
2. Under **Manage**, click **Guests** to display the **Splash Page**.

   A list of splash page profiles is displayed.
3. Ensure that the pop-up blocker on your browser window is disabled.
4. Hover over the splash profile you want to preview and click the preview icon. The Splash Page is displayed in a new window.



Please select a group to create Splash Page

Splash Pages (5)

NAME	TYPE	STATE
cg-test-splash	Username/Password	Shared
config_push_test	Username/Password, Self-Registration	Shared
config_push_test_3	Anonymous	Shared
default	Anonymous	Shared
haha	Anonymous	Shared

The **Splash Pages** page also allows you to perform any of the following actions:

- To view the Splash Page configuration text in an overlay window, click the settings icon next to the profile. You can copy the configuration text and apply it to AirWave managed APs using configuration templates.
- To modify a splash page profile, click the edit icon ext to the profile form list of profiles displayed in the Splash Page Profiles pane.
- To delete a profile, select the profile and click the delete icon next to the profile.

Associating a Splash Page Profile to an SSID

To associate a splash page profile with an SSID, complete the following steps:

1. From the **Network Operations** app, filter a group.
2. Under **Manage**, click **Device** > **Access Points**.
3. Click the configuration icon ⚙ to open the configuration window.

4. Under **WLANs**, click **+Add SSID**.

5. The **Create a New Network** pane is displayed.

6. Refer to the AP configuration page for Aruba Central Online Help for more detailed information on how to create the network .

Chapter 13
Frequently Asked Questions

How do I create an Aruba Central MSP account?

As MSP mode is an operational mode of the **Network Operations** app which is one of the apps in Aruba Central, the first step to create an MSP account is to create an Aruba Central account, subscribe only to the **Network Operations** app, and then enable **Managed Service Mode**.

- Sign up for Aruba Central evaluation here.
- Follow the steps in the Enabling the Managed Service Mode section to enable MSP mode.

Should tenants sign up for an Aruba Central account as well?

No. With MSP mode enabled, the MSP administrator manages the creation and deletion of tenant accounts. After a tenant account is created, the MSP administrator can add tenant users to the account.

To create a tenant user, the MSP administrator must provide a valid email address for the user. A verification email is sent to this email address.

Tenant users have access to their individual tenant account only. Tenant users do not have access to other tenant accounts managed by the MSP.

Who owns the hardware and subscriptions?

In the MSP mode, all the hardware and subscriptions are owned by the MSP. The MSP temporarily assigns devices and their corresponding subscriptions to tenants for the duration of the managed service contract. When the contract ends, the devices and the subscriptions are returned back to the common pool of resources of the MSP and can be reassigned to another tenant.

Can existing Aruba Central customers migrate to an MSP account?

End customers who own their own devices and subscriptions cannot transfer ownership of the devices to an MSP. However, the MSP administrator can manage the end customer network.

What are the supported devices and architectures?

MSP supports all devices and architectures supported by Aruba Central.

See Supported APs and Supported Switches.

Aruba Central support wireless, wired, and SD-WAN deployments, either independently or in combination. For example, as an MSP, you can manage the following combinations:

- Customer environments having a wireless deployment.
- Customer environments having both wired and wireless deployments.
- Customer environments having an SD-WAN deployment.

NOTE

Aruba Central does not support managing gateways at the MSP level. However, gateways can be configured and managed at the tenant account level.

Which group is the default group for the tenant account?

The MSP group associated to the Tenant account shows up as the default group for Tenant account users. All configuration changes made to the “MSP group” associated to the “Tenant account” are applied to the default group on the Tenant account.

What are predefined user roles?

The **Users & Roles** tile under **Global Settings** in the **Account Home** page allows you to configure the following types of users with system-defined roles:

User Role	Standard Enterprise Mode	MSP Mode
admin	■ Has full access to all devices. ■ Can provision devices and enable access to application services. ■ Can create or update users, groups, and labels.	■ Has full access to tenant accounts. ■ Can create, modify, provision, and manage tenant accounts.
readwrite	■ 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	■ Can view the groups and devices. ■ Can view generated reports.	Can view tenant accounts.
guestoperator	■ Can access and modify cloud guest splash page profiles. ■ Can configure visitor accounts for the cloud guest splash page profiles.	■ Can access and modify cloud guest splash page profiles. ■ Can configure visitor accounts for the cloud guest splash page profiles.

What are custom user roles?

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

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

You can create a custom role with specific access to MSP modules. The **MSP** application allows users with administrator role and privileges to define user access to MSP modules such as Customer Management and Portal Customization. The MSP tenant account user does not have access to the **MSP** application. Even if a tenant account user is assigned a custom role having **MSP** application privileges, the tenant account user will not have access to the **MSP** application and **MSP** will not appear in the **Global Settings** > **Users & Roles** > **Roles** > **Allowed Applications** list.

What tasks can be performed by an MSP user and tenant user?

In the MSP mode, MSP users have a superset of administration options compared to tenant users.

An MSP administrator can perform the following administrative tasks:

- Tenant account management.

- Device and subscription management across all tenants.
- Monitoring and event management across all tenants.
- Configuration management across all tenants.
- User management across all tenants.
- API management for the MSP and across all tenants.

A tenant account administrator can perform the following administrative tasks for their respective tenant account only:

- Monitoring and event management.
- Configuration management.
- User management.
- API management.