

Aruba Central Managed Service Provider



User Guide

Copyright Information

© Copyright 2019 Hewlett Packard Enterprise Development LP.

Open Source Code

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

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

Contents	3
About This Document	8
Intended Audience	8
Related Documents	8
Conventions	8
Contacting Support	9
About Aruba Central	10
Key Features	10
Operational Modes and Interfaces	11
Standard Enterprise Mode	11
Managed Service Provider Mode	11
Supported Web Browsers	12
MSP User Interface	12
Left Navigation Pane	13
Search Bar	14
User Icon	14
Filter bar	15
Data Pane	15
Notifications Pane	15
Supported Devices	15
Supported Instant APs	16
Supported Switch Platforms	16
Groups in the MSP Mode	17
Tenant Default Group Overrides	17
Creating an MSP UI Group	18

Frequently Asked Questions	19
How do I create an Aruba Central MSP account?	19
Should tenants sign up for an Aruba Central account as well?	19
Who owns the hardware and subscriptions?	19
Can existing Aruba Central customers migrate to an MSP account?	19
What are the supported devices and architectures?	19
Which group is the default group for the tenant account?	20
What are predefined user roles?	20
What are custom user roles?	20
What tasks can be performed by an MSP user and tenant user?	20
MSP Deployment Models	22
Deployment Model 1	22
Example Deployment Scenario	23
Deployment Model 2	26
Example Deployment Scenario	26
Using the Switch Customer Option	28
Deployment Model 3	29
Getting Started with MSP Solution	30
Steps to Complete	30
MSP Overview	31
Groups in the MSP Mode	31
User Accounts and Roles in the MSP Mode	31
Terminology	32
Enabling the Managed Service Mode	32
Disabling the Managed Service Mode	32
Creating an Aruba Central Account	33
Zones and Sign Up URLs	33
Signing up for an Aruba Central Account	33

Accessing Aruba Central Portal	37
Login URLs	37
Logging in to Aruba Central:	38
Changing Your Password	38
Logging Out of Aruba Central	38
Managing Subscriptions	39
Managing Subscription Keys	39
Viewing Subscription Key Details	40
Supported Subscription Types	40
Assigning Subscriptions	41
Manually Assigning Subscriptions	42
Assigning Network Service Subscriptions	43
Assigning Gateway Subscriptions	43
Gateway Subscriptions	43
Assigning Subscriptions to Gateways	43
Removing Subscriptions from Devices	44
Acknowledging Subscription Expiry Notifications	44
Renewing Subscriptions	44
Onboarding Devices	45
Adding Devices (Evaluation Account)	45
Adding Devices (Paid Subscription)	45
Manually Adding Devices When Device Sync Fails	46
Provisioning Tenant Accounts	48
Creating a Tenant Account and Mapping to an MSP Group	48
Points to Note:	49
Viewing Tenant Account Details	50
Editing a Tenant Account	50
Deleting a Tenant Account	50
Assigning Devices to Tenant Accounts	51

Assigning Subscriptions	51
Assigning Device Subscriptions	51
Enabling Automatic Assignment of Device Subscriptions	52
Enabling Automatic Subscription Assignment in the MSP Mode	52
Assigning Service Subscriptions to Devices	52
User Accounts and Roles in MSP Mode	53
Configuring User Accounts for the MSP Mode	53
Adding a User Account	53
Editing a User Account	54
Deleting a User Account	54
Customizing Portal	54
Uploading Certificates in the MSP Mode	54
Configuring Instant APs	56
Mapping Cloud Guest Certificates	56
Configuring Switches	57
Aruba Gateways	58
MSP Dashboard	59
Dashboard	59
Dashboard Summary	59
Overview	60
Trends	62
Navigating to the Tenant Account	62
Points to Note:	62
MSP Alerts	63
Configuring Alerts at the MSP Level	64
Configuring Alerts at the Tenant Account Level	65
Alerts Dashboard and Acknowledging Alerts	65
Viewing Enabled Alerts	66

Maintenance	67
Viewing Firmware Information	67
Setting Compliance for a Device	72
Viewing Audit Trails	75
Viewing Audit Trails in MSP	75
Classification of Audit Trails	76
Guest Access	77
Guest Access Dashboard	77
Creating Apps for Social Login	78
Creating a Facebook App	78
Creating a Google App	79
Creating a Twitter App	80
Creating a LinkedIn App	80
Configuring a Cloud Guest Splash Page Profile	81
Adding a Cloud Guest Splash Page Profile	81
Customizing a Splash Page Design	85
Previewing and Modifying a Splash Page Profile	86
Localizing a Cloud Guest Portal	86
Associating a Splash Page Profile to an SSID	90

This guide provides an overview of the Managed Service Provider (MSP) mode 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*
- *Aruba Central MSP User Guide*

Conventions

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

Table 1: *Typographical Conventions*

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

The following informational icons are used throughout this guide:



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



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



Indicates a risk of personal injury or death.

Contacting Support

Table 2: *Contact Information*

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

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

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

- [Key Features on page 10](#)
- [Supported Devices on page 15](#)

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 and wireless Infrastructure management—Offers a centralized management interface for managing wireless and wired networks in distributed environments, and thus help organizations save time and improve efficiency.
- Secure cloud based platform—Offers a secure cloud platform with HTTPS connection and certificate based authentication.
- 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.
- Health and usage monitoring—Provides a comprehensive view of your network, device status and health, and application usage. You can monitor, identify, and address issues by using data-driven dashboards, alerts, reports, and troubleshooting workflows. Aruba Central also utilizes the DPI feature of the devices to monitor, analyze and block traffic based on application categories, application type, web categories and website reputation. Using this data, you can prioritize business critical applications, limit the use of inappropriate content, and enforce access policies on a per user, device or location basis.
- Guest Access—Allows you to manage access for your visitors with a secure guest Wi-Fi experience. You can create guest sponsor roles and social logins for your guest networks. You can also design your guest landing page with custom logos, color, and banner text.
- Presence Analytics—Offers a value added service for Instant AP based networks to get an insight into user presence and loyalty. The Presence Analytics dashboard allows you to view the presence of users at a specific site and the frequency of user visits at a given location or site. Using this data, you can make business decisions to improve customer engagement.
- Analytics for Client Service Assurance—Provides a value added service called Clarity that helps you analyze and monitor client onboarding and connectivity health. Using this data, you can proactively address issues pertaining to client connectivity and enhance user experience.

Operational Modes and Interfaces

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

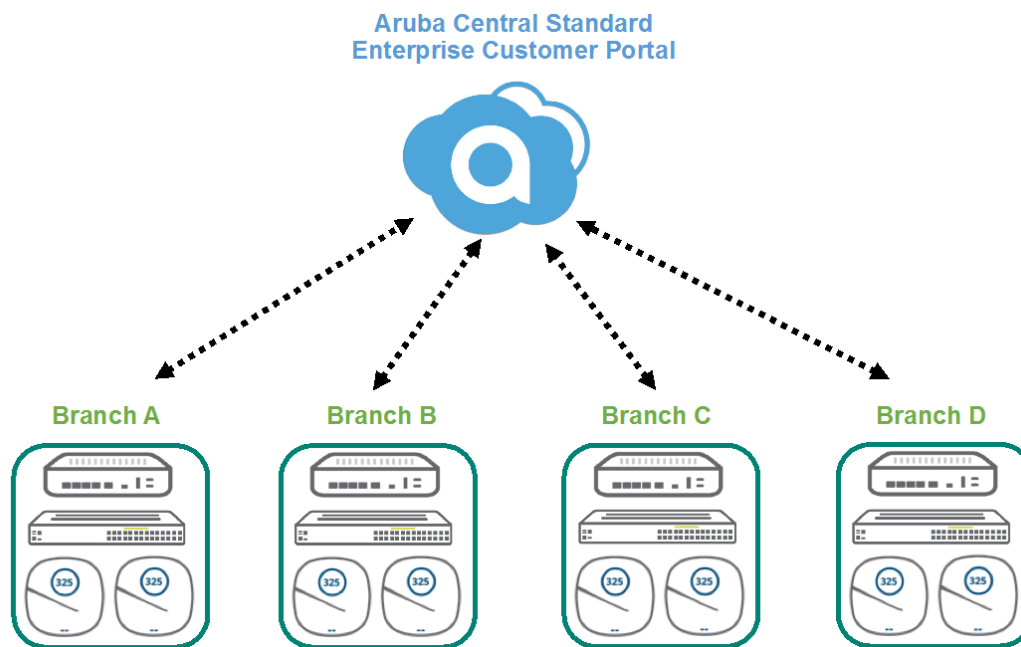
- [Standard Enterprise Mode](#)
- [Managed Service Provider Mode](#)

Standard Enterprise Mode

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

[Figure 1](#) illustrates a typical Standard Enterprise mode deployment.

Figure 1 *Standard Enterprise Mode*

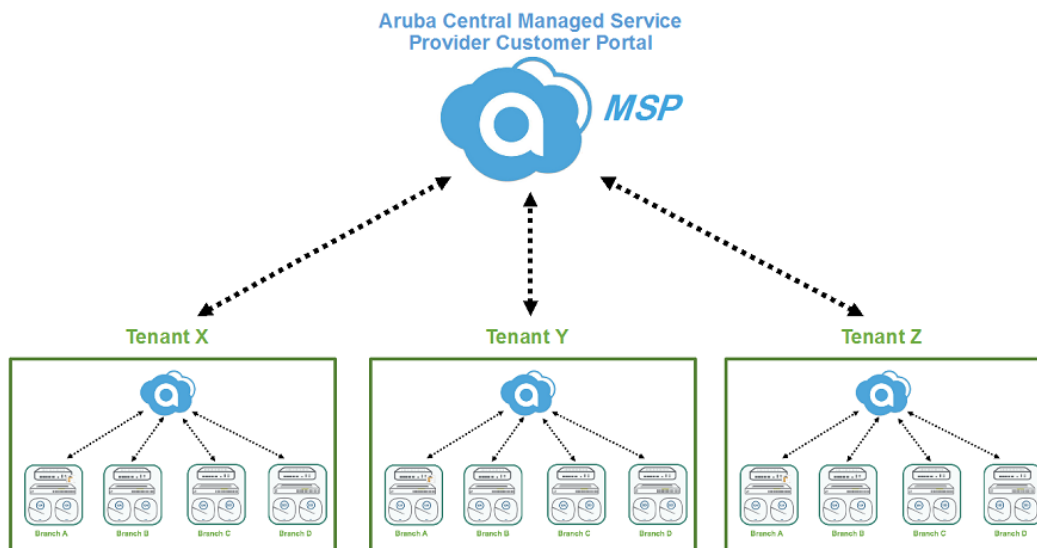


Managed Service Provider Mode

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

[Figure 2](#) illustrates a typical MSP mode deployment.

Figure 2 *Managed Service Provider Mode*



Supported Web Browsers



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

MSP User Interface

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

The MSP UI consists of the following elements:

- [Left Navigation Pane on page 13](#)
- [Search Bar on page 14](#)
- [User Icon on page 14](#)
- [Filter bar on page 15](#)
- [Data Pane on page 15](#)
- [Notifications Pane on page 15](#)

Left Navigation Pane

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

App Selector

The app selector lists the apps available for MSP users.



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

Monitoring and Reports

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

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

Wireless Configuration

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

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

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

Wired Configuration

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

Maintenance

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

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

Guest Access

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

Global Settings

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

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

Icons at the bottom pane

- The bubble icon—Displays the following options:
 - **Documentation**—Opens the Aruba Central user documentation portal.
 - **View / Update Case**—Directs you to the support site to view or update an existing support case.
 - **Open New Case**—Directs you to the support site to open a new support case.
 - **Airheads Community**—Directs you to the Airheads Community page to view existing topics to start a new a new topic.
- The Help Icon—Click the **?** icon to view a short description or definition of the selected terms and fields in a pane or dialog box. To view the online help:
 - a. Click the **(?)** at the top.
 - b. Move your cursor over a data pane item to view the help text.
 - c. To disable the help mode, click **(?)** again.

Search Bar

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

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

User Icon

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

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



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

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

Filter bar

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

Groups Selection Filter

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

- Wireless Management
- Wired Management
- Guest Access

The groups filter supports the following functions:

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

Data Pane

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

Notifications Pane

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

Supported Devices

This section provides the following information:

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

Supported Instant APs

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

Supported Switch Platforms



To manage your Aruba switches using Aruba Central, ensure that the switch software is upgraded to 16.05.0007 or a later version. For Aruba 2530 Switch Series, the recommended software version is 16.05.0008. However, if you already have switches running lower software versions in your account, you can continue to manage these devices from Aruba Central.

[Table 4](#) and [Table 5](#) 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
Aruba 2530 Switch Series	YA/YB.16.05.0008 or later	YA/YB.16.08.0001	N/A
Aruba 2540 Switch Series	YC.16.03.0004 or later	YC.16.08.0001	N/A
Aruba 2920 Switch Series	WB.16.03.0004 or later	WB.16.08.0001	Yes Switch Software Dependency: WB.16.04.0008 or later
Aruba 2930F Switch Series	WC.16.03.0004 or later	WC.16.08.0001	Yes Switch Software Dependency: WC.16.07.0002
Aruba 2930M Switch Series	WC.16.04.0008 or later	WC.16.08.0001	Yes Switch Software Dependency: WC.16.06.0006
Aruba 3810 Switch Series	KB.16.03.0004 or later	KB.16.08.0001	Yes Switch Software Dependency: KB.16.07.0002
Aruba 5400R Switch Series	KB.16.04.0008 or later	KB.16.08.0001	Yes Switch Software Dependency: KB.16.06.0008

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

Mobility Access Switch Series	Supported Software Versions
<ul style="list-style-type: none">■ S1500-12P■ S1500-24P■ S2500-24P■ S3500-24T	<ul style="list-style-type: none">ArubaOS 7.3.2.6ArubaOS 7.4.0.3ArubaOS 7.4.0.4ArubaOS 7.4.0.5ArubaOS 7.4.0.6



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

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.



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

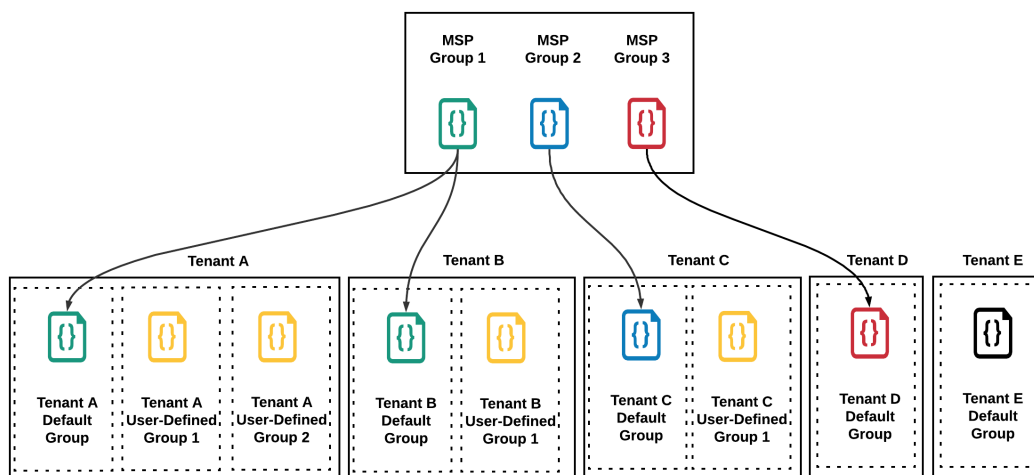
MSP Group Illustration

As shown in [Figure 3](#), 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 3 MSP Groups



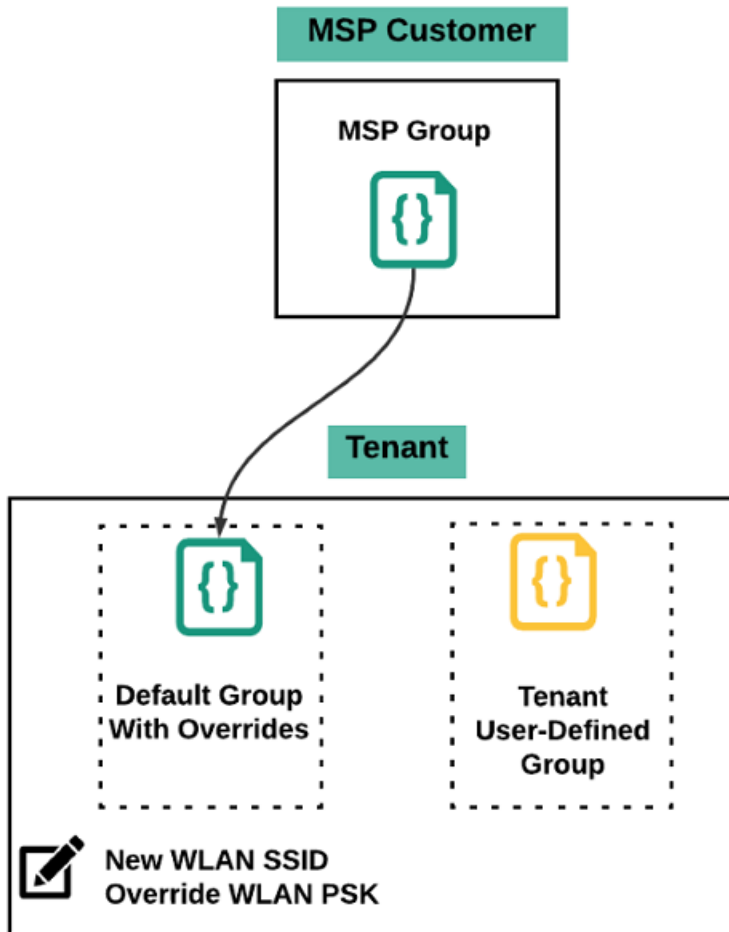
Tenant Default Group Overrides

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 [Figure 4](#), the following configuration options are allowed on a tenant default group that is mapped to an MSP group:

- Create a new WLAN SSID.
- Override the WLAN PSK for a WLAN inherited from an MSP group.

Figure 4 *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 app selector, click **Global Settings**.
2. Click **Manage Groups**. The **Groups** page opens.
3. To create a new group, click the **New Group**. The **Create New Group** pane appears.
4. Enter a name for the group.
5. Configure a password to restrict group access to authorized users only.
6. Click **Add Group**.

How do I create an Aruba Central MSP account?

As MSP mode is an operational mode of Aruba Central, the first step to create an MSP account is to create an Aruba Central account and then enable **Managed Service Mode**.

- Sign up for Aruba Central evaluation [here](#).
- Follow the steps in the [MSP Overview](#) 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. Once 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 Devices](#) for a list of supported Instant APs, switches, and gateways.

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.



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 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.

What are predefined user roles?

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

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

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.

Aruba Central 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. Aruba Central supports the following deployment models:

- MSP-owned devices and subscriptions—See [Deployment Model 1 on page 22](#).
- End-customer-owned devices and subscriptions, but managed by the MSP—See [Deployment Model 2 on page 26](#).
- Hybrid deployment model—See [Deployment Model 3 on page 29](#).

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 **Customers** section in the **Monitoring & Reports > Dashboard** page 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 [Provisioning Tenant Accounts](#).

Customizing 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 Portal](#).

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 [Managing Software Upgrade for Tenant Accounts](#).

Example Deployment Scenario

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

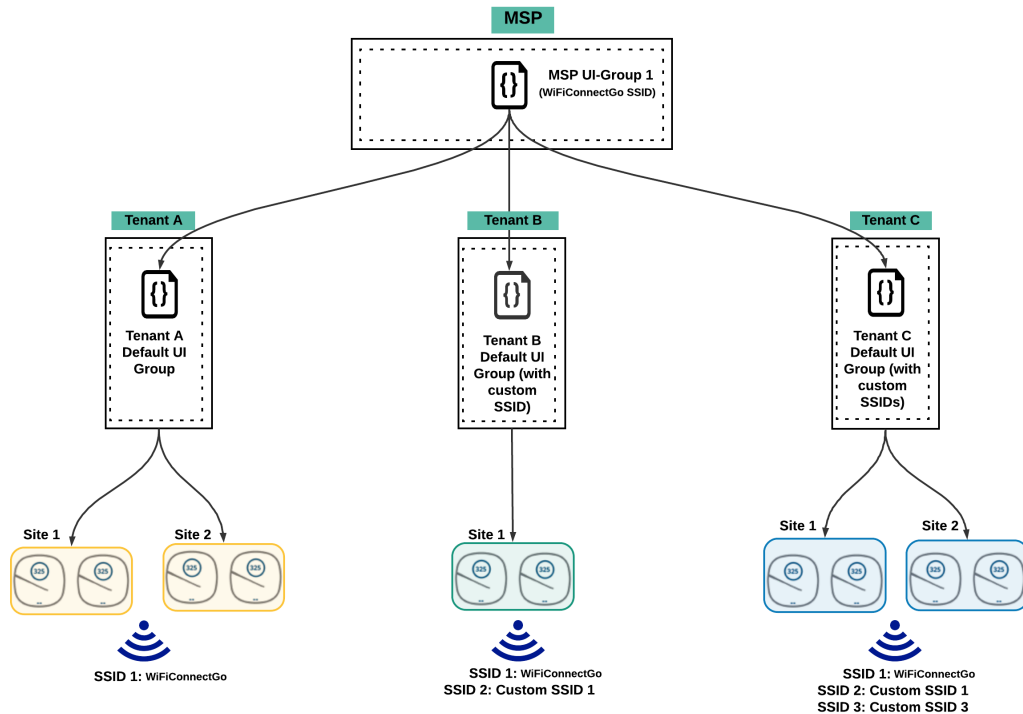
- **WiFiConnectGo**—In this program, for a monthly fee per Instant AP, customers part of this program agree to broadcast MSP's free public WiFi SSID **WiFiConnectGo**. Customers can add up to 15 additional custom SSIDs, including guest, of their own. Tenant account administrators are responsible for 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 [Figure 5](#), 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 5 Deployment Using Default UI Groups

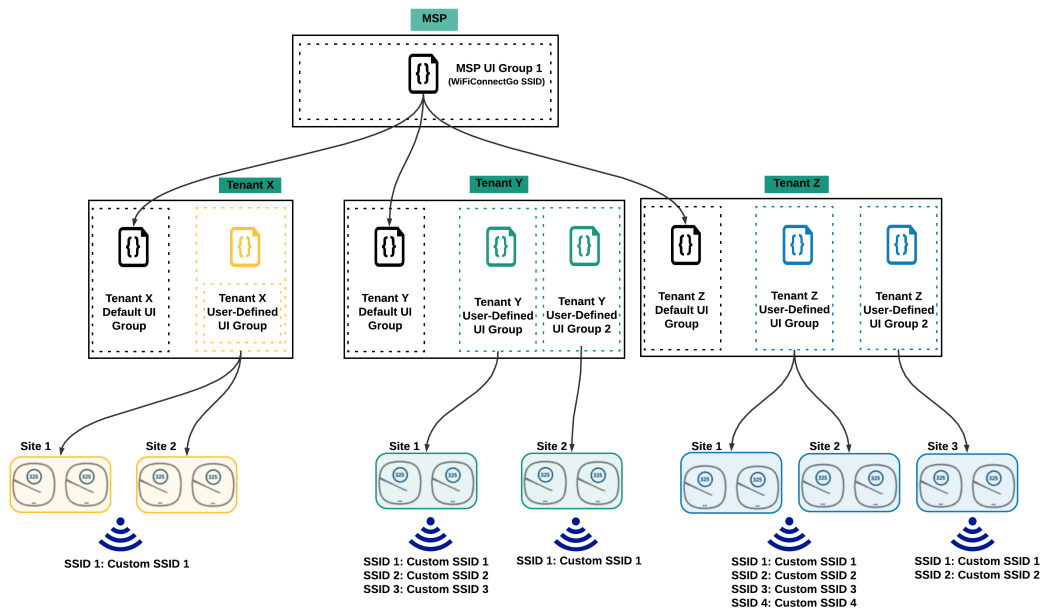


Configuring WiFiConnectGo-Plus Using User-Defined UI Groups

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 [Figure 6](#), 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 6 Deployment Using User-Defined UI Groups

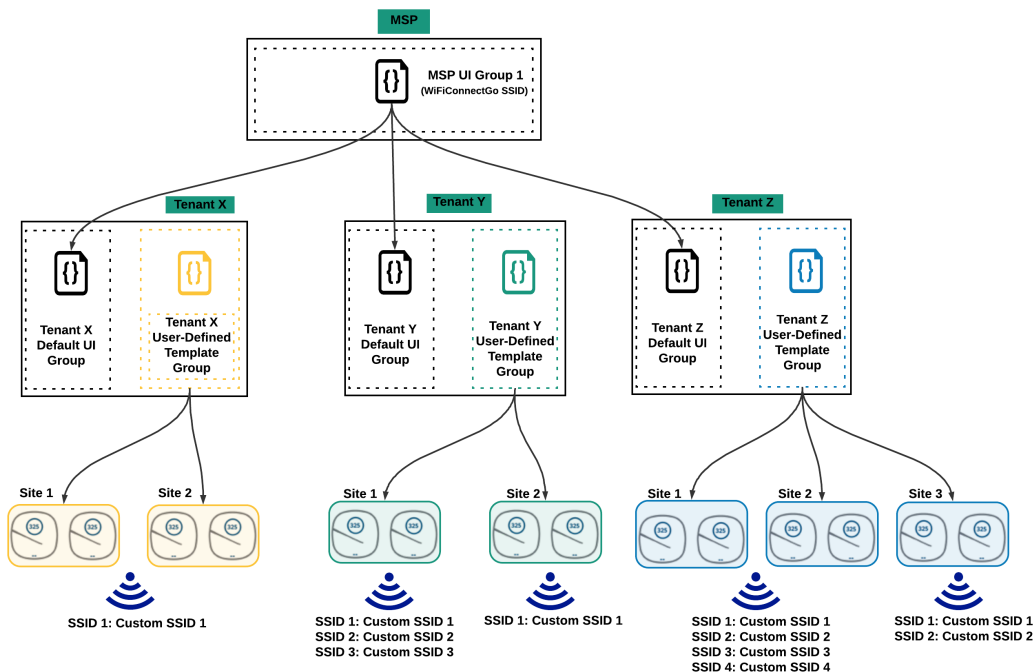


Configuring WiFiConnectGo-Plus Using Template Groups

As shown in [Figure 7](#), 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 7 Deployment Using Template Groups



Deployment Model 2

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.



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.

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 on page 28](#).

For more information about setting up Aruba Central in the Standard Enterprise mode, see [Setting up Your Aruba Central Instance](#).

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 **Monitoring & Reports** module in the Aruba Central Standard Enterprise mode to monitor the end-customer network.

For more information about monitoring and reporting in the Aruba Central Standard Enterprise mode, see [Monitoring & Reports](#).

Managing Firmware and Maintenance

The MSP has to use the **Firmware** menu in the **Maintenance** app 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.

For more information about managing software upgrades in the Aruba Central Standard Enterprise mode, see [Managing Software Upgrades](#).

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.



Template groups are not supported at the MSP level. However, template groups can be defined and managed at each tenant account individually. For more information, see [Groups in the MSP Mode on page 31](#).

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.

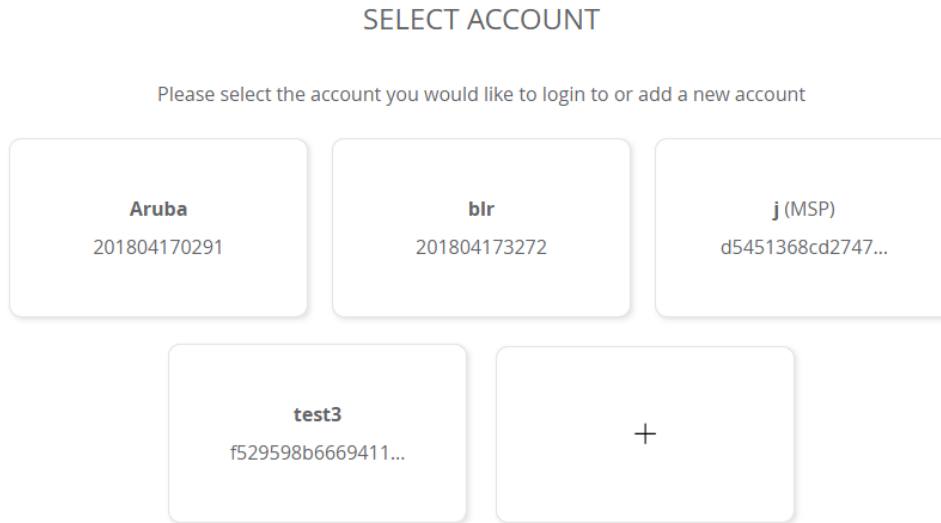
Points to Note:

- 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.

Using the Switch Customer Option

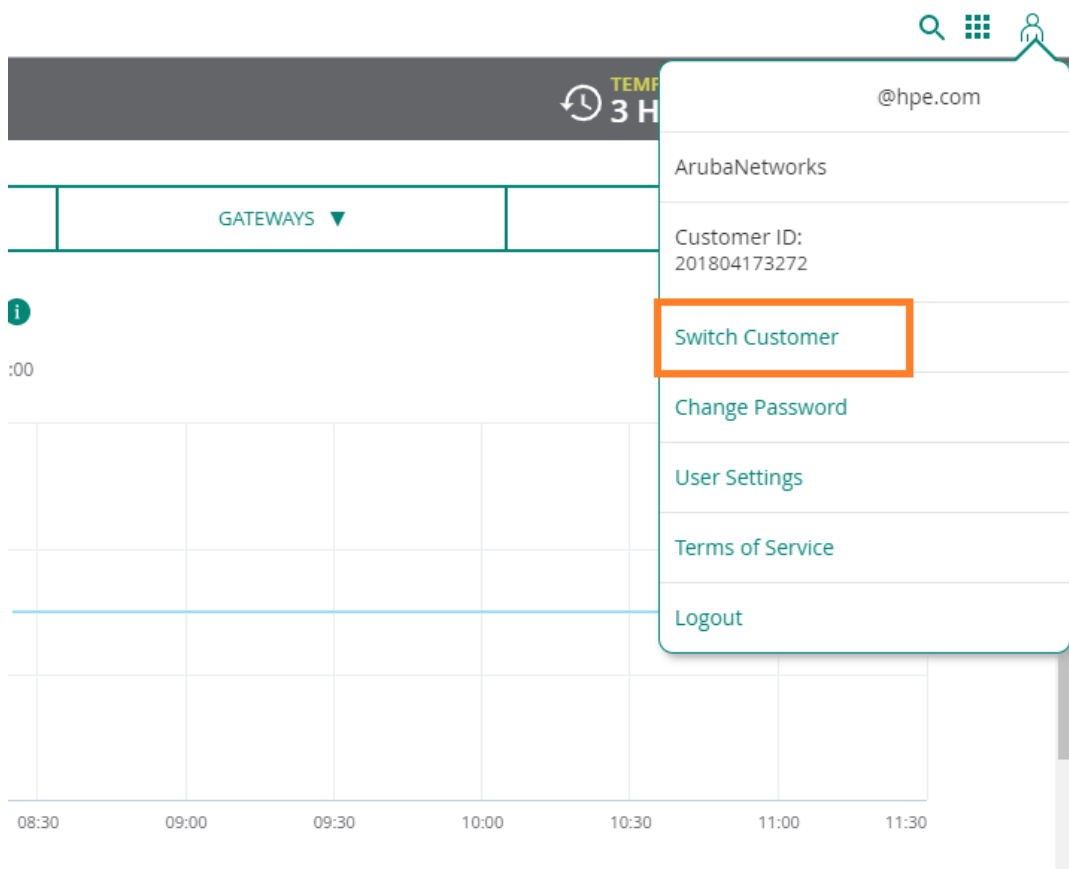
If you are an MSP administrator and if your user ID has been added to multiple tenant accounts, after you log in to Aruba Central, you must select the tenant account that you want to access. See [Figure 8](#).

Figure 8 *Select Account*



To select a different tenant account, click the **User** icon > **Switch Customer** and select the tenant account that you want to access. See [Figure 9](#).

Figure 9 *Switch Customer*



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:

- [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.
- [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.

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.

- [MSP Overview](#)
- [Supported Devices](#)
- [Groups in the MSP Mode](#)
- [User Accounts and Roles in MSP Mode](#)
- [Frequently Asked Questions](#)

Steps to Complete

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. [Enable Managed Service mode](#)
3. [Onboard devices](#)
4. [Add subscription keys](#)
5. [Create groups](#)
6. [Provision tenant accounts](#)
7. [Assign devices to tenant accounts](#)
8. [Assign subscription to devices and services](#)
9. [Configure users and roles](#)
10. [Customize tenant account view](#)
11. [Add Certificates](#)
12. [Monitor tenant accounts](#)

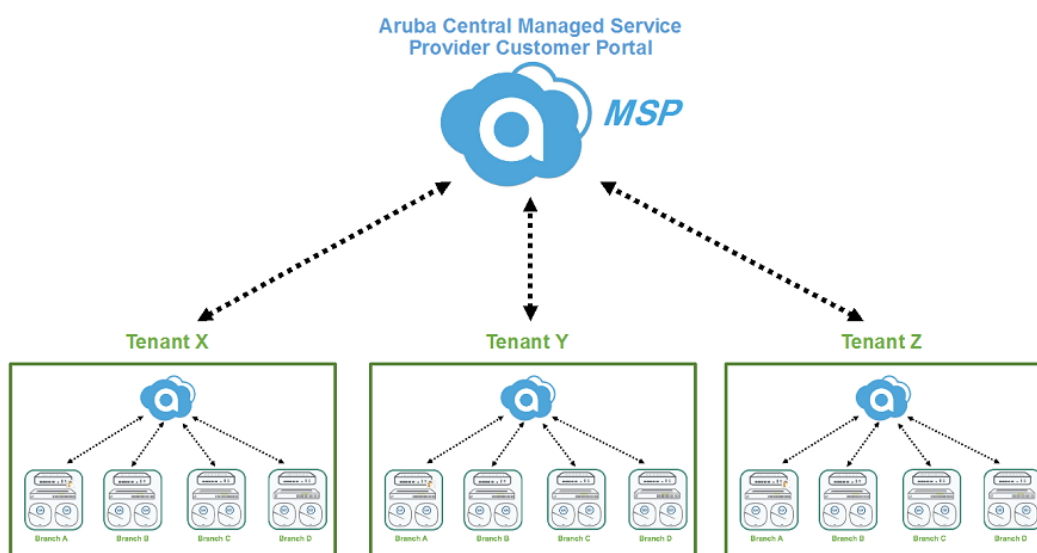
Aruba Central provides a cloud-based network management platform for managing your wireless and wired networks with Aruba Instant APs and Switches. Along with device and network management functions, Aruba Central offers value added services such as customized guest access, client presence and service assurance analytics.

The MSP mode is a multi-tenant operational mode that Aruba Central accounts can be converted into. MSPs can simplify tenant network operations using capabilities such as zero-touch setup, centralized management of Aruba APs and switches, historical data reporting, PCI compliance monitoring, and troubleshooting for hundreds of customers.

With the MSP mode enabled, MSP administrators can provision tenant accounts, allocate devices, assign subscriptions, and monitor tenant accounts. MSP administrators can drill down to a specific tenant account and perform additional administration and configuration tasks.

[Figure 10](#) illustrates a typical MSP deployment mode in which one MSP manages multiple tenant accounts.

Figure 10 *MSP Deployment Mode*



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.



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

User Accounts and Roles in the MSP Mode

Aruba Central MSP mode supports role-based access control. Aruba Central allows you to create predefined user roles and custom roles. MSP administrators can create, manage, and monitor multiple tenant accounts.

For MSP accounts, Aruba Central provides a separate MSP Dashboard using which MSP administrators can provision and manage their respective tenant accounts. The tenant account user's access is limited to their respective organization or network setup.

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.

Enabling the Managed Service Mode

To enable MSP mode, perform the following steps:

1. Log in to your Aruba Central account.
2. Click the user icon at the top right corner of the header pane.
3. Click **Enable MSP**.
4. In the **Managed Service Mode** pop-up window, click **Request Access**.
5. In the **Managed Service Mode** form, enter the details and click **Submit**. In the confirmation pop-up window, click **Close**.



After you submit the request, click the user icon at the top right corner of the header pane, the **Enable MSP** option will be grayed out and a message is displayed when you hover over the icon next to **Enable MSP** option.

6. After you get a confirmation from Aruba that the request to enable MSP mode has been approved, click the user icon at the top right corner of the header pane and click **Enable MSP**.
7. 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.

See [MSP User Interface](#) for more details about the user interface elements.



For a visual representation of the procedure, click [here](#).

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 at the top right corner of the header pane.
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**.

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 6: *Sign Up URLs*

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

Signing up for an Aruba Central Account

To sign up for an Aruba Central account:

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

Table 7: Registration Workflow

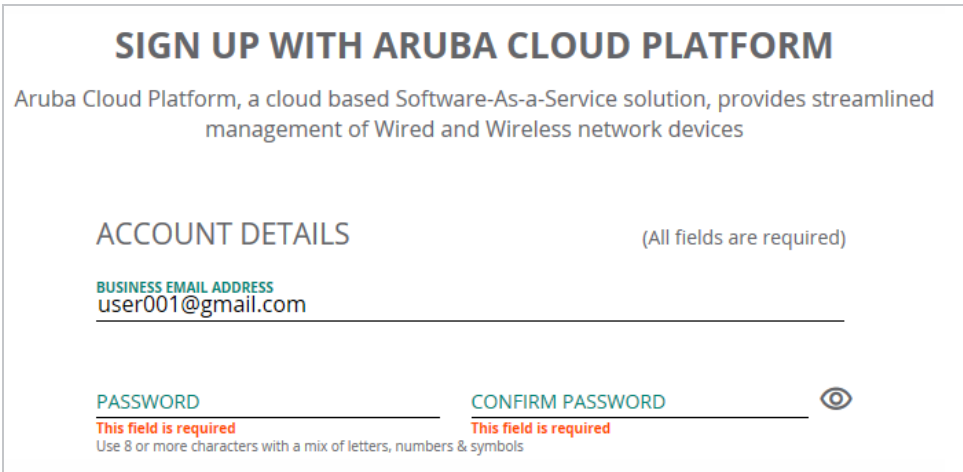
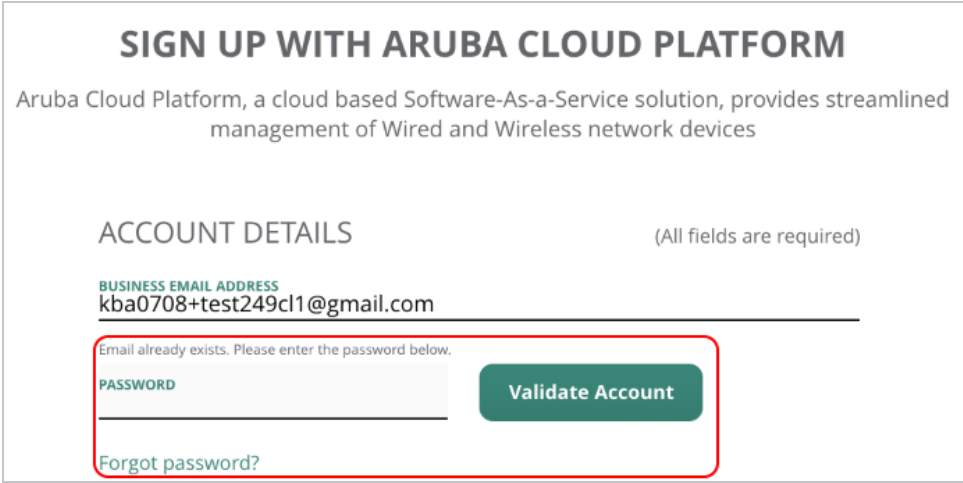

If...	Then...
If you are a new user:	<p>The Registration page prompts you to create a password. To continue with the registration, enter a password in the Password and Confirm Password fields.</p> 
If you are an existing Aruba customer, but you do not have an Aruba Central account:	<p>The Registration page displays the following message: Email already exists. Please enter the password below. To continue with registration, validate your account:</p> <ol style="list-style-type: none"> 1. Enter the password. 2. Click Validate Account. <p>NOTE: If you do not remember the password, click Forgot Password to reset the password.</p>
If your email account is already registered with Aruba, but you do not have an Aruba Central account:	
If you are invited join as a user in an existing Aruba Central customer account:	<p>The Registration page displays the following message: An invitation email has already been sent to your email ID. Resend. To continue with the registration:</p> <ol style="list-style-type: none"> 1. Go to your email box and check if you have received the email invitation. 2. If you have not received the email invitation, go to the Registration page and click Resend. A registration invitation will be sent your account. 3. Click the registration link. The user account is validated. 4. Complete the registration on the Sign Up page to sign in to Aruba Central.

Table 7: Registration Workflow

If...	Then...
	<div data-bbox="557 256 1511 625"> <h3>SIGN UP WITH ARUBA CLOUD PLATFORM</h3> <p>Aruba Cloud Platform, a cloud based Software-As-a-Service solution, provides streamlined management of Wired and Wireless network devices</p> <p>ACCOUNT DETAILS (All fields are required)</p> <p>BUSINESS EMAIL ADDRESS user10091@gmail.com</p> <p>An invitation email has already been sent to your email ID. Resend</p> </div>
<p>If you are a registered user of Aruba Central and have not verified your email yet:</p>	<p>The Registration page displays the following message:</p> <p>You are an existing Aruba Central user. Please verify your account. Resend Verification email.</p> <p>To continue:</p> <ol style="list-style-type: none"> 1. Go to your email box and check if you have received the email invitation. 2. If you have not received the email invitation, go to the Registration page and click Resend Verification email. A registration invitation will be sent your account. 3. Click the account activation link. 4. After the email verification is completed successfully, click Log in to access Aruba Central. <div data-bbox="557 993 1511 1392"> <h3>SIGN UP WITH ARUBA CLOUD PLATFORM</h3> <p>Aruba Cloud Platform, a cloud based Software-As-a-Service solution, provides streamlined management of Wired and Wireless network devices</p> <p>ACCOUNT DETAILS (All fields are required)</p> <p>BUSINESS EMAIL ADDRESS centraluser005@gmail.com</p> <p>You are an existing Aruba Central user. Please verify your account. Resend Verification email</p> </div>
<p>If you are already a registered user of Aruba Central and have verified your email:</p>	<p>The Registration page displays the following message:</p> <p>User has been registered and verified. Sign in to Central.</p> <p>Click Sign in to Central to skip the registration process and access the Aruba Central portal.</p>

Table 7: Registration Workflow

If...	Then...
	<div data-bbox="557 258 1511 625"> <h3>SIGN UP WITH ARUBA CLOUD PLATFORM</h3> <p>Aruba Cloud Platform, a cloud based Software-As-a-Service solution, provides streamlined management of Wired and Wireless network devices</p> <p>ACCOUNT DETAILS (All fields are required)</p> <p>BUSINESS EMAIL ADDRESS centraluser005@gmail.com</p> <p>User has been registered and verified. Sign in to Central</p> </div>
<p>If your email address is in the arubanetworks.com or hpe.com domain:</p>	<p>The Single Sign-On option is enabled. You can use your respective Aruba or HPE credentials to log in to your Aruba Central account after the registration.</p> <div data-bbox="557 804 1511 1245"> <h3>SIGN UP WITH ARUBA CLOUD PLATFORM</h3> <p>Aruba Cloud Platform, a cloud based Software-As-a-Service solution, provides streamlined management of Wired and Wireless network devices</p> <p>ACCOUNT DETAILS (All fields are required)</p> <p>BUSINESS EMAIL ADDRESS user1@hpe.com</p> <p> Single sign-on enabled</p> </div>

5. To continue with registration, enter your first name, last name, company name, address, country, state, ZIP code, and phone details.
6. Specify if you are an Aruba partner.
7. Ensure that you select an appropriate zone. The **Registration** page displays a list of zones in which the Aruba Central servers are available for account creation. Based on country you select, the Aruba Central server is automatically selected. If you want your account and Aruba Central data to reside on a server from another zone, you can select an Aruba Central server from the list of available servers.

Figure 11 Account Registration Page

ADDRESS
Market Square, Outer Ring Road

+
ADD LINE

CITY
Bangalore

Karnataka

ZIP CODE
560103

PHONE NUMBER
+91 9240598432

Are you an Aruba Partner? ☐ Yes ☒ No

SERVER DETAILS (All fields are required)

APAC-1

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

☒ I agree to the Terms and Conditions

May Aruba, a Hewlett Packard Enterprise Company, provide you with personalized communications about Aruba and select Aruba-partner products, services, offers and events?

☐ Email ☐ Business Phone

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

8. Select the **I agree to the Terms and Conditions** check box.
9. Set a preferred mode of communication for receiving notifications about Aruba products and services.
10. Click **Sign Up**. Your new account is created in the zone you selected and an email invitation is sent to your email address for account activation.
11. Access your email account and click the **Activate Your Account** link. After you verify your email, you can [log in](#) to Aruba Central.

Accessing Aruba Central Portal

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

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

Login URLs

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

Table 8: Cluster Zone— Portal URLs

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

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

Logging in to Aruba Central:

To log in to Aruba Central:

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



If your user credentials are stored in your organization's Identity Management server and SAML SSO authentication is enabled for your IdP on Aruba Central, complete the SSO authentication workflow. For more information on SAML configuration, see [Configuring SAML SSO Authentication for Federated Users on page 1](#).

5. Enter the password.



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

6. If you have forgotten your password,
7. Click **Continue**. The **Initial Setup** wizard opens.
 - If you have a paid subscription, click **Get Started** and set up your account.
 - If you are a trial user, click **Evaluate Now** and [start your trial](#).

Changing Your Password

To change your Aruba Central account:

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



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

Logging Out of Aruba Central

To log out of Aruba Central:

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

Managing Subscriptions

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

Managing Subscription Keys

Evaluation Subscription Key

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

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

Upgrading to a Paid Account

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

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

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

Paid Subscription Key

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

The **Global Settings > Key Management** page displays the subscription expiration date. You will receive subscription expiry notifications through email on the 90th, 60th, 30th, 15th, and 1 day before expiry and two notifications per day on the day 1 and day 2 after the subscription expiry.

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

Adding a Subscription Key

To add a subscription key:

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

Viewing Subscription Key Details

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

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

[Table 9](#) describes the contents of the **Manage Keys** table on the **Key Management** page.

Table 9: *Subscription Key Details*

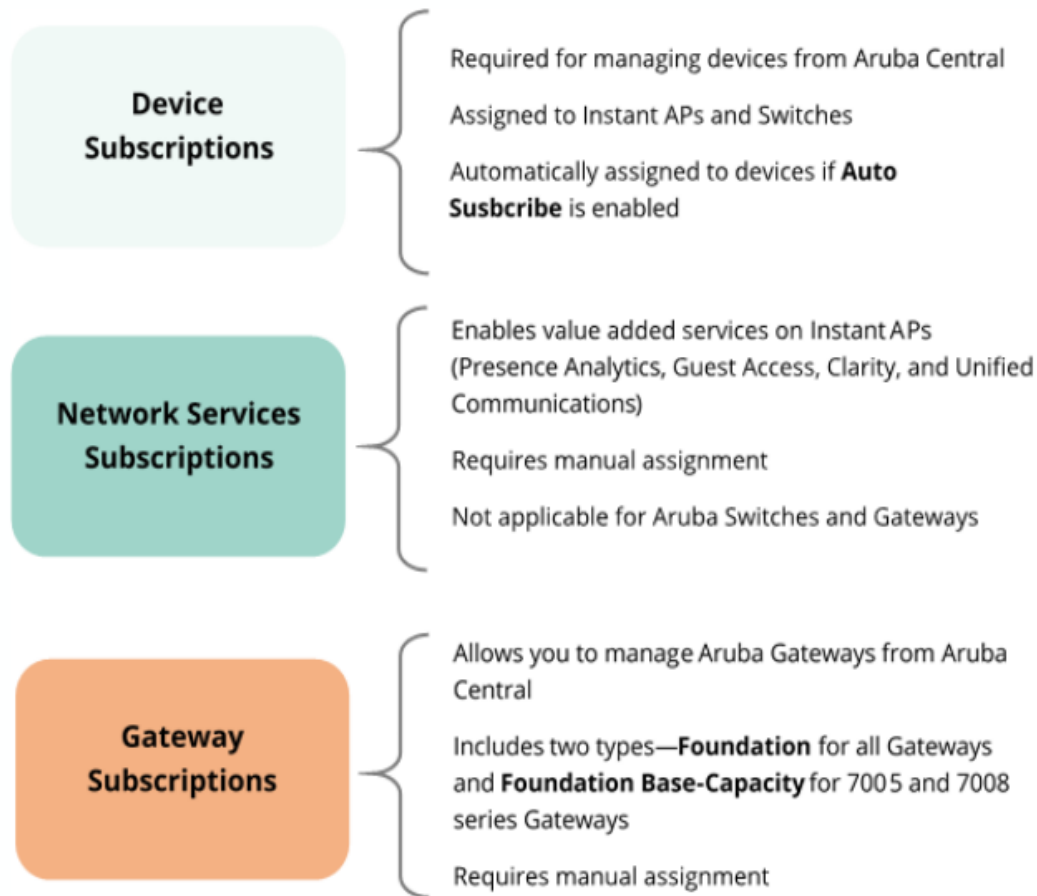
Data Pane Item	Description
Keys	Subscription key number.
Type	Type of the subscription. Aruba Central supports the following types of subscriptions: <ul style="list-style-type: none">■ Device subscriptions—The device subscription allows you to avail services such as device onboarding, configuration, management, monitoring, and reports. The device subscriptions can be assigned only to the devices managed by Aruba Central.■ Service subscriptions—Aruba Central supports application services that you can run on the devices provisioned in your setup. For example, if you have Instant APs with 6.4.4.4-4.2.3.0 or later, you can assign a service subscription for Presence Analytics.■ Gateway Subscriptions—Aruba Central supports a separate set of subscriptions for configuring and managing SD-WAN gateways. The Gateway subscriptions are marked as Foundation-<device>; for example, Foundation-70XX.
Expiration Date	Expiration date for the subscription key.
Quantity	Number of license tokens available for a subscription. Each Aruba Central subscription holds a specific number of tokens. For example, when a subscription is assigned to a device, Aruba Central binds the device with a token from the existing pool of subscriptions.
Status	Status of the subscription key. For example, if you are a trial user, Aruba Central displays the status of subscription key as Eval .

Supported Subscription Types

Aruba Central supports the following types of subscriptions:

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

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



Assigning Subscriptions

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

- [Assigning Device Subscriptions on page 41](#)
- [Assigning Subscriptions on page 41](#)
- [Assigning Gateway Subscriptions on page 43](#)

Assigning Device Subscriptions

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

Enabling Automatic Assignment of Subscriptions.

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

In the Initial Setup Wizard

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

From the Subscription Assignment Page

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



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

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

Important Notes for MSP Users

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

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

Manually Assigning Subscriptions

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

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

Important Notes for MSP Users

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

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

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

Assigning Network Service Subscriptions

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

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

Important Note for MSP Users

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

Assigning Gateway Subscriptions

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

Gateway Subscriptions

Aruba Central supports the following types of subscriptions for Gateways:

- **Foundation**—This subscription can be assigned to all Mobility Controllers irrespective of the hardware model.
- **Foundation-Base capacity** —This subscription can be assigned only to Aruba 7005 Mobility Controllers. Gateway devices with the Foundation-Base capacity subscription can support up to 75 client devices per branch.

When the client capacity reaches the threshold:

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

Assigning Subscriptions to Gateways

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

1. Go to **Global Settings > Click Subscription Assignment**. The **Subscription Assignment** page opens.
2. Under **Gateway Subscriptions**, select the device to which you want to assign a subscription.
3. Expand the drop-down in the **Assignment** column for the selected device.
4. Select the subscription; for example, **Foundation**.
5. To assign subscription to multiple devices:
 - a. Select the devices in the table.
 - b. Click **Batch Assignment**.
 - c. Select the subscription that you to assign.

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

Removing Subscriptions from Devices

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

Removing a Device Subscription from a Device

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

Removing a Network Service Subscription from a Device

To remove network service subscription from a device:

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

Acknowledging Subscription Expiry Notifications

The **Key Management** page under the **Global Settings** menu displays the expiration date for each subscription.

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

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

Acknowledging Notifications through Email

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

Acknowledging Notifications in the UI

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

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

Renewing Subscriptions

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

Onboarding Devices

Aruba Central supports the following options for adding devices.

- If you are a trial user, you must manually add the serial number and MAC address of the devices that you want manage from Aruba Central. For more information, see [Adding Devices \(Evaluation Account\) on page 45](#).
- If you are paid subscriber, Aruba Central retrieves devices associated with your purchase order from Activate. If the devices are not automatically discovered and added to Central's device inventory, set up a sync to import devices from the Activate database. [Adding Devices \(Paid Subscription\) on page 45](#).

Adding Devices (Evaluation Account)

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

In the Initial Setup Wizard

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

From the Device Inventory Page

1. Go to **Global Settings > Device Inventory**.
2. Click **Add by MAC/SN**. The **Add Devices** pop-up window opens.
3. Enter the serial number and the MAC address of each device.
You can find the serial number and MAC address of Aruba devices on the front or back of the hardware.
4. Click **Done**.
5. Review the devices in your inventory.

Adding Devices (Paid Subscription)

If you have a paid subscription, Aruba Central automatically discovers and imports the devices mapped to your purchase order. If your devices are not added to your inventory, set up a device sync by adding one device from your purchase order.

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

In the Initial Setup Wizard

1. Ensure that you have added a subscription key and click **Next**.
2. In the **Add Devices** tab, enter the serial number and MAC address of one device from your purchase order.
Most Aruba devices have the serial number and MAC address on the front or back of the hardware.
3. Click **Add Device**. Aruba Central imports all other devices mapped to your purchase order.
4. Review the devices in your inventory.
5. If the device sync fails, use any of the following options:

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

From the Device Inventory Page

1. Go to **Global Settings > Device Inventory**.
2. Click **Sync Devices**.
3. Enter the serial number and MAC address of one device from your purchase order. Aruba Central imports all other devices associated with your purchase order from Activate.
4. Review the devices in your inventory.
5. If the device sync fails, use any of the following options:
 - **Add Devices Manually**—To manually add devices by entering the MAC address and serial number of each device.
 - **Add Via Mobile App**—To add devices from the Aruba Central mobile app. You can download the Aruba Central app from Apple AppStore on iOS devices and Google Play Store on Android devices.
 - **Contact support**—To contact Aruba Technical Support.

Manually Adding Devices When Device Sync Fails

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

- [Adding Devices Using MAC address and Serial Number on page 46](#)
- [Adding Devices Using Activate Account](#)
- [Adding Devices Using Cloud Activation Key on page 47](#)

Adding Devices Using MAC address and Serial Number

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

In the Initial Setup Wizard

If you are using the Initial Setup wizard:

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

From the Device Inventory Page

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

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

3. Enter the serial number and MAC address of your device.

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

4. Click **Done**.

5. Review the devices added to the inventory.



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

Adding Devices Using Activate Account

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



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

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

To add devices from your Activate account:

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

Adding Devices Using Cloud Activation Key



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

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

Locating Cloud Activation Key and MAC Address

To know the cloud activation key:

- For Instant APs:
 1. Log in to the Instant AP UI or CLI.
 - If using the UI, go to the **Maintenance > About**.
 - If using the CLI, execute the **show about** command at the Instant AP CLI.
 2. Note the cloud activation key and MAC address.
- For Aruba Switches:
 1. Log in to the switch CLI.
 2. Execute the **show system | in Base** and **show system | in Serial** commands.
 3. Note the cloud activation key and MAC address in the command output.
- For Mobility Access Switches
 1. Log in to the Mobility Access Switch UI or CLI.

- If using the UI, go to the **Maintenance > About**.
 - If using the CLI, execute the **show inventory | include HW** and **show version** commands.
2. Note the cloud activation key and MAC address. The activation key is enabled only if the switch has access to the Internet.

Adding Devices Using Cloud Activation Key

1. Go to **Global Settings > Device Inventory**.
2. On the **Device Inventory** page, click **Advanced** and select the **Add with Cloud Activation Key**. The **Cloud Activation Key** pop-up window opens.
3. Enter the cloud activation key and MAC address of a device.
4. Click **Add**.



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

See Also:

- [Starting Your Free Trial on page 1](#)
- [Setting up Your Aruba Central Instance on page 1](#)

Provisioning Tenant Accounts

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

The **Customers** section in the **Monitoring & Reports > Dashboard** page in the MSP view allows you to add, view, edit, and delete tenant accounts:

- [Creating a Tenant Account and Mapping to an MSP Group on page 48](#)
- [Viewing Tenant Account Details on page 50](#)
- [Editing a Tenant Account on page 50](#)
- [Deleting a Tenant Account on page 50](#)

Creating a Tenant Account and Mapping to an MSP Group

To add a tenant account, complete the following steps:

1. From the app selector, go to **Monitoring & Reports > Dashboard**.
2. Click **Add New Customer**. The **Add Customer** page opens.
3. Enter the name of the tenant in the **Customer Name** text box.
4. Enter the description of the tenant in the **Description** text box.
5. If you want to associate the tenant to a group, click the **Add to group** toggle switch. See [Figure 12](#) for an illustration of the tenant mapping to MSP group.
6. From the **Group** drop-down list, select a group to which you want to assign the tenant.



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.

7. 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.

8. Click **Save**.

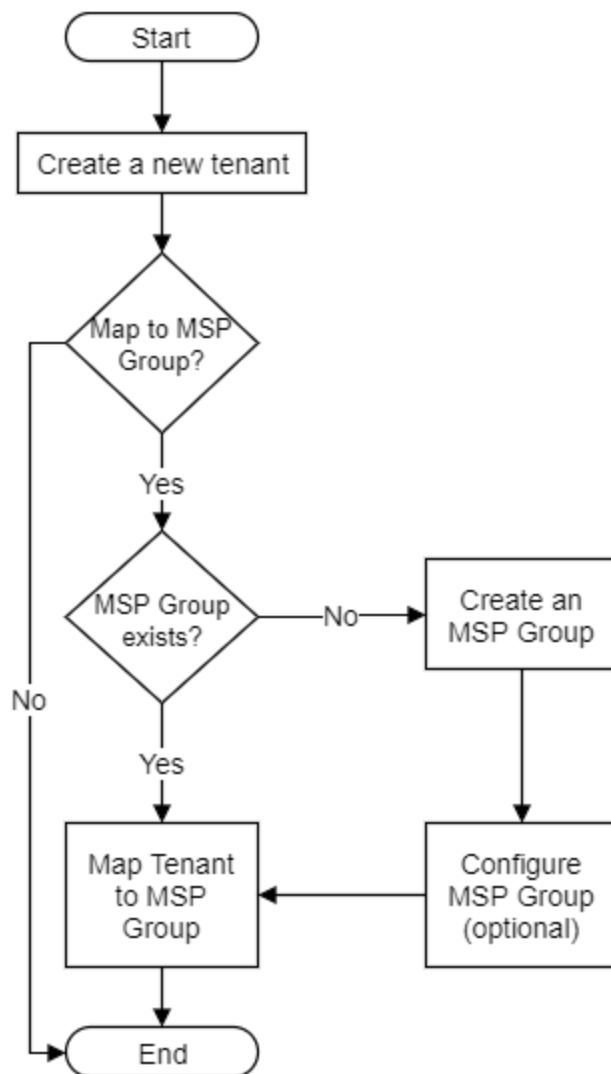


For a visual representation of the procedure, click [here](#).

Points to Note:

- 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, go to **Monitoring & Reports > Customers** table. 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.

Figure 12 *Tenant Account Mapping to an MSP Group*



Viewing Tenant Account Details

To view the tenant account details, on the **Monitoring & Reports > Customers** table, hover over the tenant account and click **expand**.

[Figure 12](#) describes the contents of the pop-up window.

Table 10: *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: <ul style="list-style-type: none">■ 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.



For a visual representation of the procedure, click [here](#).

Editing a Tenant Account

To edit a tenant account, complete the following steps:

1. On the **Monitoring & Reports > Customers** table, hover over the tenant account that you want to edit and click **edit**.
2. Modify the account details.



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

3. Click **Save**.



For a visual representation of the procedure, click [here](#).

Deleting a Tenant Account

To delete a tenant account, complete the following steps:

1. On the **Monitoring & Reports > Customers** table, hover over the tenant account that you want to delete and click **delete**.
2. 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. From the app selector, click **Global Settings**.
2. Click **Device Inventory**. A list of devices provisioned in the MSP mode is displayed.
3. 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 shows up under the table.
4. Click **Assign Customer**. A window showing a list of tenant accounts provisioned in the MSP mode appears.
5. Select the tenant account to which you want to assign the device. The groups associated with the tenant accounts are displayed.
6. Click **Assign Device (s)**.
7. Click **Yes** when prompted for confirmation.

Assigning Subscriptions

Aruba Central supports the following types of subscriptions:

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

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



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

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

Assigning Device Subscriptions

Aruba Central allows you to enable automatic assignment of device subscriptions for the devices joining Aruba Central. When a subscription assigned to a device expires or is cancelled, Aruba Central checks for the available subscription tokens in your account and assigns the longest available subscription token to the device. If your account does not have an adequate number of subscriptions, you may have to manually assign subscriptions to as many devices as possible.

Regardless of whether the automatic assignment of device subscription is enabled, any subscribed device that has an expired subscription will automatically be assigned a new valid subscription, if you have any available. You can check your available subscriptions on the [Assign Subscriptions](#) page.

Enabling Automatic Assignment of Device Subscriptions

To enable automatic assignment of subscriptions:

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

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



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

Enabling Automatic Subscription Assignment in the MSP Mode

If you are an MSP user, you can enable the **Auto Subscribe Device Subscription Keys For All Customer Devices (Recommended)** check box from the **Global Settings > Subscription Assignment** page to automatically assign subscriptions to the devices mapped to your tenant accounts.

Important Points to Note:

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

Assigning Service Subscriptions to Devices

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

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



Ensure that the device is assigned to a tenant before assigning a service subscription to it. When a device subscription or service subscription is assigned to a device that is not mapped to any specific tenant in the **Network Service Subscriptions** section, 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.**

User Accounts and Roles in MSP Mode

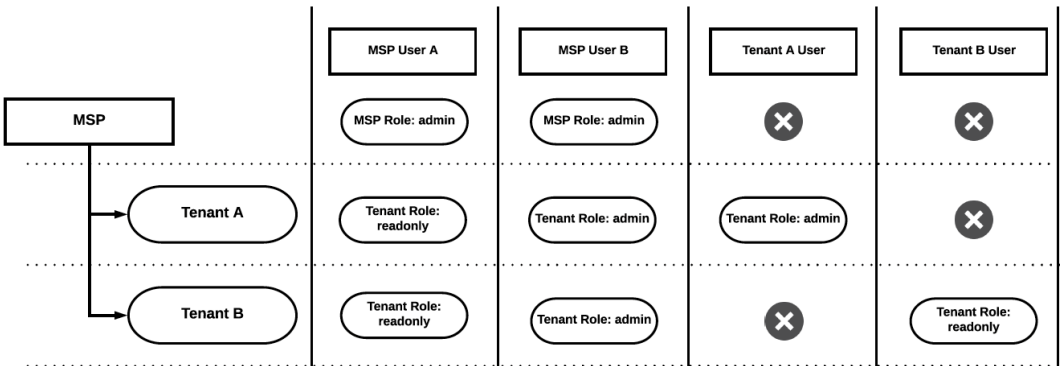
Aruba Central MSP mode supports role-based access control. Aruba Central allows you to create predefined user roles and custom roles.

Role-Based Access Control Illustration

As shown in [Figure 1](#), 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 13 *MSP Role-Based Access Control*



Configuring User Accounts for the MSP Mode

The **Users & Roles** page in the MSP view allows you to add, edit, or delete users for the MSP mode.

Adding a User Account

To configure user accounts for the MSP mode, complete the following steps:

1. From the app selector, go to **Global Settings > Users & Roles**.
2. In the **Users & Roles** page, click **+**. The **New User** window is displayed.
3. In the **New User** window, do the following:
 - a. **Username**—Enter the email address of the user.
 - b. **Description (optional)**—Enter the description.
 - c. **MSP Role**—From the drop-down list, select the access level that you want to assign to the user.
 - d. **Tenant Role (optional)**—From the drop-down list, select the access level that you want to assign to the user. If a tenant role is not specified, the MSP role is assigned by default.

- e. **Language**—From the drop-down list, select the language.
4. Click **Save**. After the user account is successfully created, the user is added and an email invitation is sent to the user.

Editing a User Account

To edit a user account, select the user and click the edit icon.

Deleting a User Account

To delete a user account, select the user and click the delete icon. MSP users can be deleted only from the MSP view.

Customizing Portal

The **Portal Customization** pane 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.

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

1. From the app selector, click **Maintenance**.
2. Click **Portal Customization**. The **Portal Customization** pane opens.
3. 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.
4. If you want customize the logo of your portal, click **Skinning**.
5. Browse to your local directory and upload the logo image.
6. Click **Save Settings**. The customized logo will appear 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 [Adding a User Account](#).

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. From the app selector, click **Global Settings > Certificates**.
2. To add a new certificate to the **Certificate Store**, Click **Add**. The **Add Certificate** dialog box opens.
3. Enter the certificate name in the **Name** text box.
4. Select the certificate type from the **Type** list. You can upload server and CA certificates.

5. Select the certificate format from the **Format** drop-down. The supported certificate formats are PEM, DER, and PKCS12.
6. For server certificates, enter the passphrase.
7. Click **Browse** to browse to your local directory and select the certificate to upload.
8. Click **Add**.



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



When a certificate is removed from the **Wireless Management > Security > Certificate Usage** section in the MSP, the respective certificate is also removed from the tenant's **Certificates Store** in the **Global Settings > Certificates > Device Certificates** section, 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.

See [Mapping Cloud Guest Certificates](#) for information about mapping Cloud Guest certificates.

The **Wireless Management** app in the MSP allows the administrators of tenant accounts to configure WLAN SSIDs, radio profiles, firewall settings, DHCP, VPN, and uplink profiles for the Instant AP devices in a group.



Both the users with administrator and read/write privileges can configure SSID s 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.

Mapping Cloud Guest Certificates

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. Ensure that the cloud guest certificate is uploaded to the Certificate Store (**Global Settings > Certificates**).
2. From the app selector, click **Wireless Management**.
3. From the group selector, select the group to which you want to assign the certificate.
4. Go to **Security > Certificate Usage**.
5. Select the required certificate from the **Captive Portal** drop-down list.
6. Click **Save Settings**.



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

The **Wired Configuration** tab allows you to configure switches, system, ports, and VLAN parameters for the Aruba Switches added in the MSP.

For more information on switch configuration procedures, see *Wired Management* in the Aruba Central Help Center.

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

The SD-WAN Gateway portfolio includes Aruba 7000 Series and Aruba 7200 Series Mobility Controllers that function as Branch Gateways and VPN Concentrators respectively.



To obtain access to SD-WAN solution in your deployments, please contact your Aruba Sales Specialist.

For more information about SD Branch and SD-WAN configuration, look up *SD-WAN Solution* or see the *Aruba SD-WAN Solution Guide* in *Aruba Central Help Center*.

The MSP Dashboard provides a summary of hardware and subscriptions owned by the MSP and the tenant accounts managed by the MSP. From the MSP Dashboard, the MSP administrator can do the following:

- View the total number of tenant accounts and consolidated device inventory and subscription status—See [Dashboard Summary on page 59](#).
- View graphs representing the devices under management, tenant accounts added, and subscription renewal schedule—See [Trends on page 62](#).
- Perform tasks such as creating a new tenant account, editing an existing tenant account, and deleting a tenant account—See [Provisioning Tenant Accounts on page 48](#).
- Navigate to each tenant account—See [Navigating to the Tenant Account on page 62](#).
- Configure, edit, view, and acknowledge alerts—See [Alerts Dashboard and Acknowledging Alerts on page 65](#).

To view the MSP Dashboard, go to the **Monitoring & Reports** app for the MSP mode.

Dashboard

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

- Dashboard Summary bar
- Customers

Dashboard Summary

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

[Table 11](#) describes the contents of the **Dashboard Summary** bar.

Table 11: *Dashboard Summary Bar*

Data Pane Item	Description
Customers	Total number of tenant accounts provisioned.
Access Points	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ■ 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.

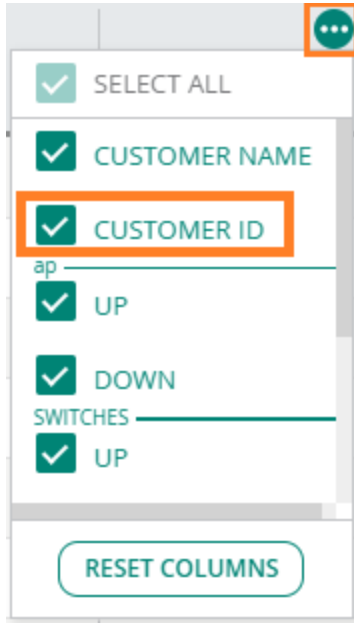
Data Pane Item	Description
Gateways	<ul style="list-style-type: none"> ■ Assigned—Number of gateways assigned to tenant accounts. Click the number to view the list of gateways in Subscribed state. ■ Unassigned—Number of gateways available for provisioning. Click the number to view the list of gateways in Unsubscribed state.
Device Subscriptions	<ul style="list-style-type: none"> ■ 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.

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 12](#) describes the contents of the table.

Table 12: *Customers Table*

Column	Description
Customer Name	<p>Name of the tenant account. Hover over the tenant account name to view the following options:</p> <ul style="list-style-type: none"> ■ expand—Opens a new pop-up window showing the tenant account details. For more information, see Viewing Tenant Account Details on page 50. ■ edit—Opens the Edit Customer pop-up window. For more information, see Editing a Tenant Account on page 50. ■ delete—Opens the confirmation dialog box. For more information, see Deleting a Tenant Account on page 50. <p>Hover over the icon next to the tenant account name to view the provisioning status. The status can be one of the following:</p> <ul style="list-style-type: none"> ■ In Progress ■ Provision Failed <p>NOTE: Use the filter icon on the column header to filter by tenant account name.</p>
Customer ID	<p>Unique ID of the tenant account. The ID can be in one of the following formats:</p> <ul style="list-style-type: none"> ■ Numerical format ■ UUID format <p>Use the column filter to search for a particular customer ID. Note that you must enter the full customer ID.</p> <p>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.</p>  <p>The screenshot shows a column selector menu with a 'SELECT ALL' option at the top. Below it, several columns are listed with checkboxes: 'CUSTOMER NAME', 'CUSTOMER ID' (which is highlighted with an orange box), 'UP', 'DOWN', 'SWITCHES', and 'UP'. At the bottom of the menu is a 'RESET COLUMNS' button.</p>
AP	<ul style="list-style-type: none"> ■ 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. <p>NOTE: Click the sort icon to sort the column in ascending or descending order.</p>

Column	Description
Switches	<ul style="list-style-type: none"> ■ 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. <p>NOTE: Click the sort icon to sort the column in ascending or descending order.</p>
Gateways	<ul style="list-style-type: none"> ■ 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. <p>NOTE: Click the sort icon to sort the column in ascending or descending order.</p>
Critical Alerts	<p>Total number of critical alerts for the tenant account. Click the number to navigate to the Alerts page of the tenant account.</p> <p>For more information, see MSP Alerts on page 63.</p>

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. By default, the device count is shown for the last 6 months. You can also view the data for the last 1, 2, or 3 years.
- **Customers** graph—Displays the total number of tenants added to Aruba Central. By default, the number of tenant accounts added in the last 6 months is displayed. You can also view the data for the last 1, 2, or 3 years. Click **Total** to view the total number of tenant accounts.

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. From the MSP view, click **Monitoring & Reports**.
2. In the **Customers** table, click the tenant account name. The tenant account view opens.



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.

MSP Alerts

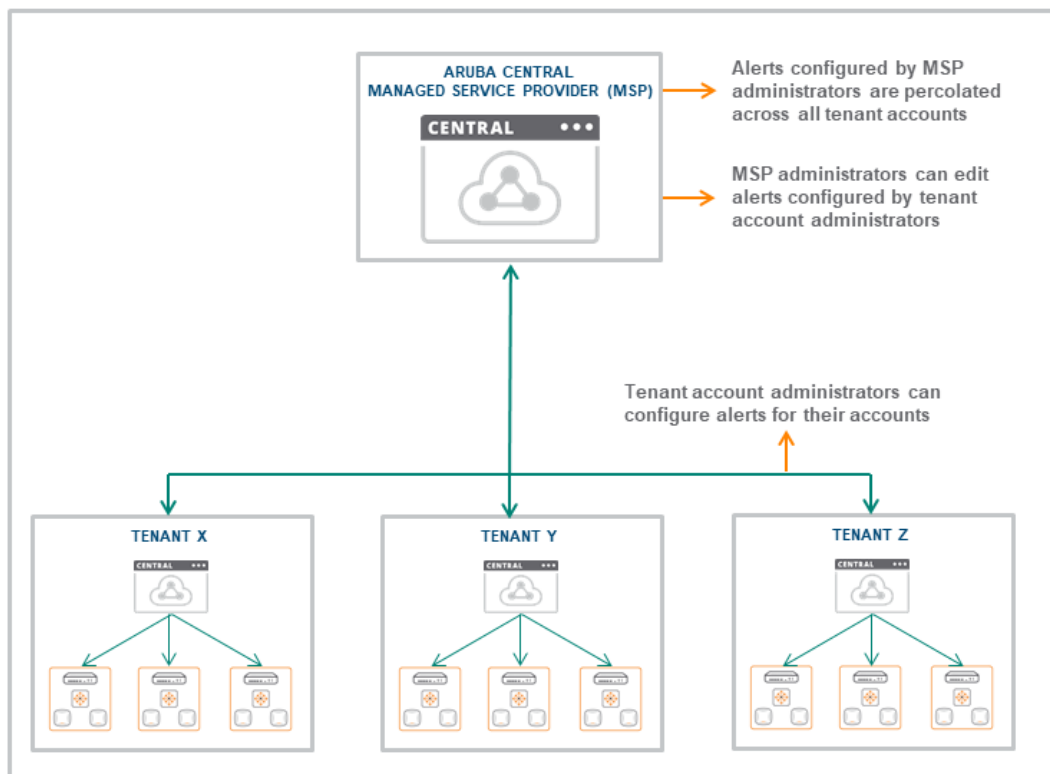
Aruba Central MSP mode enables administrators to trigger alerts when tenant provisioning, network, device, or user management events occur. An MSP administrator can configure alerts at the MSP level which percolate down to all tenant accounts managed by the MSP. For example, if the MSP administrator 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 14 *MSP Alerts*



From the **MSP View**, go to **Monitoring & Reports > Alerts** page to configure, view, and acknowledge alerts. For a complete list of alerts that you can configure, see [Alert Types on page 1](#).

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 [Webhooks on page 1](#).

This section includes the following topics:

- [Configuring Alerts at the MSP Level on page 64](#)
- [Configuring Alerts at the Tenant Account Level on page 65](#)
- [Alerts Dashboard and Acknowledging Alerts on page 65](#)
- [Viewing Enabled Alerts on page 66](#)

Configuring Alerts at the MSP Level

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

1. Go to **Monitoring & Reports > Alerts**.
2. On the **Alerts** page, click **Configure Alerts**.
3. In the **Configure Alerts** page, click **All**.



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

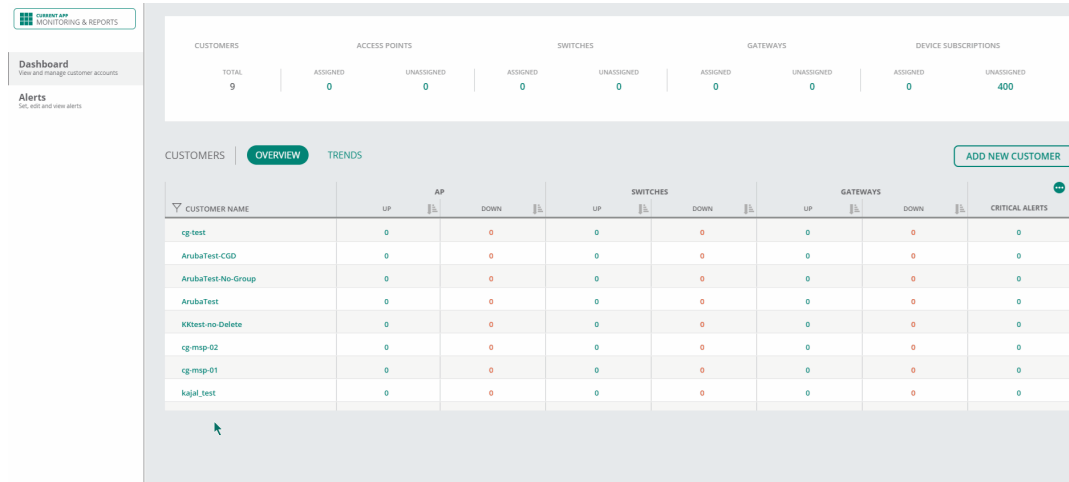
4. In the **All** tab, do one of the following:
 - Select an alert and click **+** to enable the alert with default settings.
 - To configure alert parameters, click on the alert tile (anywhere within the rectangular box) and do the following:
 - **Severity**—Set the severity. The available options are Critical, Major, Minor, and Warning. By default, the following alerts are enabled and the severity is set to **Major**: Virtual Controller Disconnected, Rogue AP Detected, New User Account Added, Switch Detected, and Switch Disconnected.



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

- **Duration**—Enter the duration in minutes.
- **Notification Options**—See [Notification Delivery Options on page 64](#).
- Click **Save**.
- **Add Rule**—(Optional) For a few alerts, the **Add Rule** option appears. For such alerts, you can add additional rule(s).

The following animation shows how to configure an alert at the MSP level:

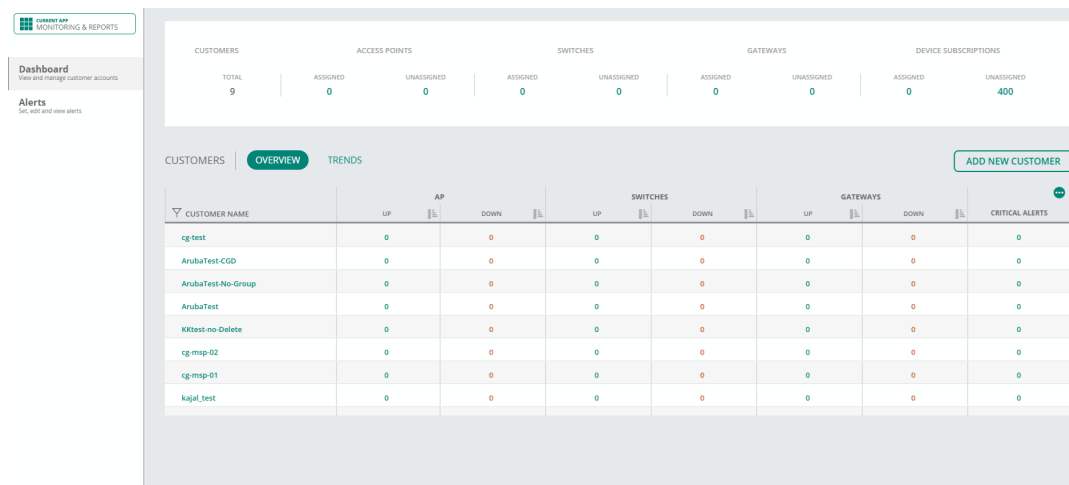


Configuring Alerts at the Tenant Account Level

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

1. From the MSP Dashboard, navigate to the tenant account for which you want to configure the alert. See [Navigating to the Tenant Account on page 62](#).
2. Complete [step 1 on page 64](#) to [step 4 on page 64](#). In [step 4 on page 64](#), optionally, you can restrict the scope of an alert by setting one or more of the following parameters in **Device Filter Options**:
 - **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.

The following animation shows how to configure an alert at the tenant account level:

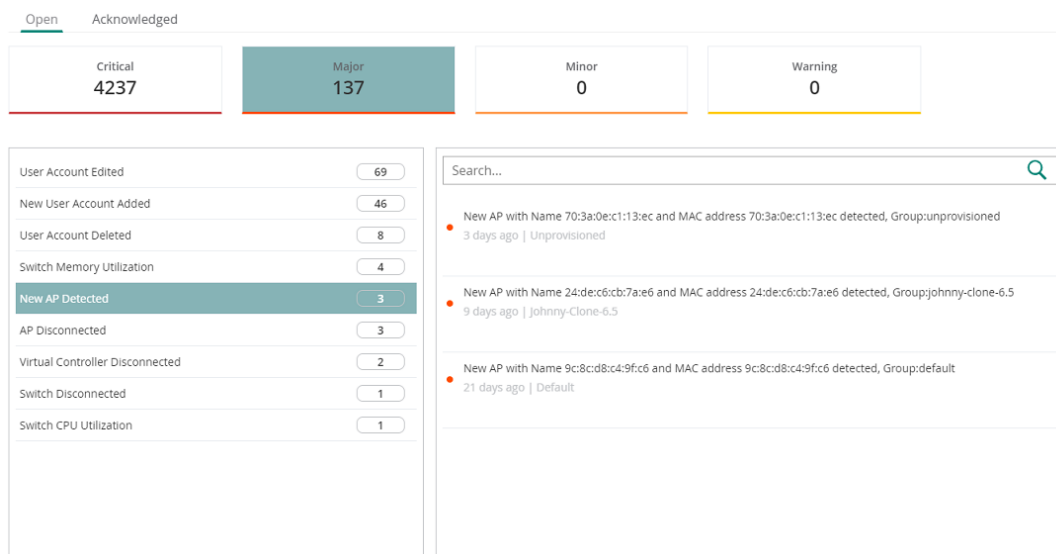


Alerts Dashboard and Acknowledging Alerts

To view a summary of alerts and acknowledge alerts, go to **Monitoring & Reports > Alerts**. The **Alerts** page displays the total number of alerts for each severity and the following options:

- **Search**—Allows you to search for alerts by tenant account. Enter the name of the tenant account and select the tenant account from the list.
- From the **Open** tab, you can do the following:

- View the total number of alerts generated for the following severities: Critical, Major, Minor, and Warning. If the number is displayed, click on the severity to view the type of alerts generated in each severity. Click on an alert type to view the list of open alerts for each alert type. The following figure illustrates the **Open** alerts dashboard:



- Search**—Allows you to search for an open alert.
 - Acknowledge**—The **Acknowledge** button appears when you hover your mouse over any alert. Click **Acknowledge** to acknowledge that specific alert.
 - Acknowledge All**—Allows you to acknowledge all alerts at once.
- **Acknowledged** tab—Displays a list of acknowledged alerts. Use the search box to search for an alert.

By default, the MSP view displays notifications for configuration events that occurred in the last one month.



The UI also shows the alerts and pending actions, such as importing a device, setting country code of Instant APs and so on, in the bottom pane of the UI. Click the link and complete the required actions.

Viewing Enabled Alerts

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

- Go to **Monitoring & Reports > Alerts**.
- On the **Alerts** page, click **Enabled**.

The **Enabled** tab lists the alerts that you have enabled.

The **Maintenance** tab displays the maintenance pane for the Aruba Central. The **Maintenance** pane consists of the following menu options:

- [Viewing Firmware Information on page 67](#)
- [Viewing Audit Trails on page 75](#)
- [Customizing Portal on page 54](#)

Viewing Firmware Information

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

Table 13: *Firmware*

Date Pane Item	Description
ID	Tenant account ID.
Name	Name of the tenant.
Firmware Status	Status of the devices associated with the tenant account. This column displays either Newer firmware available or Firmware up to date .
Compliance Status	Status of compliance for the tenant. This column indicates the compliance status such as Set , Not Set , or Set <date and time> for a specific tenant.

The **Firmware** menu in the **Maintenance** app displays the **Virtual Controller**, **Switch-MAS**, **Switch-Aruba**, and **Gateways** tab listing the all the tenants with firmware and compliance status for each of the device types. Each of these tabs have a gear icon that provides the option of setting and clearing compliance for all the tenants. The following are the two options in **Set Compliance for all tenants**:

- **Set Compliance**—To set compliance for all the tenants. Clicking this option displays the **Firmware Compliance Setting** page with the following input fields:
 - **Device Type**—List of version number from the drop-down list to which the tenants are required to be upgraded.
 - **When**—Contains radio buttons to specify if the upgrade must be carried out immediately or at a later date and time.
 - **Upgrade**—The button to perform the firmware upgrade with the above settings.
 - **Cancel**—The button to cancel the settings and go back to the **Maintenance > Firmware** page.
- **Clear Compliance**—The option to clear compliance for all tenants. Clicking **Clear Compliance** option displays a confirmation message to clear the configurations associated with compliance. Clicking the **Confirm Action** button clears the compliance set for all the tenants.



You can also set or clear compliance for specific tenants by selecting the corresponding check boxes provide in the table. When specific tenants are selected the label for the gear icon changes to **Set compliance for all selected tenants**.

To edit firmware details for a specific tenant account, select the row and click the edit icon. [Table 14](#) shows the details displayed on the **Firmware** page.

Table 14: *Firmware*

Date Pane Item	Description
Device tabs	Provides a list of the Virtual Controllers and switches provisioned in the account.
Filter by Upgrade Status	Filters the device list based on any of the following firmware upgrade status: <ul style="list-style-type: none"> ■ Need upgrade ■ Scheduled ■ In progress ■ Failed ■ Upgrade not required
Search Filter	Allows you to define a filter criterion for searching devices based on the host name, MAC address, location, firmware version, and the current upgrade status of the device.
Virtual Controllers	Displays the following information: <ul style="list-style-type: none"> ■ VC Name—Name of the VC. ■ APs—Number of APs associated to VC. ■ Firmware Version—The current firmware version running on the device. ■ Latest Available Version—The latest firmware version available on the public firmware server. ■ Firmware Status—Status of the firmware setting. ■ Compliance Status—Status of the compliance setting of the Virtual Controller. This column indicates the compliance status such as Set, Not Set, or Set <date and time> for the device.
Switch-Aruba	Displays the following details about Aruba switches managed through Aruba Central: <ul style="list-style-type: none"> ■ Host name—Host name of the switch. ■ MAC Address—MAC address of the switch. ■ Model—Hardware model of the switch. ■ Firmware Version—The current firmware version running on the switch. ■ Latest Available Version—The latest firmware version available for the switch platform. ■ Firmware Status—Status of the firmware setting. ■ Compliance Status—Status of the compliance setting of the switch. This column indicates the compliance status such as Set, Not Set, or Set <date and time> for the device.
Switch-MAS	

Manually Upgrading Firmware on Tenants

Perform the following to manually upgrade firmware for a specific tenant or all the tenants in the **Virtual Controllers**, **Switch - MAS**, **Switch - Aruba**, and **Gateways** tabs:

1. Select **Maintenance > Firmware**. The **Firmware** pane appears.
2. Select the tab based on the device type.
 1. Click the **Update All** button. The **Upgrade <Device Type> Firmware** page is displayed.

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.



2. Perform the following actions in the page:

Table 15: *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.
When	Select one of the following radio buttons to specify if the compliance must be carried out immediately or at a later date and time. <ul style="list-style-type: none">■ Now—To set the 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.

The **Maintenance > Firmware** page also displays the **Cancel All** button in the **Virtual Controllers, Switch - MAS, Switch - Aruba**, and **Gateways** tabs. Click **Cancel All** button to cancel the manual firmware upgrade for all the tenants in the MSP mode.



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.

Manually Upgrading Firmware on Tenant Devices

Perform the following to manually upgrade firmware for a specific device or all the devices of a tenant account in the **Virtual Controllers, Switch - MAS, Switch - Aruba**, and **Gateways** tabs:

1. Select **Maintenance > Firmware**. The **Firmware** pane appears.
2. Based on the device type, click the edit icon corresponding to the tenant that includes devices to be upgraded.
3. Click the **Update All** button. The **Upgrade <Device Type> Firmware** page is displayed.



You can click the check box on the table heading of device details table to include all the devices for the firmware upgrade listed in the current page. To upgrade specific devices manually, select the check box corresponding to the device that requires a manual firmware upgrade in the device 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.

4. Enter the following details in the page:

Table 16: Upgrade <Device Type> Firmware

Component	Description
Firmware Version	The firmware version to which the device 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 build or the version. NOTE: The Auto Reboot option is not applicable for Instant APs.
When	Select one of the following radio buttons to specify if the compliance must be carried out immediately or at a later date and time. <ul style="list-style-type: none"> ■ Now—To set the 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.

The **Maintenance > Firmware** page also displays the **Cancel All** button in the **Virtual Controllers, Switch - MAS, Switch - Aruba**, and **Gateways** tabs. Click **Cancel All** button to cancel the manual firmware upgrade for all the tenant devices in the MSP mode.

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. Go to **Maintenance > API Gateway**.
2. Click **Authorized Apps & Tokens** tab and generate a token key.
3. Download and copy the generated token.
4. Click the link displayed in the **APIs** tab of the **API Gateway**. The **Central Network Management APIs** page opens.
5. On the left navigation pane, select **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 17: 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 18: 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 19: *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 20: *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**

Setting Compliance for a Device

You can set compliance for devices at any of the following levels:

- [Setting Compliance at MSP Level](#)
- [Setting Compliance at Tenant Level](#)
- [Setting Compliance at Tenant Level](#)
- [Order of Precedence For Compliance](#)

Setting Compliance at MSP Level

To set compliance for a device at the MSP level, complete the following steps:

1. Go to **Maintenance > Firmware**. The **Firmware** window is displayed.
2. Select the tab based on the device type.
3. Click **Set Compliance for all tenants** next to the gear icon. The **Set compliance** and **Clear Compliance** options are displayed.
4. Click **Set Compliance** to set compliance for all the tenants. The Firmware Compliance Setting page is displayed.
5. Enter the following in the **Firmware Compliance Setting** page:
 - **Groups**—The group for which the compliance must be set. Select **All Groups** to set compliance for all the tenants.
 - **Device Type**—the version number from the drop-down list to which the device is required to be upgraded.

- **Auto Reboot**—To reboot Aruba Central automatically after the upgrade.



The **Auto Reboot** option is not applicable for Instant APs.

- **When**—Select one of the following radio buttons to specify if the compliance must be carried out immediately or at a later date and time.
 - **Now**—To set the compliance to be carried out immediately. When this option is selected, the **Save and Upgrade** button is displayed. Click **Save and Upgrade** button to save and upgrade compliance immediately.
 - **Later Date**—To set at the later date and time. When this option is selected, the **Schedule** button is displayed. Click the **Schedule** button to schedule compliance upgrade for a later date and time.
- **Cancel**—To cancel the above settings.

This includes the device for which the compliance must be set.



You can also set or clear compliance for specific tenants by selecting the corresponding check boxes provide in the table. When specific tenants are selected the label for the gear icon changes to **Set compliance for all selected tenants**.

Setting Compliance at Tenant Level

To manually upgrade to a new firmware image version, complete the following steps:

1. Select **Maintenance > Firmware**. The **Firmware** pane is displayed.
2. Click the edit icon corresponding to the tenant for which the compliance must be set in the tab based on the device type.
3. Click the gear icon. The **Firmware Compliance Setting** page is displayed.
4. Enter the following in the **Firmware Compliance Setting** page:
 - **Groups**—The group for which the compliance must be set. Select **All Groups** to set compliance at the tenant level.
 - **Device Type**—the version number from the drop-down list to which the device is required to be upgraded.
 - **Auto Reboot**—To reboot Aruba Central automatically after the upgrade.



The **Auto Reboot** option is not applicable for Instant APs.

- **When**—Select one of the following radio buttons to specify if the compliance must be carried out immediately or at a later date and time.
 - **Now**—To set the compliance to be carried out immediately. When this option is selected, the **Save and Upgrade** button is displayed. Click **Save and Upgrade** button to save and upgrade compliance immediately.
 - **Later Date**—To set at the later date and time. When this option is selected, the **Schedule** button is displayed. Click the **Schedule** button to schedule compliance upgrade for a later date and time.
- **Cancel**—To cancel the above settings.



You must reboot the device after the upgrade procedure.

Setting Compliance at Group Level

You can set the compliance at group level by selecting the group in the **Firmware Compliance Setting** page. The compliance set at the group level overrides the compliance set at the tenant level and MSP level. When the compliance is set at the MSP level with no compliance set at the group or tenant level, all the tenants inherit the compliance set at the MSP level. To set the compliance at group level, complete the following steps:

1. Select **Maintenance > Firmware**. The **Firmware** pane is displayed.
2. Click the edit icon corresponding to the tenant for which the compliance must be set in the tab based on the device type. .
3. Click the gear icon. The **Firmware Compliance Setting** page is displayed.
4. Enter the following in the **Firmware Compliance Setting** page:
 - **Groups**—The group for which the compliance must be set. Select the specific group from the drop-down list for which the compliance must be set.
 - **Device Type**—Version number from the drop-down list to which the device is required to be upgraded.
 - **Auto Reboot**—To reboot Aruba Central automatically after the upgrade.



The **Auto Reboot** option is not applicable for Instant APs.

- **When**—Select one of the following radio buttons to specify if the compliance must be carried out immediately or at a later date and time.
 - **Now**—To set the compliance to be carried out immediately. When this option is selected, the **Save and Upgrade** button is displayed. Click **Save and Upgrade** button to save and upgrade compliance immediately.
 - **Later Date**— To set at the later date and time. When this option is selected, the **Schedule** button is displayed. Click the **Schedule** button to schedule compliance upgrade for a later date and time.
- **Cancel**—To cancel the above settings.

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.

Viewing Audit Trails

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

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

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

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

To view the audit trail log details in Aruba Central:

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

Viewing Audit Trails in MSP

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 displays the following information:

Table 21: *Audit Trail Pane in the MSP*

Data Pane Content	Description
Time	Time stamp of the events for which the audit trails are shown.
Username	The username of the admin user who applied the changes.
IP Address	IP address of the client device.

Data Pane Content	Description
Classification	Type of modification and the affected device management category. For more information, see Classification of Audit Trails on page 76 .
Target	The group or device to which the changes were applied.
Source	The source tenant account from which the change was made.
Details	A short description of the changes such as subscription assignment, firmware upgrade, and configuration updates.

Classification of Audit Trails

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

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

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 77](#)
- [Creating Apps for Social Login on page 78](#)
- [Configuring a Cloud Guest Splash Page Profile on page 81](#)

Guest Access Dashboard

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

[Table 22](#) describes the contents of the **Guest Access Overview** page:

Table 22: *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.
Application Usage	The application usage by the guest clients connected to the Instant APs on which the Deep Packet Inspection feature is enabled.

Creating Apps for Social Login

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

- [Creating a Facebook App on page 78](#)
- [Creating a Google App on page 79](#)
- [Creating a Twitter App on page 80](#)
- [Creating a LinkedIn App on page 80](#)

Creating a Facebook App

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

To create a Facebook app, complete the following steps:

1. Visit the Facebook app setup URL at <https://developers.facebook.com/apps>.
2. From **My Apps**, select **Add a New App**.
3. Enter the app name and your email address in the **Display Name** and **Contact Email** text boxes, respectively.
4. Click **Create App ID**.
5. Hover the mouse on **Facebook Login** and select **Setup**.
6. Click **Web** (that is, the WWW platform).
7. Enter the website URL in the **Site URL** box. This URL is the same as the server URL mapped in the splash page configuration.
8. Click **Save**.
9. Read through the Next Steps section for further information on including Login Dialog, Access Tokens, Permissions, and App Review.
10. Go to **PRODUCTS > Facebook Login > Settings** from the left navigation menu.
11. Click the **Client OAuth Login** toggle switch to turn to **Yes**.

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



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

13. From the left navigation menu, select **App Review**.
14. Select the **Make <App Name> Public** toggle switch to make your app available to public.
15. Click **Category**.
16. In the **Choose a Category** pop-up window, select a category.
17. Click **Confirm**.
18. Select other extra permissions you want to provide for the users of your app. There are 41 permissions available for you to select from.
19. Click **Add xx Items**, where x represents the number of permissions you selected.
20. Enter the reason for providing specific permissions and click **Save**.
21. Click **Submit for Review**.
22. On the left navigation pane, click the **Settings** icon. Note the app ID and app secret key. Use the app ID and secret key when configuring Facebook login in the Aruba Central UI.
23. Under **App Domains**, enter the server URL.

Creating a Google App

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

To create a Google+ app, complete the following steps:

1. Access the Google Developer site at <https://code.google.com/apis/console>.
2. To select an existing project, click **Select a project** and select the desired project.
3. If the project is not created, click **Create a project**, enter the project name and click **Create**.
4. Click **Enable APIs and Services**.
5. Navigate to **Social** category, and then click **Google+ API**. The **Google+ API** window opens.
6. To enable the API, click **Enable**.
7. Click **Create Credentials**. If the credentials are already created, click **Go to credentials**.
8. In the **Credentials** pane, perform the following actions:
 - Under the **Where will you be calling the API from** section, select **Web Browser**.
 - Under the **What data you will be accessing** section, select **User Data**.
 - Click **What Credentials do I need**.
9. Under **Create an OAuth 2.0 client ID**. Enter the **OAuth 2.0 Client ID Name**.
10. Under **Authorized JavaScript Origins**, enter the base URL with FQDN of the cloud guest instance that will be hosting the captive portal. For example, <https://%hostname%>.
11. Under **Authorized Redirect URIs**, enter the cloud server OAuth reply URL that includes the FQDN of the cloud server instance with **/oauth/reply** appended at the end of the URL.



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

12. Click **Create Client ID**.
13. Under **Set up the OAuth 2.0 consent screen**, provide your **Email Address** and product name, and then click **Continue**. The client ID is displayed.
14. Click **Done**. A page showing the OAuth Client IDs opens.
15. Click the **OAuth client ID** to view the client ID and client secret key. Use this client ID and client secret key when configuring Google+ login in the Aruba Central UI.

Creating a Twitter App

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

To create a Twitter app, complete the following steps:

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



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

Important Note for the MSP Mode Users

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 on page 81](#)
- [Customizing a Splash Page Design on page 85](#)
- [Previewing and Modifying a Splash Page Profile on page 86](#)
- [Localizing a Cloud Guest Portal on page 86](#)
- [Associating a Splash Page Profile to an SSID on page 90](#)

Adding a Cloud Guest Splash Page Profile

To create a splash page profile:

1. From the app selector, click **Guest Access**. The guest access configuration and management menu options are displayed.
2. Click **Splash Page**. The **Splash Page** pane is displayed.
3. Select a group from the group selector. You can create splash page profiles only for the individual groups. The splash page creation function is not available if the page view is set to **All Devices**.
4. To create a new Splash page, Click the + icon. The **New Splash Page** pane is displayed.
5. On the **Configuration** tab, configure the parameters described in the following table:

Table 23: *Splash Page Configuration*

Data Pane Content	Description
Name	Enter a unique name to identify the splash profile. NOTE: If you attempt to enter an existing splash profile's name, Aruba Central displays a message stating that Splash page with this name already exists .
Type	Configure any of the following authentication methods to provide a secure network access to the guest users and visitors. <ul style="list-style-type: none">■ Anonymous■ Authenticated■ Facebook Wi-Fi
Anonymous	Configure the Anonymous login method if you want to allow guest users to log in to the Splash page without providing any credentials. For anonymous user authentication, you can also enable a pre-shared key to allow access. To enable a pre-shared key based authentication, set the Guest Key to ON and specify a password.

Table 23: Splash Page Configuration

Data Pane Content	Description
Authenticated	<p>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.</p> <p>The authenticated options available for configuring the cloud guest splash page are described in the following rows.</p>
Username/Password	<p>The Username/Password based authentication method allows pre-configured visitors to obtain access to wireless connection and the Internet. The visitors or guest users can register themselves by using the splash page when trying to access the network. The password is delivered to the users through print, SMS or email depending on the options selected during registration.</p> <p>To allow the guest users to register by themselves:</p> <ol style="list-style-type: none"> 1. Enable Self-Registration. 2. Set the Verification Required to ON if the guest user account must be verified. 3. Specify a verification criteria to allow the self-registered users to verify through email or phone. <ul style="list-style-type: none"> ■ If email-based verification is enabled and the Send Verification Link is selected, a verification link is sent to the email address of the user. The guest users can click the link to obtain access to the Internet. ■ If phone-based verification is enabled, the guest users will receive an SMS. The administrators can also customize the content of the SMS by clicking on Customize SMS. 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. <p>By default, the expiration date for the accounts of self-registered guest users is set to infinite during registration. The administrator or the guest operator can set the expiration date after registration.</p>
Social Login	<p>Social Login—Enable this option to allow guest users to use their existing login credentials from social networking profiles such as Facebook, Twitter, Google+, or LinkedIn and sign into a third-party website. When a social login based profile is configured, a new login account to access the guest network or third-party websites is not required.</p> <ul style="list-style-type: none"> ■ Facebook—Allows guest users to use their Facebook credentials to log in to the splash page. To enable Facebook integration, you must create a Facebook app and obtain the app ID and secret key. For more information on app creation, see Creating a Facebook App. Enter the app ID and secret key for client ID and client Secret respectively to complete the integration. ■ Twitter—Allows guest users to use their Twitter credentials to log in to the splash page. To enable Twitter integration, you must create a Twitter app and obtain the app ID and secret key. For more information, see Creating a Twitter App. Enter the app ID and secret key for client ID and client secret respectively to complete the integration. ■ Google+—Allows guest users to use their Google+ credentials to log in to the splash page. To enable Google+ integration, you must create a Google app and obtain the app ID and secret key. For more information, see Creating a Google App. <ol style="list-style-type: none"> 1. Enter the app ID and secret key for client ID and client secret respectively. 2. To restrict authentication attempts to only the members of a Google hosted domain, enter the domain name in the Gmail for Work Domain text box. Ensure that you have a valid domain account licensed by Google Domains or Google Apps. For more information see: <ul style="list-style-type: none"> ■ https://apps.google.com/intx/en_in/ ■ https://domains.google.com/about/ 3. Specify a text for the Sign-In button. ■ 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

Table 23: Splash Page Configuration

Data Pane Content	Description
	app ID and secret key. For more information, see Creating a LinkedIn App . Enter the app ID and secret key for client ID and client secret respectively to complete the integration.
Facebook Wi-Fi	<p>If you want to enable network access through the free Wi-Fi service offered by Facebook. Select the Facebook Wi-Fi option. The Facebook Wi-Fi feature allows you to pair your network with a Facebook business page, thereby allowing the guest users to log in from Wi-Fi hotspots using their Facebook credentials.</p> <p>If the Facebook Wi-Fi business page is set up, when the users try to access the Internet, the browser redirects the user to the Facebook page. The user can log in with their Facebook account credentials and can either check in to access free Internet or skip checking in and then continue.</p>
Facebook Wifi Configuration	<p>After selecting the Facebook Wi-Fi option, complete the following steps to continue with the Facebook Wi-Fi configuration.</p> <ol style="list-style-type: none"> 1. Click the Configure Now link. 2. Sign in to your Facebook account. 3. If you do not have a business page, click Create Page. For more information on setting Facebook Wi-Fi service, see Setting up Facebook Wi-Fi for Your Business at https://www.facebook.com/help/126760650808045. <p>NOTE: Instant AP devices support Facebook Wi-Fi services on their own, without Aruba Central. However, for enabling social login based authentication, the guest splash pages must be configured in Aruba Central. For more information on Facebook Wi-Fi configuration on an Instant AP, see the <i>Aruba Instant User Guide</i>.</p>
Allow Internet In Failure	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	<p>To override the default common name, click the Override Common Name toggle switch and specify a common name. The common name is the web page URL of the guest access portal. By default, the common name is set to securelogin.arubanetworks.com. The guest users can override this default name by adding their own common name.</p> <p>If your devices are managed by AirWave and you want to use your own certificate for the captive portal service, ensure that the captive portal certificate is pushed to the Instant AP from the AirWave management system. When the appropriate certificate is loaded on the AP, perform the following actions:</p> <ol style="list-style-type: none"> 1. Run the show captive-portal-domains command at the Instant AP command prompt. 2. Note the common name or the internal captive portal domain name. 3. Add this domain name in the Override Common Name field on the Splash Page configuration page. 4. Save the changes.
Guest Key	To set password for anonymous users, enable the Guest Key and enter a password.
Sponsored Guest	Enable the Sponsored Guest option if you (network administrator) want to give the authorization control to a guest sponsor to allow or deny a guest from accessing the network.
Allowed Sponsor Domains	This is a mandatory field. Enter accepted company domain names. The domain name must match the suffix of the sponsor's email address. The domain names must be company names and not any public domain names such as gmail, yahooemail, and so on. To add more domain names, click the add icon and enter the domain name.

Table 23: Splash Page Configuration

Data Pane Content	Description
Allowed Sponsor Emails	Optional field to enter allowed email addresses. If you leave this field empty, all emails that correspond to the allowed domains list are permitted to sponsor guests. To add more sponsor emails, click the add icon and enter the sponsor's email address.
Authentication Success Behavior	<p>If Anonymous or Authenticated option is selected as the guest user authentication method, specify a method for redirecting the users after a successful authentication. Select one of the following options:</p> <ul style="list-style-type: none"> ■ Redirect to Original URL— When selected, upon successful authentication, the user is redirected to the URL that was originally requested. ■ Redirect URL— Specify a redirect URL if you want to override the original request of users and redirect them to another URL.
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	<p>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.</p> <p>If MAC caching is enabled, the users are allowed or denied access based on the MAC address of the connective device.</p>
Share This Profile	Select this check box if you want to allow the users to share the Splash Page profile. The Splash Page profiles under All Devices can be shared across all the groups.
Simultaneous Login Limit	Specify the maximum number of devices that a user can use to access an account at a given time. For example, if you set the login limit as three, a user can simultaneously log in to an account using three different devices.
Daily Usage Limit	<p>Use this option to set a data usage limit for authenticated guest users, anonymous profiles, and Facebook Wi-Fi logins. By default, no daily usage limit is applied. To set a daily usage limit, use one of the following options:</p> <ul style="list-style-type: none"> ■ By Time— Specify the time limit in hours and minutes for data usage during a day. When a user exceeds the configured time limit, the device is disconnected from the network until the next day begins; that is, until 00.00 hours in the specified 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. <ul style="list-style-type: none"> ● Per User— This option applies the data usage limit based on authenticated user credentials. ● Per Session—This option applies the data usage limit based on user sessions. ● Per Device—This option applies the data usage limit based on the MAC address of the client device connected to the network. <p>Important Points to Note</p> <ul style="list-style-type: none"> ■ The values configured for this feature do not serve as hard limits. There might be a slight delay in enforcing daily usage limits due to the time required for processing information. ■ For anonymous and Facebook Wi-Fi logins, the daily usage limit is applied per MAC address of the client device connected to the network.
Whitelist URL	To allow a URL, click + and add the URL to the whitelist. For example, if the terms and conditions configured for the guest portal include URLs, you can add these URLs to the whitelist, so that the users can access the required web pages.

5. Click **Next**. The **Customization** pane appears. [Customizing a Splash Page Design on page 85](#).



You can edit or delete a splash page profile by clicking the respective icons in the **Splash Page Profile** pane.

Customizing a Splash Page Design

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

Table 24: *Splash page customization*

Data Pane Content	Description
Background color	To change the color of the splash page, select a color from the Background Color palette.
Button title	Specify a title for the sign in button.
Button color	To change the color of the sign in button, select a color from the Button Color palette.
Header fill color	Select the fill color for the splash page header from the Header fill color palette.
Page font color	To change the font color of the text on the splash page, select a color from the Page font color palette.
Page font Color	Select the font color of the splash page from the palette.
Logo	To upload a logo, click Browse , and browse the image file. Ensure that the image file size does not exceed 256 KB.
Background Image	Click Browse to upload a background image. Ensure that the background image file size does not exceed 512 KB.
Page Title	Add a suitable title for the splash page.
Welcome Text	Enter the welcome text to be displayed on the splash page. Ensure that the welcome text does not exceed 20,000 characters.
Terms & Conditions	<p>Enter the terms and conditions to be displayed on the splash page. Ensure that the terms and conditions text does not exceed 20000 characters.</p> <p>The text box also allows you to use HTML tags for formatting text. For example, to highlight text with italics, you can wrap the text with the <code><i> </i></code> HTML tag.</p> <p>Specify an acceptance criteria for terms and condition by selecting any of the following options from the Display "I Accept" Checkbox:</p> <ul style="list-style-type: none">■ No, Accept by default■ Yes, Display Checkbox <p>If the I ACCEPT check box must be displayed on the Splash page, select the display format for terms and conditions.</p> <p>Ensure that Display Option For Terms & Conditions has the Inline Text option auto-selected and displayed as an uneditable text.</p>
Ad Settings	<p>If you want to display advertisements on the splash page, enter the URL in the Advertisement URL.</p> <p>For Advertisement Image, click Browse and upload the image.</p>

6. Click **Preview** to preview the customized splash page or click **Finish**.

Previewing and Modifying a Splash Page Profile

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

1. From the app selector, click **Guest Access**.
2. Click the **Splash Page** menu option. A list of splash Page profiles is displayed.
3. Ensure that the pop-up blocker on your browser window is disabled.
4. Click the preview icon next to the profile you want to preview. The Splash Page is displayed in a new window.

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

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

Localizing a Cloud Guest Portal

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



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

Table 25: *Cloud Guest Portal Localization*

Data Pane Content	Description	Allowed Length of Text
Login Section		
Login button title	Enter the custom label text to be localized for the Login button.	1–255 characters
Network login title	Enter the custom title text that you want to localize for the Network Login page.	1–255 characters
Login page title	Enter the custom text for title in the Login page.	1–255 characters
Access denied page title	Enter the custom title text for the Access Denied page.	1–255 characters
Logged in title	Enter the custom Logged in title text for the page that allows access.	1–255 characters
Username label	Enter the custom text for Username label.	1–255 characters
Username placeholder	Enter the custom text to show in in the Username placeholder.	1–255 characters

Table 25: *Cloud Guest Portal Localization*

Data Pane Content	Description	Allowed Length of Text
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		
Phone help message	Enter a custom help message to show for the Phone help field.	Up to 20000 characters
Phone number placeholder	Enter the custom placeholder text for the Phone Number input UI control.	1–255 characters
'Back' button text	Enter the custom text label to show for the Back button control.	1–255 characters
'Continue' button text	Enter the custom text label to show for the Continue button control.	1–255 characters
Email radio button	Enter a custom text label for the Email option.	—
Phone radio button	Enter a custom label text for the Phone option.	—
Register page title	Enter a custom title text for the Register page.	1–255 characters

Table 25: *Cloud Guest Portal Localization*

Data Pane Content	Description	Allowed Length of Text
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
Verify button title	Enter a custom label text for the Verify button.	1–255 characters
Verify title	Enter a custom text for Verify title.	1–255 characters
Network login message	Enter a custom text message to show in the Network Login page.	Up to 20000 characters
Sponsored Guest Section		
Sponsor approval granted title	Enter a custom title for the sponsor's Approval Granted page.	1–255 characters

Table 25: *Cloud Guest Portal Localization*

Data Pane Content	Description	Allowed Length of Text
Sponsor approval pending title	Enter a custom title for the sponsor's Approval Pending page.	1–255 characters
Sponsor approve button title	Enter a custom title for the sponsor's Approve button.	1–255 characters
Sponsor approve title	Enter a custom title for the sponsor's Approve page.	1–255 characters
Sponsor approved title	Enter a custom title to be shown on the Approved page.	1–255 characters
Sponsor label	Enter a custom text for the Sponsor label.	1–255 characters
Sponsor placeholder	Enter a custom placeholder text for sponsor input control.	1–255 characters
Sponsor approval granted message	Enter a custom message to show in the Approval Granted page when the guest sponsor had granted approval for the guest to access the network.	Up to 20000 characters
Sponsor approval mail message	Enter an optional alternative email message to send when a guest requests for a Wi-Fi access. Ensure that the email includes the [account:username] and [account:sponsor-approval-url] tokens. To customize the contents of email message, or to change the email message to a local language: 1. Click Customize Sponsor Approval Mail . 2. Edit the email message. 3. Click Save .	N/A
Sponsor approval pending message	Enter a custom message to show in the Approval Pending page when the guest sponsor is yet to approve or deny the guest from accessing the network.	Up to 20000 characters
Sponsor approve message	Enter a custom message to show in the Approve page.	Up to 20000 characters
Sponsor approved message	Enter a custom message to show in the Approved page when the guest sponsor had approved the guest to access the network.	Up to 20000 characters
Sponsor message	Enter a custom message to show in the Registration page for the guest to know that sponsor's approval is required.	Up to 20000 characters

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

Associating a Splash Page Profile to an SSID

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

1. Select **Configuration > Access Points > Networks** and then click **Create New**. The **Create a New Network** pane is displayed.
2. For **Type**, select **Wireless**.
3. Enter a name that is used to identify the network in the **Name(SSID)** box.
4. For **Primary Usage**, select **Guest** and click **Next**.
5. In the **VLANs** tab, if required, configure a VLAN assignment mode, and then click **Next**.
6. In the **Security** tab:
 - a. Select **Cloud Guest** from the **Splash Page Type** list.
 - b. Select the splash page profile name from the **Guest Captive Portal Profile** list and click **Next**.



If the user configures the default Aruba certificate, the **You are using Aruba default certificate. You shall configure new certificate** alert message is displayed for the user to configure a new certificate.

- c. To enable encryption, set **Encryption** to **Enabled** and configure encryption parameters.
 - d. To exclude uplink, select an uplink from **Disable If Uplink Type Is**.
 - e. Click **Next**.
7. In the **Access** tab, if required, modify and create access rules set the configuration if required, and then click **Finish**.