

# Aruba Central MSP User Guide



a Hewlett Packard  
Enterprise company

**Copyright Information**

© Copyright 2022 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

<b>Contents</b>	<b>3</b>
<b>About This Document</b>	<b>5</b>
Intended Audience	5
Related Documents	5
Conventions	5
Terminology Change	6
Contacting Support	6
<b>What is Aruba Central?</b>	<b>7</b>
Key Features	7
Terminology	8
Supported Web Browsers	9
Operational Modes and Interfaces	9
<b>Supported Devices for MSP</b>	<b>12</b>
Supported Instant APs	12
Supported AOS-S Platforms	15
<b>Accessing Aruba Central</b>	<b>17</b>
Logging Out of Aruba Central	18
<b>MSP Deployment Models</b>	<b>19</b>
MSP Owns Devices and Subscriptions (Deployment Model 1)	19
End-Customer Owns Both Devices and Subscriptions But MSP Manages (Deployment Model 2)	23
Hybrid MSP Deployment Model (Deployment Model 3)	25
<b>Network Structure</b>	<b>26</b>
Viewing the Network Structure Page	26
MSP Certificates	26
Device Preprovisioning in an MSP Account	28
<b>Getting Started with MSP Solution</b>	<b>30</b>
Enabling Managed Service Mode in HPE GreenLake	31
About the Managed Service Portal User Interface	33
MSP Device Management in HPE GreenLake	40
MSP Tenant Management in HPE GreenLake	40
Customizing the Portal in MSP Mode	42
About Provisioning Tenant or Customer Accounts	43
Navigating to the Tenant Account	47
<b>Groups in the MSP Mode</b>	<b>47</b>
MSP Group Illustration	48
Tenant Default Group Overrides	48
Considerations for Editing a Tenant Default Group	49
MSP Group Persona	50
Creating an MSP Group Persona with ArubaOS 8 Architecture	50
Cloning an MSP UI Group	52
Deleting an MSP UI Group	53
<b>SD-WAN Support in MSP Mode</b>	<b>54</b>
Assigning a Gateway Persona to an MSP Group	54
Mapping Scenarios for MSP Groups	54
Important Notes for SD-WAN Support in MSP Mode	55
Priority of Configuration Percolation in MSP Mode	55

---

Checking the Gateway Persona of a Customer Group .....	55
<b>MSP Dashboard .....</b>	<b>57</b>
Viewing the MSP Dashboard .....	57
Dashboard Summary .....	58
Customer   Overview .....	58
Customers   Trends .....	60
Navigating to the Tenant Account .....	61
<b>Configuring Instant APs .....</b>	<b>62</b>
<b>Configuring Switches .....</b>	<b>63</b>
<b>Configuring Gateways .....</b>	<b>64</b>
<b>Analyzing and Maintaining MSP Tenant Accounts .....</b>	<b>65</b>
MSP Alerts .....	65
Firmware Upgrades for MSP Mode .....	70
MSP Reports .....	76
MSP Audit Trails .....	83
<b>Guest Access .....</b>	<b>84</b>
Guest Access Dashboard .....	84
Mapping Cloud Guest Certificates .....	85
Configuring a Guest Splash Page Profile .....	86
<b>Managed Service Provider .....</b>	<b>98</b>
How do I create an Aruba Central MSP account? .....	98
Should tenants sign up for an Aruba Central account as well? .....	98
Who owns the hardware and subscriptions? .....	98
Can existing Aruba Central customers migrate to an MSP account? .....	98
What are the supported devices and architectures? .....	98
What happens to a device on Aruba Central when it's subscription expires ? .....	99
Which group is the default group for the tenant account? .....	99
What are predefined user roles? .....	99
What are custom user roles? .....	100
What tasks can be performed by an MSP user and tenant user? .....	100

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

## Intended Audience

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

## Related Documents

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

- [Aruba Central Help Center](#)
- [Aruba Central User Guide](#)

## Conventions

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

**Table 1:** *Typographical Conventions*

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

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.

## Terminology Change

As part of advancing HPE's commitment to racial justice, we are taking a much-needed step in overhauling HPE engineering terminology to reflect our belief system of diversity and inclusion. Some legacy products and publications may continue to include terminology that seemingly evokes bias against specific groups of people. Such content is not representative of our HPE culture and moving forward, Aruba will replace racially insensitive terms and instead use the following new language:

Usage	Old Language	New Language
Campus Access Points + Controllers	Master-Slave	Conductor-Member
Instant Access Points	Master-Slave	Conductor-Member
Switch Stack	Master-Slave	Conductor-Member
Wireless LAN Controller	Mobility Master	Mobility Conductor
Firewall Configuration	Blacklist, Whitelist	Denylist, Allowlist
Types of Hackers	Black Hat, White Hat	Unethical, Ethical

## Contacting Support

**Table 2:** *Contact Information*

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

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

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

This section includes the following topics:

- [Key Features](#)
- [Terminology](#)
- [Supported Web Browsers](#)
- [Operational Modes and Interfaces](#)

## Key Features

Aruba Central offers the following key features and benefits:

- Streamlined configuration and deployment of devices—Leverages the ZTP capability of Aruba devices to bring up your network in no time. Aruba Central supports group configuration of devices, which allows you to provision and manage multiple devices with similar configuration requirements with less administrative overhead.
- Integrated wired, WAN, and wireless Infrastructure management—Offers a centralized management interface for managing wireless, WAN, and wired networks in distributed environments, and thus help organizations save time and improve efficiency.
- Advanced analytics and assurance—With continuous monitoring, AI-based analytics provide real-time visibility and insight into what's happening in the Wi-Fi network. The insights utilize machine learning that leverage a growing pool of network data and deep domain experience.
- Secure cloud-based platform—Offers a secure cloud platform with HTTPS connection, certificate-based authentication, and Cloud Authentication and Policy.
- Interface for Managed Service Providers—Offers an additional interface for MSPs to provision and manage their respective tenant accounts. Using the MSP mode, service provider organizations can administer network infrastructure for multiple organizations in a single interface.
- SD-Branch management—Offers a simplified solution for managing and monitoring SD Branch devices such as Branch Gateways, VPN Concentrators, Instant APs, and Aruba Switches. It also provides detailed dashboards showing WAN health and pictorial depictions of the branch setup. The Aruba SD-Branch solution extends the SD-WAN concepts to all elements in a branch setup to deliver a full-stack solution for managing WLAN, LAN and WAN connections. The SD-Branch solution provides a

common cloud-management model that simplifies deployment, configuration, and management of all components of a branch setup. The solution leverages the ZTP and cloud management capabilities of Aruba devices to integrate management and infrastructure for WAN, WLAN, and LAN and provide a holistic solution from access network to edge with end-to-end security. It also addresses all communications in distributed deployments, from micro branches to medium or large branches. For more information, see the [Aruba SD-Branch Solution Guide](#).

- **Health and usage monitoring**—Provides a comprehensive view of your network, device status and health, and application usage. You can monitor, identify, and address issues by using data-driven dashboards, alerts, reports, and troubleshooting workflows. Aruba Central also utilizes the DPI feature of the devices to monitor, analyze and block traffic based on application categories, application type, web categories and website reputation. Using this data, you can prioritize business critical applications, limit the use of inappropriate content, and enforce access policies on a per user, device or location basis.
- **Guest Access**—Allows you to manage access for your visitors with a secure guest Wi-Fi experience. You can create guest sponsor roles and social logins for your guest networks. You can also design your guest landing page with custom logos, color, and banner text.
- **Presence Analytics**—Offers a value added service for Instant AP based networks to get an insight into user presence and loyalty. The Presence Analytics dashboard allows you to view the presence of users at a specific site and the frequency of user visits at a given location or site. Using this data, you can make business decisions to improve customer engagement.

## Terminology

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

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



## Supported Web Browsers



---

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 100.0.4896.88 or later	Windows and macOS
Mozilla Firefox 99.01 or later	Windows and macOS
Safari 15.4 or later	macOS
Microsoft Edge version 100.0.1185.36 or later	Windows

## Operational Modes and Interfaces

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

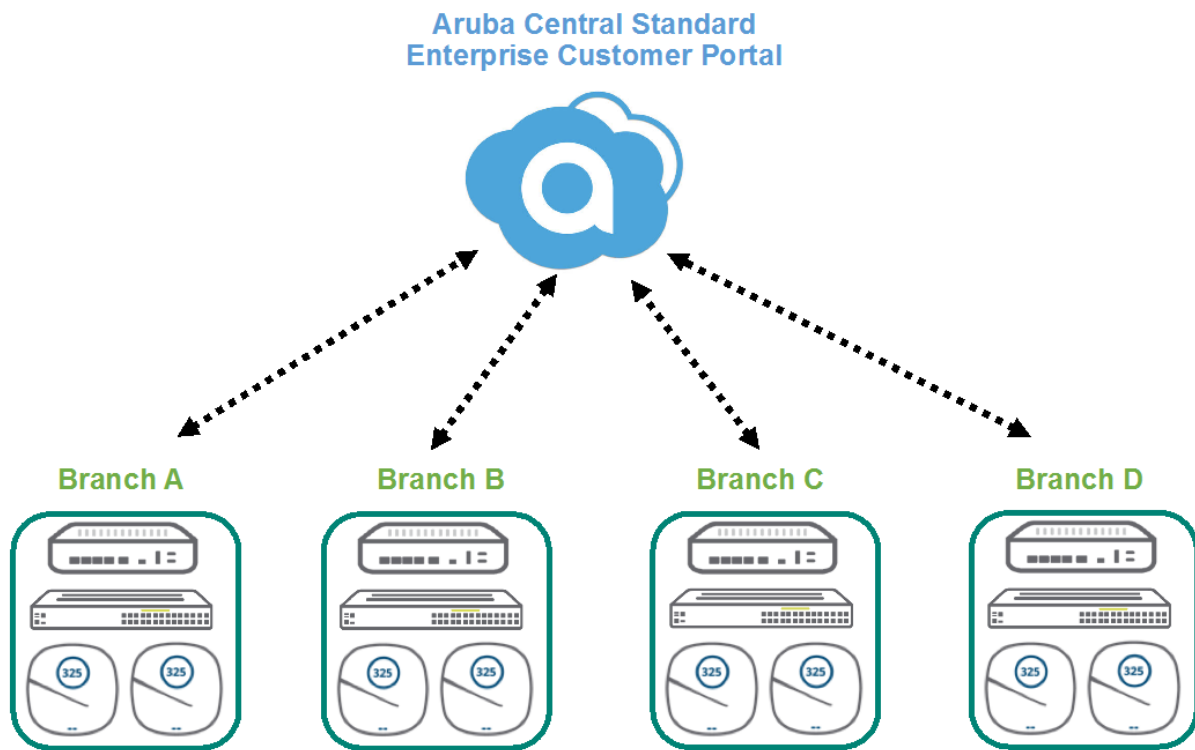
- [Standard Enterprise Mode](#)
- [Managed Service Provider Mode](#)

### Standard Enterprise Mode

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

The following figure illustrates a typical Standard Enterprise mode deployment.

**Figure 1** *Standard Enterprise Mode*

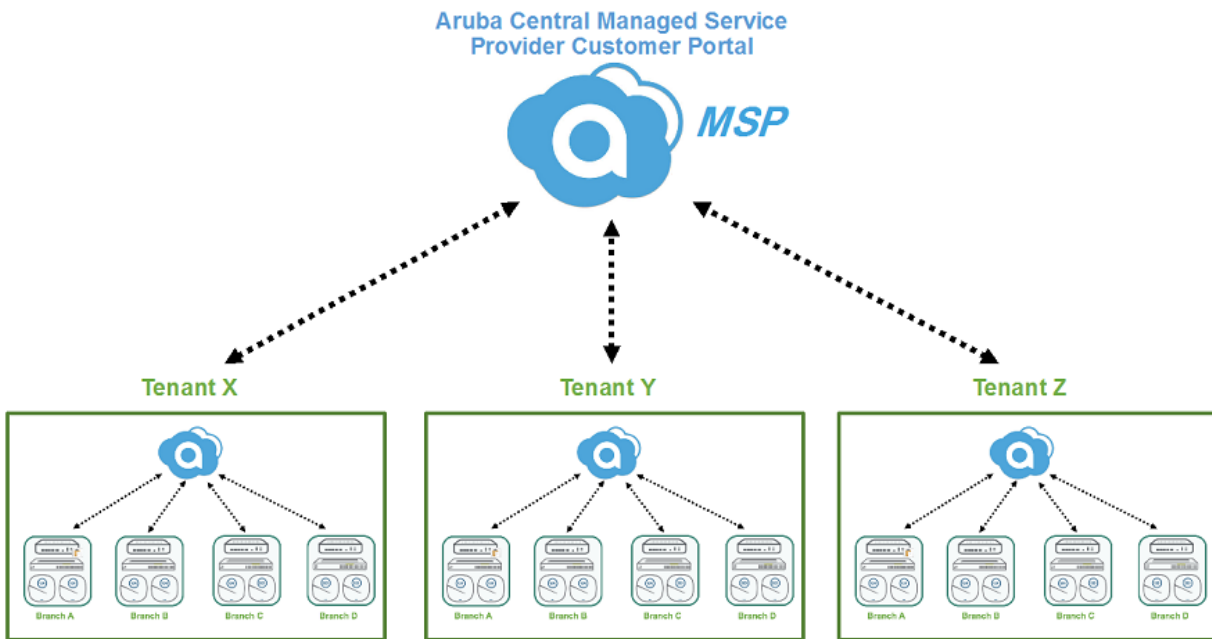


## Managed Service Provider Mode

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

The following figure illustrates a typical MSP mode deployment.

**Figure 2** *Managed Service Provider Mode*



This section provides the following information:

- [Supported Instant APs](#)
- [Supported AOS-S Platforms](#)

## Supported Instant APs

The following table lists the Instant AP platforms, the installation mode, the minimum supported Aruba Instant software versions, and the Instant APs supporting power draw:

**Table 4:** *Supported Instant AP Platforms*

Instant AP Platform	Installation Mode	Minimum Supported Aruba Instant Software Version
AP-587	Outdoor	Aruba Instant 8.10.0.0
AP-585	Outdoor	Aruba Instant 8.10.0.0
AP-584	Outdoor	Aruba Instant 8.10.0.0
AP-375ATEX	Outdoor	Aruba Instant 8.8.0.0
AP-655	Indoor	Aruba Instant 8.10.0.0
AP-635	Indoor	Aruba Instant 8.9.0.0
AP-567EX	Outdoor	Aruba Instant 8.7.1.0
AP-567	Outdoor	Aruba Instant 8.7.1.0
AP-565EX	Outdoor	Aruba Instant 8.7.1.0
AP-565	Outdoor	Aruba Instant 8.7.1.0
AP-503H	Indoor	Aruba Instant 8.7.1.0
AP-577EX	Outdoor	Aruba Instant 8.7.0.0
AP-577	Outdoor	Aruba Instant 8.7.0.0
AP-575EX	Outdoor	Aruba Instant 8.7.0.0
AP-575	Outdoor	Aruba Instant 8.7.0.0
AP-574	Outdoor	Aruba Instant 8.7.0.0
AP-518	Indoor	Aruba Instant 8.7.0.0

Instant AP Platform	Installation Mode	Minimum Supported Aruba Instant Software Version
AP-505H	Indoor	Aruba Instant 8.7.0.0
AP-505	Indoor	Aruba Instant 8.6.0.0
AP-504	Indoor	Aruba Instant 8.6.0.0
AP-555	Indoor	Aruba Instant 8.5.0.0
AP-535	Indoor	Aruba Instant 8.5.0.0
AP-534	Indoor	Aruba Instant 8.5.0.0
AP-515	Indoor	Aruba Instant 8.4.0.0
AP-514	Indoor	Aruba Instant 8.4.0.0
AP-387	Outdoor	Aruba Instant 8.4.0.0
AP-303P	Indoor	Aruba Instant 8.4.0.0
AP-377EX	Outdoor	Aruba Instant 8.3.0.0
AP-377	Outdoor	Aruba Instant 8.3.0.0
AP-375EX	Outdoor	Aruba Instant 8.3.0.0
AP-375	Outdoor	Aruba Instant 8.3.0.0
AP-374	Outdoor	Aruba Instant 8.3.0.0
AP-345	Indoor	Aruba Instant 8.3.0.0
AP-344	Indoor	Aruba Instant 8.3.0.0
AP-318	Indoor	Aruba Instant 8.3.0.0
AP-303	Indoor	Aruba Instant 8.3.0.0
AP-203H	Indoor	Aruba Instant 6.5.3.0
AP-367	Outdoor	Aruba Instant 6.5.2.0
AP-365	Outdoor	Aruba Instant 6.5.2.0
AP-303HR	Indoor	Aruba Instant 6.5.2.0
AP-303H	Indoor	Aruba Instant 6.5.2.0
AP-203RP	Indoor	Aruba Instant 6.5.2.0
AP-203R	Indoor	Aruba Instant 6.5.2.0
IAP-305	Indoor	Aruba Instant 6.5.1.0-4.3.1.0

Instant AP Platform	Installation Mode	Minimum Supported Aruba Instant Software Version
IAP-304	Indoor	Aruba Instant 6.5.1.0-4.3.1.0
IAP-207	Indoor	Aruba Instant 6.5.1.0-4.3.1.0
IAP-335	Indoor	Aruba Instant 6.5.0.0-4.3.0.0
IAP-334	Indoor	Aruba Instant 6.5.0.0-4.3.0.0
IAP-315	Indoor	Aruba Instant 6.5.0.0-4.3.0.0
IAP-314	Indoor	Aruba Instant 6.5.0.0-4.3.0.0
IAP-325	Indoor	Aruba Instant 6.4.4.3-4.2.2.0
IAP-324	Indoor	Aruba Instant 6.4.4.3-4.2.2.0
IAP-277	Outdoor	Aruba Instant 6.4.3.1-4.2.0.0
IAP-228	Indoor	Aruba Instant 6.4.3.1-4.2.0.0
IAP-205H	Indoor	Aruba Instant 6.4.3.1-4.2.0.0
IAP-215	Indoor	Aruba Instant 6.4.2.0-4.1.1.0
IAP-214	Indoor	Aruba Instant 6.4.2.0-4.1.1.0
IAP-205	Indoor	Aruba Instant 6.4.2.0-4.1.1.0
IAP-204	Indoor	Aruba Instant 6.4.2.0-4.1.1.0
IAP-275	Outdoor	Aruba Instant 6.4.0.2-4.1.0.0
IAP-274	Outdoor	Aruba Instant 6.4.0.2-4.1.0.0
IAP-103	Indoor	Aruba Instant 6.4.0.2-4.1.0.0
IAP-225	Indoor	Aruba Instant 6.3.1.1-4.0.0.0
IAP-224	Indoor	Aruba Instant 6.3.1.1-4.0.0.0
IAP-115	Indoor	Aruba Instant 6.3.1.1-4.0.0.0
IAP-114	Indoor	Aruba Instant 6.3.1.1-4.0.0.0
RAP-155P	Indoor	Aruba Instant 6.2.1.0-3.3.0.0
RAP-155	Indoor	Aruba Instant 6.2.1.0-3.3.0.0
RAP-109	Indoor	Aruba Instant 6.2.0.0-3.2.0.0
RAP-108	Indoor	Aruba Instant 6.2.0.0-3.2.0.0
RAP-3WN	Indoor	Aruba Instant 6.1.3.1-3.0.0.0
RAP-3WNP	Indoor	Aruba Instant 6.1.3.1-3.0.0.0



- AP-635 and AP-655 IAPs are Wi-Fi 6E capable APs that support 6 GHz radio band, in addition to 2.4 GHz and 5 GHz radio bands.
- The tri-radio feature is available only for AP-555. In the **5 GHz** tab, the **Radio 5 GHz (Secondary)** data is available only if the tri-radio mode is enabled. For more information, see **About Tri-Radio Mode** section in the latest Aruba Central user guide.
- RAP-155, RAP-155P, IAP-214, IAP-215, IAP-224, IAP-225, IAP-228, IAP-274, IAP-275, and IAP-277 IAPs are no longer supported from Aruba Instant 8.7.0.0 onwards.
- IAP-103, RAP-108, RAP-109, IAP-114, IAP-115, IAP-204, IAP-205, and IAP-205H IAPs are no longer supported from Aruba Instant 8.3.0.0 onwards.
- By default, AP-318, AP-374, AP-375, and AP-377 IAPs have Eth1 as the uplink port and Eth0 as the downlink port. Aruba does not recommend you to upgrade these IAPs to Aruba Instant 8.5.0.0 or 8.5.0.1 firmware versions, as the upgrade process changes the uplink port from Eth1 to Eth0 port thereby making the devices unreachable.
- For more information about Aruba's End-of-life policy and the timelines for hardware and software products at the end of their lives, see: <https://www.arubanetworks.com/support-services/end-of-life/>.
- Data sheets and technical specifications for the supported AP platforms are available at: <https://www.arubanetworks.com/products/networking/access-points/>.

## Supported AOS-S Platforms



- Aruba Central uses the SSL certificate by GeoTrust Certificate Authority for device termination and web services. As the SSL certificate is about to expire, Aruba is replacing it with a new certificate from another trusted Certificate Authority. During the certificate upgrade window, all devices managed by Aruba Central will be disconnected. After the upgrade, the devices reconnect to Aruba Central and resume their services with Aruba Central. However, for AOS-S switches to reconnect to Aruba Central after the certificate upgrade, you must ensure that the switches are upgraded to the recommended software version listed in [Table 5](#).
- Aruba Central does not support switch software versions below 16.08 release for firmware upgrade. In addition, only the latest three switch software versions of all major release versions will be available for firmware upgrade from Aruba Central. For example, if the latest switch software version released is 16.10.0016, the following versions will be available for firmware upgrade: 16.10.0014, 16.10.0015 and 16.10.0016.
- Changing AOS-S switches firmware from latest version to earlier major versions is not recommended if the switches are managed in UI groups. For features that are not supported or not managed in Aruba Central on earlier AOS-S versions, changing firmware to earlier major versions might result in loss of configuration.

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

**Table 5: Supported AOS-S Switch Series, Software Versions, and Switch Stacking**

Switch Platform	Supported Software Version	Recommended Software Version	Switch Stacking Support	Supported Stack Type (Frontplane (VSF) / Backplane (BPS))	Supported Configuration Group Type for Stacking (UI / Template)
Aruba 2530 Switch Series	<ul style="list-style-type: none"> <li>YA/YB.16.08.0021 or later</li> <li>YA/YB.16.09.0016 or later</li> <li>YA/YB.16.10.0012 or later</li> <li>YA/YB.16.11.0002</li> </ul>	<ul style="list-style-type: none"> <li>YA/YB.16.08.0023 or later</li> <li>YA/YB.16.09.0018 or later</li> <li>YA/YB.16.10.0016 or later</li> <li>YA/YB.16.11.0002</li> </ul>	N/A	N/A	N/A
Aruba 2540 Switch Series	<ul style="list-style-type: none"> <li>YC.16.08.0019 or later</li> <li>YC.16.09.0015 or later</li> <li>YC.16.10.0012 or later</li> <li>YC.16.11.0002</li> </ul>	<ul style="list-style-type: none"> <li>YC.16.08.0023 or later</li> <li>YC.16.09.0018 or later</li> <li>YC.16.10.0016 or later</li> <li>YC.16.11.0002</li> </ul>	N/A	N/A	N/A
Aruba 2920 Switch Series	<ul style="list-style-type: none"> <li>WB.16.08.0019 or later</li> <li>WB.16.09.0015 or later</li> <li>WB.16.10.0011 or later</li> <li>WB.16.11.0002</li> </ul>	<ul style="list-style-type: none"> <li>WB.16.08.0023 or later</li> <li>WB.16.09.0018 or later</li> <li>WB.16.10.0016 or later</li> <li>WB.16.11.0002</li> </ul>	Yes <b>Switch Software Dependency:</b> <ul style="list-style-type: none"> <li>WB.16.08.0019 or later</li> <li>WB.16.09.0015 or later</li> <li>WB.16.10.0011 or later</li> <li>WB.16.11.0002</li> </ul>	BPS	UI and Template
Aruba 2930F Switch Series	<ul style="list-style-type: none"> <li>WC.16.08.0019 or later</li> <li>WC.16.09.0015 or later</li> <li>WC.16.10.0012 or later</li> <li>WC.16.11.0002</li> </ul>	<ul style="list-style-type: none"> <li>WC.16.08.0023 or later</li> <li>WC.16.09.0018 or later</li> <li>WC.16.10.0016 or later</li> <li>WC.16.11.0002</li> </ul>	Yes <b>Switch Software Dependency:</b> <ul style="list-style-type: none"> <li>WC.16.08.0019 or later</li> <li>WC.16.09.0015 or later</li> <li>WC.16.10.0012 or later</li> <li>WC.16.11.0002</li> </ul>	VSF	UI and Template



Switch Platform	Supported Software Version	Recommended Software Version	Switch Stacking Support	Supported Stack Type (Frontplane (VSF) / Backplane (BPS))	Supported Configuration Group Type for Stacking (UI / Template)
Aruba 2930M Switch Series	<ul style="list-style-type: none"> <li>WC.16.08.0019 or later</li> <li>WC.16.09.0015 or later</li> <li>WC.16.10.0012 or later</li> <li>WC.16.11.002</li> </ul>	<ul style="list-style-type: none"> <li>WC.16.08.0023 or later</li> <li>WC.16.09.0018 or later</li> <li>WC.16.10.0016 or later</li> <li>WC.16.11.0002</li> </ul>	Yes <b>Switch Software Dependency:</b> <ul style="list-style-type: none"> <li>WC.16.08.0019 or later</li> <li>WC.16.09.0015 or later</li> <li>WC.16.10.0012 or later</li> <li>WC.16.11.0002</li> </ul>	BPS	UI and Template
Aruba 3810 Switch Series	<ul style="list-style-type: none"> <li>KB.16.08.0019 or later</li> <li>KB.16.09.0015 or later</li> <li>KB.16.10.0012 or later</li> <li>KB.16.11.002</li> </ul>	<ul style="list-style-type: none"> <li>KB.16.08.0023 or later</li> <li>KB.16.09.0018 or later</li> <li>KB.16.10.0016 or later</li> <li>KB.16.11.0002</li> </ul>	Yes <b>Switch Software Dependency:</b> <ul style="list-style-type: none"> <li>KB.16.08.0019 or later</li> <li>KB.16.09.0015 or later</li> <li>KB.16.10.0012 or later</li> <li>KB.16.11.0002</li> </ul>	BPS	UI and Template
Aruba 5400R Switch Series	<ul style="list-style-type: none"> <li>KB.16.08.0019 or later</li> <li>KB.16.09.0015 or later</li> <li>KB.16.10.0012 or later</li> <li>KB.16.11.002</li> </ul>	<ul style="list-style-type: none"> <li>KB.16.08.0023 or later</li> <li>KB.16.09.0018 or later</li> <li>KB.16.10.0016 or later</li> <li>KB.16.11.0002</li> </ul>	Yes <b>Switch Software Dependency:</b> <ul style="list-style-type: none"> <li>KB.16.08.0019 or later</li> <li>KB.16.09.0015 or later</li> <li>KB.16.10.0012 or later</li> <li>KB.16.11.0002</li> </ul>	VSF	Template only



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

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

## Accessing Aruba Central

You can access Aruba Central from the HPE GreenLake portal. For more information about accessing and navigating the HPE GreenLake portal, see the [HPE GreenLake User Guide](#).

1. To access the **Aruba Central** app from the HPE GreenLake home page, use one of the following options:
  - On the Aruba Central tile, click **App Catalog**.
  - Under the **Settings** ( ≡ ) menu, click **Applications**.
  - Under **Activities & Tasks** group, click **Explore Catalog** on the **App Catalog** tile.


The **Applications > My Apps** page is displayed.

2. In the **Choose Region** drop-down list, select **All Regions** or the region in which you want to access the **Aruba Central** app.
3. On the Aruba Central tile, click **Launch**.

The following animation shows you how to access Aruba Central from the HPE GreenLake portal.

## Logging Out of Aruba Central

To log out of Aruba Central, complete the following steps:

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

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

- [MSP Owns Devices and Subscriptions \(Deployment Model 1\)](#)
- [End-Customer Owns Both Devices and Subscriptions But MSP Manages \(Deployment Model 2\)](#)
- [Hybrid MSP Deployment Model \(Deployment Model 3\)](#)

## MSP Owns Devices and Subscriptions (Deployment Model 1)

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

### Setup and Provisioning

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

- Set up the Aruba Central account.
- Onboard devices.
- Assign device to tenant and apply subscriptions.

MSPs can provide Network as a Service to end-customers using Aruba Central MSP mode capabilities. Aruba Central provides simplified provisioning. The MSP administrator must map the device to the tenant account for device management and monitoring operations.

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

For more information, see [About Provisioning Tenant Accounts](#).

### Customizing the Portal

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

For more information, see [Customizing the Portal in MSP Mode](#).

### Monitoring and Reporting

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

MSPs can do the following from the MSP Dashboard:

- View total number of tenant accounts and consolidated device inventory and subscription status.
- View graphs representing the devices under management, tenant accounts added, and subscription renewal schedule
- Navigate to each tenant account.

For more information, see [MSP Dashboard](#).

## Managing Firmware and Maintenance

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

For more information, see [Firmware Upgrades for MSP Mode](#).

## Example Deployment Scenario

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

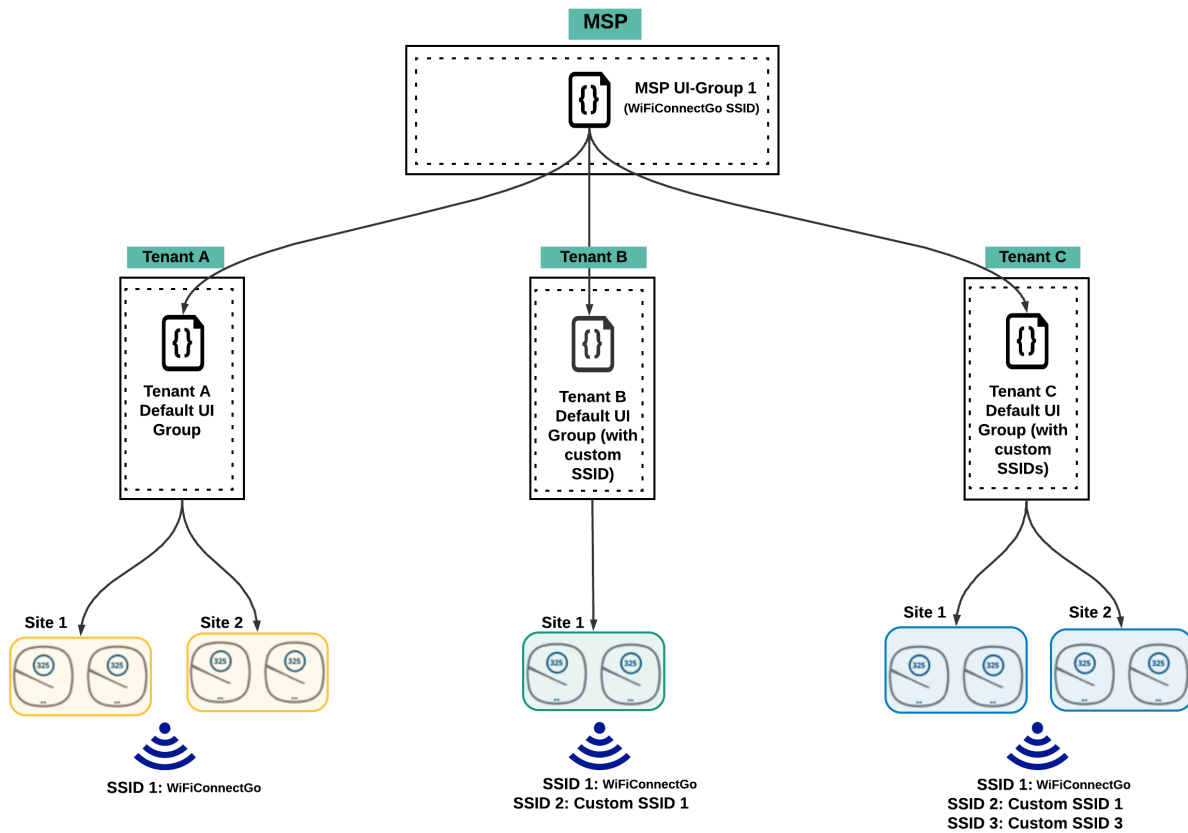
- **WiFiConnectGo**—In this program, for a monthly fee per Instant AP, customers part of this program agree to broadcast MSP's free public WiFi SSID **WiFiConnectGo**. Customers can add up to 15 additional custom SSIDs, including guest, of their own. Tenant account administrators are responsible for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

## Configuring WiFiConnectGo Using Default UI Groups

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

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

**Figure 3** MSP Deployment Using Default UI Groups

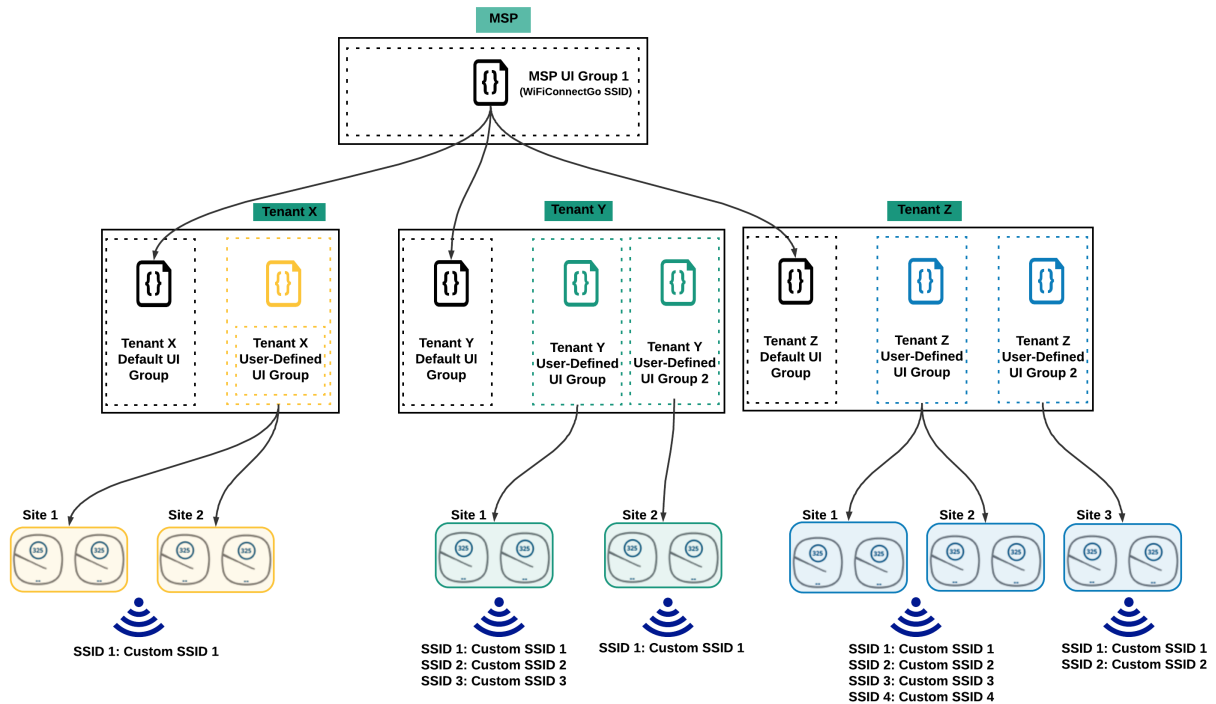


## Configuring WiFiConnectGo-Plus Using User-Defined UI Groups

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

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

**Figure 4** MSP Deployment Using User-Defined UI Groups

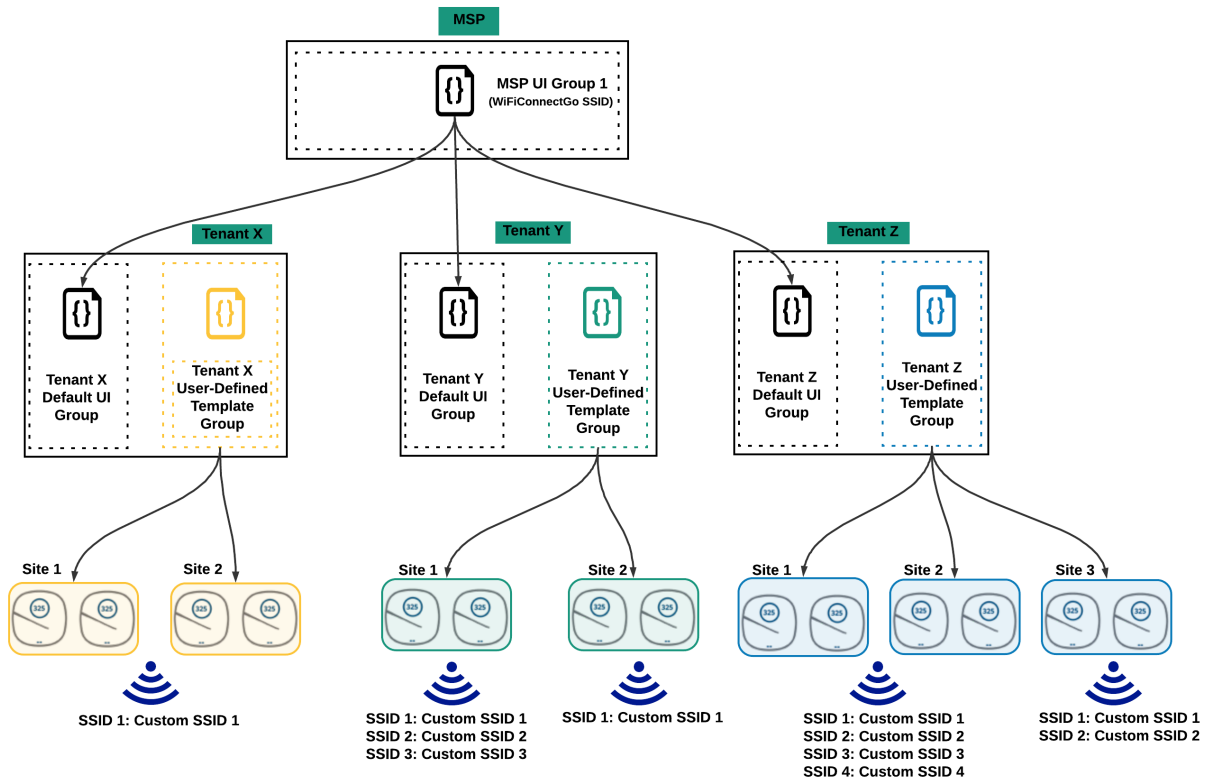


## Configuring WiFiConnectGo-Plus Using Template Groups

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

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

**Figure 5** MSP Deployment Using Template Groups



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



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

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

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

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

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

## Setup and Provisioning

The end-customer purchases the devices and subscriptions. The end-customer contacts the MSP to manage the network. As the devices and subscriptions are owned by the end-customer, the MSP uses

the Aruba Central Standard Enterprise mode to set up and provision the tenant account.

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

## Monitoring and Reporting

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

## Managing Firmware and Maintenance

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

## Example Deployment Scenario

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

### Site 1

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

### Site 2

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

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

## Deployment Using User-Defined UI Groups

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

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

1. Create a new UI group for each site.
2. Configure the UI group with Wi-Fi settings specific to each site.
3. Map the Instant APs in each site to the respective UI group.

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

1. Create one tenant template group.
2. Configure the newly created template group by uploading a base configuration with the **WiFi\_CE** setting and a variable for the SSID VLAN.
3. Upload a variable file with unique entries for each Instant AP. For the Instant APs part of **Site 1**, the VLAN variable value is 20. For the Instant APs part of **Site 2**, the VLAN variable value is 40.
4. Map **Site 1** and **Site 2** Instant APs to the common template group.

### Points to Note:

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

## Hybrid MSP Deployment Model (Deployment Model 3)

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

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



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

## Network Structure

The **Network Structure** page shows tiles view for groups, install manager, and certificates sections. You can click on a tile to navigate to the respective page in Aruba Central.

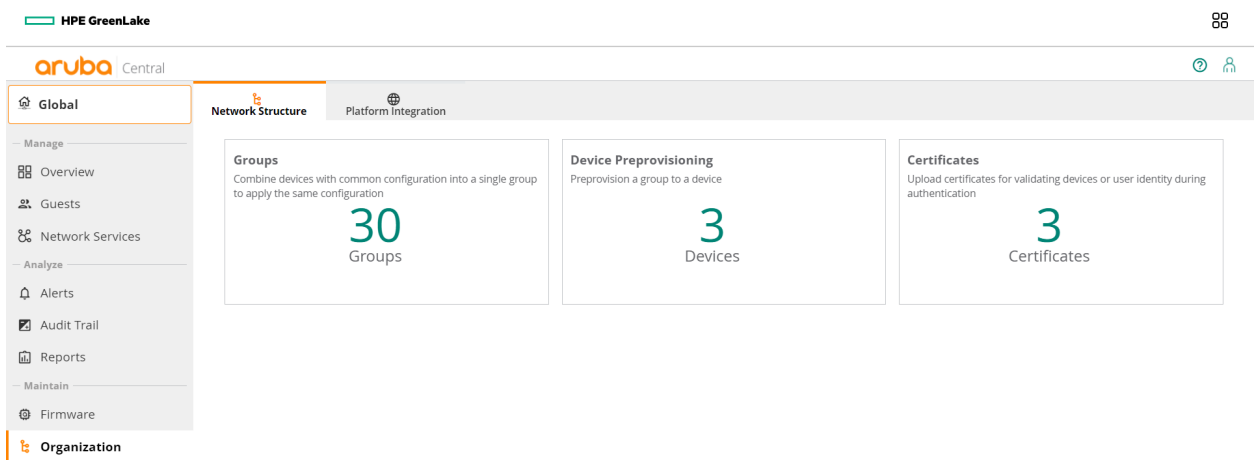
### Viewing the Network Structure Page

To view the **Network Structure** page, complete the following steps:

1. In the **Aruba Central** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
3. Select the **Network Structure** tab.

The **Network Structure** page is displayed.

**Figure 6** *Network Structure Page*



The **Network Structure** page displays tiles view for the following sections:

- **Groups**—Displays the number of groups and number of unprovisioned devices. Click the tile to navigate to the [Groups in the MSP Mode](#) page.
- **Device Preprovisioning**—Displays the number of devices available for preprovisioning for a selected tenant account. Click the tile to navigate to the [Device Preprovisioning in an MSP Account](#) page.
- **Certificates**—Displays the number of certificates available to upload. Click the tile to navigate to the [MSP Certificates](#) page.

## MSP Certificates

You can view and add certificates in MSP.

This section discusses the following topics:

- [Viewing Certificates in MSP Mode](#)
- [Uploading Certificates in the MSP Mode](#)

## Viewing Certificates in MSP Mode

To view certificates in MSP mode, complete the following steps:

1. In the **Aruba Central** app, use the filter to select **All Groups**.  
The global dashboard is displayed for the MSP mode.
2. Under **Maintain**, click **Organization**.  
By default, the **Network Structure** tab is displayed
3. Click the **Certificates** tile.  
The Certificates page is displayed.

The **Certificate Store** displays the following information:

**Table 6:** *Certificate Store Parameters*

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

## Uploading Certificates in the MSP Mode

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

To upload certificates to the certificate store, complete the following steps:

1. In the **Aruba Central** app, use the filter to select **All Groups**.  
The global dashboard is displayed for the MSP mode.
2. Under **Maintain**, click **Organization**.  
By default, the **Network Structure** tab is displayed
3. Click the **Certificates** tile.  
The Certificates page is displayed.
4. To add a new certificate to the **Certificate Store**, click the + sign.  
The **Add Certificate** dialog box is displayed.

5. Enter the certificate name in the **Name** text box.
6. Select the certificate type from the **Type** list.
7. Select the certificate format from the **Format** drop-down.  
The supported certificate formats are PEM, DER, and PKCS12.
8. For server certificates, enter and then retype the passphrase.
9. Click **Choose File** to browse to your local directory and select the certificate to upload.
10. Click **Add**.

---

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

---



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

## Device Preprovisioning in an MSP Account

For an MSP account, the tenant creation and device on-boarding procedures like creating and provisioning tenant accounts, adding devices, and assigning licenses, which were earlier available on the **Account Home** page of Aruba Central are now available on the HPE GreenLake platform.

### Viewing Devices List

The devices provisioned in an MSP account are listed in the **Organization > Network Structure > Device Preprovisioning** pane.

To view the Device Preprovisioning page, complete the following steps:

1. In the **Aruba Central** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.  
By default, the **Network Structure** tab is displayed.
3. Click the **Device Preprovisioning** tile.  
The **Device List** table is displayed.
4. In the **Select Customer** drop-down, select a tenant account to see the Device List table with the list of devices available for the tenant.




---

The Device List table will not appear unless you select a tenant in the Select Customer drop-down.

---

The **Device List** table lists the total number of devices; and the number of access points, switches, and gateways in the inventory for the selected customer account.




---

In the Serial Number column, you must enter the serial number in full for filtering the device data. Entering a partial serial number does not show any search results in the table.

---

**Figure 7** MSP Device Preprovisioning

The screenshot shows the Aruba Central web interface for device preprovisioning. The left sidebar contains navigation links: Global, Manage, Overview, Guests, Network Services, Alerts, Audit Trail, Reports, Maintain, and Firmware. The main content area is titled 'Device Preprovisioning' and includes a sub-header 'Preprovision a group to a device' with a 'Select Customer' dropdown set to '22Dec2021'. Below this is a 'Device List' table with 5 items. The table has columns: Serial Nu..., MAC Address, Device Type, Part Number, IP Address, Name, and Group. The data rows are as follows:

Serial Nu...	MAC Address	Device Type	Part Number	IP Address	Name	Group
C10026906	18:5A:72:C3:22:2F	AP	IAP-225-RW	--	--	--
SG66FLK9K7	ED:07:1B:ES:2B:00	SWITCH	J9727A	10.21.20.116	Switch-2920-standalone	unprovisioned
SG83JQLDZW	04:09:73:87:92:40	SWITCH	JL320A	--	--	--
SG87JQLM8T	B8:83:03:E9:02:40	SWITCH	JL320A	--	--	--
SG98KN5042	B8:3A:30:9C:3D:00	SWITCH	JL666A	--	--	--

At the bottom right of the table, there is a status bar that says '1 item(s) selected' and a 'Clear' button.

The following table describes the columns in the **Device List** table.

**Table 7: Device Details**

Parameter	Description
<b>Serial Number</b>	Serial number of the device.
<b>MAC Address</b>	MAC address of the device.
<b>Device Type</b>	Type of device. For example Instant AP, switch, or gateway.
<b>Model</b>	Hardware model of the device.
<b>Part Number</b>	Part number of the device.
<b>IP Address</b>	IP address of the device.
<b>Name</b>	Name of the device.
<b>Group</b>	Group assigned to the device.

## Assigning Devices to Groups

To assign factory default devices to a group, complete the following steps in the **Device Preprovisioning** page:



The following procedure is only for assigning groups to the devices that are not connected. The group management actions like moving devices between groups, or moving devices from unprovisioned group to other groups is done on the **Groups** page.

1. In the **Aruba Central** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.  
By default, the **Network Structure** tab is displayed.

3. Click the **Device Preprovisioning** tile.

The **Device List** table is displayed.

4. In the **Select Customer** drop-down, select a tenant account for which you want to see the device list.
5. Select the device(s) which you want to move to a selected group.



---

If the selected device is already connected to Aruba Central, the **Move** devices option will not be available for the device.

---

6. Click the **Move** devices icon.

The Assign Group page is displayed.

7. Select the **Destination Group** from the drop-down list.



---

You can assign only particular device types for which the group is created. For example, if a group is created for Access Points only, then only Access Points can be assigned to that group. You cannot assign other device types to it.

---

8. Click **Assign**.

The selected device(s) are moved to the destination group. These devices will adopt the destination group configuration.



---

For every device preprovisioning operation, a warning pop-up is displayed to check the audit trail log for the status. If you are assigning the devices in bulk, ensure to check the audit trail to confirm if the all devices are successfully assigned and reason for the rejected devices.

---

## Getting Started with MSP Solution

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

- [Operational Modes and Interfaces](#)
- [About the Managed Service Portal User Interface](#)

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

### [Step 1: Accessing Aruba Central](#)

You can now access Aruba Central from HPE GreenLake.

### [Step 2: Provision tenant accounts](#)

Create tenant accounts and map to MSP group.

### [Step 3: Create Groups](#)

Create MSP groups.

### [Step 4: Customize tenant account view](#)

Customize the tenant account portal.

### [Step 5: Add Certificates](#)

Upload and map certificates.

### [Step 6: Monitor tenant accounts](#)

View top tenants, subscription renewal schedule, devices under management, and total number of new tenants provisioned

## Enabling Managed Service Mode in HPE GreenLake

To enable MSP mode, complete the following steps:

1. Log in to HPE GreenLake portal as an administrator user.
2. Select the account that you want to change from standard enterprise account to an MSP account.
3. Click **Go to Account**.  
The HPE GreenLake console home page for the account is displayed.
4. Click the **Settings** (≡) menu and select **Manage**.  
The **Manage Account** page is displayed.
5. On the account details tile, click **Manage Account Type**.
6. In the **Manage Account Type** page, ensure you complete the following steps:
  - a. **Step 1: Check Eligibility**—Find out if you are eligible for an MSP account.
  - b. **Step 2: Remove Assignments and Licenses from All Devices**—Before starting the conversion process, all assigned devices must be removed from all supported and unsupported applications and the associated licenses. Follow the instructions on screen to complete this process.
  - c. **Step 3: Remove All Unsupported Applications**—Any applications that do not support MSP mode will have to be removed prior to conversion. This will result in the loss of all application data. Follow the instructions on screen to complete this process.
  - d. **Step 4: Convert Your Account**—Once everything is set up, the final step is to convert the account to MSP mode. This will log out all the active users once the conversion is complete.
7. Click **Convert to MSP** mode.  
The **Convert Your Account** pop-up is displayed.
8. Click **Yes, Convert Now**.

Converting your account will immediately log out all the current users and active sessions. Your account will be unavailable until the conversion is complete. You will be informed through email once the conversion is complete.

## 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, complete the following steps:

1. Log in to HPE GreenLake portal as an administrator user.
2. Select the MSP account that you want to change back to standard enterprise account.

3. Click **Go to Account**.

The HPE GreenLake console home page for the account is displayed.

4. Click the **Settings** (≡) menu and select **Manage**.

The **Manage Account** page is displayed.

5. On the account details tile, click **Manage Account Type**.

6. In the **Manage Account Type** page, ensure you complete the following steps:

- a. **Step 1: Remove All Customer Accounts**—Before starting the conversion process, all customer accounts must be removed. Removal of customer accounts will result in a permanent loss of customer data.
- b. **Step 2: Convert Your Account**—Once everything is set up, the final step is to convert to Standard Enterprise mode. This will log out all active users once the conversion is complete.

7. Click **Convert to Standard Enterprise** mode.

The **Convert Your Account** pop-up is displayed.

8. Click **Yes, Convert Now**.

Converting your account will immediately log out all the current users and active sessions. Your account will be unavailable until the conversion is complete. You will be informed through email once the conversion is complete.



## About the Managed Service Portal User Interface

The MSP mode is intended for the managed service providers who manage multiple distinct tenant accounts. The MSP mode allows service providers 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 following topics are discussed:

- [Launching the Aruba Central app for MSP](#)
- [Parts of the Aruba Central app for MSP](#)
- [Help Icon](#)
- [User Icon](#)
- [Filter](#)
- [Time Range Filter](#)
- [The Global Dashboard in MSP Mode](#)
- [The Group Dashboard in MSP Mode](#)

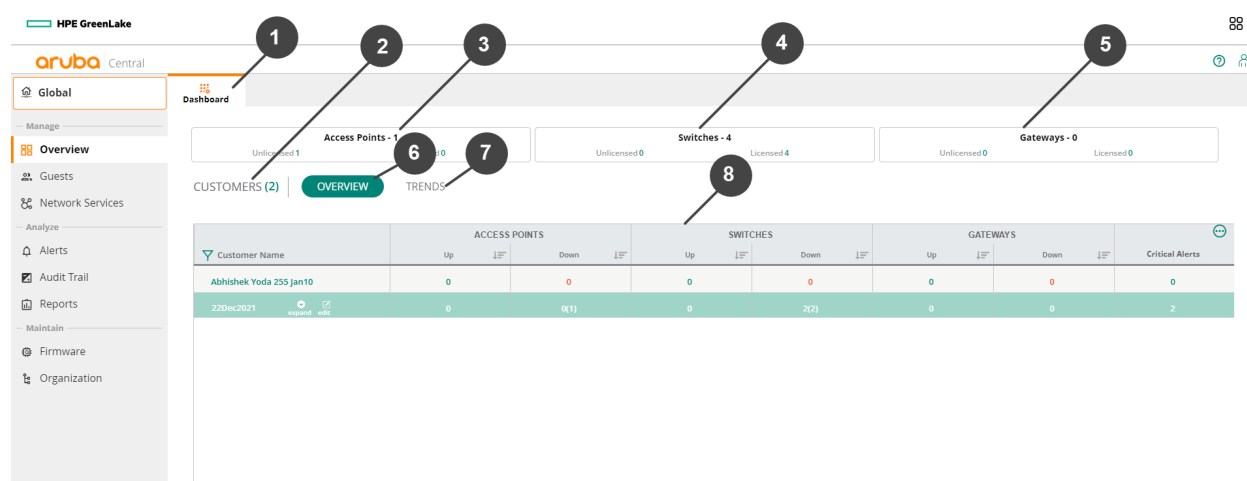
## Launching the Aruba Central app for MSP

You can access Aruba Central from the HPE GreenLake portal. For more information, see [Accessing Aruba Central](#)

## MSP Dashboard View

After you launch the **Aruba Central** app, the MSP dashboard view opens.

**Figure 8** *Parts of the MSP Dashboard*



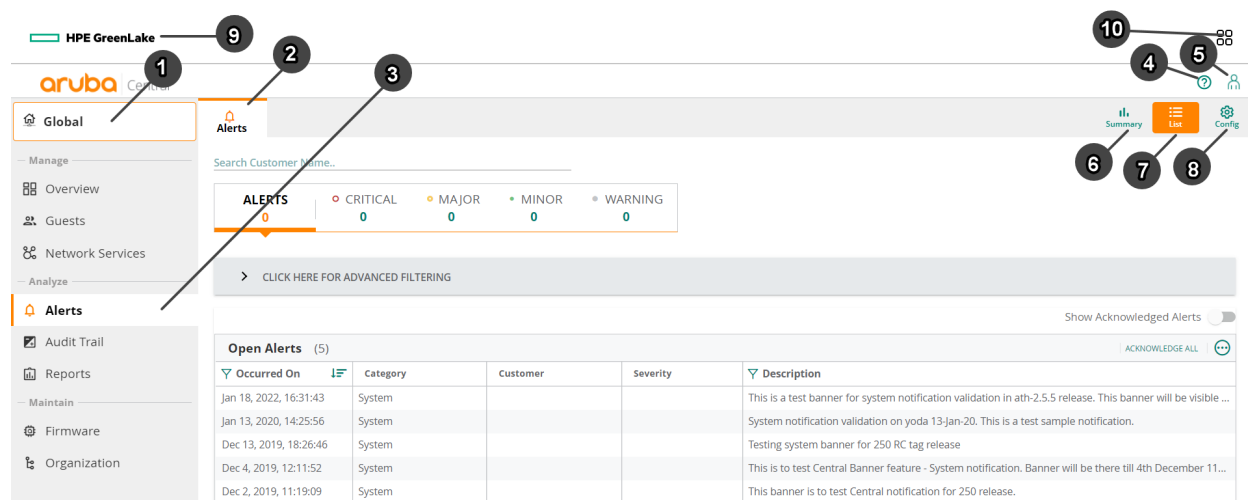
The MSP Dashboard view displays the following information:

Callout Number	Description
1	Access Points—The total number of APs assigned to the tenants. Unlicensed—Number of APs assigned to the tenants but not licensed. Licensed—Number of APs assigned to the tenants and also licensed.
2	Switches—The total number of switches assigned to the tenants. Unlicensed—Number of switches assigned to the tenant but not licensed. Licensed—Number of switches assigned to the tenant and also licensed.
3	Gateways—The total number of gateways assigned to the tenants. Unlicensed—Number of gateways assigned to the tenant but not licensed. Licensed—Number of gateways assigned to the tenant and also licensed.
4	Customers—Number of tenants in the MSP account.
5	Overview—Displays the list of customers, the types of devices assigned to each customer, as well as critical alerts, if any.
6	Trends—Displays charts for license renewal, the number of devices under MSP management, and the number of customers added over the last year.
7	Customer List Table—Provides an overview of tenant accounts for the MSP. You can click the customer name to go to the tenant account view for the customer. Hover over the tenant account name to expand the tenant account and see the tenant account details and edit the account.

## Parts of the Aruba Central app for MSP

After you launch the **Aruba Central** app, the MSP view opens.

**Figure 9** *Parts of the Aruba Central User Interface for MSP*



Callout Number	Description
1	Filter to select a group or all groups. Here, the global dashboard is displayed as the filter is set to <b>All Groups</b> .


Callout Number	Description
2	First-level tab on dashboard. The dashboard may also have second and third-level tabs dependent on the filter selection.
3	Menu item under left navigation contextual menu. Menu is dependent on the filter selection.
4	Help icon. For more information, see <a href="#">Help Icon</a> .
5	User Settings icon. For more information, see <a href="#">User Icon</a> .
6	Summary view. Click the <b>Summary</b> icon to view a graphical representation of the data. Only applicable for the global dashboard.
7	List view. Click the <b>List</b> icon to view a tabular representation of the data. Only applicable for the global dashboard.
8	Config view. Click the <b>Config</b> icon to enable configuration mode.
9	HPE GreenLake icon. Click this icon to go back to the HPE GreenLake portal home page.
10	Services icon. Hover over the icon to see the links to HPE GreenLake, Cloud Services, Cloud Consoles and HPE Resources.

## Help Icon

The help icon  contains the following options:

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

## User Icon

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


## ■ User Settings

- **Time Zone**— Displays the zone, date, time, and time zone of the region.
- **Language**— Administrators can set a language preference. The Aruba Central web interface is available in English, French, Spanish, German, Brazilian Portuguese, Chinese, and Japanese languages.
- **Idle Timeout**— Displays the timeout value for inactive user sessions. The value is in minutes.

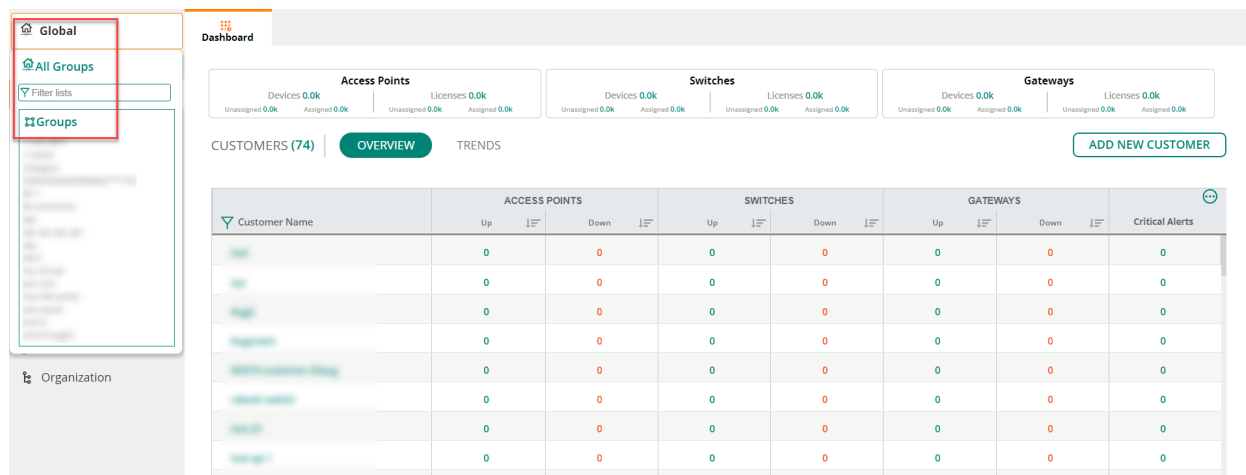
## ■ Terms of Service— Displays the terms and conditions for using Aruba Central services.

## ■ Logout— Enables you to log out of from your account.


## Filter

The filter  enables you to select a group or **All Groups** for performing specific configuration and monitoring tasks. If no filter is applied, by default the filter is set to **All Groups**. When you set the filter to **All Groups**, the global dashboard is displayed and when you set the filter to a group, the group dashboard is displayed. You can type a group name to start your search for a filter value.

**Figure 10** MSP Filter set to Global on Selecting All Groups



## Time Range Filter

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




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

## The Global Dashboard in MSP Mode

In the **Aruba Central** app in MSP mode, use the filter to select **All Groups**. The global dashboard is displayed.

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

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

- **Summary** — Click the  icon to view a graphical representation of the data. Only applicable for the global dashboard.
- **List** — Click the  icon to view a tabular representation of the data. Only applicable for the global dashboard.
- **Config** — Click the  icon to enable configuration mode.

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



Some tabs may not be seen in your dashboard view if you are not an administrator for the Aruba Central account.

**Table 8: Contents of the Global Dashboard in MSP Mode**

Left Navigation Menu	First-Level Tabs	Description
<b>Manage &gt; Overview</b>	<b>Dashboard</b>	Provides a summary of hardware and subscriptions owned by the MSP and the tenant accounts managed by the MSP. MSP administrators can perform tasks such as drilling down to a tenant account, editing an existing tenant account, and deleting a tenant account. For more information, see <a href="#">MSP Dashboard</a> .
<b>Manage &gt; Guests</b>	<b>Splash Pages</b>	Enables an 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. For more information, see <a href="#">Configuring a Cloud Guest Splash Page Profile</a> .
<b>Manage &gt; Network Services</b>	<b>Virtual Gateways</b>	Enables an MSP administrator to assign a virtual gateway to a tenant account and generate a device identity such it can be managed in a Cloud Provider's console.
<b>Analyze &gt; Alerts</b>	<b>Alerts</b>	Displays and configures a list of alerts. This page also enables you to acknowledge these alerts. For more information, see <a href="#">MSP Alerts</a> .
<b>Analyze &gt; Audit Trail</b>	<b>Audit Trail</b>	Shows the total number logs generated for all device management, configuration, and user management events triggered in Aruba Central. For more information, see <a href="#">MSP Audit Trails</a> .
<b>Analyze &gt; Reports</b>	<b>Reports</b>	Enables you to create various types of reports. You can create recurrent reports or configure the reports to run on demand. For more information, see <a href="#">MSP Reports</a> .
<b>Maintain &gt; Firmware</b>	<b>Access Points Switch- MAS Switches Gateways</b>	Provides an overview of the latest supported version of firmware for the device, details of the device, and the option to upgrade the device. For more information, see <a href="#">Firmware Upgrades for MSP Mode</a> .

Left Navigation Menu	First-Level Tabs	Description
<b>Maintain</b> > <b>Organization</b>	<b>Network Structure</b>	<p>Shows tiles view for groups, install manager, and certificates sections. You can click on a tile to navigate to the respective page in Aruba Central. For more information, see <a href="#">Network Structure</a>.</p> <p><b>Groups</b>— A group in Aruba Central is the primary configuration element that functions as a container for device management, monitoring, and maintenance. Groups enable administrators to manage devices efficiently by using either a UI-based configuration workflow or CLI-based configuration template. For more information, see <a href="#">Groups</a>.</p> <p><b>Install Manager</b>—Simplifies and automates site deployments, and helps IT administrators manage site installations with ease.</p> <p><b>Certificates</b>— Enables administrators to upload a valid certificate signed by a root CA so that devices are validated and authorized to use Aruba Central. For more information, see <a href="#">MSP Certificates</a>.</p> <p><b>Device Preprovisioning</b>— Enables administrators to assign factory default devices to a group. For more information, see <a href="#">Device Preprovisioning in an MSP Account</a>.</p>
	<b>Platform Integration</b>	<p>Shows tiles view for Data collectors, API Gateway, and Webhooks. You can click on a tile to navigate to the respective page in Aruba Central.</p> <p><b>Data collectors</b>— Host applications that process network data. Data collectors are available as a physical appliance or a virtual appliance.</p> <p><b>API Gateway</b>—Supports the REST API for all Aruba Central services. This feature allows Aruba Central users to write custom applications, embed, or integrate the APIs with their own applications.</p> <p><b>Webhooks</b>—Webhooks allow you to implement event reactions by providing real-time information or notifications to other applications.</p>

## The Group Dashboard in MSP Mode

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

**Figure 11** Launching the Group Dashboard for MSP

The screenshot shows the Aruba Central interface in MSP mode. The left navigation menu has 'Device' selected. The top navigation bar shows 'Access Points', 'Switches', and 'Gateway' tabs. The main content area displays a table of Wireless SSIDs. The table has columns for NAME, SECURITY, ACCESS TYPE, ZONE, and NETWORK ENABLED. Two SSIDs are listed, both with 'Unrestricted' access and 'Yes' for network enabled. A '+ Add SSID' button is at the bottom left, and '2 SSID(s)' is at the bottom right.

NAME	SECURITY	ACCESS TYPE	ZONE	NETWORK ENABLED
SSID1	WPA2-PSK	Unrestricted		Yes
SSID2	WPA2-PSK	Unrestricted		Yes



Some tabs or options may not be seen in your dashboard view if you are not an administrator for the Aruba Central account.

**Table 9: Contents of the Group Dashboard in MSP Mode**

Left Navigation Menu	First-Level Tabs	Description
<b>Manage &gt; Device</b>	<b>Access Points Switches Gateways</b>	Enables you to configure APs and AOS-S switches for a specific group. For more information, see the Aruba Central documentation for APs, switches and gateways.  <b>NOTE:</b> In the MSP mode, configuration for AOS-CX switches is not supported. To configure AOS-CX switches, you must navigate to a specific tenant account. For more information, see <a href="#">Navigating to the Tenant Account</a> .
<b>Manage &gt; Guests</b>	<b>Splash Pages</b>	Enables an 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. For more information, see <a href="#">Configuring a Cloud Guest Splash Page Profile</a> .

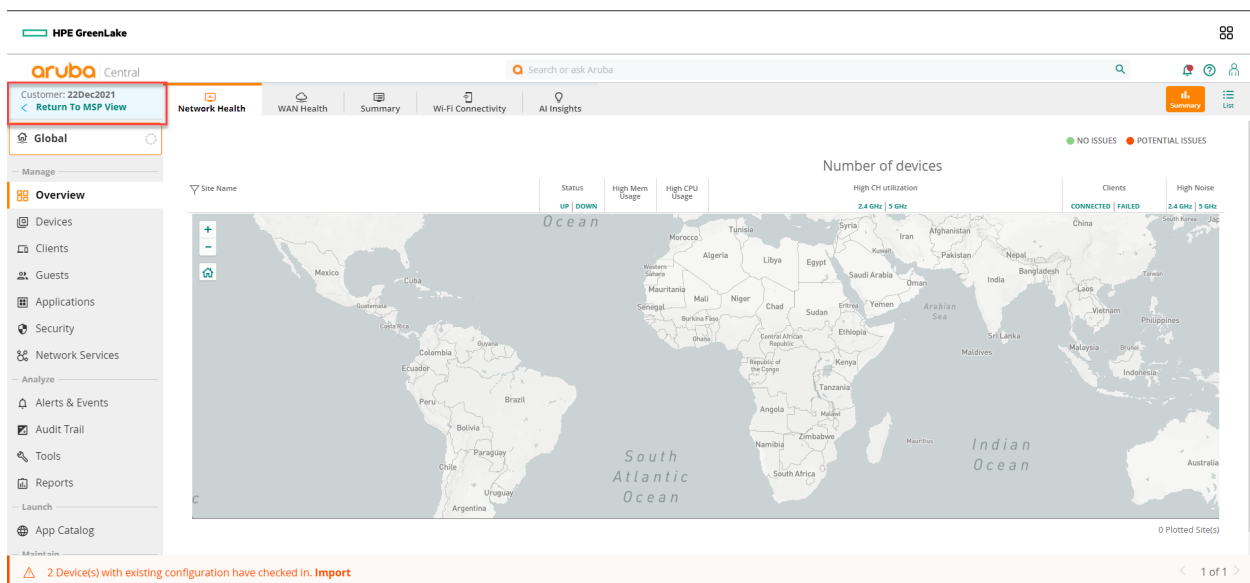
In the group dashboard under the left navigation pane, you can see the **Device** and **Guest** options under **Manage**.

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

## The Tenant View

In the MSP dashboard page, click a tenant name in the Customers table to see the tenant account details. The tenant view UI looks same as an standard enterprise account view. Click **Return to MSP View** to go back to the MSP Dashboard.

**Figure 12** *Tenant View for MSP*



## MSP Device Management in HPE GreenLake

You can view, manage, onboard, and assign subscriptions to the all the devices in your account using the **Devices** option in HPE GreenLake platform.

For more information, see the section in the HPE GreenLake Edge to Cloud Platform User Guide, using the following link:

<https://www.arubanetworks.com/techdocs/central/latest/content/nms/intro-pages/related-info.htm>

## MSP Tenant Management in HPE GreenLake

The HPE GreenLake portal allows you to create and manage tenant accounts from the customer accounts page.

### Creating a Tenant or Customer Account and Assigning to Aruba Central

The MSP administrator user can create a tenant account in the HPE GreenLake portal and assign the account to a Aruba Central instance.

#### Creating a Tenant Account

To add a new customer, complete the following steps:

1. Log in to HPE GreenLake portal as an MSP administrator user.  
The HPE GreenLake console home page for the account is displayed.
2. Click the **Settings** ( ≡ ) menu and select **Customer Account**.  
The Customer Accounts page is displayed. This page allows you to view and manage customer accounts.
3. Click **Add Customer**.  
The **Set Up Customer Account** pop-up is displayed.
4. Enter the following account information:
  - Company Name
  - Description
  - Country
  - Company Address
  - ZIP / Postal Code
5. Click **Create Account**.

#### Assigning the Tenant Account to a Aruba Central Instance

After creating a tenant account in HPE GreenLake, you need to assign it to an Aruba Central instance.

To assign the tenant account to an Aruba Central instance, complete the following steps:

1. Log in to HPE GreenLake portal as an MSP administrator user.  
The HPE GreenLake console home page for the account is displayed.
2. Click the **Settings** ( ≡ ) menu and select **Customer Account**.  
The Customer Accounts page is displayed. This page allows you to view and manage customer accounts.



3. Navigate to the newly created account and click **Launch**.  
The tenant account dashboard page is displayed.
4. Click the **Settings** (≡) menu and select **Applications**.  
The Applications page is displayed.
5. Click **Available Applications**.  
The Available Applications page is displayed. This page displays applications available for the tenant.
6. Select the Aruba Central account and click **Add**.  
The Add Application pop-up is displayed.
7. Select the check box for terms of service and click **Add**.  
The tenant account is assigned to an Aruba Central instance.

## Editing a Tenant or Customer Account

The MSP administrator user can edit a tenant account in the HPE GreenLake portal.

To edit a tenant account, complete the following steps:

1. Log in to HPE GreenLake portal as an MSP administrator user.  
The HPE GreenLake console home page for the account is displayed.
2. Click the **Settings** (≡) menu and select **Customer Account**.  
The Customer Accounts page is displayed. This page allows you to view and manage customer accounts.
3. Select the tenant account and click the ... icon and then click **Edit**.  
The **Account Details** page is displayed. This page allows you to edit the account details like Company Name, Description, Country, Company Address, Email and Phone Number.
4. Edit the account details.
5. Click **Save Changes**.

## Deleting a Tenant or Customer Account

The MSP administrator user can delete a tenant account in the HPE GreenLake portal.



---

Before deleting a tenant account, you must remove all the applications associated to the tenant account.

---

To remove all the applications associated to a tenant account, complete the following steps:

1. Log in to HPE GreenLake portal as an MSP administrator user.  
The HPE GreenLake console home page for the account is displayed.
2. Click the **Settings** (≡) menu and select **Customer Account**.  
The Customer Accounts page is displayed. This page allows you to view and manage customer accounts.
3. Select the tenant account and click **Launch**.  
The tenant account dashboard is deleted.
4. Click the **Settings** (≡) menu and select **Applications**.  
The Applications page is displayed.
5. In the My Applications page, select the application to remove and click **View Details**.

6. Click the ... icon and the select **Remove All Applications**.

A confirm removal pop-up is is displayed.

7. Click **Remove All Applications** to confirm.



---

Removing an application will result in the unassignment of all devices and can result in operational outages and loss of user access.

---

To delete a tenant account, complete the following steps:

1. Log in to HPE GreenLake portal as an MSP administrator user.  
The HPE GreenLake console home page for the account is displayed.
2. Click the **Settings** (≡) menu and select **Customer Account**.  
The Customer Accounts page is displayed. This page allows you to view and manage customer accounts.
3. Select the tenant account and click the ... icon and then click **Delete**.  
A confirmation window is displayed.
4. Type '**DELETE**' and then click **Delete Customer**.

## Customizing the Portal in MSP Mode

The **Portal Customization** functionality is now available in the HPE GreenLake portal. The **Portal Customization** page 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. For more information, see the [HPE GreenLake documentation](#).

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

1. Log in to HPE GreenLake portal as an administrator user.
2. Select your account and click **Go to Account**.
3. The HPE GreenLake console home page for the account is displayed.
4. Click the **Settings** (≡) menu and select **Manage**.  
The **Manage Account** page is displayed.
5. Click the **Portal Customization** tile.  
The **Portal Customization** page is displayed. This page allows you to customize portal details with your own business information and branding.
6. Click **Edit Portal Details**.
7. The following information can be customized based on your requirement:
  - **Company Information**—You can add the company name, product name, mailing address and so on.
  - **Company Branding**—You can add the company logo for header footer and logo. You can also add a smaller version of your logo in the web browser tab.
  - **Email Communication**—You can add logo for automated emails and forwarding email address. You can also send a sample email.

## About Provisioning Tenant or Customer Accounts

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

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

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

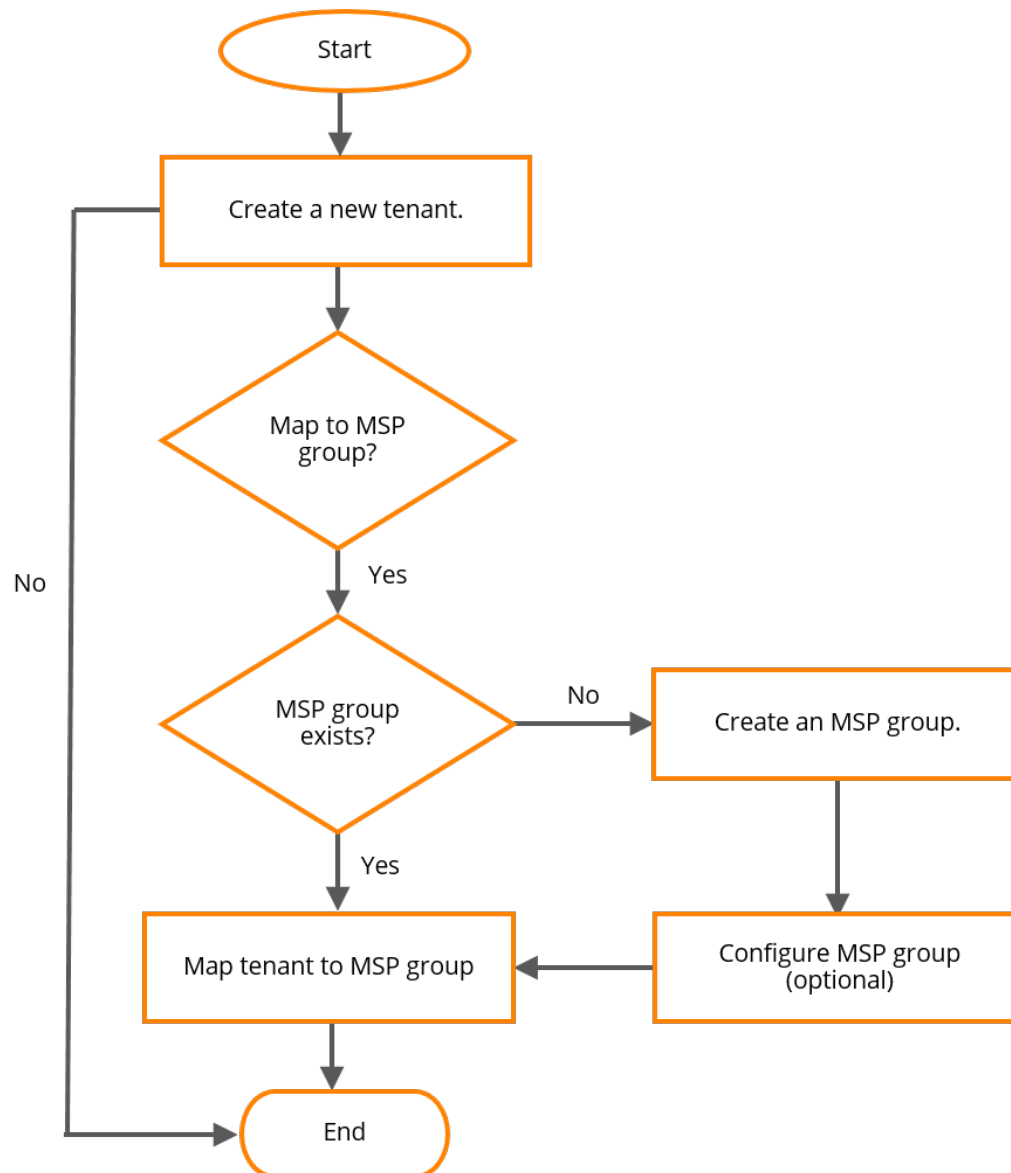
The following topics are discussed in this section:

- [Flowchart for Tenant Account Mapping in MSP](#)
- [Creating a Tenant Account and Mapping to an MSP Group](#)
- [Viewing Tenant Account Details](#)
- [Editing a Tenant Account](#)
- [Deleting a Tenant Account](#)

### Flowchart for Tenant Account Mapping in MSP

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

**Figure 13** *Tenant Account Mapping to an MSP Group*



- **Create a new Tenant**—The MSP administrator creates tenant accounts and provisions the tenant accounts to Aruba Central application in the HPE GreenLake portal. For more information, see the [HPE GreenLake User Guide](#).
- **Map to MSP Group**—The MSP administrator maps the tenant users to an existing group in Aruba Central. For more information, see [Groups in the MSP Mode](#).
- **Create an MSP Group**—The MSP administrator creates MSP groups in Aruba Central(**Organization > Groups > Add Group**).
- **Configure an MSP Group**—The MSP administrator configures the MSP groups in Aruba Central.

## Creating a Tenant Account and Mapping to an MSP Group

The MSP administrator can create a tenant account in the Greenlake portal. For more information about creating new tenant account, see the [HPE GreenLake User Guide](#).

Mapping a tenant account to an MSP group is done using the edit tenant account workflow. For more information, see [Editing a Tenant Account](#)

## Viewing Tenant Account Details

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

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

The customer details window displays the following sections. Click the X mark on the top right-corner of the screen to exit the window and return to the dashboard.

### Summary

- **Customer ID**—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.
- **Customer Created**—Displays the count of devices that are managed in the network over a period of time.
- **MSP Group**—Displays the total number of tenants added to Aruba Central over a period of time.
- **Description**—Description of the tenant account.
- **Customer Name**—Name of the tenant account.

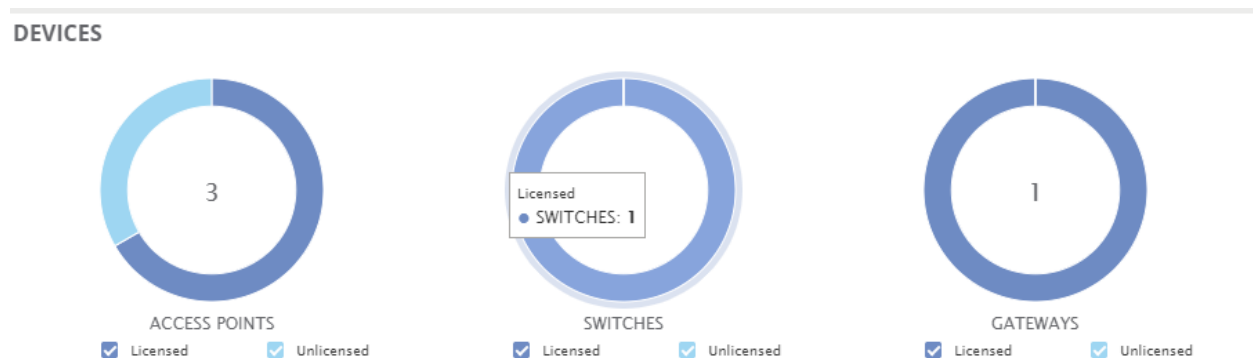
### Devices

This section is a graphical representation of the devices assigned to the selected tenant account, as well as the licensed and unlicensed count for each device type.

- The section consists of three doughnut charts, each chart representing one of the following types of devices, APs, switches, and gateways.
- The number in the center of the chart indicates the total number of devices, both *licensed* and *unlicensed*, of a specific type allocated to the tenant account.
- The two colors on the ring of the doughnut indicates the number of licensed and unlicensed devices of a specific type allocated to the tenant account. You can hover over one segment of the doughnut to see the numbers corresponding to the selected segment.
- You can also deselect and reselect the **Licensed** and **Unlicensed** options for each chart.

For example, in the following image, the tenant account has three APs, one switch, and one gateway. Out of this, only one AP is unlicensed.

**Figure 14** *Devices Section of the Expand Tenant Account Page*



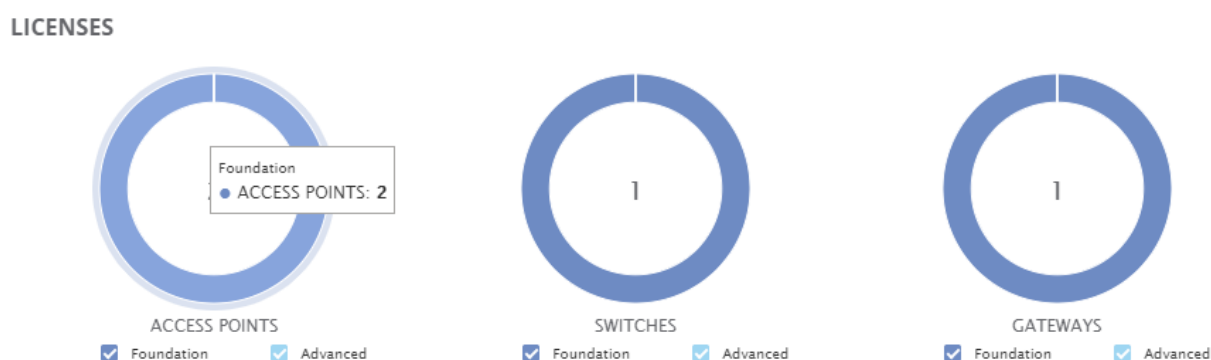
## Licenses

This section is a graphical representation of the device subscriptions assigned to the devices for the selected tenant account. The section also shows the number of Foundation and Advanced licenses for each type of device.

- The section consists of three doughnut charts, each chart representing one of the following types of devices, APs, switches, and gateways.
- The number in the center of the chart indicates the total number of *licensed* devices of a specific type allocated to the tenant account.
- The two colors on the ring of the doughnut indicates the number of Advanced and Foundation licenses assigned to a device of a specific type allocated to the tenant account. You can hover over one segment of the doughnut to see the numbers corresponding to the selected segment.
- You can also deselect and reselect the **Advanced** and **Foundation** options for each chart.

For example, in the following image, the tenant account has two APs, one switch, and one gateway, each assigned with a Foundation license.

**Figure 15** Licenses Section of the Expand Tenant Account Page



## Editing a Tenant Account

When editing the group associated with the MSP customer or tenant, the default group configuration of the tenant account is also impacted.

To edit a tenant account, complete the following steps:

1. From the **Aruba Central** app, filter **All Groups**.
2. Under **Manage**, click **Overview**.  
The **Dashboard** is displayed.
3. Hover over the tenant account that you want to edit and click **edit**.
4. If you want to associate the tenant account to a different group, turn on the **Add to group** toggle switch and select a group.



The customer name and description can be edited only on the HPE GreenLake portal.

5. Click **Save**.

## Deleting a Tenant Account

The MSP administrator can delete a tenant account in the HPE GreenLake portal. For more information, see the [HPE GreenLake User Guide](#).

## Navigating to the Tenant Account

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

To drill down to a specific tenant account:

1. In the **Aruba Central** app, set the filter to **All Groups**.
2. Under **Manage**, click **Overview** to display the **Dashboard**.  
The **Dashboard** page includes the following sections:
  - Dashboard summary bar
  - Overview and trends for customers
3. In the **Customers | Overview** table, click the tenant account name and click **Expand**.  
The tenant account details window is displayed. Close the window.
4. To go to the tenant account, click on the tenant account name.  
The tenant account is displayed in Standard Enterprise Mode.



---

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.

---

### 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 in the HPE GreenLake portal.
- Tenant account administrators can allow or prevent user access to specific groups by configuring custom roles.

## 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, Microbranch, WLAN gateways, VPNC, AOS-CX, Monitoring only, and gateways with ArubaOS 10 architecture groups are not supported in the MSP mode. Creating, editing, and cloning of these groups is not allowed at MSP. However, these groups can be created and managed at each tenant account individually.

---

This section describes the following topics:

- [MSP Group Illustration](#)
- [Tenant Default Group Overrides](#)
- [MSP Group Persona](#)
- [Creating an MSP Group Persona with ArubaOS 8 Architecture](#)
- [Cloning an MSP UI Group](#)
- [Deleting an MSP UI Group](#)

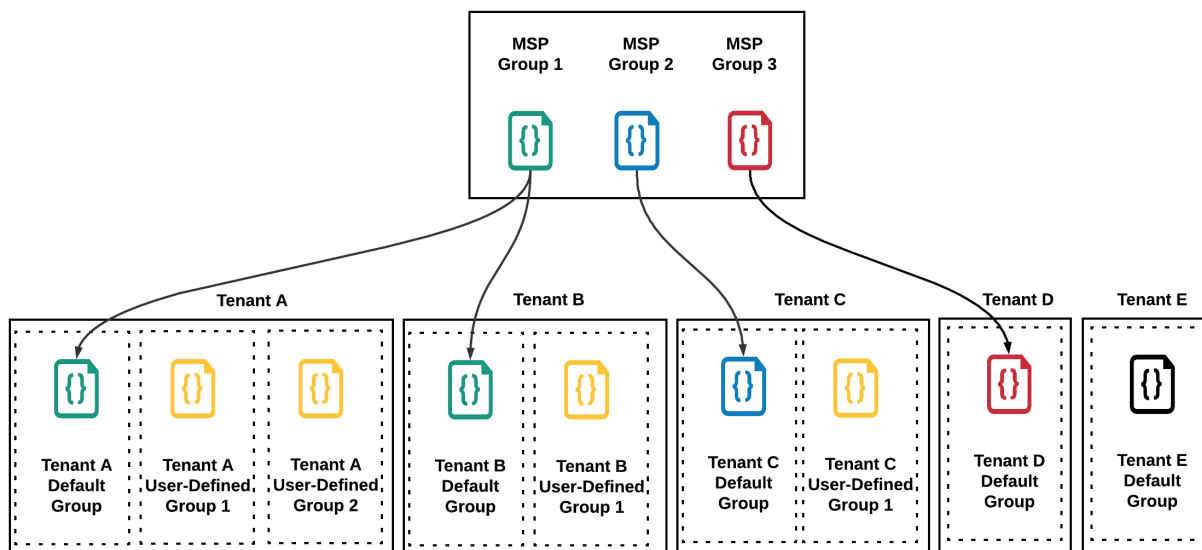
## MSP Group Illustration

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

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

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

**Figure 16** MSP Groups



## Tenant Default Group Overrides

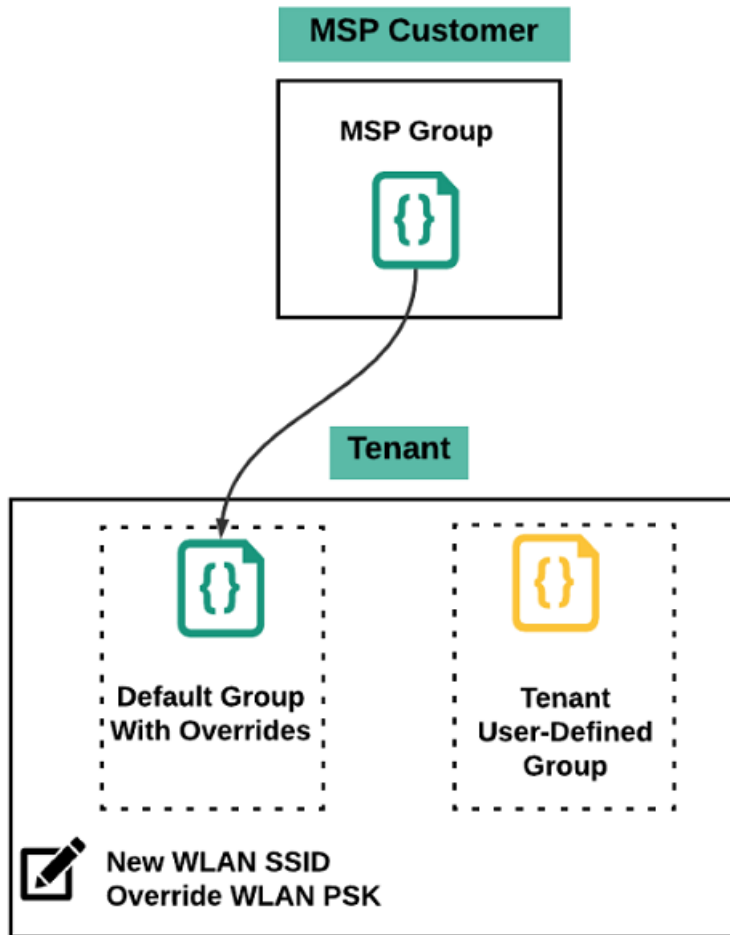
If a tenant is mapped to an MSP group, the configuration of its default group is inherited from the MSP group it is mapped to. Once mapped, except for any newly created WLAN SSID and WLAN PSK, other configurations are overridden.

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

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



**Figure 17** *Default Group Overrides*



## Considerations for Editing a Tenant Default Group

- If a tenant default group does not have any devices assigned to it, then any MSP group can be mapped to that tenant default group.
- If a tenant default group has any devices assigned to it, mapping to a new MSP group is allowed only if the MSP group architecture and persona match with that of the tenant default group. If the MSP group and tenant default group persona do not match then the percolation is not allowed.  
As a workaround, you can move all the devices from the tenant default group to a non-default group and then try mapping the MSP group.
- If a tenant default group has only access points assigned to it and is not shown in monitoring, mapping to a new MSP group is still allowed even if the MSP group and tenant default group persona and architecture do not match.
- If a tenant default group does not support a device type, adding such a type of factory default devices to the tenant default group is not supported. These devices will be moved to the unprovisioned group when they come up in Aruba Central.
- When a standard enterprise account is converted to an MSP account in Aruba Central 2.5.4 release, the MSP default group contains the gateway properties even if the MSP account is not an allowlisted account for gateways.

- When a standard enterprise account is converted to an MSP account in Aruba Central 2.5.4 release, such MSP default group will have an AOS-CX Switch persona along with AOS-S Switch. The AOS-CX persona is not supported in the MSP mode. Hence, mapping of this MSP default group to a tenant is not allowed.

## MSP Group Persona

A persona of a device represents the role that the device plays in a network deployment. Creating persona for devices helps in customizing configuration workflows, automating parts of configurations, showing the default configuration, showing relevant settings for the device. Persona configuration also helps in customizing the monitoring screens and troubleshooting workflows appropriate for the device.



---

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

---

## Creating a Persona

Persona can be created when creating a group. Persona and architecture can be set at the group level. All devices within a group inherit the same persona from the group settings.

While creating a group, the architecture and persona settings of the current group can be marked as preferred settings for adding subsequent groups. For subsequent groups, you can either automatically apply the preferred settings or manually select settings for the new group.

### Persona for Access Points

Access Points can have the following persona:

- **Campus/Branch**—In this persona, AP provides WLAN functionality. This persona applies to ArubaOS 8 (including IAP-VPN) architecture.

### Persona for Gateways

Gateways can have the following persona:

- **Branch**—In this persona, gateways provide ArubaOS 8 SD-Branch (LAN + WAN) functionality. This persona applies to ArubaOS 8 architecture.

### Architecture

The following architecture is supported for creating groups:

- **ArubaOS 8**—Instant AP-based deployment, including Aruba InstantOS 6.x or Aruba InstantOS 8.x (IAP, IAP-VPN), or Aruba InstantOS 8.x SD-Branch deployments.

For information on creating groups with a persona and architecture, see the following topic:

- [Creating an MSP Group Persona with ArubaOS 8 Architecture](#)

## Creating an MSP Group Persona with ArubaOS 8 Architecture

To manage device configuration using UI configuration containers in Aruba Central, you can create a UI group and assign devices. During the group creation, you can assign a persona and select an

architecture for the group.



The gateway configuration is supported in this release as selectively available features. Contact your Aruba Account Manager to enable it in your Aruba Central account.

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

## Adding an MSP UI Group

To create an MSP UI group and assign a persona and ArubaOS 8 architecture, complete the following steps:

1. From the **Aruba Central** app, filter **All Groups**.
2. Under **Maintain**, click **Organization**.  
By default, the **Network Structure** tab is displayed.
3. Click the **Groups** tile.  
The Groups page is displayed.
4. Click **(+) Add Group**.  
The Add Group page is displayed.
5. Enter a name for the group.
6. Select device types that will be part of this group. A group can contain following devices:
  - Access points
  - Gateways
  - Switches (Only AOS-S switch type is supported at MSP UI groups)For detailed device combinations, refer to the **Device Combinations** table.
7. Select check box for **Make these the preferred group settings** optionally to save the architecture and persona settings of the current group for subsequent group creations.
8. Click **Add Group**.  
A group with persona configuration is created.

### Device Combinations for MSP Group Persona

The following are the valid combinations for a group persona with Aruba Instant OS architecture.

**Table 10: Device Combinations**


Device Type	Architecture	AP Network Role	GW Network Role	Switches	Monitoring Only
AP	ArubaOS 8	Campus/Branch	N/A	N/A	N/A
Gateway	ArubaOS 8	N/A	Branch	N/A	N/A
Switch	No architecture	N/A	N/A	AOS-S only	N/A
<ul style="list-style-type: none"><li>▪ AP</li><li>▪ Gateway</li></ul>	ArubaOS 8	Campus/Branch	Branch	N/A	N/A

Device Type	Architecture	AP Network Role	GW Network Role	Switches	Monitoring Only
<ul style="list-style-type: none"> <li>AP</li> <li>Switch</li> </ul>	ArubaOS 8	Campus/Branch	N/A	AOS-S only	N/A
<ul style="list-style-type: none"> <li>AP</li> <li>Gateway</li> <li>Switch</li> </ul>	ArubaOS 8	Campus/Branch	Branch	AOS-S only	N/A

## Editing an MSP UI Group

You can edit an MSP UI group to add a new device type to the group. The group architecture and persona cannot be changed through group edit. You can mark the settings of an edited group as preferred settings for subsequent group creations.

To edit an MSP UI group, complete the following steps:

1. From the **Aruba Central** app, filter **All Groups**.
2. Under **Maintain**, click **Organization**.  
By default, the **Network Structure** tab is displayed.
3. Click the **Groups** tile.  
The Groups page is displayed.
4. To edit an existing group, hover over the the group in the groups table and click the  **Edit Group** icon.  
The Edit Group page is displayed.
5. Add a new device type.
6. Select check box for **Make these the preferred group settings** optionally to save the architecture and persona settings of the current group for subsequent group creations.
7. Click **Save**.  
The group edit changes are saved.

The group edit is not allowed in the following scenarios:


- If an MSP group is mapped to any tenant, the MSP group edit is not allowed.
- If the tenant default group is mapped to any MSP group, the tenant default group edit is not allowed.

## Cloning an MSP UI Group

Cloning a group will clone the same architecture and persona as is from the source group.

To clone an MSP UI group, complete the following steps:

1. From the **Aruba Central** app, filter **All Groups**.
2. Under **Maintain**, click **Organization**.  
By default, the **Network Structure** tab is displayed.
3. Click the **Groups** tile.  
The Groups page is displayed.

4. To create a clone of an existing group, hover over the group in the groups table and click the  **Clone Group** icon.

The Clone Group page is displayed.

5. Enter a name for the group.
6. Click **Clone**.

The group is cloned.

## Deleting an MSP UI Group

If you no longer required a group, you can delete it. The delete option is available only if the group is not mapped to a tenant account.




---

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

---

To delete a group, complete the following steps:

1. In the **Aruba Central** app, filter **All Groups**.
2. Under **Maintain**, click **Organization**.  
By default, the **Network Structure** tab is displayed.
3. Click the **Groups** tile.  
The Groups page is displayed.
4. From the list of groups, hover over the group in the groups table and click the  **Delete Group** icon.  
The Delete Group confirmation window is displayed.
5. Click **Yes** to confirm.  
The group is deleted.

The MSP UI groups now support Gateway management in addition to wired and wireless device management. Currently, for MSP UI groups, an MSP administrator can set the group persona to **Branch Gateway**. When this MSP group is mapped to a customer default group, the configurations from the MSP group is percolated to the customer group. Ensure that the MSP account is allow-listed to support Branch Gateway Persona Group and Device type.

The inherited configuration defined at the customer default group can be overridden at the device level.

### Assigning a Gateway Persona to an MSP Group

All the MSP groups are automatically assigned the **Branch Gateway** persona when the admin accesses the gateway configuration tab for that group.

### Mapping Scenarios for MSP Groups

The following table describes the result of mapping different types of MSP groups to a customer default group.

**Table 11:** *Scenarios for Mapping an MSP Group to a Customer Group for SD -WAN Support*

MSP Group Persona	Initial Customer Group Persona	Mapping Notes
Set to Branch Gateway persona.	No persona defined.	Mapping is successful.
Set to VPNC persona.  You cannot define a VPNC persona at the MSP level for a group. However, if a group had the VPNC persona already defined at the Enterprise mode and the account is later converted to MSP mode, the VPNC persona is preserved.	No persona defined.	Mapping is not allowed.  In the MSP mode, when you display the group dashboard for the VPNC persona, and then click <b>Gateway</b> , the following message is displayed: The group's persona is set to vpnc so any configurations made will not be percolated to the customer.
No persona defined.	No persona defined.	Mapping is successful.
Set to Branch Gateway persona.	Set to Branch Gateway persona.	Mapping is successful.
Set to Branch Gateway persona.	Set to VPNC persona.	Mapping is not allowed.  The mapping fails with the following error message:

MSP Group Persona	Initial Customer Group Persona	Mapping Notes
		Mapping of MSP to Customer default group (with VPNC persona) is not supported.

## Important Notes for SD-WAN Support in MSP Mode

- Setting the persona type to VPNC persona for an MSP group is not supported during this release.
- A single MSP group can be mapped to a customer default group, also known as a one-to-one mapping.
- Other non-default groups defined at the customer level do not inherit the MSP group configuration.
- The configuration defined at the customer default group can be overridden at the device level.
- Configurations related to SD-WAN services, such as DC preference or SD-WAN global configurations are supported at the customer level for now.
- To see the override configuration at the tenant default group level, run the following:  
`<fqdn>/caas/v1/showcommand/object/committed?node_name=default`
- Use the audit trails at the MSP level to debug issues related to configuration percolation. If there is no percolation issue at the MSP level, then the device level configuration sync issue has to be debugged at the customer level.
- If the Gateway persona is not set at the MSP level, the group is called a no-personna group. Currently, MSP supports only the Branch Gateway persona, so if the group is defined with a Branch Gateway persona, it is called a Branch Gateway persona group.
- If an MSP administrator upgrades to the current Aruba Central version and the original configuration contains an MSP gateway group without a persona.

## Priority of Configuration Percolation in MSP Mode

For IAPs and switches configured in Aruba Central MSP mode, the following is the order of priority for configuration changes: Device Level > MSP level or Tenant (customer) group level whichever is updated later. This priority order indicates that a property for an IAP or switch that is modified at the tenant level cannot be retained when changes are made at the MSP level. Similarly, the device level override is retained when the configuration is changed at the MSP level or tenant (customer) group level.

For Gateways configured in Aruba Central MSP mode, the following is the order of priority for configuration changes: Device level > Tenant (customer) group level > MSP level. This priority order indicates that a property that is modified at the device level is retained while making any changes at the tenant (customer) level and MSP Level. Similarly any property that is modified at the tenant (customer) group level is retained while making changes at the MSP group level.

## Checking the Gateway Persona of a Customer Group

The persona for the customer group is assigned as **Branch Gateway** after the MSP group with **Branch Gateway** persona is mapped to the customer group. If the administrator clicks the **Gateway** tab in the customer group before the configuration percolates from the MSP group. The VPNC option is disabled.

To check the persona set for a customer group containing at least one Gateway device, for the MSP account:

1. In the **Aruba Central** app for the MSP account, set the filter to **All Groups**.
2. Under **Manage**, click **Overview** to display the **Dashboard**.  
The **Dashboard** page includes the following sections:
  - Dashboard summary bar
  - Overview and trends for customers
3. In the **Customers | Overview** table, click the tenant account name and click **Expand**.
4. To go to the tenant account, click on the tenant account name.  
The tenant account is displayed in Standard Enterprise Mode.
5. In the **Aruba Central** app for the customer account, use the filter to select a **Gateway** group.
6. Under **Manage**, click **Devices > Gateways** to see the display: Selected Group Type Branch Gateway

**Figure 18** Group Type Displayed for Gateway Group of Customer Account





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

The hardware includes APs, switches, and gateways.

This section includes the following topics:

- [Viewing the MSP Dashboard](#)
- [Dashboard Summary](#)
- [Customer | Overview](#)
- [Customers | Trends](#)
- [MSP Dashboard](#)

## Viewing the MSP Dashboard

To view the MSP dashboard, perform the following steps:

1. In the **Aruba Central** app, set the filter to **All Groups**.

The filter context changes to **Global**.

2. Under **Manage**, click **Overview** to display the **Dashboard**.

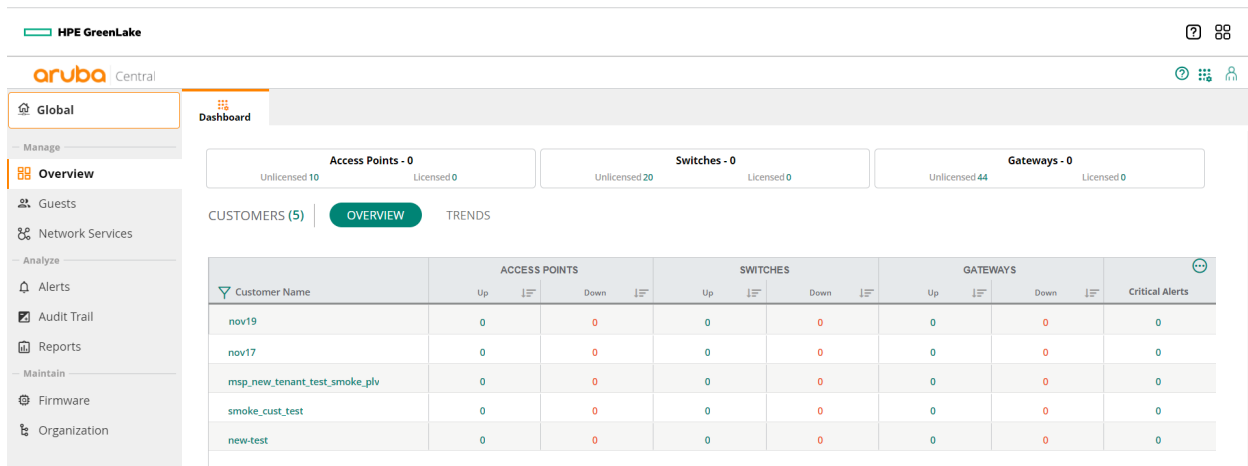
The number in parenthesis () for **Customers** indicates the total number of customers for that MSP account.

In the following image, the total number of customers is 5.

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

- A summary section for the dashboard—Displays the assigned and unassigned devices and the assigned and unassigned licenses for APs, switches, and gateways.
- **Overview**—Displays the list of customers, the types of devices assigned to each customer, as well as critical alerts, if any.
- **Trends**—Displays charts for license renewal, the number of devices under MSP management, and the number of customers added over the last year.

**Figure 19** Viewing the MSP Dashboard



## Dashboard Summary

The summary section for **Dashboard** displays the total number of assigned or allocated devices to tenants and the total number of assigned and unassigned licenses for three categories of hardware devices that include APs, switches, and gateways. In MSP mode, you must first assign a device to a tenant account before assigning a license to the device.

The summary section includes the following details:

- **Access Points** - <total number of APs assigned to the tenant>
  - **Unlicensed**—Number of APs assigned to the tenant but not licensed.
  - **Licensed**—Number of APs assigned to the tenant and also licensed.
- **Switches** - <total number of switches assigned to the tenant>
  - **Unlicensed**—Number of switches assigned to the tenant but not licensed.
  - **Licensed**—Number of switches assigned to the tenant and also licensed.
- **Gateways** - <total number of gateways assigned to the tenant>
  - **Unlicensed**—Number of gateways assigned to the tenant but not licensed.
  - **Licensed**—Number of gateways assigned to the tenant and also licensed.

## Customer | Overview

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

- **Customer Name**

Name of the tenant account. Click the customer name to go to the tenant account view for the customer. Hover over the tenant account name to view the following options:

  - **expand**—Opens a new pop-up window showing the tenant account details. For more information, see [Viewing Tenant Account Details](#).
  - **edit**—Opens the **Edit Customer** pop-up window. For more information, see [Editing a Tenant Account](#).




---

Use the filter icon on the column header to filter by tenant account name.

---

### ■ Customer ID

Unique ID of the tenant account. The ID can be in one of the following formats:

- Numerical format
- UUID format

Use the column filter to search for a particular customer ID. Note that you must enter the full customer ID.

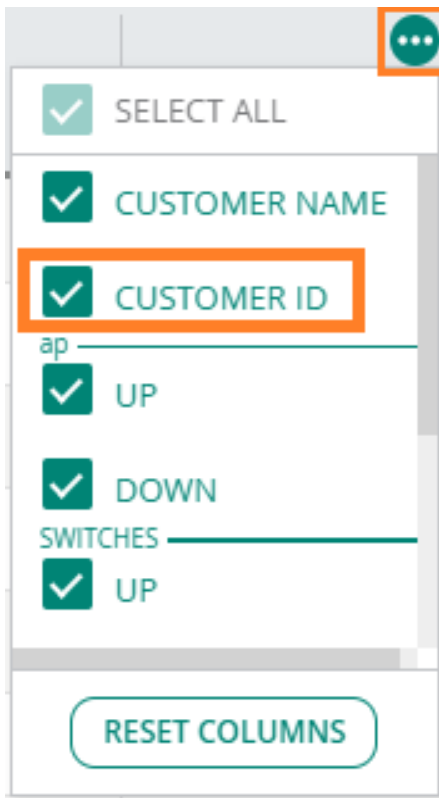



---

The **Customer ID** column is not displayed in the default view. Use the column selector and select the **Customer ID** check box to add the column to the table.

---

**Figure 20** *Selecting the Customer ID for Display*



### ■ Access Points

- **Up**—Total number of online APs. Click the number to view the list of online APs.
- **Down**—Total number of offline APs. Click the number to view the list of offline APs.

Click the sort icon to sort the column in ascending or descending order.

Sometimes, the total number of APs that are displayed as **Down** for a tenant account in MSP view may not equal the total number of corresponding APs displayed as **Offline** under **Manage > Access Points** in the tenant account view. This discrepancy is corrected by an automatic and periodic sync between the MSP database and tenant view database. The periodic sync happens every 12 hours. The number in parentheses () indicates the number of devices that are not onboarded.

## ■ Switches

- **Up**—Total number of online switches. Click the number to view the list of online switches.
- **Down**—Total number of offline switches. Click the number to view the list of offline switches.

Click the sort icon to sort the column in ascending or descending order.

Sometimes, the total number of switches that are displayed as **Down** for a tenant account in MSP view may not equal the total number of corresponding switches displayed as **Offline** under **Manage > Switches** in the tenant account view. This discrepancy is corrected by an automatic and periodic sync between the MSP database and tenant view database. The periodic sync happens every 12 hours. The number in parentheses () indicates the number of devices that are not onboarded.



---

The number of switches displayed in the MSP dashboard corresponds to the total number of switches available for the tenant. However, in the tenant view, a switch stack is considered as a single entity. For example, if there are two switch stacks for a tenant account, and each stack has two members, the MSP dashboard displays the count as four whereas the tenant account displays the count as two.

---

## ■ Gateways

- **Up**—Total number of online gateways. Click the number to view the list of online gateways.
- **Down**—Total number of offline gateways. Click the number to view the list of offline gateways.

Click the sort icon to sort the column in ascending or descending order.

Sometimes, the total number of gateways that are displayed as **Down** for a tenant account in MSP view may not equal the total number of corresponding gateways displayed as **Offline** under **Manage > Gateways** in the tenant account view. This discrepancy is corrected by an automatic and periodic sync between the MSP database and tenant view database. The periodic sync happens every 12 hours. The number in parentheses () indicates the number of devices that are not onboarded.

## ■ Critical Alerts

Total number of critical alerts for the tenant account. Click the number to navigate to the **Alerts** page of the tenant account.

For more information, see [MSP Alerts](#).

## Customers | Trends

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

- **License Renewal Schedule (1 Year)**—Displays the subscription renewal schedule for the next 12 months. The entries include the license renewal date and the total count of subscriptions of each type that are due for renewal on that date.
- **Device Under Management** graph—Displays the count of devices that are managed in the network over the last 12 months. The dates are plotted on the x-axis and the number of devices on the y-axis. Hover over any part of the chart to see the number of devices the MSP is managing on that specific date.
- **Customers** graph—Displays the total number of tenants added to Aruba Central over the last 12 months. The dates are plotted on the x-axis and the number of tenants on the y-axis. Hover over any part of the chart to see the number of tenants the MSP added on that specific date. Click **Total** to view the total number of tenant accounts.

To select a different tenant account, use the **Menu** option in the HPE GreenLake portal.

## Navigating to the Tenant Account

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

To drill down to a specific tenant account:

1. In the **Aruba Central** app, set the filter to **All Groups**.
2. Under **Manage**, click **Overview** to display the **Dashboard**.  
The **Dashboard** page includes the following sections:
  - Dashboard summary bar
  - Overview and trends for customers
3. In the **Customers | Overview** table, click the tenant account name and click **Expand**.  
The tenant account details window is displayed. Close the window.
4. To go to the tenant account, click on the tenant account name.  
The tenant account is displayed in Standard Enterprise Mode.



---

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.

---

### 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 in the HPE GreenLake portal.
- Tenant account administrators can allow or prevent user access to specific groups by configuring custom roles.

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

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

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

The following is a list of configuration guidelines:

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

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

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

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

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

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 Software-Defined Wide Area Network. SD-WAN applies SDN technology to WAN connections that connect enterprise networks distributed across different locations., which is a specific application of the Software-Defined Networking (SDN) technology applied to WAN connections for enterprise networks, including branch offices and data centers, spread across different geographic locations.

In MSP mode, gateways can be configured in **Aruba Central** when they are allow-listed, they are also configurable at the tenant level.



# Chapter 11

## Analyzing and Maintaining MSP Tenant Accounts

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

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

### MSP Alerts

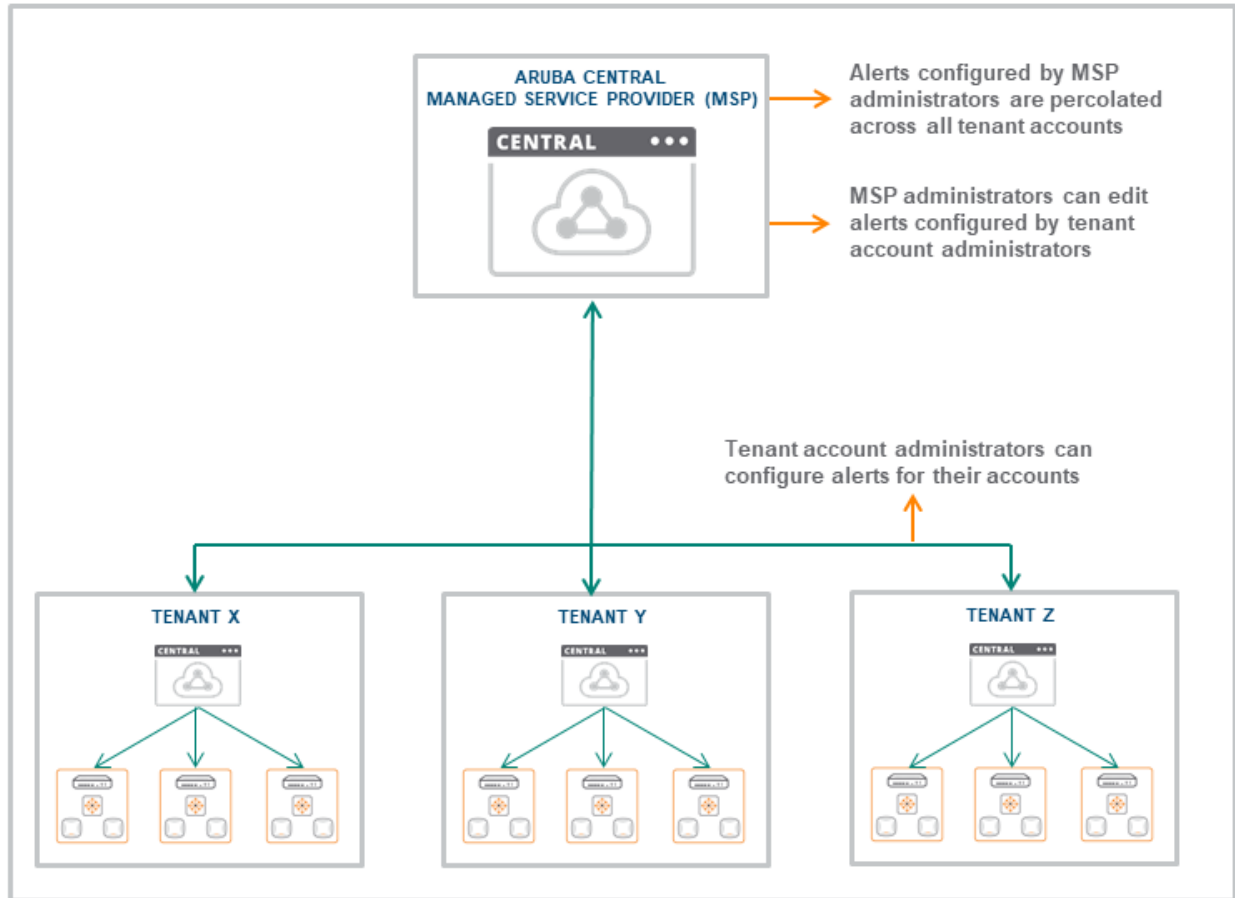
Aruba Central MSP mode enables administrators to trigger alerts when tenant provisioning, network, device, or user management events occur. An MSP administrator can configure alerts at the MSP level which percolate down to all tenant accounts managed by the MSP. For example, if the MSP administrator 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 21** *MSP Alerts*



This section includes the following topics:


- [Viewing MSP Alerts Dashboard](#)
- [MSP Alerts in List View](#)
- [MSP Alerts in Summary View](#)
- [MSP Alerts in Config View](#)

## Viewing MSP Alerts Dashboard

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

The **Alerts** dashboard enables you to configure, view, and acknowledge alerts. The dashboard has three views:

- Alerts in **List** View
- Alerts in **Summary** View
- Alerts in **Config** View

3. The **Search** bar allows you to search for alerts by tenant account. Enter the name of the tenant account and select the tenant account from the list.
4. To view the list of alerts, click the **List** icon.
  - a. The list view displays the number of alerts in the following categories:
    - **Critical**
    - **Major**
    - **Minor**
    - **Warning**
  - b. Click **Acknowledge All** to acknowledge all the alerts at once.
  - c. Enable the **Show Acknowledged Alerts** button to display the list of acknowledged alerts.
  - d. Clicking  icon enables you to customize the **Alerts** table columns or set it to the default view.
5. To view detailed graphs about the alerts, click the **Summary** icon . Select each tab, **All**, **Access Points**, **Switches**, or **Gateways** to view the graphs pertaining to each device type.
6. To configure alerts, click the **Config** icon.

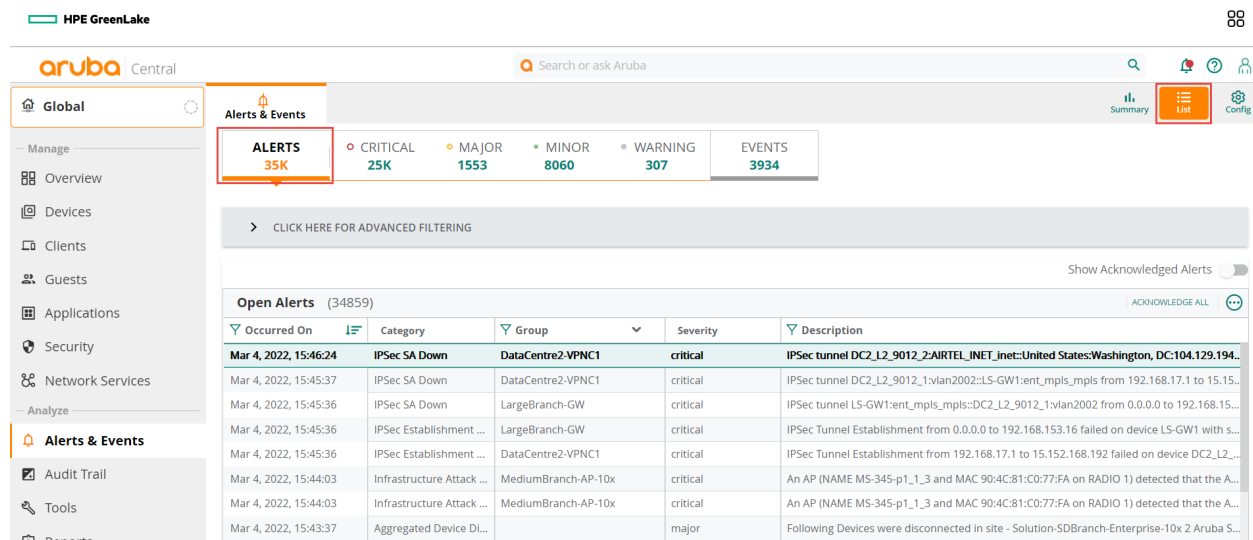
## MSP Alerts in List View

The MSP Alerts page in list view displays a list of alerts for all customers associated with the MSP account.

Use the **Search Customer Name** field to filter alerts by customer name.

The Alerts summary bar displays a list of all the alerts categorized by severity level. You can click on any of the categories to display the list of alerts for that category.

**Figure 22** MSP Alerts in List View



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

**Table 12:** Viewing the MSP Alerts in List View

Data Pane Content	Description
<b>Occurred On</b>	Timestamp of the alert. Use the sort option to sort the alerts by date and time.

Data Pane Content	Description
<b>Category</b>	Displays the category of the alert. Use the filter option to filter the alert by category.
<b>Label</b>	Displays the label name of the alert.
<b>Site</b>	Displays the site name of the alert.
<b>Customer</b>	Displays the customer name of the alert.
<b>Group</b>	Displays the group name of the alert.
<b>Severity</b>	Displays the severity level of the alert. The severity can be Critical, Major, Minor, or Warning.
<b>Description</b>	Displays a description of the alert. Use the search option in filter bar to filter the alert based on description.

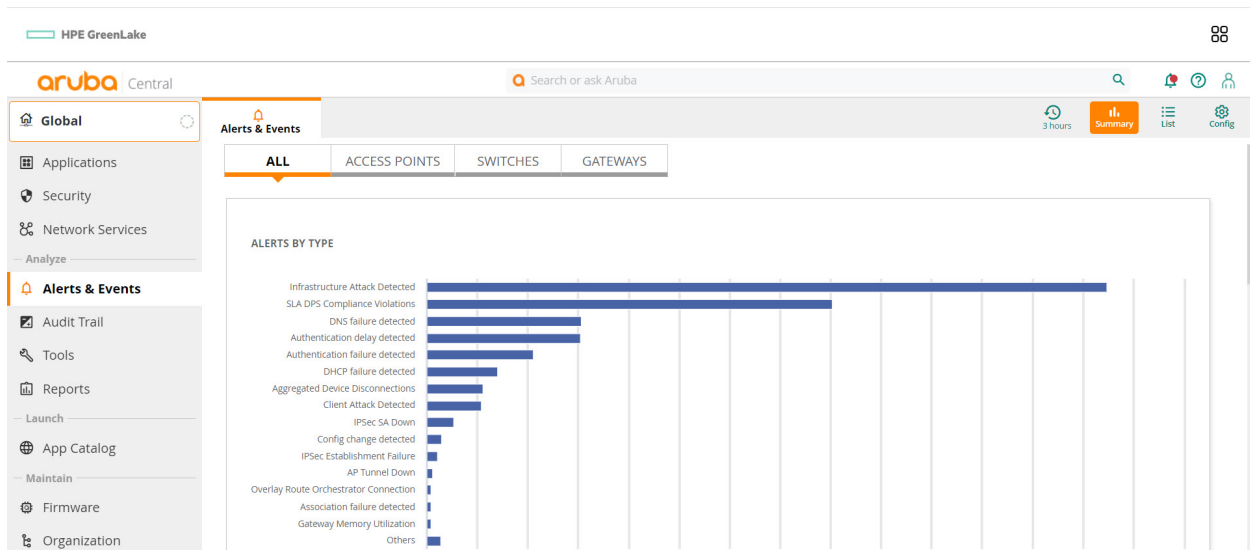
## MSP Alerts in Summary View

The **Summary** view lists all the alerts in charts.

The available charts are:

- **Alerts by Type**—This horizontal bar chart plots the number of alerts versus the category of alerts. You can hover over a bar to get the exact data for the number of alerts for that category. Clicking on a bar redirects you to the list view for that category of alerts. An example is displayed in the next image.
- **Alerts by Severity**—This vertical bar chart plots the number of alerts versus the severity of alerts. You can hover over a bar to get the exact data for the number of alerts for that severity. Clicking on a bar redirects you to the list view for that severity of alerts.

**Figure 23** Alerts by Type Chart in MSP Alerts Summary View



Select each tab, **All**, **Access Points**, **Switches**, or **Gateways** to view the graphs pertaining to each device type.

## MSP Alerts in Config View

The **Alerts** page in **Config** view enables you to configure alerts. You can configure alerts at the MSP level and the tenant account level.

### Configuring Alerts at the MSP Level

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

1. In the **Aruba Central** app, filter **All Groups**.
2. Under **Analyze**, click **Alerts** to display the **Alerts** dashboard.
3. Click the **Config** icon .



---

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

---

4. Use the tabs to navigate between the alert categories. Select an alert and click + to enable the alert with default settings. To configure alert parameters, click on the alert tile (anywhere within the rectangular box) and do the following:
  - a. **Severity**—Set the severity. The available options are Critical, Major, Minor, and Warning. By default, the following alerts are enabled and the severity is **Major**:
    - Virtual Controller Disconnected
    - Rogue AP Detected
    - New User Account Added
    - Switch Detected
    - Switch Disconnected
  - b. **Notification Options**—See [Alert Notification Delivery Options](#).
    - Click **Save**.
    - **Add Rule**—(Optional) For a few alerts, the **Add Rule** option appears. For such alerts, you can add additional rule(s).

### Configuring Alerts at the Tenant Account Level

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

1. Navigate to the tenant account. See [Navigating to the Tenant Account](#).
2. In the **Aruba Central** app, set the filter to a group or a device.
3. To configure alerts, click the settings icon under **Analyze > Alerts & Events**. By default, the **Alerts & Events > User** category is displayed.
4. Use the tabs to navigate between the alert categories. Select an alert and click + to enable the alert with default settings. To configure alert parameters, click on the alert tile (anywhere within the rectangular box) and do the following:
  - a. **Severity**—Set the severity. The available options are Critical, Major, Minor, and Warning. By default, the following alerts are enabled and the severity is **Major**:
    - Virtual Controller Disconnected
    - Rogue AP Detected
    - New User Account Added
    - Switch Detected
    - Switch Disconnected



---

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

---

- b. **Duration**—Enter the duration in minutes.
- c. **Device Filter Options**—(Optional) You can restrict the scope of an alert by setting one or more of the following parameters:
  - **Group**—Select a group to limit the alert to a specific group.
  - **Label**—Select a label to limit the alert to a specific label.
  - **Device**—Select a device to limit the alert to a specific device.
  - **Sites**—Select a site to limit the alert to a specific site.
- d. **Notification Options**
  - **Email**—Select the **Email** check box and enter an email address to receive notifications when an alert is generated. You can enter multiple email addresses, separate each value with a comma.
  - **Webhook**—Select the **Webhook** check box and select the Webhook from the drop-down list.
- e. Click **Save**.
- f. **Add Rule**—(Optional) For a few alerts, the **Add Rule** option appears. For such alerts, you can add additional rule(s). The rule summaries appear at the top of the page.

## Viewing Enabled Alerts

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

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

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

## Alert Notification Delivery Options

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

- **Email**—Select the **Email** check box and enter an email address to receive notifications when an alert is generated. You can enter multiple email addresses; separate each value with a comma.
- **Webhook**—Select the **Webhook** check box and select the desired Webhooks from the drop-down list. Before you select this option, you must create Webhooks. For more information about creating and modifying Webhooks, see the Aruba Central Online documentation.

## Firmware Upgrades for MSP Mode

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

The following topics are discussed:

- [Viewing the Firmware Dashboard](#)
- [Managing Firmware Compliance Based on Device Tabs](#)

- [Managing Firmware Compliance Based on Tenant Account](#)
- [Firmware Upgrade in MSP Through NB API](#)
- [Order of Precedence For Compliance](#)

## Viewing the Firmware Dashboard

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

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

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

**Table 13:** *Firmware Dashboard Parameters for APs Tab*

Date Pane Item	Description
<b>Customer Name</b>	Name of the customer.
<b>Firmware Version</b>	Current firmware version.
<b>Recommended Version</b>	Recommended firmware version.
<b>Upgrade Status</b>	Status of the devices associated with the tenant account. This column displays one of the following: <ul style="list-style-type: none"> <li>▪ Upgrading</li> <li>▪ Scheduling in progress</li> <li>▪ Downloading firmware</li> <li>▪ Upgrade successful, ready for reboot</li> <li>▪ Upgrade successful and rebooting AP</li> <li>▪ Upgrade in process</li> <li>▪ Firmware upgrade failed. Please try again.</li> <li>▪ Rebooting</li> <li>▪ Live upgrade initiating</li> <li>▪ Live upgrade initiated</li> </ul>
<b>Compliance Status</b>	Status of compliance for the tenant. This column indicates the compliance status such as <b>Set</b> , <b>Not Set</b> , or <b>Compliance scheduled on &lt;date and time&gt;</b> for a specific tenant.
<b>Manage Firmware Compliance</b>	Enables you to plan upgrades.

## Managing Firmware Compliance Based on Device Tabs

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

4. Click **Manage Firmware Compliance** at the top right.  
The **Manage Firmware Compliance** window opens.
5. Select the firmware version and the time for upgrade.
6. Select **Auto Reboot** if you want Aruba Central to automatically reboot the device after a successful device upgrade. The **Auto Reboot** option is not available for **Access Points**.
7. Select one of the following options as required:
  - Select **Now** to set the compliance to be carried out immediately.
  - Select **Later Date** to set the compliance at the later date and time.
8. Click **Save and Upgrade**.
9. MSP initiates a firmware upgrade operation only for the devices that support the selected firmware version. If any of selected devices do not support the firmware version selected for the upgrade, a list of unsupported devices is displayed.

## Managing Firmware Compliance Based on Tenant Account

1. In the **Aruba Central** app, use the filter to select **All Groups**.
2. Under **Maintain**, click **Firmware**.
3. Select one of the following tabs: **Access Points**, **Switch-Aruba**, or **Gateways**
4. From the dashboard, select one or more customer name and click **Continue**.
5. The **Upgrade <Device Type> Firmware** page is displayed.



You can click the check box on the table heading of tenant details table to include all the tenants for the firmware upgrade listed in the current page. To manually upgrade firmware for specific tenants, select the check box corresponding to the tenant that requires a manual firmware upgrade in the tenant details table. Clicking the **Continue** button displays the **Upgrade <Device Type> Firmware** page. The **Filter by upgrade status** drop-down list disappears when the **Update All** button is clicked.

6. Perform the following actions:

**Table 14:** *Upgrade <Device Type> Firmware*

Component	Description
<b>Firmware Version</b>	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.
<b>Auto Reboot</b>	Select this check box to reboot the device automatically after the download of the new version.  <b>NOTE:</b> The <b>Auto Reboot</b> option is not applicable for Instant APs.
<b>Schedule</b>	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"> <li>▪ <b>Now</b>—To set the firmware upgrade to be carried out immediately.</li> <li>▪ <b>Later Date</b>—To set the firmware upgrade to take place at a later date and time.</li> </ul> Click the <b>Upgrade</b> button to upgrade the firmware.
<b>Cancel</b>	Click this button to cancel the settings and go back to the <b>Maintenance &gt; Firmware</b> page.



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



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

## Firmware Upgrade in MSP Through NB API

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

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

1. In the **Aruba Central** app, navigate to **Organization > Platform Integration > API Gateway**.
2. Click **System Apps & Tokens** tab and generate a token key.
3. Download and copy the generated token.
4. Click the link displayed in the **APIs** tab of the **API Gateway**. The **Central Network Management APIs** page opens.
5. On the left navigation pane, select **Firmware** from the **URL** drop-down list.
6. Paste the token key in the **Token** field and press enter.
7. In **Firmware Management**, the following options are displayed:
  - **[POST] /firmware/v1/msp/upgrade**—Upgrades firmware at the MSP level. To configure the firmware upgrade for all the tenants of a specific device type, enter the following inputs in the corresponding labels of the script

```
{
  "firmware_scheduled_at": 0,
  "device_type": "string",
  "firmware_version": "string",
  "reboot": true,
  "exclude_groups": "string",
  "exclude_customers": "string"
}:
```

**Table 15:** *Firmware Upgrade at MSP level*

Label	Description
<b>Firmware_scheduled_at</b>	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.
<b>Device_type</b>	The type of device for which the firmware upgrade must be initiated.
<b>Firmware_version</b>	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.
<b>Reboot</b>	True or false value to enable or disable the reboot of device once the firmware upgrade build is downloaded.  <b>NOTE:</b> The <b>Reboot</b> option is not applicable for Instant APs.

Label	Description
<b>Exclude-groups</b>	The list of groups to be excluded from firmware upgrade.
<b>Exclude_customers</b>	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 16:** *Firmware Upgrade at the Tenant level*

Label	Description
<b>Firmware_scheduled_at</b>	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.
<b>Device_type</b>	The type of device for which the firmware upgrade must be initiated.
<b>Firmware_version</b>	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.
<b>Reboot</b>	True or false value to enable or disable the reboot of device once the firmware upgrade build is downloaded.  <b>NOTE:</b> The <b>Reboot</b> option is not applicable for Instant APs.
<b>Exclude-groups</b>	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 17:** *Cancel Scheduled Upgrade at MSP Level*

Label	Description
<b>Device_type</b>	The type of device for which the firmware upgrade schedule must be canceled.
<b>Exclude-groups</b>	List of groups to be excluded while canceling scheduled upgrade.
<b>Exclude_customers</b>	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 18:** *Cancel Scheduled Upgrade at the Tenant Level*

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

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

- **[POST] /firmware/v1/msp/upgrade/cancel**
- **[POST] /firmware/v1/msp/upgrade/customers/{customer\_id}/cancel**

## Order of Precedence For Compliance

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

- Group level
- Tenant level
- MSP level

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

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

## MSP Reports

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



---

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

---

The following topics are discussed in this section:

- [Viewing the MSP Reports Page](#)
- [Types of Reports](#)
- [Creating a Report](#)
- [Editing a Report](#)
- [Viewing or Downloading a Report](#)
- [Deleting a Report or Multiple Reports](#)

### Viewing the MSP Reports Page

To navigate to the **Reports** page, complete the following procedure:

1. From the **Aruba Central** app, set the filter to **All Groups**.  
The **Global** dashboard is displayed.
2. Under **Analyze**, click **Reports**.  
The **Reports** dashboard is displayed.  
The **Reports** dashboard has the following sections:
  - **Browse**—Explore, email, download, or delete generated reports.  
Displays the number of generated reports.  
Click **Browse** to displays the **Reports** page in **List** view.
  - **Manage**—Edit or delete scheduled reports.  
Displays the number of scheduled reports.  
Click **Manage** to displays the **Reports** page in **Config** view.  
In the **Config** view, click + to generate a new report.
  - **Create**—Creates a report that can be run instantly or periodically.  
Displays the number of report categories and the number of report types.  
Click **Create** to generate a new report. Currently, only **Device and Subscription Inventory** reports are supported in MSP.

### Types of Reports

To access the **Reports** dashboard, set the filter to **All Groups** in the **Aruba Central** app. Under **Analyze**, click **Reports**. Reports that are already run are listed under **Browse > Generated Reports**. If any report is yet to run, that report is available under **Browse > Scheduled Reports**.

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

**Table 19: Device and Subscription Inventory Report Description**

Parameter	Description
<b>Access Points Inventory</b>	<p>The <b>Access Points Inventory</b> page lists the following options both in table and graph form:</p> <ul style="list-style-type: none"> <li>▪ <b>Opening Stock</b>—Total number of unassigned APs in the beginning of the time period.</li> <li>▪ <b>Purchased</b>—Number of APs purchased during the time period.</li> <li>▪ <b>Returned</b>—Number of APs returned by the tenants to the customer during the time period.</li> <li>▪ <b>Assigned</b>—Number of APs assigned to the tenants during the time period.</li> <li>▪ <b>Closing Stock</b>—Total of (Opening + Purchased + Returned - Assigned)</li> </ul>
<b>Switch Inventory</b>	<p>The <b>Switch Inventory</b> page lists the following options both in table and graph form:</p> <ul style="list-style-type: none"> <li>▪ <b>Opening Stock</b>—Total number of unassigned switches in the beginning of the time period.</li> <li>▪ <b>Purchased</b>—Number of switches purchased during the time period.</li> <li>▪ <b>Returned</b>—Number of switches returned by the tenants to the customer during the time period.</li> <li>▪ <b>Assigned</b>—Number of switches assigned to the tenants during the time period.</li> <li>▪ <b>Closing Stock</b>—Total of (Opening + Purchased + Returned - Assigned)</li> </ul>
<b>Gateway Inventory</b>	<p>The <b>Gateway Inventory</b> page lists the following options both in table and graph form:</p> <ul style="list-style-type: none"> <li>▪ <b>Opening Stock</b>—Total number of unassigned gateways in the beginning of the time period.</li> <li>▪ <b>Purchased</b>—Number of gateways purchased during the time period.</li> <li>▪ <b>Returned</b>—Number of gateways returned by the tenants to the customer during the time period.</li> <li>▪ <b>Assigned</b>—Number of gateways assigned to the tenants during the time period.</li> <li>▪ <b>Closing Stock</b>—Total of (Opening + Purchased + Returned - Assigned)</li> </ul>
<b>Gateway Foundation License</b>	<p>The <b>Gateway Foundation License</b> page lists the following options both in table and graph form:</p> <ul style="list-style-type: none"> <li>▪ <b>Opening Stock</b>—Total number of licenses in the beginning of the time period.</li> <li>▪ <b>Purchased</b>—Number of licenses purchased during the time period.</li> <li>▪ <b>Returned</b>—Number of licenses returned by the tenants to the customer during the time period.</li> <li>▪ <b>Assigned</b>—Number of licenses assigned to the tenants during the time period.</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>▪ <b>Expired</b>—Number of licenses that expired during the time period.</li> <li>▪ <b>Closing Stock</b>—Total of (Opening + Purchased + Returned - Assigned -Expired)</li> </ul>
<b>Gateway Advanced License</b>	<p>The <b>Gateway Advanced License</b> page lists the following options both in table and graph form:</p> <ul style="list-style-type: none"> <li>▪ <b>Opening Stock</b>—Total number of licenses in the beginning of the time period.</li> <li>▪ <b>Purchased</b>—Number of licenses purchased during the time period.</li> <li>▪ <b>Returned</b>—Number of licenses returned by the tenants to the customer during the time period.</li> <li>▪ <b>Assigned</b>—Number of licenses assigned to the tenants during the time period.</li> <li>▪ <b>Expired</b>—Number of licenses that expired during the time period.</li> <li>▪ <b>Closing Stock</b>—Total of (Opening + Purchased + Returned - Assigned -Expired)</li> </ul>
<b>Gateway Base License</b>	<p>The <b>Gateway Base License</b> page lists the following options both in table and graph form:</p> <ul style="list-style-type: none"> <li>▪ <b>Opening</b>—Total number of licenses in the beginning of the time period.</li> <li>▪ <b>Purchased</b>—Number of licenses purchased during the time period.</li> <li>▪ <b>Returned</b>—Number of licenses returned by the tenants to the customer during the time period.</li> <li>▪ <b>Assigned</b>—Number of licenses assigned to the tenants during the time period.</li> <li>▪ <b>Expired</b>—Number of licenses that expired during the time period.</li> <li>▪ <b>Closing Stock</b>—Total of (Opening + Purchased + Returned - Assigned -Expired)</li> </ul>
<b>Access Points Foundation License</b>	<p>The <b>Access Points Foundation License</b> page lists the following options both in table and graph form:</p> <ul style="list-style-type: none"> <li>▪ <b>Opening Stock</b>—Total number of licenses in the beginning of the time period.</li> <li>▪ <b>Purchased</b>—Number of licenses purchased during the time period.</li> <li>▪ <b>Returned</b>—Number of licenses returned by the tenants to the customer during the time period.</li> <li>▪ <b>Assigned</b>—Number of licenses assigned to the tenants during the time period.</li> <li>▪ <b>Expired</b>—Number of licenses that expired during the time period.</li> <li>▪ <b>Closing Stock</b>—Total of (Opening + Purchased + Returned - Assigned -Expired)</li> </ul>

Parameter	Description
<b>Access Points Advanced License</b>	<p>The <b>Access Points Advanced License</b> page lists the following options both in table and graph form:</p> <ul style="list-style-type: none"> <li>▪ <b>Opening Stock</b>—Total number of licenses in the beginning of the time period.</li> <li>▪ <b>Purchased</b>—Number of licenses purchased during the time period.</li> <li>▪ <b>Returned</b>—Number of licenses returned by the tenants to the customer during the time period.</li> <li>▪ <b>Assigned</b>—Number of licenses assigned to the tenants during the time period.</li> <li>▪ <b>Expired</b>—Number of licenses that expired during the time period.</li> <li>▪ <b>Closing Stock</b>—Total of (Opening + Purchased + Returned - Assigned - Expired)</li> </ul>
<b>Switch Foundation License</b>	<p>The <b>Switch Foundation License</b> page lists the following options both in table and graph form:</p> <ul style="list-style-type: none"> <li>▪ <b>Opening Stock</b>—Total number of licenses in the beginning of the time period.</li> <li>▪ <b>Purchased</b>—Number of licenses purchased during the time period.</li> <li>▪ <b>Returned</b>—Number of licenses returned by the tenants to the customer during the time period.</li> <li>▪ <b>Assigned</b>—Number of licenses assigned to the tenants during the time period.</li> <li>▪ <b>Expired</b>—Number of licenses that expired during the time period.</li> <li>▪ <b>Closing Stock</b>—Total of (Opening + Purchased + Returned - Assigned - Expired)</li> </ul>
<b>Switch Advanced License</b>	<p>The <b>Switch Advanced License</b> page lists the following options both in table and graph form:</p> <ul style="list-style-type: none"> <li>▪ <b>Opening Stock</b>—Total number of licenses in the beginning of the time period.</li> <li>▪ <b>Purchased</b>—Number of licenses purchased during the time period.</li> <li>▪ <b>Returned</b>—Number of licenses returned by the tenants to the customer during the time period.</li> <li>▪ <b>Assigned</b>—Number of licenses assigned to the tenants during the time period.</li> <li>▪ <b>Expired</b>—Number of licenses that expired during the time period.</li> <li>▪ <b>Closing Stock</b>—Total of (Opening + Purchased + Returned - Assigned - Expired)</li> </ul>

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

**Table 20: Generated Reports** *Description*

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

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

**Table 21: Scheduled Reports** *Description*

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

## Creating a Report

The MSP **Reports** page in **Summary** view enables you to browse, manage, and create reports. To create a report, perform the following steps:

1. From the **Aruba Central** app, set the filter to **All Groups**.  
The **Global** dashboard is displayed.
2. Under **Analyze**, click **Reports**.  
The **Reports** page is displayed.
3. In the **Reports** page, click the **Summary** icon. Click the **Create** tile.  
Else, click the **Config** view and then click the + sign in the **Scheduled Reports** page.  
The **Infrastructure** page is displayed.
4. Under **Infrastructure**, click **Device and Subscription Inventory** and then click **Next**.
5. Under **Scope**, select **All** or a combination of the other choices and then click **Next**:
  - **All**—Generates a report for all access points, gateways, switches, and subscriptions.
  - **Access Points**—Generates a report only for access points.
  - **Gateways**—Generates a report only for gateways.



- **Switches**—Generates a report only for switches.
  - **Subscriptions**—Generates a report only for subscriptions.
6. Under **Report period**, select one of the following options and then click **Next**:
    - **Last Month**
    - **Last 3 Months**
    - **Last 6 Months**
    - **Custom Range**
  7. Select one of the recurrent options:
    - **One Time (now)**
    - **One Time (later)**
    - **Every day**
    - **Every week**
    - **Every month**
  8. For **Report Information**, enter the title of the report and an email address where the report will be delivered.
  9. Select the format as either **PDF** or **CSV**.
  10. Click **Generate**.
  11. If you select **One Time** as an option in step 6, the report is available in the **Generated** view as **Generated Reports**. If the report is yet to run, the report is available under **Scheduled Reports**.

## Editing a Report

To edit a report, complete the following procedure:

1. From the **Aruba Central** app, set the filter to **All Groups**.  
The **Global** dashboard is displayed.
2. Under **Analyze**, click **Reports**.  
The **Reports** page is displayed.
3. In the **Reports** page, click the **Scheduled** view icon.  
The **Scheduled Reports** dashboard is displayed.
4. Under **Scheduled Reports**, select the report you want to edit and then click the edit icon.  
The **Infrastructure** page is displayed.
5. Under **Scope**, select one or a combination of the following choices and then click **Next**:
  - **All**—Generates a report for all access points, gateways, switches, and subscriptions.
  - **Access Points**—Generates a report only for access points.
  - **Gateways**—Generates a report only for gateways.
  - **Switches**—Generates a report only for switches.
  - **Subscriptions**—Generates a report only for subscriptions.
6. Under **Report period**, select one of the following options and then click **Next**:
  - **Last Month**
  - **Last 3 Months**
  - **Last 6 Months**
  - **Custom Range**

7. Select one of the recurrent options:
  - **One Time (now)**
  - **One Time (later)**
  - **Every day**
  - **Every week**
  - **Every month**
8. For **Report Information**, enter the title of the report and an email address where the report will be delivered.
9. Select the format as either **PDF** or **CSV**.
10. Click **Generate**.
11. If you select **One Time** as an option, the report is available under **Generated Reports**. If the report is yet to run, the report is available under **Scheduled Reports**.

## Viewing or Downloading a Report

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

1. From the **Aruba Central** app, set the filter to **All Groups**.  
The **Global** dashboard is displayed.
2. Under **Analyze**, click **Reports**.  
The **Reports** page is displayed.
3. In the **Reports** page, click the **Generated** view icon.  
The **Generated Reports** dashboard is displayed.
4. Under **Generated Reports**, select the report you want to view or download.
  - To view the report online, click the report name.
  - To download the report, click the report and then click the download icon for either the CSV or PDF file.
  - To email the report, click the email to icon.
  - To delete the report, click the delete icon.

## Deleting a Report or Multiple Reports

To delete a report or multiple reports, complete the following procedure:

1. From the **Aruba Central** app, set the filter to **All Groups**.  
The **Global** dashboard is displayed.
2. Under **Analyze**, click **Reports**.  
The **Reports** page is displayed.
3. In the **Reports** page, click the **Generated** view icon.  
Reports that are already run are listed under **Generated Reports**. If any report is yet to run, that report is available under **Scheduled Reports**.
4. Select the report you want to delete and then click the delete icon.  
You can select multiple reports to delete.

## MSP Audit Trails

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



---

To see the audit trail logs for actions such as tenant creation, tenant deletion, editing description, updating logo, enabling MSP, and disabling MSP account are available in the HPE GreenLake portal. For more information, see the [HPE GreenLake User Guide](#).

---

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

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

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

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

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

## Guest Access Dashboard

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

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

**Table 22:** *Guest Access Overview Page*

Data Pane Item	Description
<b>Time Range</b>	Time range for the graphs and charts displayed on the <b>Overview</b> pane. You can choose to view graphs for a time period of 1 day, 1 week, and 1 month.
<b>Guests</b>	Number of guests connected to the SSIDs with Cloud Guest splash page profiles.
<b>Guest SSID</b>	Number of guest SSIDs that are configured to use the Cloud Guest splash page profiles.
<b>Avg. Duration</b>	The average duration of client connection on the SSIDs with Cloud Guest splash page profiles.
<b>Max Concurrent Connections</b>	Maximum number of client devices connected concurrently on the guest SSIDs.
<b>Guest Connection (graph)</b>	Time stamp for the client connections on the cloud guest for the selected time range.

Data Pane Item	Description
<b>Guest Count by Authentication</b>	Number of client devices based on the authentication type configured on the cloud guest SSIDs.
<b>Guest Count by SSID</b>	Number of guest connections per SSID.
<b>Client Type</b>	Type of the client devices connected on the guest SSIDs.

## Mapping Cloud Guest Certificates



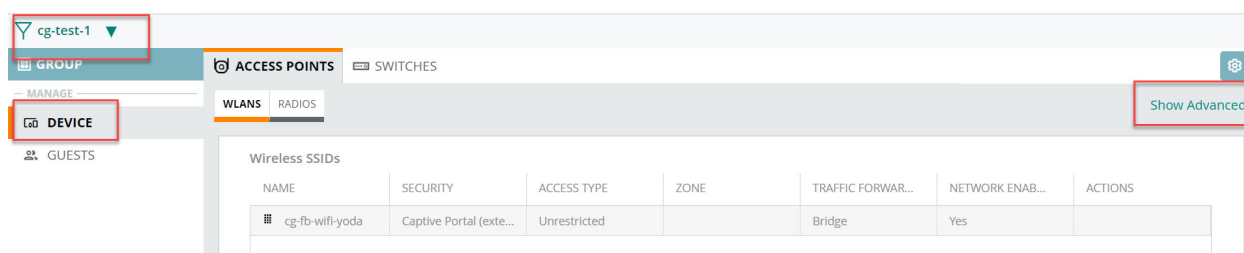
To enable certificates for the Cloud Guest Service, contact the Aruba Central support team.

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

To map the cloud guest certificate to Captive Portal:

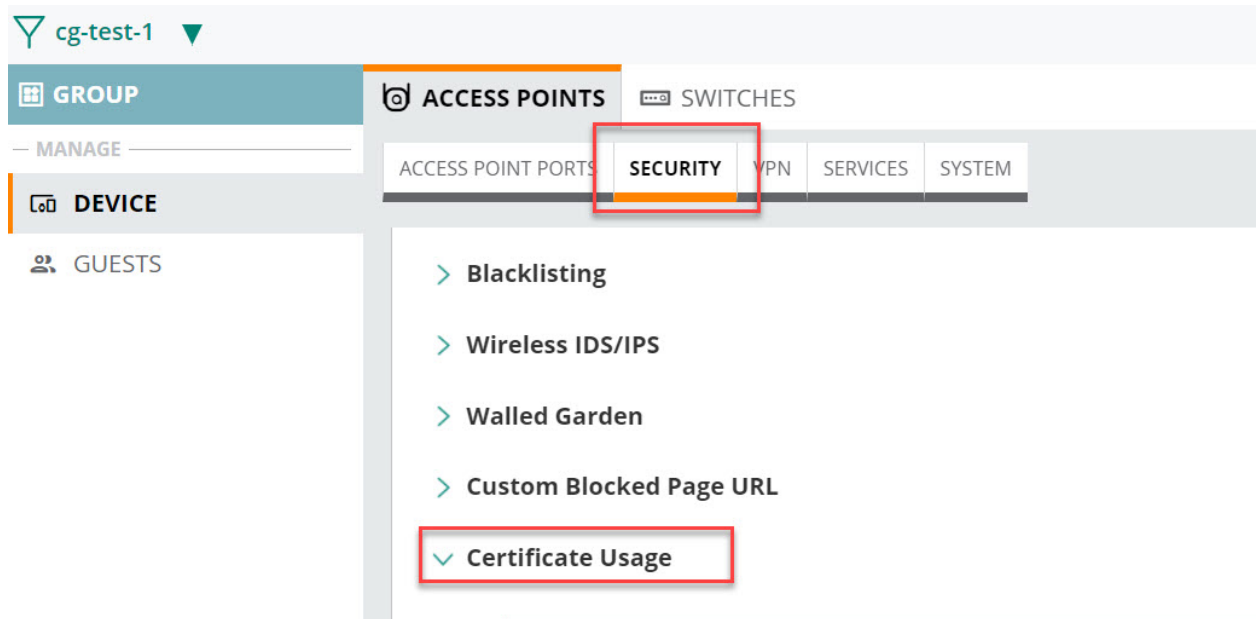
1. In the **Aruba Central** app, use the filter to select **All Groups**.
2. Under **Maintain**, click **Organization**.  
By default, the **Network Structure** tab is displayed
3. Click the **Certificates** tile.  
The Certificates page is displayed.
4. Click the + sign to upload a certificate to the **Certificate Store**.
5. Use the filter to select the group to which you want to assign the certificate.  
For example, in the following image, a group called **cg-test-1** is selected.
6. Under **Manage**, click **Device** and then click **Show Advanced > Security**.

**Figure 24** *Show Advanced*



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

**Figure 25** *Certificate Usage Accordion*



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

## Configuring a Guest Splash Page Profile

The Guest app allows MSP administrators to configure Splash Page profiles for tenant accounts. If the tenant account is mapped to a group and the Guest 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. The guest 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 Guest Splash Page Profile](#)
- [Customizing a Splash Page Design](#)
- [Previewing and Modifying a Splash Page Profile](#)
- [Localizing a Guest Portal](#)
- [Associating a Splash Page Profile to an SSID](#)

### Adding a Guest Splash Page Profile

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

1. In the **Aruba Central** app, set the filter to a group.  
The dashboard context for the group is displayed.
2. Under **Manage**, click **Guests**.  
The **Guest Access > Splash Pages** page is displayed.

3. To create a new splash page, click the + icon.  
The **New Splash Page** pane is displayed.
4. On the **Configuration** tab, configure the parameters described in the following table:

**Table 23:** *Splash Page Configuration*

Data Pane Content	Description
<b>Name</b>	<p>Enter a unique name to identify the splash profile.</p> <p><b>NOTE:</b> If you attempt to enter an existing splash profile's name, Aruba Central displays a message stating that <b>Splash page with this name already exists</b>.</p>
<b>Type</b>	<p>Configure any of the following authentication methods to provide a secure network access to the guest users and visitors.</p> <ul style="list-style-type: none"> <li>■ <b>Anonymous</b></li> <li>■ <b>Authenticated</b></li> <li>■ <b>Facebook Wi-Fi</b></li> </ul>
<b>Anonymous</b>	<p>Configure the <b>Anonymous</b> login method if you want to allow guest users to log in to the Splash page without providing any credentials.</p> <p>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 <b>Guest Key</b> to ON and specify a password.</p>
<b>Authenticated</b>	<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 guest splash page are described in the following rows.</p>
<b>Username/Password</b>	<p>The <b>Username/Password</b> 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"> <li>1. Enable <b>Self-Registration</b>.</li> <li>2. Set the <b>Verification Required</b> to <b>ON</b> if the guest user account must be verified.</li> <li>3. Enable the <b>Bypass Apple Captive Network Assistant (CNA)</b> to bypass the CNA on the iOS devices. Enabling CNA bypass allows users to bypass the Apple Captive Network Assistant pop-up on their iOS devices. However, users still need to verify their credentials with a browser. When the CNA bypass is disabled, the iOS clients have to enter the credentials in the CNA pop-up on their devices. The <b>Bypass Apple Captive Network Assistant (CNA)</b> toggle button is displayed only when <b>Verification Required</b> is enabled. Users can either enable or disable CNA bypass based on their requirement.</li> <li>4. Specify a verification criteria to allow the self-registered users to verify</li> </ol>

**Table 23: Splash Page Configuration**

Data Pane Content	Description
	<p>through email or phone.</p> <ul style="list-style-type: none"> <li>▪ If email-based verification is enabled and the <b>Send Verification Link</b> 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.</li> <li>▪ 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 <b>Customize SMS</b>.</li> </ul> <p>5. Specify the duration within the range of 1-60 minutes, during which the users can access free Wi-Fi to verify the link. The users can log in to the network for the specified duration and click the verification link to obtain access to the Internet.</p> <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>
<b>Social Login</b>	<p>Enable <b>Social Login</b> to allow guest users to use their existing login credentials from social networking profiles such as Facebook, Twitter, Google, or LinkedIn and sign on to 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> <p><b>NOTE:</b> When configuring the OAuth for the social login, specify the cloud guest URL provided in the Aruba Central as the Redirect URI. For information about how to obtain the guest URL, see <a href="#">Obtaining the Redirect URI for OAuth</a>.</p> <p>The following social logins are available:</p> <ul style="list-style-type: none"> <li>▪ <b>Facebook</b>—Allows guest users to use their Facebook credentials to log on 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 <a href="#">Create an App</a> in the Facebook documentation portal.</li> </ul> <p>Enter details obtained during creation of Facebook app for the following parameters:</p> <ul style="list-style-type: none"> <li>◦ <b>Client ID</b>—Enter the app ID obtained from Facebook.</li> <li>◦ <b>Client Secret</b>—Enter the secret key obtained from Facebook.</li> </ul> <ul style="list-style-type: none"> <li>▪ <b>Twitter</b>—Allows guest users to use their Twitter credentials to log on 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 <a href="#">Developer Apps</a> in the Twitter documentation portal.</li> </ul> <p>Enter details obtained during creation of the Twitter app for the following parameters:</p> <ul style="list-style-type: none"> <li>◦ <b>Client ID</b>—Enter the app ID obtained from Twitter.</li> <li>◦ <b>Client Secret</b>—Enter the secret key obtained from Twitter.</li> </ul> <ul style="list-style-type: none"> <li>▪ <b>Google</b>—Allows guest users to use their Google credentials to log on 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</li> </ul>



**Table 23:** *Splash Page Configuration*

Data Pane Content	Description
	<p><a href="#">Creating your Project</a> in the Google documentation portal.</p> <p>Enter details obtained during creation of the Google app for the following parameters:</p> <ul style="list-style-type: none"> <li>◦ <b>Client ID</b>—Enter the app ID obtained from Google.</li> <li>◦ <b>Client Secret</b>—Enter the secret key obtained from Google.</li> <li>◦ <b>Gmail for Work Domain</b>—Enter the domain name to restrict authentication attempts to only the members of a Google hosted domain. Ensure that you have a valid domain account licensed by Google Domains or Google Apps.</li> <li>◦ <b>Sign-in Button Text</b>—Specify a text for the sign-in button.</li> <li>▪ <b>LinkedIn</b>—Allows guest user to use their LinkedIn credentials to log on to the splash page. To enable LinkedIn integration, you must create a LinkedIn app and obtain the app ID and secret key. For more information, see <a href="#">Creating an App</a> and <a href="#">Sign In with LinkedIn</a> in the LinkedIn documentation portal.</li> </ul> <p>Enter details obtained during creation of the LinkedIn app for the following parameters:</p> <ul style="list-style-type: none"> <li>◦ <b>Client ID</b>—Enter the app ID obtained from LinkedIn.</li> <li>◦ <b>Client Secret</b>—Enter the secret key obtained from LinkedIn.</li> </ul>
<b>Facebook Wi-Fi</b>	<p>If you want to enable network access through the free Wi-Fi service offered by Facebook. Select the <b>Facebook Wi-Fi</b> 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>
<b>Facebook Wifi Configuration</b>	<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"> <li>1. Click the <b>Configure Now</b> link.</li> <li>2. Sign in to your Facebook account.</li> <li>3. If you do not have a business page, click <b>Create Page</b>. For more information on setting Facebook Wi-Fi service, see <a href="#">Facebook Wi-Fi</a> in the Facebook documentation portal.</li> </ol> <p><b>NOTE:</b> 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>
<b>Allow Internet In Failure</b>	<p>To allow users access the Internet when the external captive portal server is not available, click the <b>Allow Internet In Failure</b> toggle switch. By default, this option is disabled.</p>

**Table 23:** *Splash Page Configuration*

Data Pane Content	Description
<b>Override Common Name</b>	<p>To override the default common name, click the <b>Override Common Name</b> toggle switch and specify a common name. The common name is the web page URL of the guest portal. By default, the common name is set to <b>securelogin.arubanetworks.com</b>. 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"> <li>1. Run the <b>show captive-portal-domains</b> command at the Instant AP command prompt.</li> <li>2. Note the common name or the internal captive portal domain name.</li> <li>3. Add this domain name in the <b>Override Common Name</b> field on the <b>Splash Page</b> configuration page.</li> <li>4. Save the changes.</li> </ol>
<b>Guest Key</b>	To set password for anonymous users, enable the Guest Key and enter a password.
<b>Sponsored Guest</b>	Enable the <b>Sponsored Guest</b> option to provide authorization control to a guest sponsor for allowing and denying a guest from accessing the network.
<b>Allowed Sponsor Domains</b>	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, Yahoo, and so on. To add more domain names, click the add icon and enter the domain name. This is a mandatory field.
<b>Allowed Sponsor Emails</b>	Enter the allowed email addresses. If you leave this field empty, all emails that correspond to the allowed domains list are permitted to sponsor guests. To add more sponsor emails, click the add icon and enter the sponsor's email address. This is an optional field.
<b>Authentication Success Behavior</b>	<p>If <b>Anonymous</b> or <b>Authenticated</b> 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"> <li>▪ <b>Redirect to Original URL</b>— When selected, upon successful authentication, the user is redirected to the URL that was originally requested.</li> <li>▪ <b>Redirect URL</b>— Specify a redirect URL if you want to override the original request of users and redirect them to another URL.</li> </ul>
<b>Authentication Failure Message</b>	If the <b>Authenticated</b> 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.
<b>Session Timeout</b>	<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>

**Table 23:** *Splash Page Configuration*

Data Pane Content	Description
<b>Share This Profile</b>	<p>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.</p> <p><b>NOTE:</b> When you clone an existing group, the unshared splash page profile in the existing group is not cloned to the new group. In the existing group, if an unshared splash page is associated with a guest network, then the splash page value is empty in the guest network of the new group.</p>
<b>Daily Usage Limit</b>	<p>Use this option to set a data usage limit for authenticated guest users, anonymous profiles, and Facebook Wi-Fi logins. By default, no daily usage limit is applied.</p> <p>To set a daily usage limit, use one of the following options:</p> <ul style="list-style-type: none"><li>▪ <b>By Time</b>— Specify the time limit in hours and minutes for data usage during a day. When a user exceeds the configured time limit, the device is disconnected from the network until the next day begins; that is, until 00.00 hours in the specified time zone.</li><li>▪ <b>By Data</b>— Specify a limit for data usage in MB. You can set this limit to either <b>Per User</b>, <b>Per Session</b>, or <b>Per Device</b>. 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"><li>◦ <b>Per User</b>— This option applies the data usage limit based on authenticated user credentials.</li><li>◦ <b>Per Session</b>—This option applies the data usage limit based on user sessions.</li><li>◦ <b>Per Device</b>—This option applies the data usage limit based on the MAC address of the client device connected to the network.</li></ul></li></ul> <p><b>Important Points to Note</b></p> <ul style="list-style-type: none"><li>▪ 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.</li><li>▪ For anonymous and Facebook Wi-Fi logins, the daily usage limit is applied per MAC address of the client device connected to the network.</li></ul>
<b>Allowlist URL</b>	<p>To allow a URL, click + and add the URL to the allowlist. For example, if the terms and conditions configured for the guest portal include URLs, you can add these URLs to the allowlist, so that the users can access the required web pages.</p>

## Obtaining the Redirect URI for OAuth

When creating social login apps for the splash page, the configuration of OAuth requires a Redirect URI. Use the server URL provided in the splash page configuration in Aruba Central with [/oauth/reply](#) suffix. 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>.

To get the cloud guest URL, complete the following steps:

1. In the **Aruba Central** app, set the filter to a group.  
The dashboard context for the group is displayed.

2. Under **Manage**, click **Guests**.

The **Guest Access > Splash Pages** page is displayed.



---

Ensure that the pop-up blocker of the browser is disabled.

---

3. Hover over the splash page profile for which you want to view the cloud guest URL and click the



settings icon.

The Splash Page Configuration window is displayed.

**Figure 26** Cloud Guest URL


#### SPLASH PAGE CONFIGURATION



```
! Include the next four lines on your guest SSID
auth-server AS1_#guest#_
auth-server AS2_#guest#_
set-role-pre-auth TP-TEST_#guest#_
captive-portal external profile TP-TEST_#guest#_

wlan access-rule TP-TEST_#guest#_
rule alias licdn.com match tcp 443 443 permit
rule alias twimg.com match tcp 443 443 permit
rule alias bam.nr-data.net match tcp 443 443 permit
rule alias nr-data.net match tcp 443 443 permit
rule alias js-agent.newrelic.com match tcp 443 443 permit
rule alias crt.comodoca.com match tcp 80 80 permit
rule alias crt.comodoca.com match tcp 80 80 permit
rule alias secure.comodo.com match tcp 80 80 permit
rule alias symcb.com match tcp 80 80 permit
rule alias symcd.com match tcp 80 80 permit
rule alias digicert.com match tcp 80 80 permit
rule alias any match tcp 80 80 permit
rule alias match 6 80 80 permit

wlan auth-server AS1_#guest#_
radsec
ip yoda-cgga.arubathena.com
port 1812
acctport 1813
timeout 20
nas-id 7d2e4c68-b04f-44c2-ba35-3ae6279d03c3
rfc3576
```

4. Copy the cloud guest URL from the **Splash Page Configuration** window and use it to specify as the Redirect URI in the social login app configuration for OAuth.
5. Alternatively, you can also click the  preview icon.

The Splash page is displayed in the browser.



---

This is the page the guest user will see and use it to sign on to the application.

---

6. Copy the URL from the address bar on the browser and use it to specify as the Redirect URI in the social login app configuration for OAuth.

## Customizing a Splash Page Design

To customize a splash page design, complete the following steps:

1. In the **Aruba Central** app, set the filter to a group.  
The dashboard context for the group is displayed.
2. Under **Manage**, click **Guests**.  
The **Guest Access > Splash Pages** page is displayed.
3. To create a new splash page, click the **+** icon.  
The **New Splash Page** pane is displayed.
4. To customize a splash page design, on the **Guest > Splash Page > New Splash Page > Customization** pane, configure the parameters described in the following table:

**Table 24: Splash Page Customization**

Data Pane Content	Description
<b>Layout</b>	<p>To customize the page layout based on the device type. Specify a layout by selecting one of the following options:</p> <ul style="list-style-type: none"> <li>▪ <b>Horizontal, better for computers</b></li> <li>▪ <b>Vertical, better for phones</b></li> </ul> <p>The horizontal layout is selected by default. To change the layout, click the drop-down list and select the required layout type.</p>
<b>Background color</b>	To change the color of the splash page, select a color from the <b>Background Color</b> palette.
<b>Button color</b>	To change the color of the sign in button, select a color from the <b>Button Color</b> palette.
<b>Header fill color</b>	Select the fill color for the splash page header from the <b>Header fill color</b> palette.
<b>Page font color</b>	To change the font color of the text on the splash page, select a color from the <b>Page font color</b> palette.
<b>Logo</b>	To upload a logo, click <b>Browse</b> , and browse the image file. Ensure that the image file size does not exceed 256 KB.
<b>Background Image</b>	Click <b>Browse</b> to upload a background image. Ensure that the background image file size does not exceed 512 KB.
<b>Page Title</b>	Add a suitable title for the splash page.
<b>Welcome Text</b>	Enter the welcome text to be displayed on the splash page. Ensure that the welcome text does not exceed 20,000 characters.
<b>Terms &amp; Conditions</b>	<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>&lt;i&gt; &lt;/i&gt;</code> HTML tag.</p> <p>Specify an acceptance criteria for terms and condition by selecting any of the following options from the <b>Display "I Accept" check box</b>:</p> <ul style="list-style-type: none"> <li>▪ <b>No, Accept by default</b></li> <li>▪ <b>Yes, Display check box</b></li> </ul> <p>If the <b>I ACCEPT</b> check box must be displayed on the Splash page, select the display format for terms and conditions.</p> <p>Ensure that <b>Display Option For Terms &amp; Conditions</b> has the Inline Text option auto-selected and displayed as an uneditable text.</p>
<b>Ad Settings</b>	<p>If you want to display advertisements on the splash page, enter the URL in the <b>Advertisement URL</b>.</p> <p>For <b>Advertisement Image</b>, click <b>Browse</b> and upload the image.</p>

## Localizing a Guest Portal

To localize a guest portal, complete the following steps:

1. In the **Aruba Central** app, set the filter to a group.  
The dashboard context for the group is displayed.

2. Under **Manage**, click **Guests**.  
The **Guest Access > Splash Pages** page is displayed.
3. To create a new splash page, click the **+** icon.  
The **New Splash Page** pane is displayed.
4. To localize or translate the Guest portal content, on the **Guest > 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:** *Guest Portal Localization*

Data Pane Content	Description	Allowed Length of Text
<b>Login Section</b>		
<b>Login button title</b>	Enter the custom label text to be localized for the <b>Login</b> button.	1-255 characters
<b>Network login title</b>	Enter the custom title text that you want to localize for the <b>Network Login</b> page.	1-255 characters
<b>Login page title</b>	Enter the custom text for title in the <b>Login</b> page.	1-255 characters
<b>Access denied page title</b>	Enter the custom title text for the <b>Access Denied</b> page.	1-255 characters
<b>Logged in title</b>	Enter the custom <b>Logged in</b> title text for the page that allows access.	1-255 characters
<b>Username label</b>	Enter the custom text for <b>Username</b> label.	1-255 characters
<b>Username placeholder</b>	Enter the custom text to show in in the <b>Username</b> placeholder.	1-255 characters
<b>Password placeholder</b>	Enter the custom text to show in in the <b>Password</b> placeholder.	1-255 characters
<b>Email address placeholder</b>	Enter the custom text to show in in the <b>Email Address</b> placeholder.	1-255 characters
<b>Register button title</b>	Enter the custom title text for <b>Register</b> button.	1-255 characters
<b>Network login button title</b>	Enter the custom title text for <b>Network Login</b> button.	1-255 characters
<b>Terms and Conditions title</b>	Enter the custom text to show in the <b>Terms and Conditions</b> title.	1-255 characters

**Table 25:** *Guest Portal Localization*

Data Pane Content	Description	Allowed Length of Text
<b>I accept the Terms and Conditions' text</b>	Enter the custom text to show for the ' <b>I accept the Terms and Conditions</b> ' text adjacent to the check box.	Up to 20000 characters
<b>Welcome Text</b>	Enter a custom Welcome text to the guest portal user.	Up to 20000 characters
<b>Login failed message</b>	Enter a custom text to show for the <b>Login Failed</b> message when a user's login attempt gets denied or fails.	Up to 20000 characters
<b>Logged in message</b>	Enter a custom text to show for the <b>Logged in</b> message in the access allowed page.	Up to 20000 characters
<b>Register Section</b>		
<b>Phone help message</b>	Enter a custom help message to show for the <b>Phone</b> help field.	Up to 20000 characters
<b>Phone number placeholder</b>	Enter the custom placeholder text for the <b>Phone Number</b> input UI control.	1-255 characters
<b>'Back' button text</b>	Enter the custom text label to show for the <b>Back</b> button control.	1-255 characters
<b>'Continue' button text</b>	Enter the custom text label to show for the <b>Continue</b> button control.	1-255 characters
<b>Email radio button</b>	Enter a custom text label for the <b>Email</b> option.	—
<b>Phone radio button</b>	Enter a custom label text for the <b>Phone</b> option.	—
<b>Register page title</b>	Enter a custom title text for the <b>Register</b> page.	1-255 characters
<b>Accept button title</b>	Enter a custom title text for the <b>Accept</b> button.	1-255 characters
<b>Register Page instructions</b>	Enter a custom message to show in the <b>Register</b> page.	Up to 20000 characters
<b>Verification Section</b>		
<b>Verification code label</b>	Enter a custom text to show for the <b>Verification code</b> label.	1-255 characters
<b>Verification code placeholder</b>	Enter a custom text to show for the <b>Verification code</b> placeholder.	1-255 characters
<b>Verification email check message</b>	Enter a custom text for the <b>Verification Email Check</b> message. This is shown in the verification pending page.	Up to 20000 characters

**Table 25:** *Guest Portal Localization*

Data Pane Content	Description	Allowed Length of Text
<b>Verification email notice message</b>	Enter a custom text for the <b>Verification Email Notice</b> message. This is the message notifying the user when the email will be sent.	Up to 20000 characters
<b>Verification email sent message</b>	Enter a custom text for the <b>Verification Email Sent</b> message.	Up to 20000 characters
<b>Verification phone notice message</b>	Enter a custom text for the <b>Verification Phone Notice</b> message. This is the message notifying the user that an SMS has been sent.	Up to 20000 characters
<b>Verified account message</b>	Enter a custom text for the <b>Verified Account</b> message. This is the message that will be shown in the Verified page.	Up to 20000 characters
<b>Verify account message</b>	Enter a custom text for the <b>Verify Account</b> message. This is the message that will be shown in the Verify page.	Up to 20000 characters
<b>Verify button title</b>	Enter a custom label text for the <b>Verify</b> button.	1-255 characters
<b>Verify title</b>	Enter a custom text for <b>Verify</b> title.	1-255 characters
<b>Network login message</b>	Enter a custom text message to show in the <b>Network Login</b> page.	Up to 20000 characters

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

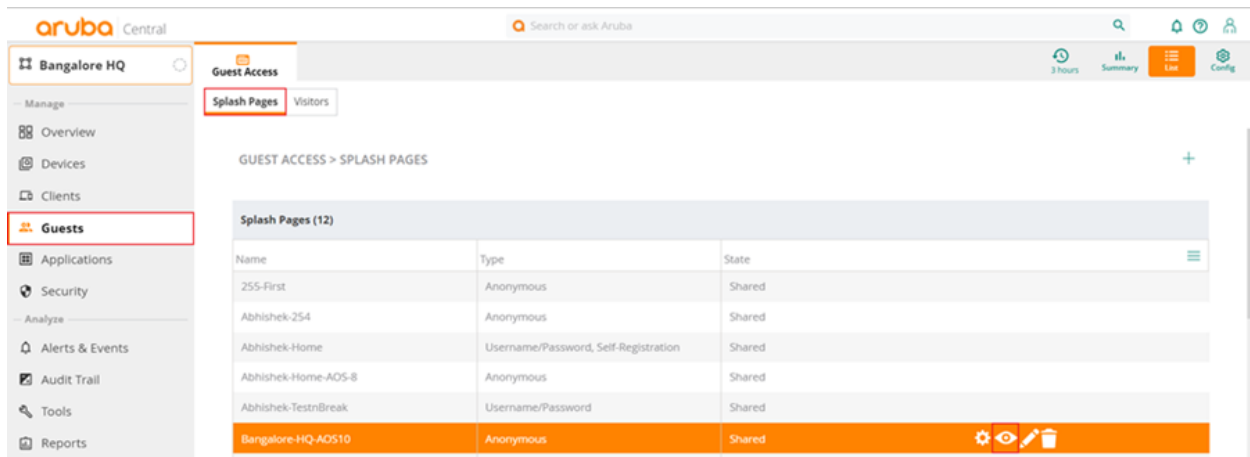
## Previewing and Modifying a Splash Page Profile

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

1. In the **Aruba Central** app, set the filter to a group.  
The dashboard context for the group is displayed.
2. Under **Manage**, click **Guests**.  
The **Guest Access > Splash Pages** page is displayed.
3. Ensure that the pop-up blocker on your browser window is disabled.
4. Hover over the splash profile you want to preview and click the preview icon. The Splash Page is displayed in a new window.



**Figure 27** *Splash Pages Tab*



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

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

## Associating a Splash Page Profile to an SSID

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

1. In the **Aruba Central** app, set the filter to a group.  
The dashboard context for the group is displayed.
2. Under **Manage**, click **Device > Access Points**.
3. Click the **Config** icon.
4. Under **WLANS**, click **+Add SSID**.
5. The **Create a New Network** pane is displayed.

### How do I create an Aruba Central MSP account?

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

- Sign up for Aruba Central evaluation [here](#).
- Enable MSP mode. You can enable the MSP mode in the HPE GreenLake portal. For more information, see the [HPE GreenLake documentation](#).

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

No. With MSP mode enabled, the MSP administrator manages the creation and deletion of tenant accounts. After a tenant account is created, the MSP administrator can add tenant users to the account. To create a tenant user, the MSP administrator must provide a valid email address for the user. A verification email is sent to this email address.

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

### Who owns the hardware and subscriptions?

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

### Can existing Aruba Central customers migrate to an MSP account?

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

### What are the supported devices and architectures?

MSP supports all devices and architectures supported by Aruba Central.

See [Supported Instant APs](#) and [Supported AOS-S Platforms](#).

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.

## What happens to a device on Aruba Central when it's subscription expires ?

When the subscription assigned to a device on Aruba Central expires and auto-subscribe is not enabled for the device, there is a 30-day grace period from the date of expiration during which the device continues to operate within the Aruba Central application instance. If no new subscription is assigned to the device by the end of its grace period, the device is removed from the application instance and transferred to the **Device Inventory** in HPE GreenLake platform.

## Which group is the default group for the tenant account?

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

## What are predefined user roles?

The HPE GreenLake portal allows you to configure the following types of users with system-defined roles. For more information, see the **Assignments** section in the HPE GreenLake Edge to Cloud Platform User Guide, using the following link:

<https://www.arubanetworks.com/techdocs/central/latest/content/nms/intro-pages/related-info.htm>

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

User Role	Standard Enterprise Mode	MSP Mode
	<ul style="list-style-type: none"> <li>Can configure visitor accounts for the cloud guest splash page profiles.</li> </ul>	<ul style="list-style-type: none"> <li>Can configure visitor accounts for the cloud guest splash page profiles.</li> </ul>

## What are custom user roles?

The user roles can be created in the HPE GreenLake Portal. Along with the predefined user roles, you can 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 HPE GreenLake portal.

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.

## 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.