HPE Aruba Networking Central MSP User Guide

Hewlett Packard Enterprise

Open Source Code

This product includes code licensed under certain open source licenses which require source compliance. The corresponding source for these components 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, please check if the code is available in the HPE Software Center at https://myenterpriselicense.hpe.com/cwp-ui/software but, if not, send a written request for specific software version and product for which you want the open source code. Along with the request, please send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
WW Corporate Headquarters
1701 E Mossy Oaks Rd, Spring, TX 77389
United States of America

HPE aruba networking

Contents

Chapter 1
About This Document

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

Intended Audience

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

Related Documents

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

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

Conventions

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

Table 1: *Typographical Conventions*

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

The following informational icons are used throughout this guide:

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

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

WARNING

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

Chapter 2

About HPE Aruba Networking Central

HPE Aruba Networking Central is a powerful cloud networking solution that offers simplicity for today's networks. As the management and orchestration console for ESP (Edge Services Platform), HPE Aruba Networking Central provides a single point of control to oversee all aspects of wired and wireless LANs, WANs, and VPNs across campus, branch, and remote office locations.

AI-powered analytics, end-to-end orchestration and automation, and advanced security features are built into the solution. Live upgrades, robust reporting, and live chat support are also included, bringing more efficiency in day-to-day maintenance activities.

Built on a cloud-native, micro services architecture, HPE Aruba Networking Central delivers on enterprise requirements for scale and resiliency, but is also driven by intuitive workflows and dashboards that make it a perfect fit for SMBs with limited IT personnel. So, whether you have one business location or several, IT can spend less time on managing network infrastructure and more time on creating value for the business.

Key Features

Listed below are some of the key features of HPE Aruba Networking Central:

- Unified management of wireless, wired, VPN, and SD-WAN for simplified operations.
- AI-based insights for faster troubleshooting and continuous network optimization.
- Integration with UXI to proactively monitor and improve the end-user experience.
- Advanced IDS/IPS threat defense management.
- Powerful monitoring and troubleshooting for remote or home office networks.
- APIs and webhooks for ease of integration with other leading IT platforms.
- Live Chat and an AI-based search engine for an enhanced support experience.
- SaaS, on-premises, and managed service options for flexible consumption and financing.

Central Key Terms

Before getting started with configuring, it is important to understand some important configuration concepts and terminology. The following topics are discussed in this section:

- **Cluster Zone**—Refers to an deployment area within a specific region. In other words, cluster zones are regional grouping of one or more container instances on which is deployed. Cluster zones allow your deployments to restrict customer data to a specific region and plan time zone specific maintenance windows. Each cluster zone has separate URLs for signing up for , accessing portal, and for allowing devices to communicate with . To view the zone in UI, click the User Settings menu at the bottom of the left navigation pane.

- **Enterprise Mode**—Refers to the solution deployment mode in which the customers provision, manage, and maintain their networks end-to-end for their respective organizations or businesses.
- **Managed Services Mode**—Refers to the deployment mode in which the service providers, resellers, administrators, and retailers to centrally manage and monitor multiple tenant or end-customer accounts from a single management interface.
- **Evaluation Account**—Refers to the account created for evaluating solution and its services.
- **Paid Subscriber**—Refers to the customers who have purchased a subscription to obtain access to and its services.
- **Customer ID**—Refers to the identity number of your account.
- **Zero Touch Provisioning**—Refers to one of the following:Zero Touch Provisioning (ZTP) of accounts— When you purchase a subscription key and add this subscription key in , queries the Activate database to retrieve the devices mapped to your purchase order and add these devices to the inventory. This process is referred to as zero touch provisioning in .Zero Touch Provisioning of Devices—Most devices support self-provisioning; that is, when you connect a device to a provisioning network, it can automatically download provisioning parameters from the Activate server and connect to their management entity.
- **Onboarding**—You can view, manage, and onboard all the devices in your account using the Devices option in HPE GreenLake platform.
- For more information, see the **Devices** section in the HPE GreenLake Edge to Cloud Platform User Guide.
- **Device Sync**—Refers to the process of synchronizing devices from the Activate database. The device sync operation allows to retrieve devices from Activate and automatically add these devices to the device inventory in .
- **Provisioning**—Refers to the process of setting up a device for deploying networks as per the configuration requirements of your organization.
- **Group**—Refers to the device configuration container in . You can combine devices with common configuration requirements into a single group and apply the same configuration to all the devices in that group.
- **Site**— Refers to the physical locations where devices are installed. Organizing devices per sites allows you to filter your dashboard view per site.
- **Label**—Refers to the tags used for logically grouping devices based on various parameters such as ownership, specific areas within a site, departments, and so on.
- **Standard Enterprise mode**—Refers to the 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 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 mode. Each tenant is an independent instance of .
- **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 mode. The administrator can create a tenant account.
- **SSIDs**—Wireless networks are identified using a service set identifier (SSID). The SSIDs distinguish a wireless network from other networks configured within a WLAN boundary. HPE Aruba Networking uses the SSIDs of APs to orchestrate and configure a number of management policies. For more information, see About HPE Aruba Networking Central.
- **Traffic Forwarding Modes**—Depending on the type of WLAN setup, the SSIDs are also used to specify the traffic forwarding modes. AOS-10 supports automated workflows to set up these SSID profiles. For more information, see About HPE Aruba Networking Central.
- **Supported Authentication Methods**—In creating the SSID profiles in the automated workflows, you must specify an authentication method. AOS-10 supports a number of authentication methods and each is recommended for a specific deployment type. For more information, see About HPE Aruba Networking Central.
- **Supported Encryption Methods**—In creating the SSID profiles in the automated workflows, you must specify an encryption method. AOS-10 supports a number of encryption methods and each is recommended for a specific deployment type. For more information, see About HPE Aruba Networking Central.
- **Cloud-Assisted Roaming Services**—The Cloud-Assisted Roaming Services feature facilitates fast roaming of 802.11r and Opportunistic Key Caching (OKC) clients, to enable seamless roaming with minimal or no disruption to the application traffic such as voice and video. For more information, see About HPE Aruba Networking Central.
- **Cloud-Assisted Roaming Services**—The Cloud-Assisted Roaming Services feature facilitates fast roaming of 802.11r and Opportunistic Key Caching (OKC) clients, to enable seamless roaming with minimal or no disruption to the application traffic such as voice and video. For more information, see About HPE Aruba Networking Central.
- **Access Rules and Firewall Policies**—The Access Control List (ACL) is a logic that handles stateless inspection of traffic. An ACL is used in many types of implementations including routing policies and user policies. A firewall is a device that performs stateful inspection of traffic (checks for encapsulation) passing through a part of the network and decides whether to allow or deny the traffic. You can configure both ACLs and firewall policies on APs and Gateways. For more information, see About HPE Aruba Networking Central.
- **User Roles and VLANs**—A client connecting to a WLAN SSID that is broadcast by an AP is assigned a user role or VLAN to define the client's network privileges, the frequency of re-authentication, and the applicable bandwidth contracts. For more information, see About HPE Aruba Networking Central.
- **Supported Device Configuration Methods in HPE Aruba Networking Central**—In order to configure the management layer, HPE Aruba Networking Central supports a number of configuration options that includes UI workflows, templates, and APIs. For more information, see Device Configuration Methods in HPE Aruba Networking Central.

Device Configuration Methods in HPE Aruba Networking Central

HPE Aruba Networking Central offers the following options for configuring devices in your account:

- **Groups**—You can use the Groups feature to create a logical subset of devices. If you have devices that must share common configuration settings, ensure that you assign these devices to the same

group. Any new device joining a group inherits the configuration that is already applied on the devices in a group.

- **Device-specific configuration**—If you have fewer devices that do not have the same configuration requirements, you can apply configuration changes at the device level. In some cases, although the devices are assigned to a group, you may want to have a slightly different configuration on one specific device in a group. In such cases, you can modify the device configuration and apply changes at the device level.
- **Configuration templates**—You can also leverage the configuration templates feature to quickly deploy. To use a template-based configuration method for APs, ensure that you enable the template-based configuration mode when creating AP groups.
- **APIs**—Allow you to configure and monitor devices using NB APIs.

Operational Modes and Interfaces

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

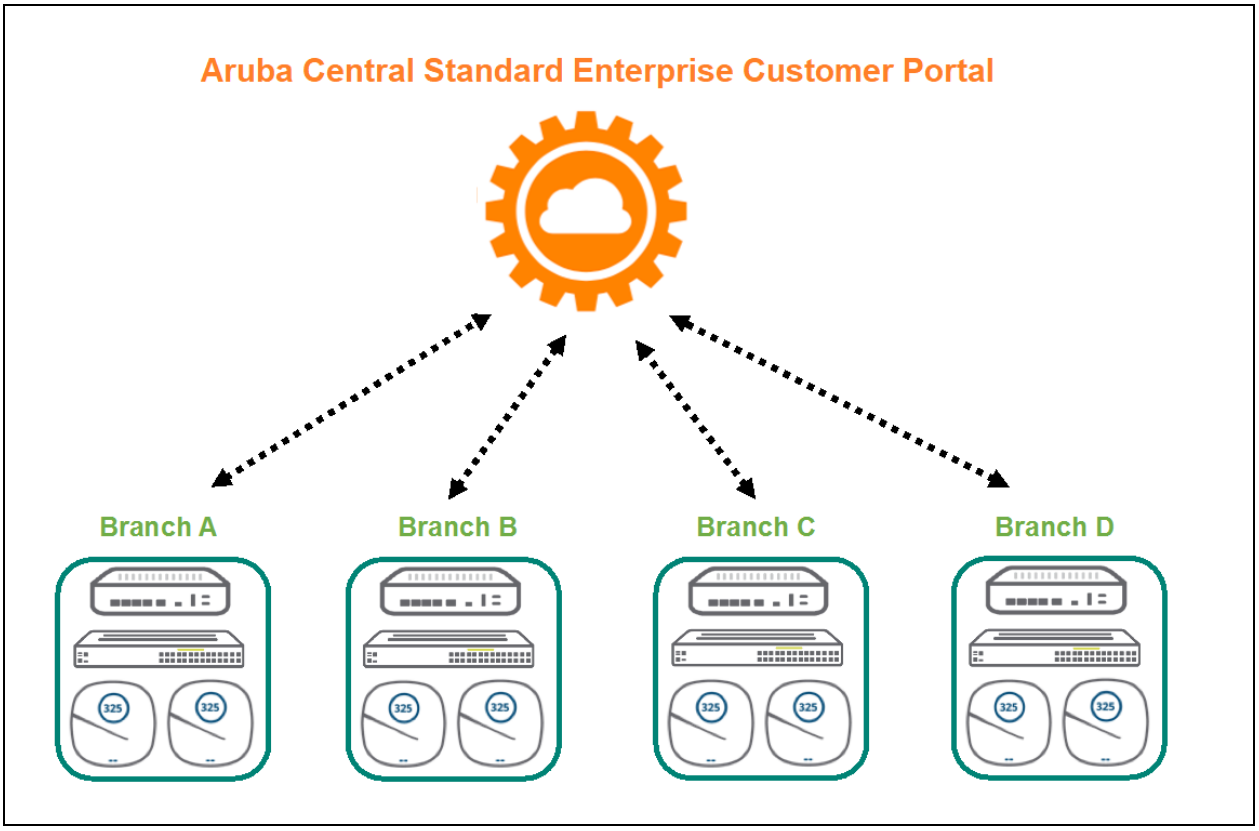
- Standard Enterprise Mode
- Managed Service Provider Mode

Standard Enterprise Mode

Users can manage their respective accounts using the Standard Enterprise interface. 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*

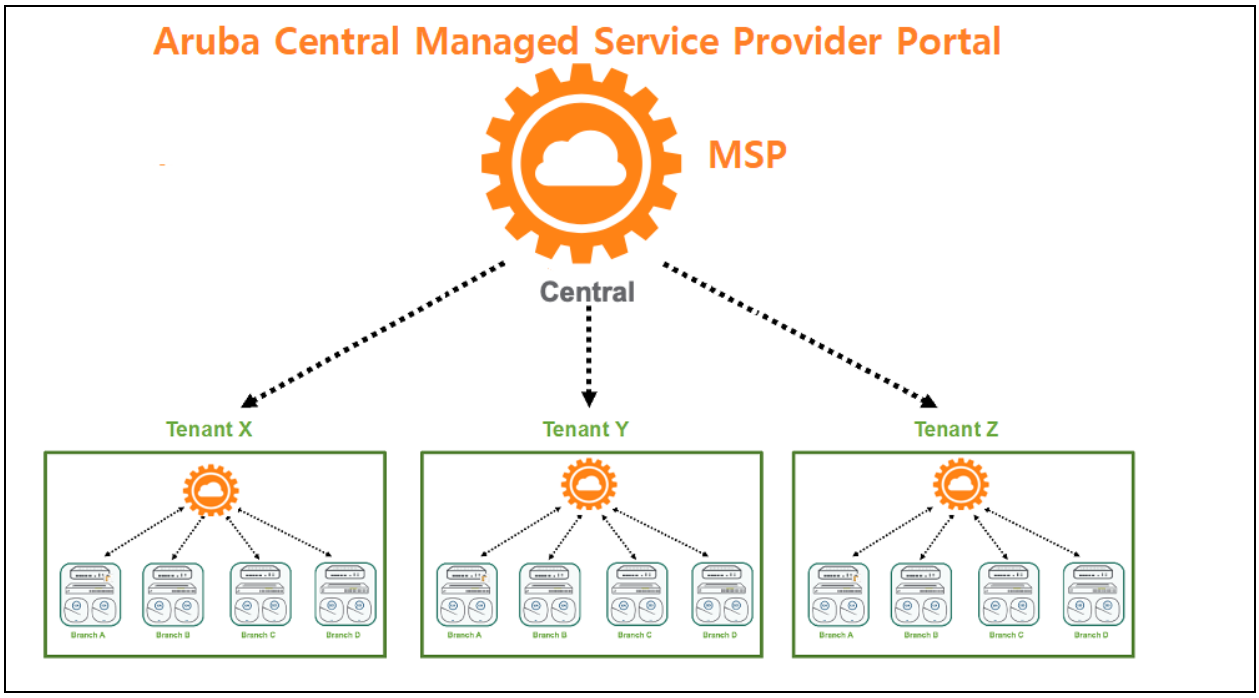


Managed Service Provider Mode

HPE Aruba Networking Central offers the MSP mode for managed service providers who must 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

The following table lists the Instant APs (IAPs), the installation mode, the minimum supported Aruba Instant software releases, and the last supported Aruba Instant software releases.

Table 3: *Supported Instant APs*

AP Model	Installation Mode	Minimum Supported Aruba Instant Software Release	Last Supported Aruba Instant Software Release
AP-679	Outdoor	Aruba Instant 8.12.0.0	N/A
AP-677	Outdoor	Aruba Instant 8.12.0.0	N/A
AP-675	Outdoor	Aruba Instant 8.12.0.0	N/A
AP-655	Indoor	Aruba Instant 8.10.0.0	N/A
AP-635	Indoor	Aruba Instant 8.9.0.0	N/A
AP-615	Indoor	Aruba Instant 8.11.0.0	N/A
AP-605H	Indoor	Aruba Instant 8.12.0.0	N/A
AP-587EX	Outdoor	Aruba Instant 8.10.0.0	N/A
AP-587	Outdoor	Aruba Instant 8.10.0.0	N/A
AP-585EX	Outdoor	Aruba Instant 8.10.0.0	N/A
AP-585	Outdoor	Aruba Instant 8.10.0.0	N/A
AP-584	Outdoor	Aruba Instant 8.10.0.0	N/A
AP-577EX	Outdoor	Aruba Instant 8.7.0.0	N/A
AP-577	Outdoor	Aruba Instant 8.7.0.0	N/A
AP-575EX	Outdoor	Aruba Instant 8.7.0.0	N/A
AP-575	Outdoor	Aruba Instant 8.7.0.0	N/A

AP Model	Installation Mode	Minimum Supported Aruba Instant Software Release	Last Supported Aruba Instant Software Release
AP-574	Outdoor	Aruba Instant 8.7.0.0	N/A
AP-567EX	Outdoor	Aruba Instant 8.7.1.0	N/A
AP-567	Outdoor	Aruba Instant 8.7.1.0	N/A
AP-565EX	Outdoor	Aruba Instant 8.7.1.0	N/A
AP-565	Outdoor	Aruba Instant 8.7.1.0	N/A
AP-555	Indoor	Aruba Instant 8.5.0.0	N/A
AP-535	Indoor	Aruba Instant 8.5.0.0	N/A
AP-534	Indoor	Aruba Instant 8.5.0.0	N/A
AP-518	Indoor	Aruba Instant 8.7.0.0	N/A
AP-515	Indoor	Aruba Instant 8.4.0.0	N/A
AP-514	Indoor	Aruba Instant 8.4.0.0	N/A
AP-505H	Indoor	Aruba Instant 8.7.0.0	N/A
AP-505	Indoor	Aruba Instant 8.6.0.0	N/A
AP-504	Indoor	Aruba Instant 8.6.0.0	N/A
AP-503H	Indoor	Aruba Instant 8.7.1.0	N/A
AP-503	Indoor	Aruba Instant 8.11.1.0	N/A
AP-387	Outdoor	Aruba Instant 8.4.0.0	Aruba Instant 8.10.0.x
AP-377EX	Outdoor	Aruba Instant 8.3.0.0	N/A
AP-377	Outdoor	Aruba Instant 8.3.0.0	N/A
AP-375ATEX	Outdoor	Aruba Instant 8.8.0.0	N/A
AP-375EX	Outdoor	Aruba Instant 8.3.0.0	N/A
AP-375	Outdoor	Aruba Instant 8.3.0.0	N/A
AP-374	Outdoor	Aruba Instant 8.3.0.0	N/A
AP-367	Outdoor	Aruba Instant 6.5.2.0	N/A
AP-365	Outdoor	Aruba Instant 6.5.2.0	N/A
AP-345	Indoor	Aruba Instant 8.3.0.0	Aruba Instant 8.10.0.x

AP Model	Installation Mode	Minimum Supported Aruba Instant Software Release	Last Supported Aruba Instant Software Release
AP-344	Indoor	Aruba Instant 8.3.0.0	Aruba Instant 8.10.0.x
IAP-335	Indoor	Aruba Instant 6.5.0.0	Aruba Instant 8.10.0.x
IAP-334	Indoor	Aruba Instant 6.5.0.0	Aruba Instant 8.10.0.x
IAP-325	Indoor	Aruba Instant 6.4.4.0	Aruba Instant 8.10.0.x
IAP-324	Indoor	Aruba Instant 6.4.4.0	Aruba Instant 8.10.0.x
AP-318	Indoor	Aruba Instant 8.3.0.0	N/A
IAP-315	Indoor	Aruba Instant 6.5.0.0	N/A
IAP-314	Indoor	Aruba Instant 6.5.0.0	N/A
IAP-305	Indoor	Aruba Instant 6.5.1.0	N/A
IAP-304	Indoor	Aruba Instant 6.5.1.0	N/A
AP-303P	Indoor	Aruba Instant 8.4.0.0	N/A
AP-303H	Indoor	Aruba Instant 6.5.2.0	N/A
AP-303	Indoor	Aruba Instant 8.3.0.0	N/A
IAP-277	Outdoor	Aruba Instant 6.4.0.0	Aruba Instant 8.6.0.x
IAP-275	Outdoor	Aruba Instant 6.4.0.0	Aruba Instant 8.6.0.x
IAP-274	Outdoor	Aruba Instant 6.4.0.0	Aruba Instant 8.6.0.x
IAP-228	Outdoor	Aruba Instant 6.4.0.0	Aruba Instant 8.6.0.x
IAP-207	Indoor	Aruba Instant 4.3.1.0	Aruba Instant 8.10.0.x
AP-203RP	Indoor	Aruba Instant 6.5.2.0	Aruba Instant 8.10.0.x
AP-203R	Indoor	Aruba Instant 6.5.2.0	Aruba Instant 8.10.0.x
AP-203H	Indoor	Aruba Instant 6.5.2.0	Aruba Instant 8.10.0.x

- HPE Aruba Networking USB LTE modem is supported when connected to APs running Aruba Instant 8.10.0.0 or later versions.
- AP-615, AP-635, and AP-655 APs 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 APs. 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 Access Points in Tri-Radio Mode.
- By default, AP-318, AP-374, AP-375, and AP-377 APs have Eth1 as the uplink port and Eth0 as the downlink port. HPE Aruba Networking Central does not recommend you to upgrade these APs 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.

- 320 Series, 340 Series, and AP-387 access points are not supported from Aruba Instant 8.11.0.0 and later versions. However, you may find the images, Hercules and Draco, available for download. They are meant for installation only on platforms supported by Aruba Instant 8.11.0.0 version. Attempting to install Aruba Instant 8.11.0.x firmware on the aforementioned APs may cause these APs to disconnect themselves from the current cluster and form a new cluster running the software version available in the partition. Therefore, ensure that 320 Series, 340 Series, and AP-387 access points are removed from the cluster before upgrading it to Aruba Instant 8.11.0.0 version.
- For more information about HPE Aruba Networking's End-of-life policy, see https://www.arubanetworks.com/support-services/end-of-life/end-of-life-policy/.
- For end of life timelines for hardware or software, see https://networkingsupport.hpe.com/notifications.
- For data sheets and technical specifications for the supported AP platforms, see https://www.arubanetworks.com/products/networking/access-points/.

Supported AOS-S Platforms

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

- HPE Aruba Networking 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 HPE Aruba Networking 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.
- If the switches are managed in UI groups, it is not recommended to change the AOS-S switches firmware from latest version to earlier major versions. For features that are not supported or not managed in HPE Aruba Networking 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 HPE Aruba Networking Central, and switch stacking details.

Table 4: *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 or Template)
Aruba 2530 Switch Series	▪ YA/YB.16.08.0021 and later ▪ YA/YB.16.09.0016 and later ▪ YA/YB.16.10.0012 and later ▪ YA/YB.16.11.0002 and later	▪ YA/YB.16.08.0027 ▪ YA/YB.16.09.0022 ▪ YA/YB.16.10.0025 ▪ YA/YB.16.11.0015	N/A	N/A	N/A
Aruba 2540 Switch Series	▪ YC.16.08.0019 and later ▪ YC.16.09.0015 and later ▪ YC.16.10.0012 and later ▪ YC.16.11.0002 and later	▪ YC.16.08.0027 ▪ YC.16.09.0022 ▪ YC.16.10.0025 ▪ YC.16.11.0015	N/A	N/A	N/A
Aruba 2930F Switch Series	▪ WC.16.08.0019 and later ▪ WC.16.09.0015 and later ▪ WC.16.10.0011 and later ▪ WC.16.11.0002 and later	▪ WC.16.08.0027 ▪ WC.16.09.0022 ▪ WC.16.10.0025 ▪ WC.16.11.0015	Yes **Switch Software Dependency**: ▪ WC.16.08.0019 and later ▪ WC.16.09.0015 and later ▪ WC.16.10.0012 and later ▪ WC.16.11.0002 and later	VSF	UI and Template
Aruba 2930M Switch Series	▪ WC.16.08.0019 and later ▪ WC.16.09.0015 and later ▪ WC.16.10.0012 and later ▪ WC.16.11.0002 and later	▪ WC.16.08.0027 ▪ WC.16.09.0022 ▪ WC.16.10.0025 ▪ WC.16.11.0015	Yes **Switch Software Dependency**: ▪ WC.16.08.0019 and later ▪ WC.16.09.0015 and later ▪ WC.16.10.0012 and later ▪ WC.16.11.0002 and later	BPS	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 or Template)
Aruba 3810 Switch Series	▪ KB.16.08.0019 and later ▪ KB.16.09.0015 and later ▪ KB.16.10.0012 and later ▪ KB.16.11.0002 and later	▪ KB.16.08.0027 ▪ KB.16.09.0022 ▪ KB.16.10.0025 ▪ KB.16.11.0015	Yes **Switch Software Dependency**: ▪ KB.16.08.0019 and later ▪ KB.16.09.0015 and later ▪ KB.16.10.0012 and later ▪ KB.16.11.0002 and later	BPS	UI and Template
Aruba 5400R Switch Series	▪ KB.16.08.0019 and later ▪ KB.16.09.0015 and later ▪ KB.16.10.0012 and later ▪ KB.16.11.0002 and later	▪ KB.16.08.0027 ▪ KB.16.09.0022 ▪ KB.16.10.0025 ▪ KB.16.11.0015	Yes **Switch Software Dependency**: ▪ KB.16.08.0019 and later ▪ KB.16.09.0015 and later ▪ KB.16.10.0012 and later ▪ KB.16.11.0002 and later	VSF	Template only

Provisioning and configuring of Aruba 5400R switch series and switch stacks are supported only through configuration templates. HPE Aruba Networking 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 HPE Aruba Networking Central.

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

Accessing HPE Aruba Networking Central

You can access HPE Aruba Networking Central from the HPE GreenLake portal.

For more information about accessing and navigating through the HPE GreenLake portal, see the **Applications** section in the *HPE GreenLake Edge to Cloud Platform User Guide*, using the following link:

https://support.hpe.com/hpesc/public/docDisplay?docId=a00120892en_us

1. To access the **HPE Aruba Networking Central** app from the HPE GreenLake home page, click **Applications** in the top navigation.

   The **My Applications** page is displayed.

2. In the **Choose Region** drop-down list, select **All Regions** or the region in which you want to access the WebUI.
3. Click the application.

   The **Deployment Regions** page is displayed.
4. Click **Launch**.

Logging Out of HPE Aruba Networking Central

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

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

Chapter 4
MSP Deployment Models

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 HPE Aruba Networking Central account.
- Onboard devices.
- Assign device to tenant and apply subscriptions.

MSPs can provide Network as a Service to end-customers using HPE Aruba Networking Central MSP mode capabilities. HPE Aruba Networking 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 HPE Aruba Networking 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. HPE Aruba Networking 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:

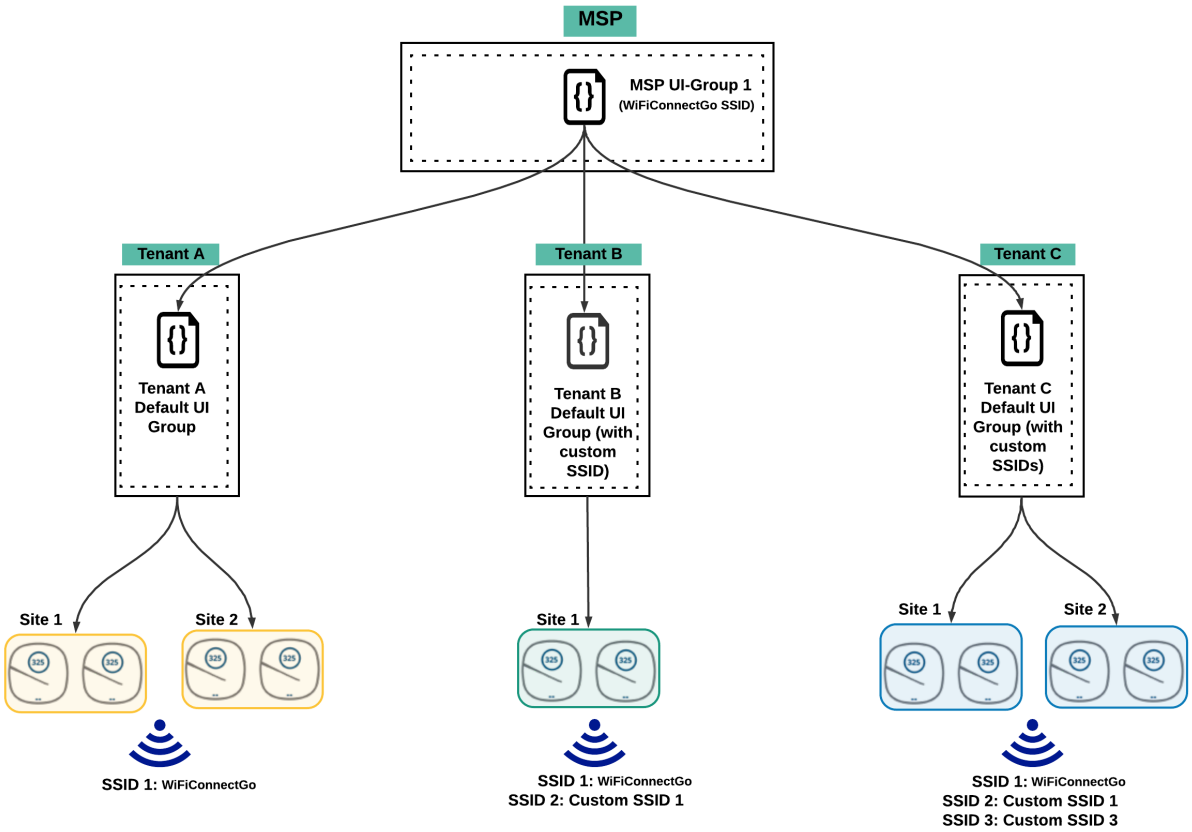
- **WiFiConnectGo**—In this program, for a monthly fee per Instant AP, customers part of this program agree to broadcast MSP's free public WiFi SSID **WiFiConnectGo**. Customers can add up to 15 additional custom SSIDs, including guest, of their own. Tenant account administrators are responsible for 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*

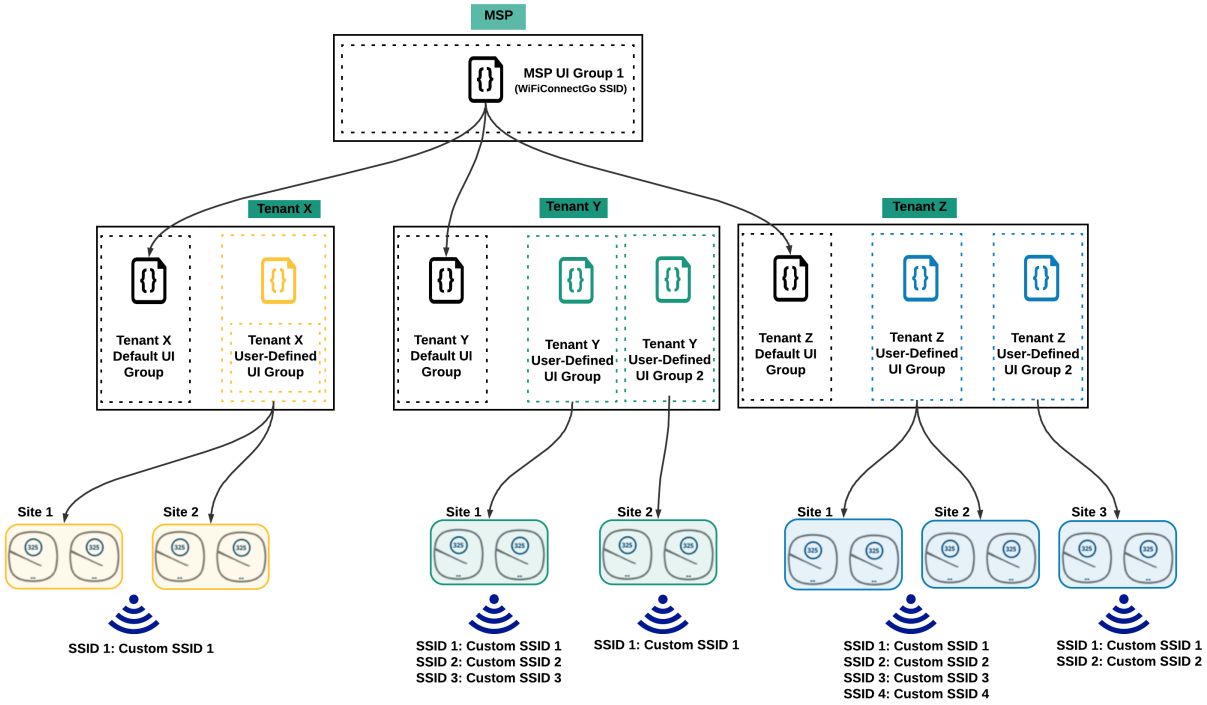


Configuring WiFiConnectGo-Plus Using User-Defined UI Groups

Use this deployment model if your customer deployments are unique and if you wish to use the HPE Aruba Networking 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*

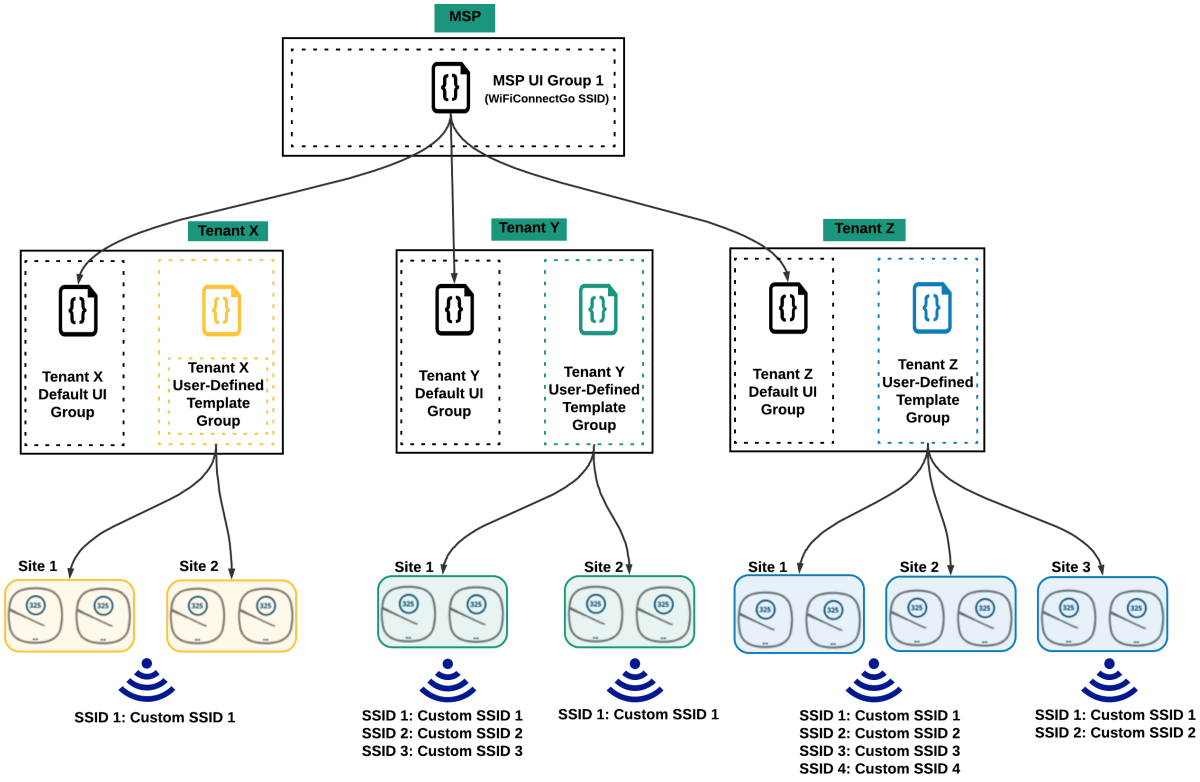


Configuring WiFiConnectGo-Plus Using Template Groups

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 HPE Aruba Networking CLIs and HPE Aruba Networking Central APIs.

Figure 5 *MSP Deployment Using Template Groups*



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

NOTE

HPE Aruba Networking recommends that you contact your HPE Aruba Networking Central sales representative or the HPE Aruba Networking Central Support team if you are an MSP proposing this model to your end-customer.

Please contact your HPE GreenLake sales representative or your HPE HPE Aruba Networking account manager to enable this feature in your HPE GreenLake workspace. Managing tenants who own devices and subscriptions is an allow-listed feature.

In this model, the end-customer owns both the devices and subscriptions, but the MSP manages the end-customer's network. MSP can use the HPE Aruba Networking Central MSP mode to have the capability of managing the tenant who owns both devices and subscriptions. Managing tenants who own devices and subscriptions is an allow-listed feature.

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, MSP requires to set up and provision the tenant account.

MSP can use HPE Aruba Networking Central MSP mode to have the capability of managing the tenant who owns both devices and subscriptions. Managing tenants who own devices and subscriptions is an allow-listed feature. The HPE Aruba Networking Central MSP mode functionality enables the seamless onboarding of devices and subscriptions into the tenant workspace. For detailed instructions on creating a new tenant account, please refer the *HPE GreenLake Edge to Cloud Platform User Guide*, using the following link- https://support.hpe.com/hpesc/public/docDisplay?docId=a00120892en_us.

In the HPE Aruba Networking Central MSP dashboard, the total device count, device trends data is based only on the MSP owned devices and subscriptions allocated to Customers.
The MSP Reports data is based on the MSP owned devices and subscriptions.

Monitoring and Reporting

MSP provides Network as a Service to end-customers in a single pane view using HPE Aruba Networking Central MSP mode. HPE Aruba Networking Central provides simplified provisioning and monitoring. The MSP administrator manages the tenant network, performs device management and monitoring using the HPE Aruba Networking Central MSP dashboard.

Managing Firmware and Maintenance

The MSP have the option 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 for all tenant accounts. 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, HPE Aruba Networking 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 HPE Aruba Networking 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. MSP can use the HPE Aruba Networking Central MSP mode to have the capability of managing the tenant who owns both devices and subscriptions. Managing tenants who own devices and subscriptions is an allow-listed feature. This functionality enables the seamless onboarding of devices and subscriptions into the tenant workspace. For detailed instructions on creating a new tenant account, please refer the *HPE GreenLake Edge to Cloud Platform User Guide*, using the following link- https://support.hpe.com/hpesc/public/docDisplay?docId=a00120892en_us.

NOTE

In the HPE Aruba Networking Central MSP dashboard, the total device count, device trends data is based only on the MSP owned devices and subscriptions allocated to Customers.
The MSP Reports data is based on the MSP owned devices and subscriptions.

NOTE

This is an allow-listed feature. HPE Aruba Networking recommends that you contact your HPE Aruba Networking Central sales representative or yourHPE Aruba Networking Central Account Manager if you are an MSP proposing this model to your end-customer.

Viewing the Network Structure

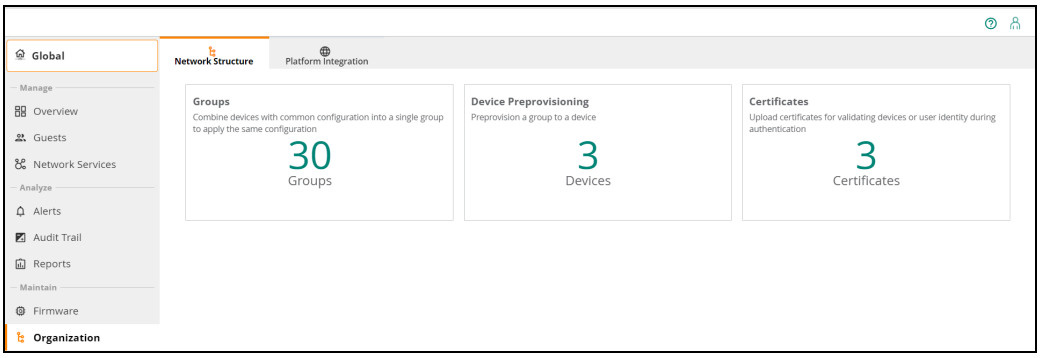
The **Network Structure** page shows tiles view for groups, install manager, and certificates sections. You can click on a tile to navigate to the respective page in HPE Aruba Networking Central.

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

1. In the WebUI, 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

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

1. In the WebUI, use the filter to select **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 5: *Certificate Store Parameters*

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

Uploading Certificates in the MSP Mode

MSP administrators can upload certificates to HPE Aruba Networking 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 WebUI, 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 **Device Certificate**, 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**.

HPE Aruba Networking 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 HPE Aruba Networking Central are now available on the HPE GreenLake platform.

For more information, see the following topics:

- Viewing Devices List
- Assigning Devices to Groups

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 WebUI, 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.

NOTE

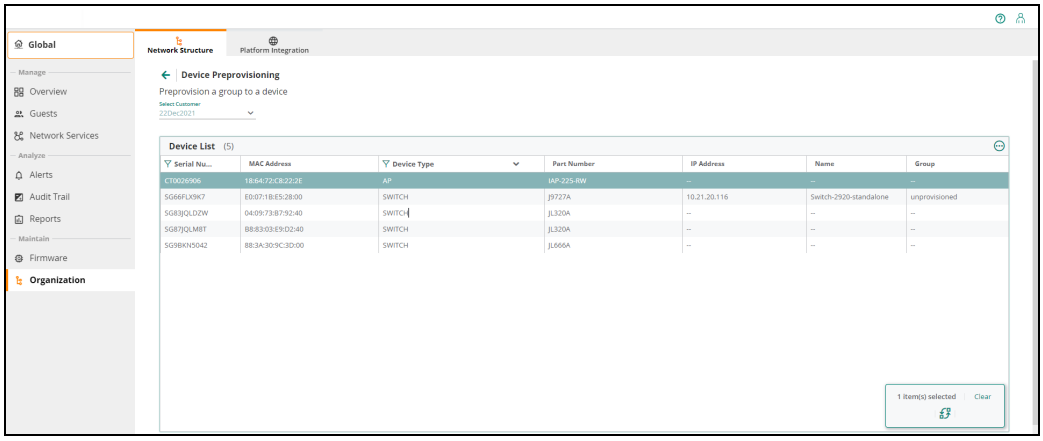
The Device List table will not appear unless you select a tenant in the Select Customer drop-down.

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.

NOTE

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

Table 6: *Device Details*

Parameter	Description
Serial Number	Serial number of the device.
MAC Address	MAC address of the device.
Device Type	Type of device. For example Instant AP, switch, or gateway.
Model	Hardware model of the device.
Part Number	Part number of the device.
IP Address	IP address of the device.
Name	Name of the device.
Group	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 WebUI, 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 HPE Aruba Networking 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-drown 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 HPE Aruba Networking 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:

Accessing HPE Aruba Networking Central

You can now access HPE Aruba Networking Central from HPE GreenLake.

About Provisioning Tenant or Customer Accounts

Create tenant accounts and map to MSP group.

Groups in the MSP Mode

Create MSP groups.

Customizing the Portal in MSP Mode

Customize the tenant account portal.

MSP Certificates

Upload and map certificates.

MSP Dashboard

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 the managed service mode in HPE GreenLake, see Enabling the MSP Mode and Creating your company workspace.

Disabling the Managed Service Mode in HPE GreenLake

To disable the Managed Service mode in HPE GreenLake, see Disabling the MSP mode.

About the Managed Service Portal User Interface

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

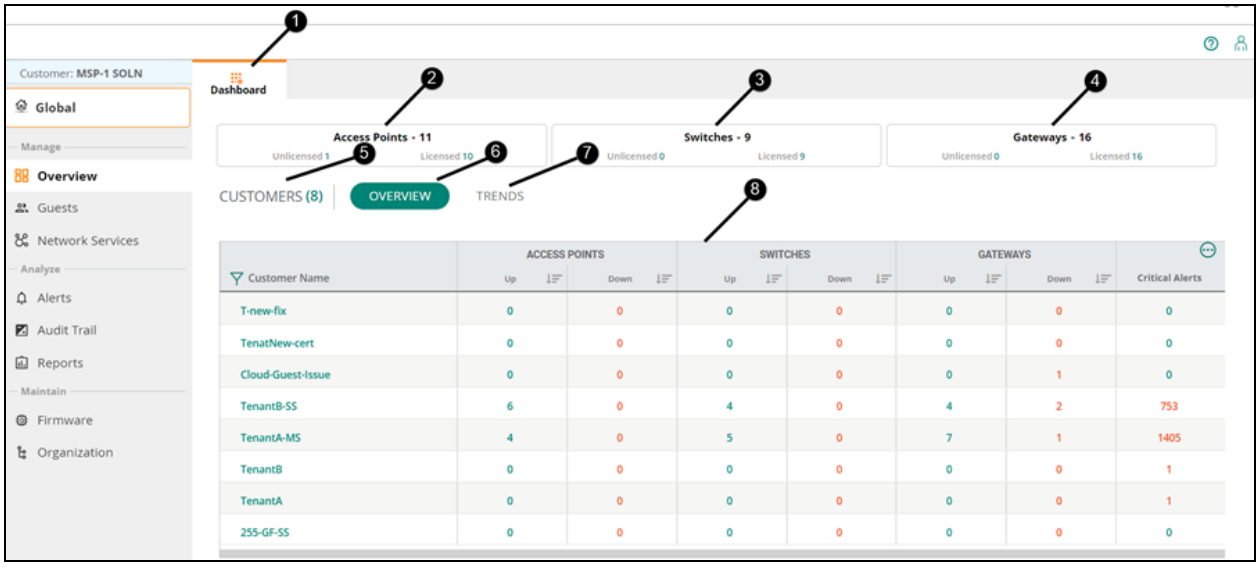
See the following sections:

- MSPDashboard View
- Parts of the WebUI for MSP
- Time Range Filter
- Global Dashboard in MSP Mode
- Group Dashboard in MSP Mode
- Tenant View

MSPDashboard View

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

Figure 8 *Parts of the MSP Dashboard*



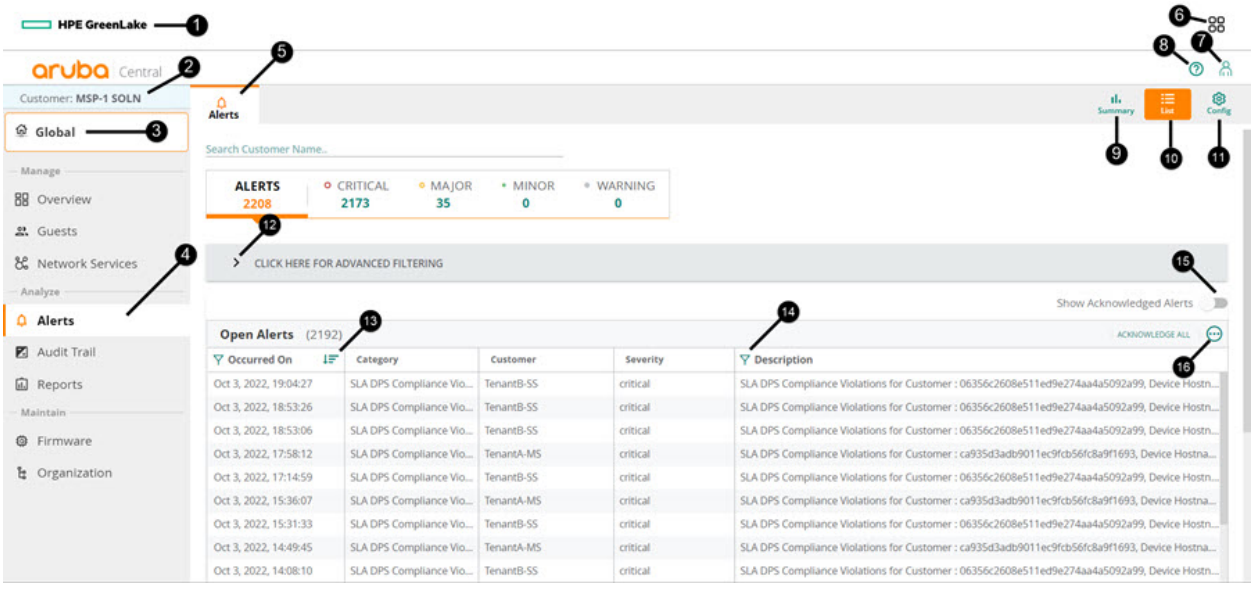
The MSP Dashboard view displays the following information:

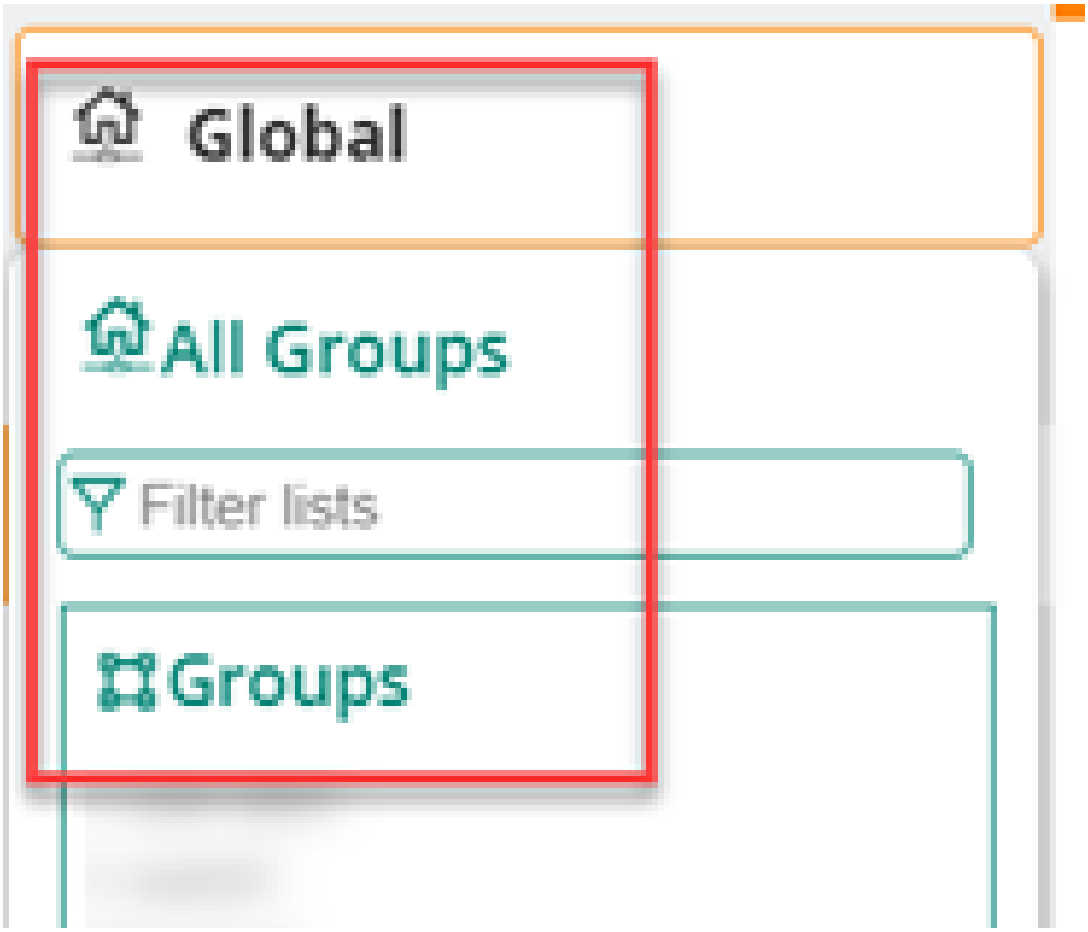
Callout Number	Description
1	First-level tab on dashboard. The dashboard may also have second and third-level tabs based on the filter selection.
2	**Access Points**—The total number of APs assigned to the tenants. **Unlicensed**—Number of APs assigned to the tenants but not licensed. **Licensed**—Number of APs assigned to the tenants and also licensed.
3	**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.
4	**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.
5	**Customers**—Number of tenants in the MSP account.
6	**Overview**—Displays the list of customers, the types of devices assigned to each customer, as well as critical alerts, if any.
7	**Trends**—Displays charts for license renewal, the number of devices under MSP management, and the number of customers added over the last year.
8	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 WebUI for MSP

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

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



Callout Number	Description
1	**HPE GreenLake** icon. Click the icon to go back to the HPE GreenLake portal home page.
2	Displays the customer name.
3	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. 
4	The left navigation pane is a *contextual* menu that displays a number of configuration, monitoring, and troubleshooting options depending on filter value. Menu is dependent on the filter selection.
5	First-level tab on dashboard. The dashboard may also have second and third-level tabs based on the filter selection.
6	**Services** icon. Click the icon to see the links to HPE GreenLake, Cloud Services, Cloud Consoles and HPE Resources.
7	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:

Callout Number	Description
	▪ **User Settings** ◦ **Time Zone**—Displays the zone, date, time, and time zone of the region. ◦ **Language**— Administrators can set a language preference. The HPE Aruba Networking 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 HPE Aruba Networking Central services. ▪ **Logout**—Click to log out of from your account.
8	The help icon contains the following options: ▪ **Tutorials**— Displays the HPE Aruba Networking Central product learning center. ▪ **Feedback**—Allows you to provide feedback on the HPE Aruba Networking 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 HPE Aruba Networking support forum. ▪ **View / Update Case**—Enables you to view or edit an existing support ticket in the HPE Networking Support Portal at https://networkingsupport.hpe.com/home. You must log in to this portal. ▪ **Open New Case**—Enables you to create a new support ticket in the HPE Networking Support Portal at https://networkingsupport.hpe.com/home. You must log in to this portal.
9	Summary icon. Click the **Summary** icon to view a graphical representation of the data. Only applicable for the global dashboard.
10	List icon. Click the **List** icon to view a tabular representation of the data. Only applicable for the global dashboard.
11	Config icon. Click the **Config** icon to enable configuration mode.
12	Accordion icon. Enables you to expand in place to expose some hidden information or fields.
13	Enables you to sort the columns in ascending and descending order.
14	Icon for filtering the data of the selected column. The filter option displays dynamic results for a selected column as soon as you start typing the keyword.
15	Toggle switch. Enables you to change a setting between two states, such as ON and OFF.
16	Icon for selecting or resetting the column headers for the selected page.

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

Global Dashboard in MSP Mode

In the HPE Aruba Networking 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**.

If you are not an administrator for the HPE Aruba Networking Central account, you may not see some tabs in your dashboard view.

Table 7: *Contents of the Global Dashboard in MSP Mode*

Left Navigation Menu	First-Level Tabs	Description
Manage > **Overview**	**Dashboard**	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 MSP Dashboard.

Left Navigation Menu	First-Level Tabs	Description
Manage > **Guests**	**Splash Pages**	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 Configuring a Cloud Guest Splash Page Profile.
Manage > **Network Services**	**Virtual Gateways**	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.
Analyze > **Alerts**	**Alerts**	Displays and configures a list of alerts. This page also enables you to acknowledge these alerts. For more information, see MSP Alerts.
Analyze > **Audit Trail**	**Audit Trail**	Displays the total number logs generated for all device management, configuration, and user management events triggered in HPE Aruba Networking Central. For more information, see MSP Audit Trails.
Analyze > **Reports**	**Reports**	Displays you to create various types of reports. You can create recurrent reports or configure the reports to run on demand. For more information, see MSP Reports.

Left Navigation Menu	First-Level Tabs	Description
Maintain > **Firmware**	**Access Points** **Switch- MAS** **Switches** **Gateways**	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 Firmware Upgrades for MSP Mode.
Maintain **>Organization**	**Network Structure**	Displays the tiles view for groups, install manager, and certificates sections. You can navigate to a specific page in HPE Aruba Networking Central by clicking on a tile. For more information, see Network Structure. ■ **Groups**—A group in HPE Aruba Networking 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 Groups. ■ **Install Manager**—Simplifies and automates site deployments, and helps IT administrators manage site installations with ease.

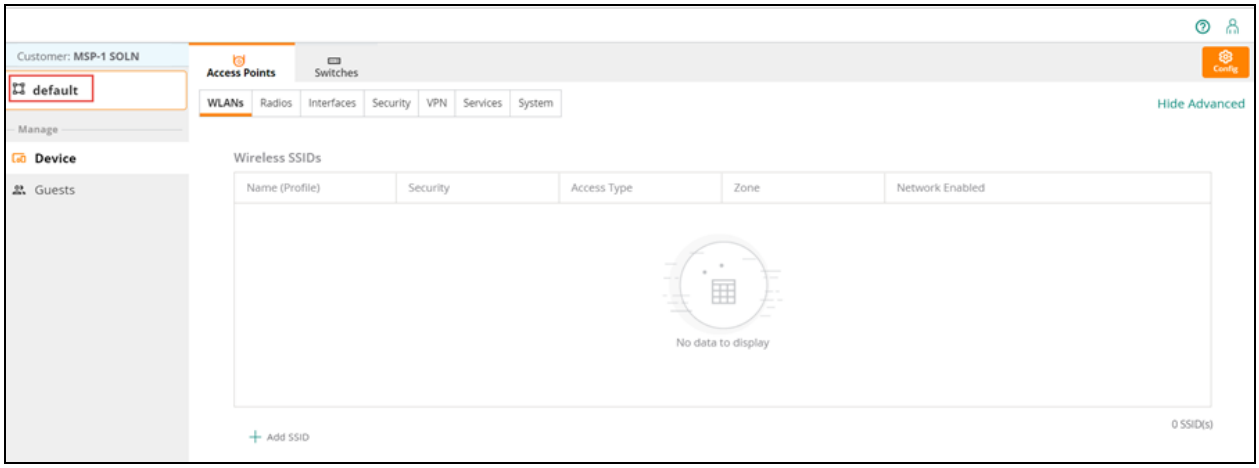
Left Navigation Menu	First-Level Tabs	Description
		■ **Certificates**—Enables administrators to upload a valid certificate signed by a root CA so that devices are validated and authorized to use HPE Aruba Networking Central. For more information, see MSP Certificates. ■ **Device Preprovisioning**—Enables administrators to assign factory default devices to a group. For more information, see Device Preprovisioning in an MSP Account.
	Platform Integration	Displays the tiles view for Data collectors, API Gateway, and Webhooks. You can navigate to a specific page in HPE Aruba Networking Central by clicking on a tile. ■ **API Gateway**—Supports the REST API for all HPE Aruba Networking Central services. This feature allows HPE Aruba Networking Central users to write custom applications, embed, or integrate the APIs with their own applications.

Left Navigation Menu	First-Level Tabs	Description
		▪ **Webhooks**—Webhooks allow you to implement event reactions by providing real-time information or notifications to other applications.

Group Dashboard in MSP Mode

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

Figure 10 *Launching the Group Dashboard for MSP*



NOTE

If you are not an administrator for the HPE Aruba Networking Central account, you may not see some tabs in your dashboard view.

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

Left Navigation Menu	First-Level Tabs	Description
Manage > **Device**	**Access Points** **Switches** **Gateways**	Enables you to configure APs and AOS-S switches for a specific group. For more information, see the HPE Aruba Networking Central documentation for APs, switches and gateways.

Left Navigation Menu	First-Level Tabs	Description
Manage > **Guests**	**Splash Pages**	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 Configuring a Cloud Guest Splash Page Profile.

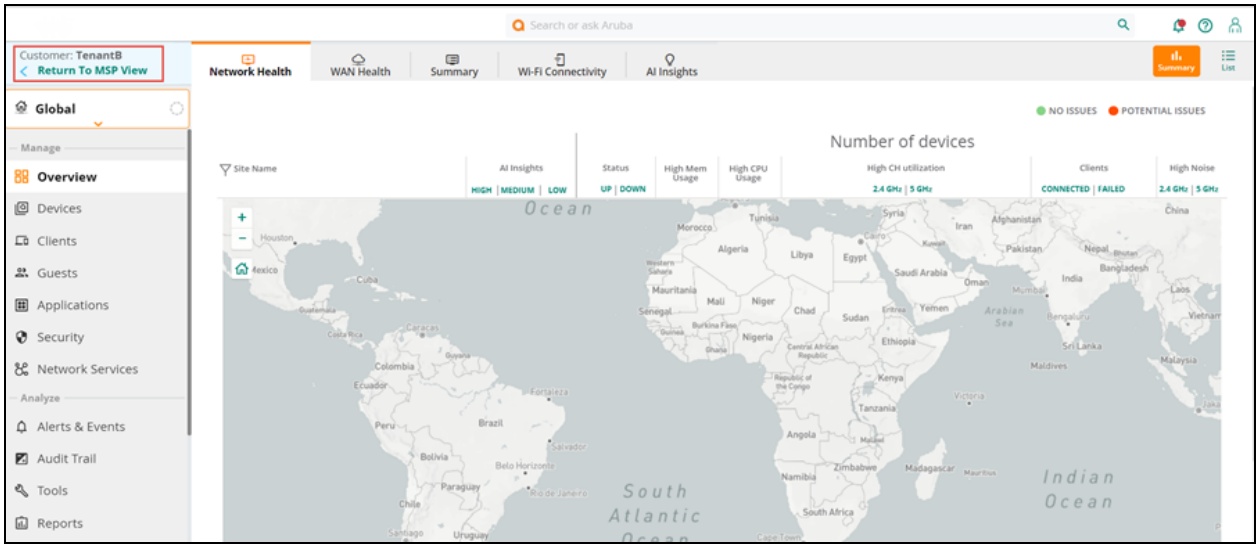
In the group dashboard under the left navigation pane, you can see the **Device** and **Guest** options under **Manage**.

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.

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 11 *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 **Manage** section in the *HPE GreenLake Edge to Cloud Platform User Guide*, using the following link:

https://support.hpe.com/hpesc/public/docDisplay?docId=a00120892en_us.

MSP Tenant Management in HPE GreenLake

The HPE GreenLake portal allows you to create and manage tenant accounts from the customer accounts page. The MSP administrator user can create a tenant account in the HPE GreenLake portal and assign the account to a HPE Aruba Networking Central instance.

For more information, see the topics listed below:

- Creating a Tenant Account
- Assigning a Tenant Account to an HPE Aruba Networking Central Instance
- Mapping a Tenant or Customer Account to MSP Group
- Deleting a Tenant or Customer Account

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 **Customer**.

   The Customer Accounts page is displayed. This page allows you to view and manage customer accounts.

3. Click **Add Customers**.

   The **Create 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 a Tenant Account to an HPE Aruba Networking Central Instance

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

To assign the tenant account to an HPE Aruba Networking 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 **Customers**.

   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 **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 HPE Aruba Networking 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 HPE Aruba Networking Central instance.

Mapping a Tenant or Customer Account to MSP Group

The MSP administrator can edit the customer group for a tenant account . The MSP administrator cannot edit the name or description of the customer account or delete it at the HPE Aruba Networking portal. The MSP administrator can perform these actions at the GLCP portal.

To edit a tenant account, complete the following steps:

1. In the HPE Aruba Networking Central app, complete the following steps:
   a. Set the filter to **Global**.
   b. Under **Manage**, click **Overview**. The **Dashboard** page is displayed.
2. Hover over the **Customer Name** you want to edit.
3. Click the **Edit** icon.
   The **EDIT CUSTOMER GROUP** pop-up is displayed.
4. Enable the **Add to Group** toggle.
5. Select the group you want to map.
6. Click **SAVE**.

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 **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 **Launch**.
   The tenant account dashboard is deleted.
4. Click **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 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 **Customer**.
   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 **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:

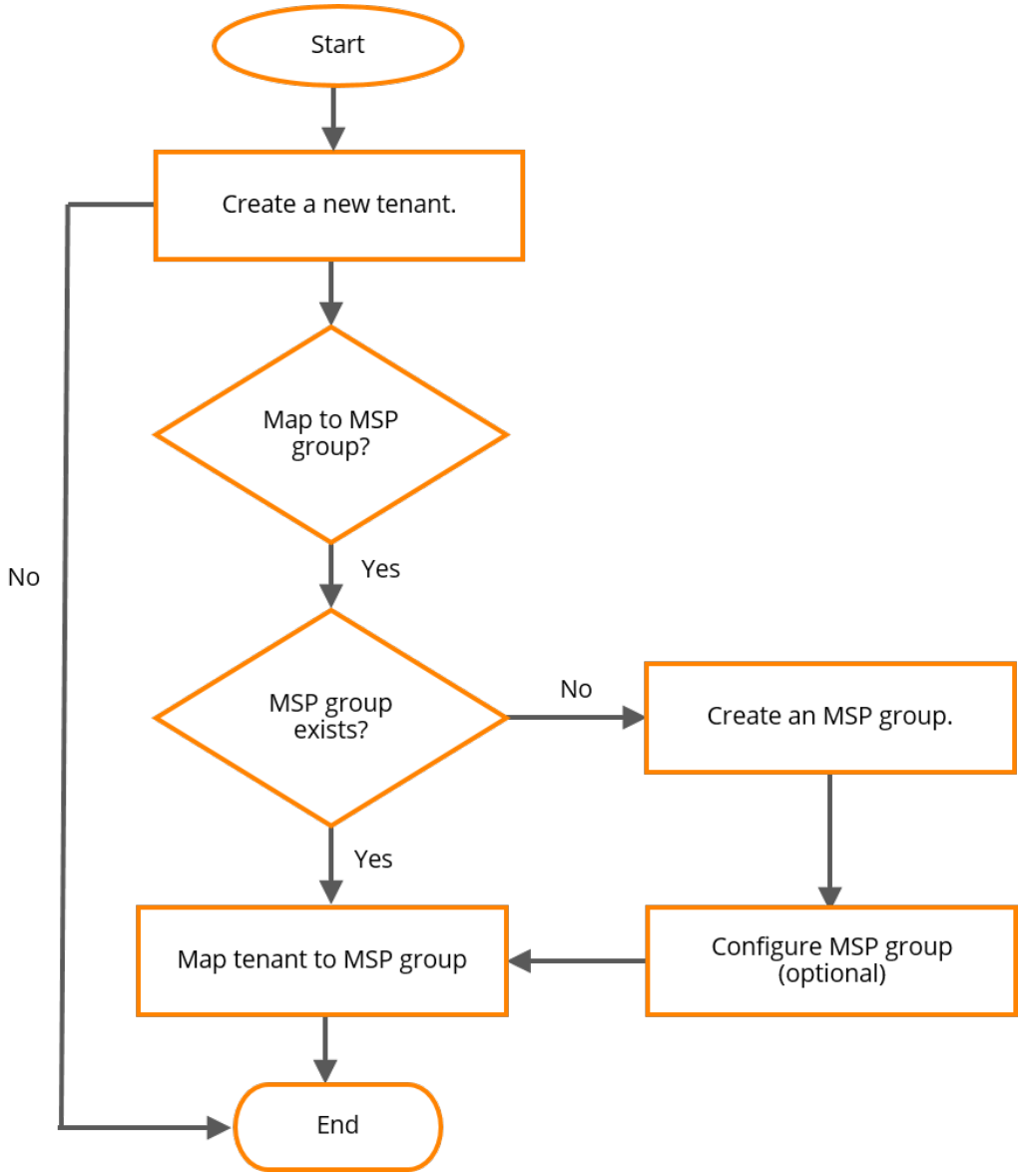
- Flowchart for Tenant Account Mapping in MSP
- Creating a Tenant Account and Mapping to an MSP Group

- 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 12 *Tenant Account Mapping to an MSP Group*



- **Create a new Tenant**—The MSP administrator creates tenant accounts and provisions the tenant accounts to HPE Aruba Networking Central application in the HPE GreenLake portal.

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

  https://support.hpe.com/hpesc/public/docDisplay?docId=a00120892en_us.

- **Map to MSP Group**—The MSP administrator maps the tenant users to an existing group in HPE Aruba Networking Central. For more information, see Groups in the MSP Mode.
- **Create an MSP Group**—The MSP administrator creates MSP groups in HPE Aruba Networking Central (**Organization** > **Groups** > **Add Group**).
- **Configure an MSP Group**—The MSP administrator configures the MSP groups in HPE Aruba Networking 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 Edge to Cloud Platform User Guide*, using the following link- https://support.hpe.com/hpesc/public/docDisplay?docId=a00120892en_us.

Mapping a tenant account to an MSP group is done using the edit tenant account workflow. For more information, see Mapping a Tenant or Customer Account to MSP Group

Viewing Tenant Account Details

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

1. From the WebUI, filter **All Groups**.
2. Under **Manage**, click **Overview** to display the **Dashboard** page.
3. The **Customers** section displays.
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 HPE Aruba Networking Central over a period of time.
- **Description**—Description of the tenant account.
- **Customer Name**—Name of the tenant account.

Devices

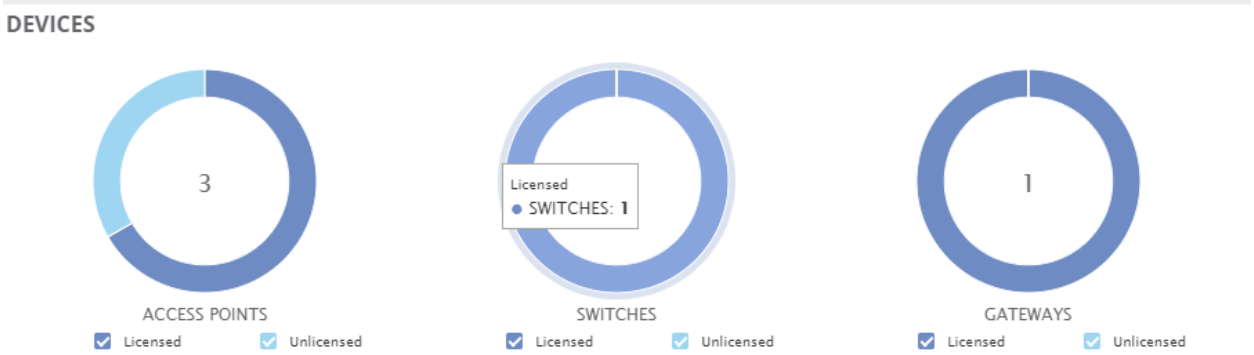
This section is a graphical representation of the devices assigned to the selected tenant account, as well as the licensed and unlicensed count for each device type.

- 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 13 *Devices Section of the Expand Tenant Account Page*



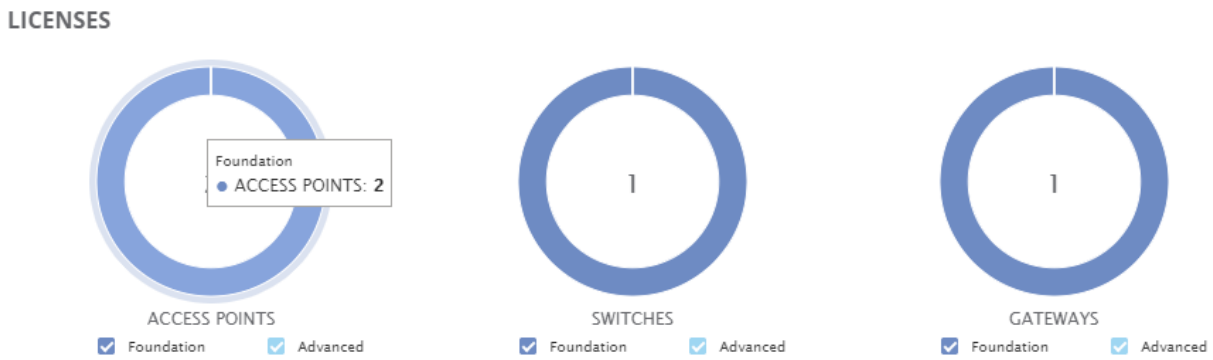
Licenses

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 14 *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 WebUI, 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 Edge to Cloud Platform User Guide*, using the following link- https://support.hpe.com/hpesc/public/docDisplay?docId=a00120892en_u.

Managed Service Mode Operations

This section describes the tenant and device management workflows for the MSP users. See the following topics for more information:

- **MSP Architecture** - You can view this page to understand how HPE Aruba Networking Central provides a cloud-based network management platform for managing your wireless, WAN, and wired networks with HPE Aruba NetworkingInstant APs, Gateways, and Switches.
- **Getting Started** - You can view the onboarding and provisioning procedures for MSP and tenant accounts.
- **Managing Subscriptions** - You can view the assigned subscriptions and activate them using the **Subscription** option under **Device** section in HPE GreenLake platform.

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

  https://support.hpe.com/hpesc/public/docDisplay?docId=a00120892en_us.
- **Onboarding Devices** - You can view, manage, and onboard all the devices in your account using the **Devices** option in HPE GreenLake platform.

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

  https://support.hpe.com/hpesc/public/docDisplay?docId=a00120892en_us.
- **Groups in the MSP Mode** - You can view, create, override, clone, and delete groups in the tenant account.
- **MSP Dashboard** - You can view the summary of hardware and subscriptions owned by MSP and the details about the tenant accounts managed by MSP.

- **Assigning Devices to Tenant Accounts** - You can assign, update, or unassign the subscription of a device from the tenant using the **Devices** option in the HPE GreenLake platform.

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

  https://support.hpe.com/hpesc/public/docDisplay?docId=a00120892en_us.

- **Provisioning Tenant Accounts** - You can create and provision tenant accounts.
- **User Accounts and Roles in MSP Mode** - You can assign roles to users using the **Assign Roles** option in HPE GreenLake platform.

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

  https://support.hpe.com/hpesc/public/docDisplay?docId=a00120892en_us.

- **Customizing the Portal in MSP Mode** - You can customize the look and feel of the user interface and the email notifications sent to the customers and users.
- **Uploading Certificates in MSP** - You can view and add certificates in MSP.
- **Viewing Firmware Information** - You can view the list of tenant accounts and the status of the devices assigned to the tenant accounts.
- **MSP Deployment Scenarios** - You can view this page to understand the deployment scenarios.
- **Frequently Asked Questions** - You can view the frequently asked questions, related to MSP.

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 WebUI, 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**. HPE Aruba Networking 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 maps to the default group on the tenant account.
- The administrators can add users to a specific tenant account in the HPE GreenLake portal.
- Tenant account administrators can allow or prevent user access to specific groups by configuring .restriction policy.

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. WLAN gateways, AOS-CX, Monitoring only, and gateways with AOS-10 architecture groups are supported in the MSP mode.

Template, Microbranch, and VPNC 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.

For more information, see the following topics:

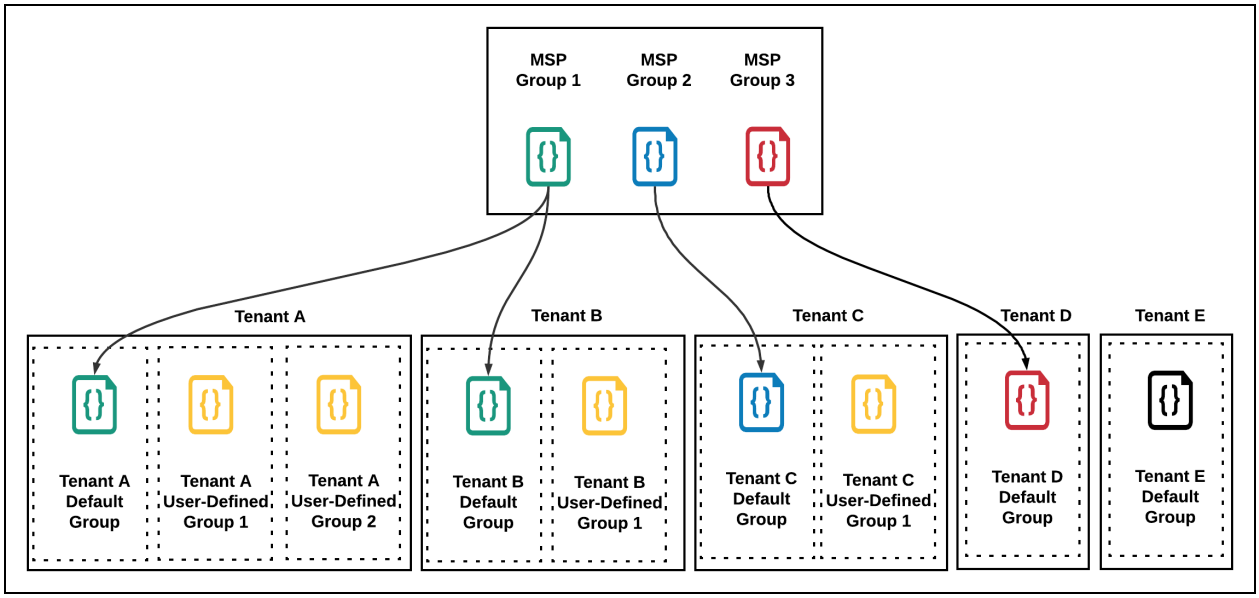
MSP Group Illustration

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 15 *MSP Groups*



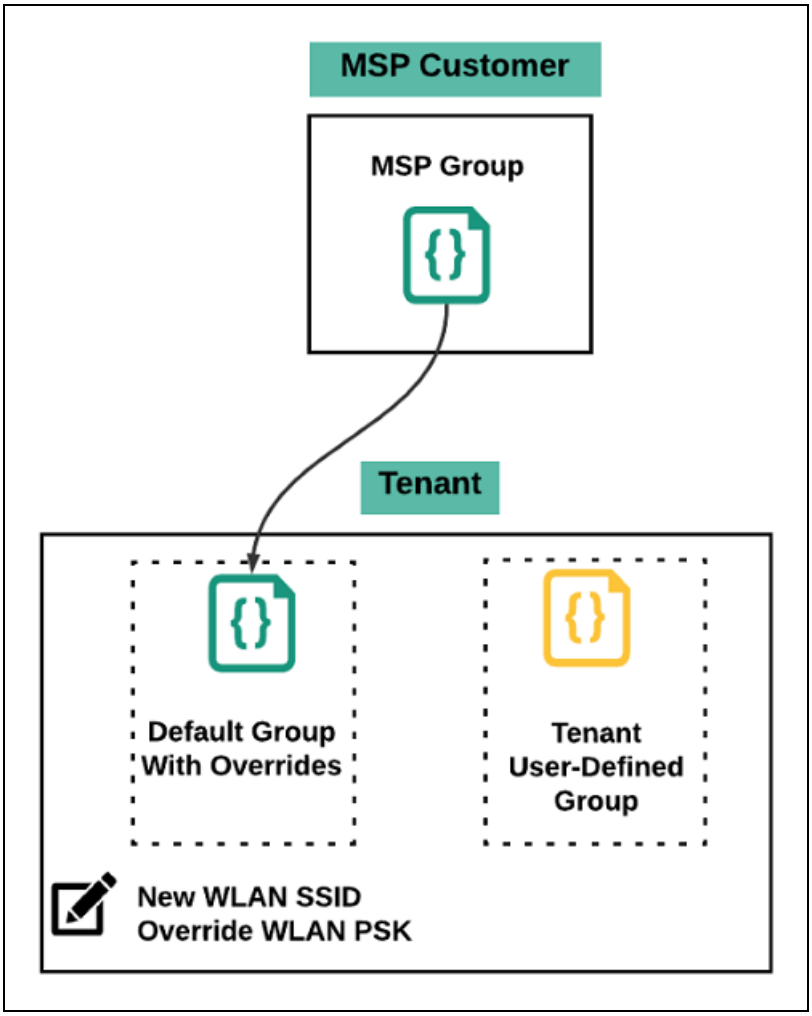
Tenant Default Group Overrides

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 16 *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 HPE Aruba Networking Central.

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.

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 AOS-8 (including IAP-VPN) architecture and AOS-10 architecture.

Persona for Gateways

Gateways can have the following persona:

- **Branch**—In this persona, gateways provide AOS-8 SD-Branch (LAN + WAN) functionality. This persona applies to AOS-8 architecture and AOS-10 architecture.

Architecture

The following architecture is supported for creating groups:

- **AOS-8**—Instant AP-based deployment, including AOS-6.x or Instant AOS-8.x (IAP, IAP-VPN), orInstant AOS-8.x SD-Branch deployments.
- **AOS-10**—Instant AP-based deployment, including AOS-AOS-10.x (IAP, IAP-VPN), or AOS-10.x SD-Branch deployments.

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

- Creating an MSP Group Persona with AOS-8 Architecture
- Creating an MSP Group Persona with AOS-10 Architecture

Creating an MSP Group Persona with AOS-8 Architecture

To manage device configuration using UI configuration containers in HPE Aruba Networking 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.

Device Combinations for MSP Group Persona

The following are the valid combinations for a group persona with Instant AOS-8 architecture.

Table 9: Device Combinations

Device Type	Architecture	AP Network Role	GW Network Role	Switches	Monitoring Only
AP	AOS-8	Campus/Branch	N/A	N/A	N/A
Gateway	AOS-8	N/A	Branch	N/A	N/A
Switch	No architecture	N/A	N/A	AOS-S and AOS-CX	N/A
▪ AP ▪ Gateway	AOS-8	Campus/Branch	Branch	N/A	N/A
▪ AP ▪ Switch	AOS-8	Campus/Branch	N/A	AOS-S and AOS-CX	N/A
▪ AP ▪ Gateway ▪ Switch	AOS-8	Campus/Branch	Branch	AOS-S and AOS-CX	N/A

For more information, see the topics below:

- Adding an MSP UI Group
- Editing an MSP UI Group

Adding an MSP UI Group

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

1. From the WebUI, 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

   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.

Editing an MSP UI Group

You can edit a 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 WebUI, filter **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.

Creating an MSP Group Persona with AOS-10 Architecture

To manage device configuration using UI configuration containers in HPE Aruba Networking 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.

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

Device Combinations for MSP Group Persona

The following are the valid combinations for a group persona with AOS-10 architecture.

Table 10: Device Combinations

Device Type	Architecture	AP Network Role	GW Network Role	Switches	Monitoring Only
AP	AOS-10/AOS-8	Campus/Branch	N/A	N/A	N/A
Gateway	AOS-10	N/A	Branch/Mobilty	N/A	N/A

Device Type	Architecture	AP Network Role	GW Network Role	Switches	Monitoring Only
Gateway	AOS-8	N/A	Branch	N/A	N/A
Switch	No architecture	N/A	N/A	AOS-S and AOS-CX	N/A
▪ AP ▪ Gateway	AOS-10	Campus/Branch	Branch/Mobilty	N/A	N/A
▪ AP ▪ Gateway	AOS-8	Campus/Branch	Branch	N/A	N/A
▪ AP ▪ Switch	AOS-10	Campus/Branch	N/A	AOS-S and AOS-CX	N/A
▪ AP ▪ Gateway ▪ Switch	AOS-8	Campus/Branch	Branch/Mobilty	AOS-S only	N/A

AOS-10 Configuration Notes

- The AOS-10 gateway configurations supports AOS-10 gateway UI at the MSP level.
- The **Clustering** option is available only at tenant level.
- The **Clustering** tab under **High Availability** will not be available for AOS-10 gateways at the MSP level.
- When the AOS-10 group is set to branch gateway persona for Gateway, the clustering is expected to be set to auto-site and default gateway-mode by default at the tenant level.
- AOS 10 access point configurations at MSP level supports bridge SSID for AOS-10. Overlay SSIDs can be only configured from tenant level.
- At the MSP level in the group configuration **Basic Mode** in **Manage** > **Devices** > **Gateways** > **System** > **Platform** page, the **This gateway group includes HA pairs** option is not available.
- At the MSP level in the group configuration **Advanced Mode** in **Manage** > **Devices** > **Gateways** the **High Availability** tab is removed.
- At the MSP level in the group configuration **Guided Setup** under the **System** section in the **Platform** page the **This gateway group includes HA pairs** option is not available.

For more information, see:

- Adding an MSP UI Group with AOS-10 Architecture
- Editing an MSP UI Group with AOS-10 Architecture

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 WebUI, 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, HPE Aruba Networking Central removes all configuration, templates, and variable definitions associated with the group. Before deleting a group, ensure that there no tenant accounts mapped to the group.

To delete a group, complete the following steps:

1. In the WebUI, 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 **Gateway**, 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 HPE Aruba Networking 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 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 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.

For more information, see the topic listed below:

- Checking the Gateway Persona of a Customer Group

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.

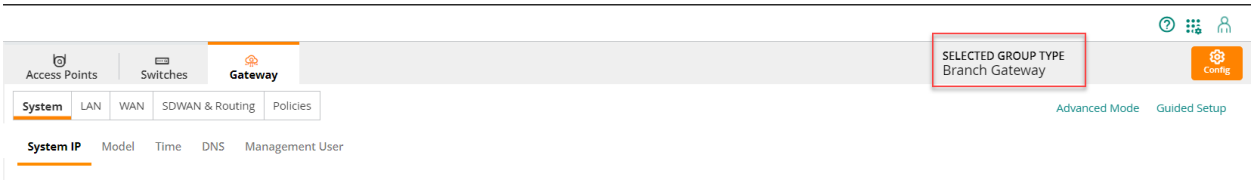
To check the persona set for a customer group containing at least one Gateway device, for the MSP account:

1. In the WebUI 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 WebUI 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 17 *Group Type Displayed for Gateway Group of Customer Account*



Chapter 7
MSP Dashboard

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.

For more information, see the topics below:

Viewing the MSP Dashboard

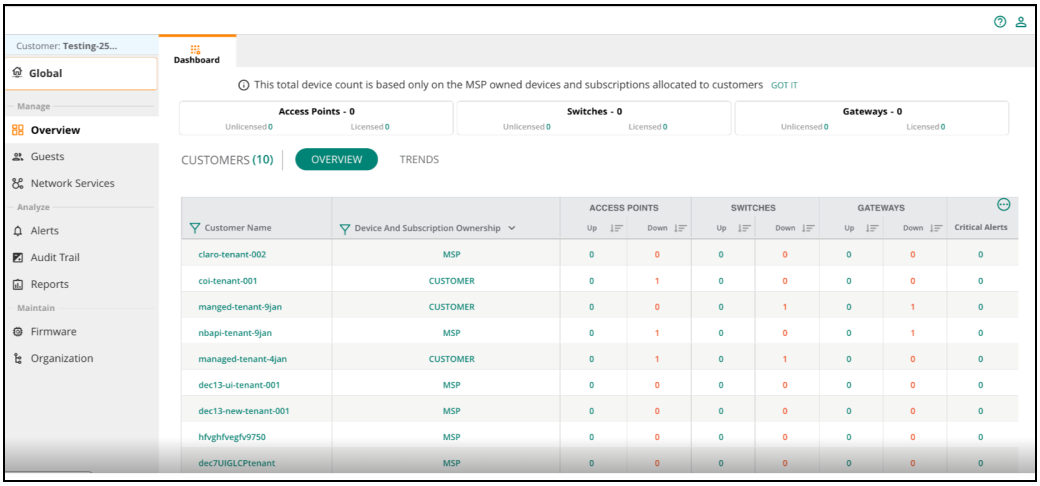
To view the MSP dashboard, perform the following steps:

1. In the WebUI, 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 18 *Viewing the MSP Dashboard*



Viewing 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. To view the dashboard summary, perform the following steps:

1. In the HPE Aruba Networking 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.
3. A summary section for the dashboard—Displays the assigned and unassigned devices and the assigned and unassigned licenses for APs, switches, and gateways.

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.

Viewing the Customers Overview

To view the Customers Overview section, perform the following steps:

1. In the HPE Aruba Networking 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.
3. 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.

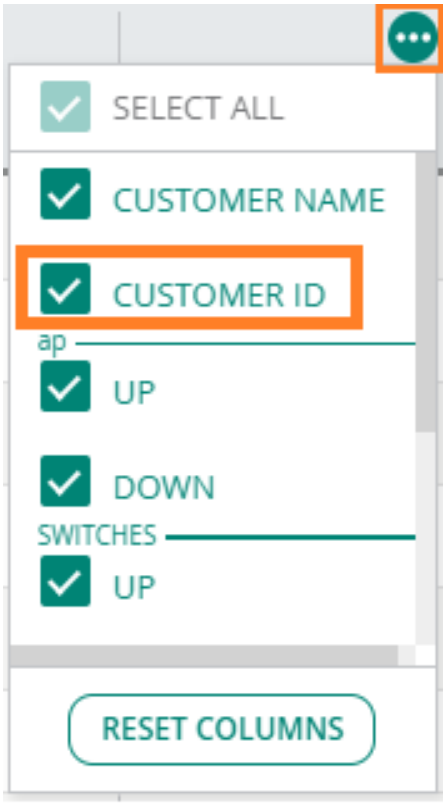
- **Customer ID**

  Unique ID of the tenant account. The ID can be in one of the following formats:
  - Numerical format
  - UUID format

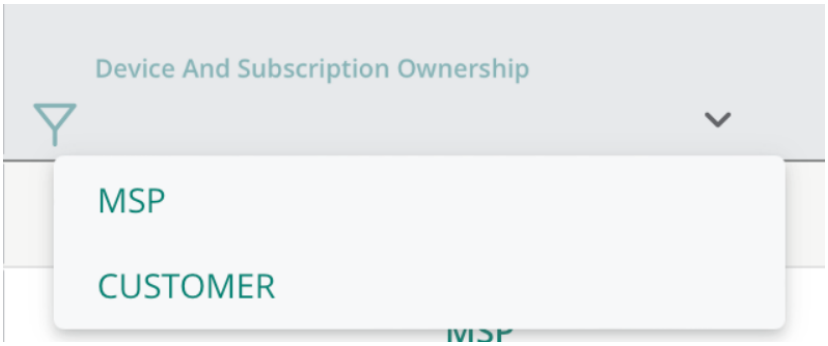
  Use the column filter to search for a particular customer ID. Note that you must enter the full customer ID.

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 19 *Selecting the Customer ID for Display*



- **Device and Subscription Ownership**
  Displays whether the device and subscription ownership falls under the MSP or a customer. You can use the filter icon to view the inventory ownership if devices and subscriptions are MSP or customer owned.



- **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.

Viewing the Customers Trends

To view the Customers Trends section, perform the following steps:

1. In the HPE Aruba Networking 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.
3. 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 HPE Aruba Networking 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 WebUI, 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**. HPE Aruba Networking 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 maps to the default group on the tenant account.
- The administrators can add users to a specific tenant account in the HPE GreenLake portal.
- Tenant account administrators can allow or prevent user access to specific groups by configuring .restriction policy.

Chapter 8
Configuring Instant APs

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

Instant APs run the Instant AOS-8 software that virtualizes HPE Aruba Networking 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 *HPE Aruba Networking Central Online Help*.

Chapter 9
Configuring Switches

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

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

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

Chapter 10
Configuring Gateways

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

In MSP mode, gateways can be configured in **HPE Aruba Networking Central**, they are also configurable at the tenant level.

Chapter 11

Analyzing and Maintaining MSP Tenant

In the WebUI 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**—HPE Aruba Networking 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 HPE Aruba Networking 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 HPE Aruba Networking 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

HPE Aruba Networking 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.

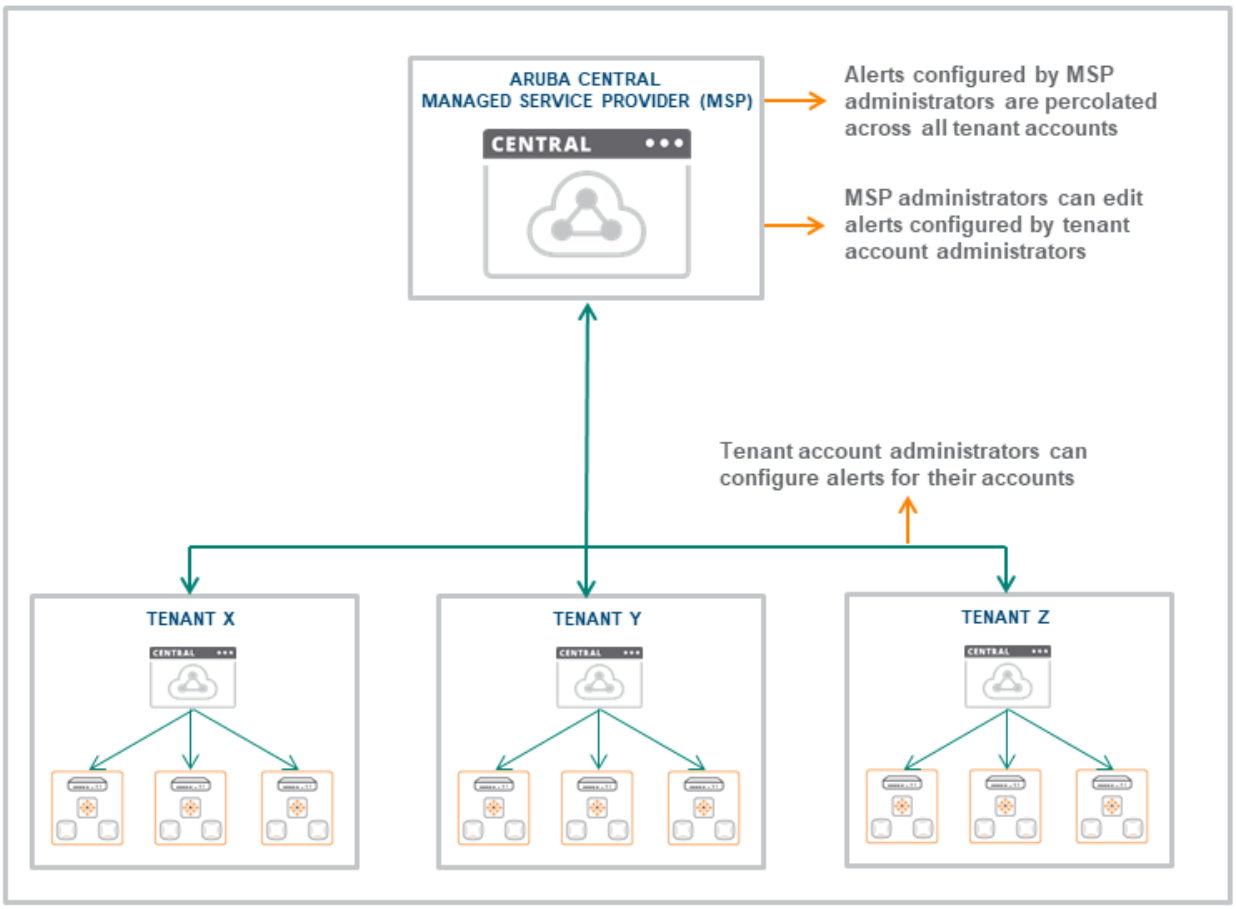
The MSP administrator can configure additional alerts at the tenant account level. At the tenant account level, alerts can be configured based on groups, labels, sites, or devices. Tenant account administrators

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 20 *MSP Alerts*



Alert Notification Delivery Options

When you configure an alert, you can select how you want to be notified when an alert is generated. HPE Aruba Networking 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 HPE Aruba Networking Central Online documentation.

For more information, see the following topics:

- Viewing MSP Alerts Dashboard
- MSP Alerts in List View

Viewing MSP Alerts Dashboard

To view the MSP Alerts Dashboard, perform the following steps:

1. In the WebUI, 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.

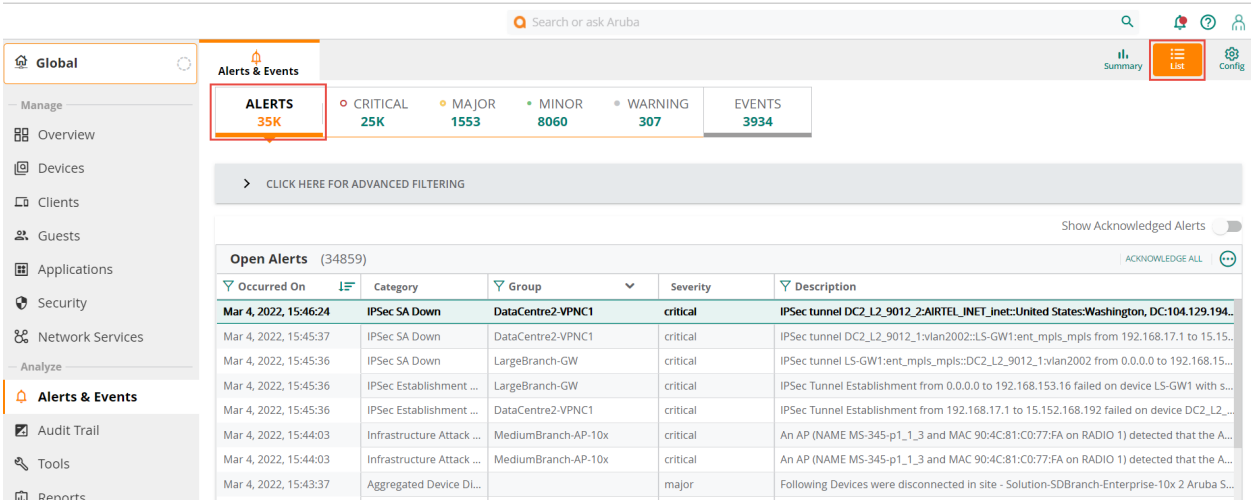
MSP Alerts in List View

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 21 *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
Occurred On	Timestamp of the alert. Use the sort option to sort the alerts by date and time.
Category	Displays the category of the alert. Use the filter option to filter the alert by category.
Label	Displays the label name of the alert.
Site	Displays the site name of the alert.
Customer	Displays the customer name of the alert.
Group	Displays the group name of the alert.
Severity	Displays the severity level of the alert. The severity can be Critical, Major, Minor, or Warning.
Description	Displays a description of the alert. Use the search option in filter bar to filter the alert based on description.

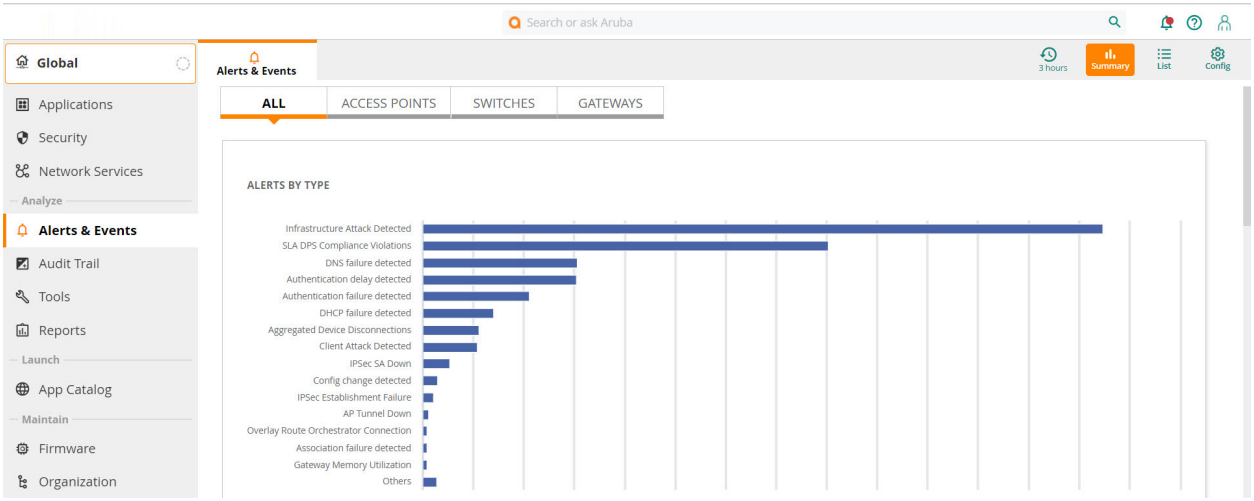
MSP Alerts in Summary View

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 22 *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.

Configuring Alerts at the MSP Level

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

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

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

NOTE

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

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

    b. **Notification Options**—See Configuring Alerts at the MSP Level.
        - 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 WebUI, 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 WebUI, filter **All Groups**.
2. Under **Analyze**, click **Alerts** to display the **Alerts** dashboard.
3. On the **Alerts** page, click **Enabled**.

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

Firmware Upgrades for MSP Mode

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

The following topics are discussed:

Viewing the Firmware Dashboard

To view the firmware dashboard, perform the following steps:

1. In the WebUI, 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
Customer Name	Name of the customer.
Firmware Version	Current firmware version.
Recommended Version	Recommended firmware version.
Upgrade Status	Status of the devices associated with the tenant account. This column displays one of the following: ■ Upgrading ■ Scheduling in progress ■ Downloading firmware ■ Upgrade successful, ready for reboot ■ Upgrade successful and rebooting AP ■ Upgrade in process ■ Firmware upgrade failed. Please try again. ■ Rebooting ■ Live upgrade initiating ■ Live upgrade initiated

Date Pane Item	Description
Compliance Status	Status of compliance for the tenant. This column indicates the compliance status such as **Set**, **Not Set**, or **Compliance scheduled on <date and time>** for a specific tenant.
Manage Firmware Compliance	Enables you to plan upgrades.

Managing Firmware Compliance Based on Device Tabs

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

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

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

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

- **[POST] /firmware/v1/msp/upgrade/customers/{customer_id}**—Upgrades firmware at the tenant level. To configure the firmware upgrade for a specific tenant of a specific device type, enter the following inputs in the corresponding labels of the script

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

Table 16: *Firmware Upgrade at the Tenant level*

Label	Description
Firmware_ scheduled_at	The time at which the firmware upgrade must be initiated. The value entered in this field is the count in seconds from the current time.
Device_type	The type of device for which the firmware upgrade must be initiated.

Label	Description
Firmware_ version	The firmware version to which the device is required to be upgraded. HPE Aruba Networking Central takes the recommended firmware version as the default version if no version is specified in the field.
Reboot	True or false value to enable or disable the reboot of device once the firmware upgrade build is downloaded. **NOTE:** The **Reboot** option is not applicable for Instant APs.
Exclude-groups	List of groups to be excluded from firmware upgrade.

- **[POST] /firmware/v2/msp/upgrade/cancel**—Cancels a scheduled upgrade firmware of devices specified by device_type. Enter the following inputs in the corresponding labels of the script

```
{
  "device_type": "string",
  "exclude_groups": "string",
  "exclude_customers": "string"
}.
```

Table 17: *Cancel Scheduled Upgrade at MSP Level*

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

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

```
{
  "device_type": "string",
  "exclude_groups": "string"
}.
```

Table 18: *Cancel Scheduled Upgrade at the Tenant Level*

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

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

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

Order of Precedence For Compliance

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

- Group level
- Tenant level
- MSP level

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

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

MSP Reports

The MSP **Reports** 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.

For more information. see the topics listed below:

- 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 WebUI, 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 view the types of reports, perform the following steps:

1. From the WebUI, set the filter to **All Groups**.
   The **Global** dashboard is displayed.
2. Under **Analyze**, click **Reports**.
3. 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
Access Points Inventory	The **Access Points Inventory** page lists the following options both in table and graph form: ■ **Opening Stock**—Total number of unassigned APs in the beginning of the time period. ■ **Purchased**—Number of APs purchased during the time period. ■ **Returned**—Number of APs returned by the tenants to the customer during the time period. ■ **Assigned**—Number of APs assigned to the tenants during the time period. ■ **Closing Stock**—Total of (Opening + Purchased + Returned - Assigned)
Switch Inventory	The **Switch Inventory** page lists the following options both in table and graph form: ■ **Opening Stock**—Total number of unassigned switches in the beginning of the time period. ■ **Purchased**—Number of switches purchased during the time period. ■ **Returned**—Number of switches returned by the tenants to the customer

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

Parameter	Description
	▪ **Expired**—Number of licenses that expired during the time period. ▪ **Closing Stock**—Total of (Opening + Purchased + Returned - Assigned - Expired)
Access Points Foundation License	The **Access Points Foundation License** page lists the following options both in table and graph form: ▪ **Opening Stock**—Total number of licenses in the beginning of the time period. ▪ **Purchased**—Number of licenses purchased during the time period. ▪ **Returned**—Number of licenses returned by the tenants to the customer during the time period. ▪ **Assigned**—Number of licenses assigned to the tenants during the time period. ▪ **Expired**—Number of licenses that expired during the time period. ▪ **Closing Stock**—Total of (Opening + Purchased + Returned - Assigned - Expired)
Access Points Advanced License	The **Access Points Advanced License** page lists the following options both in table and graph form: ▪ **Opening Stock**—Total number of licenses in the beginning of the time period. ▪ **Purchased**—Number of licenses purchased during the time period. ▪ **Returned**—Number of licenses returned by the tenants to the customer during the time period. ▪ **Assigned**—Number of licenses assigned to the tenants during the time period. ▪ **Expired**—Number of licenses that expired during the time period. ▪ **Closing Stock**—Total of (Opening + Purchased + Returned - Assigned - Expired)
Switch Foundation License	The **Switch Foundation License** page lists the following options both in table and graph form: ▪ **Opening Stock**—Total number of licenses in the beginning of the time period. ▪ **Purchased**—Number of licenses purchased during the time period. ▪ **Returned**—Number of licenses returned by the tenants to the customer during the time period. ▪ **Assigned**—Number of licenses assigned to the tenants during the time period. ▪ **Expired**—Number of licenses that expired during the time period. ▪ **Closing Stock**—Total of (Opening + Purchased + Returned - Assigned - Expired)
Switch Advanced License	The **Switch Advanced License** page lists the following options both in table and graph form: ▪ **Opening Stock**—Total number of licenses in the beginning of the time period. ▪ **Purchased**—Number of licenses purchased during the time period. ▪ **Returned**—Number of licenses returned by the tenants to the customer during the time period.

Parameter	Description
	▪ **Assigned**—Number of licenses assigned to the tenants during the time period. ▪ **Expired**—Number of licenses that expired during the time period. ▪ **Closing Stock**—Total of (Opening + Purchased + Returned - Assigned - Expired)

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

Table 20: *Generated Reports* *Description*

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

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

Table 21: *Scheduled Reports* *Description*

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

Creating a Report

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 WebUI, 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 WebUI, 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 WebUI, 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 WebUI, 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 HPE Aruba Networking 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.

Chapter 12
Guest Access

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

HPE Aruba Networking 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.

Cloud guest feature runs on the AP Foundation License. .

Guest Access Dashboard

The **Summary** page in the **Manage > Guest > 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
Time Range	Time range for the graphs and charts displayed on the **Overview** pane. You can choose to view graphs for a time period of 1 day, 1 week, and 1 month.
Guests	Number of guests connected to the SSIDs with Cloud Guest splash page profiles.
Guest SSID	Number of guest SSIDs that are configured to use the Cloud Guest splash page profiles.
Avg. Duration	The average duration of client connection on the SSIDs with Cloud Guest splash page profiles.
Max Concurrent Connections	Maximum number of client devices connected concurrently on the guest SSIDs.

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

Mapping Cloud Guest certificates

To enable certificates for the Cloud Guest Service, contact the HPE Aruba Networking 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 WebUI, use the filter to select **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 plus + icon to add a certificate to the certificate store.
5. In the **ADD CERTIFICATES** dialog box, do the following:
   a. In the **Name** text box, enter the certificate name.
   b. From the **Type** drop-down list, select the type of certificate. You can select any one of the following certificates:
      - **CA Certificate**—Digital certificates issued by the CA.
      - **Server Certificate**—Server certificates required for communication between devices and authentication servers.
      - **CRL**—Certificate Revocation List that contains the serial numbers of certificates that have been revoked. This certificate is required for performing a certificate revocation check.
      - **OCSP Responder Cert**—OCSP Responder certificates.
      - **OCSP Signer Cert**—OCSP Response Signing Certificate.

        OCSP certificates are required for OCSP server authentication.
   c. From the **Format** drop-down list, select a certificate format; for example, PEM, DER, and PKCS12.
   d. In the **Passphrase** text box, enter a passphrase.
   e. In the **Retype Passphrase** text box, retype the passphrase for confirmation.

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

f. In the **Certificate File** field, click **Choose file** and select the certificate files.
g. Click **Add**. The certificate is added to the Certificate Store.

6. 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.

7. Under **Manage**, click **Device** and then click **Show Advanced** > **Security**.

   Figure 23 *Show Advanced*

8. Expand the **Certificate Usage** accordion.

   Figure 24 *Certificate Usage Accordion*

9. Select the required certificate from the **Captive Portal** drop-down list.
10. 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:

Meta will terminate Facebook Wi-Fi service soon. With this, existing visitor deployments within HPE Aruba Networking Central Guest and HPE Aruba Networking ClearPass Guest that use Facebook Wi-Fi will stop working. This only impacts the Facebook Wi-Fi functionality offered through Meta. Customers using Facebook authentication as a remote identity source are not affected. Customers are advised to read and complete the recommended configuration changes explained in the HPE Aruba Networking Central and ClearPass Policy Manager - Guest Access after Facebook Wi-Fi Service Ends support advisory at HPE Networking Support Portal at the earliest to ensure guest network authentication remains functional after the termination of Facebook Wi-Fi.

Chapter 13

Managed Service Provider FAQs

How do I create an HPE Aruba Networking Central MSP account?

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

- Sign up for HPE Aruba Networking 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 HPE Aruba Networking 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 HPE Aruba Networking 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 HPE Aruba Networking Central.

See Supported Instant APs and Supported AOS-S Platforms.

HPE Aruba Networking 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.

HPE Aruba Networking 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 HPE Aruba Networking Central when its subscription expires?

For information about subscription expiry for a device on HPE Aruba Networking Central, see Lifecycle Management.

Which group on the tenant inherits the MSP group configuration upon mapping?

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
admin	▪ Has full access to all devices. ▪ Can provision devices and enable access to application services. ▪ Can create or update users, groups, and labels.	▪ Has full access to tenant accounts. ▪ Can create, modify, provision, and manage tenant accounts.

User Role	Standard Enterprise Mode	MSP Mode
readwrite	■ Has access to the groups and devices assigned in the account. ■ Can add, modify, configure, and delete a device in the account.	Can access and modify tenant accounts.
readonly	■ Can view the groups and devices. ■ Can view generated reports.	Can view tenant accounts.
guestoperator	■ Can access and modify cloud guest splash page profiles. ■ Can configure visitor accounts for the cloud guest splash page profiles.	■ Can access and modify cloud guest splash page profiles. ■ Can configure visitor accounts for the cloud guest splash page profiles.

What are custom user roles?

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.