Cloud Authentication and Policy Feature 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

Contents **3**

About This Document **4**
- Intended Audience 4
- Conventions 4
- Terminology Change 6
- Contacting Support 6

Cloud Authentication and Policy Overview **7**
- Cloud Authentication and Policy Architecture 7
- Roles Applicable for Configuring Cloud Authentication and Policy 8
- Supported Devices and Operating Systems 9
- Supported Deployment Types 10
- Prerequisites 11
- Caveats 12
- Configuring Cloud Authentication and Policy Server in a WLAN Network 17
- Configuring Cloud Authentication and Policy Server in a Wired Network 19
- Cloud Identity Store 20
- Configuring Cloud Authentication and Policy 30
- Updating Cloud Authentication and Policy 65
- Provisioning Clients 68
- Monitoring Cloud Authentication and Policy 83
- Client Security 96
- Cloud Authentication and Policy FAQs 98

Chapter 1
About This Document

This document describes the HPE Aruba Networking Central Cloud Authentication and Policy application and provides detailed information about the Cloud Authentication and Policy architecture and how to implement Cloud Authentication and Policy.

Intended Audience

This guide is intended for network administrators who manage and monitor cloud-based network access control (NAC).

Conventions

Table 1 lists the typographical conventions 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.

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
Cloud Authentication and Policy

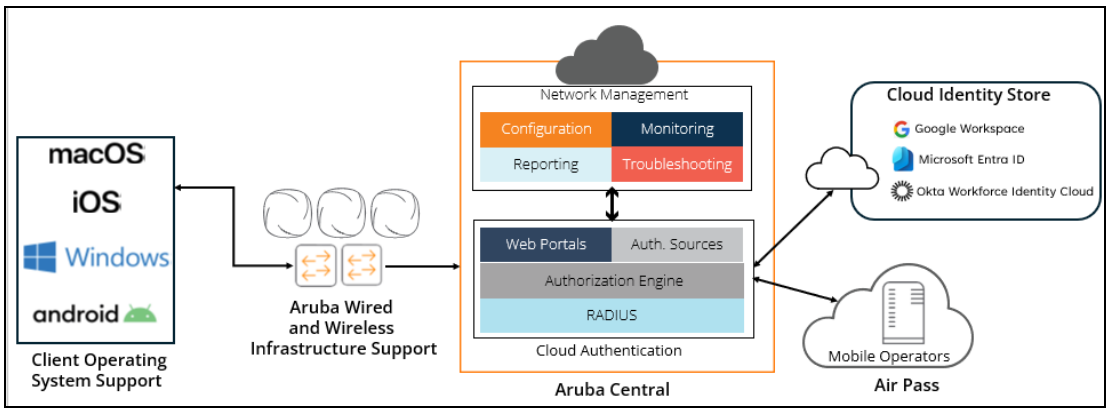
Cloud Authentication and Policy allows you to configure user and client access policies that provide a secured, cloud-based network access control (NAC). In HPE Aruba Networking Central, you can configure these policies and provide an on-boarding URL for the network users to connect to the network. As the users attempt to connect to the network, you can monitor the authentication access requests and sessions on the monitoring dashboards. You can view more details of each access request and session to analyze them or identify any issues.

- **User Access Policy**: In the user access policy, a network administrator can connect the user groups, defined in the cloud identity stores, to the client roles defined in HPE Aruba Networking Central. User groups must be predefined in the cloud identity stores, from cloud providers like Google Workspace, Microsoft Entra ID, and Okta Workforce Identity Cloud. Client roles can be defined in the HPE Aruba Networking IAP network profiles while creating the WLAN SSIDs.
- **Client Access Policy**: In the client access policy, a network administrator can add a list of client MAC addresses that will be allowed access to the network. The administrator can then map the client tags, which are defined for the different client categories, to the client roles. The client tags are defined in the **Clients** > **Clients Profile** page in HPE Aruba Networking Central.

Cloud Authentication and Policy Architecture

The following Cloud Authentication and Policy architecture provides an overview of how the cloud identity store, user and client policy, the WLAN network, and the clients connect to establish a secured cloud network.

Figure 1 *Cloud Authentication and Policy Architecture*



- **Clients and HPE Aruba Networking Devices**: Based on the client access policy in the Cloud Authentication and Policy configuration, the HPE Aruba Networking devices that are managed through HPE Aruba Networking Central help to connect the clients to the enterprise network. The client roles and WLAN SSIDs set up on the IAPs are used in the Cloud Authentication and Policy to control the network access. You must use the on-boarding URL provided by the network administrator to download the wireless network profiles and connect the clients to the network,

through HPE Aruba Networking devices. You can also use the HPE Aruba Networking Onboard app to connect the clients to the network.

- **Cloud Authentication and Policy**: With HPE Aruba Networking Central, administrators can configure separate user and client access policies. This flexibility of configuring independent user and client access policies allows the administrator to configure security levels at both the user and client level. For more information about configuring user and client access policy, see Configuring Cloud Authentication and Policy .
- **Cloud Identity Store**: HPE Aruba Networking Cloud Identity configuration uses user group information from the identity store to allow end users to connect to Wi-Fi networks securely and automatically. With HPE Aruba Networking Central, you can configure and manage users and user groups in a centralized fashion. Cloud Authentication and Policy integrates with your existing cloud identity providers to authenticate user's information and assign them the right level of network access. It retrieves and validates all the necessary attributes from the identity providers before enforcing role-based access policies associated with the user groups. Cloud Authentication and Policy supports three external identity providers, Google Workspace, Microsoft Entra ID, and Okta Workforce Identity Cloud.

  For more information about these identity providers, see the following topics:

  - Google Workspace
  - Microsoft Entra ID
  - Okta Workforce Identity Cloud

Roles Applicable for Configuring Cloud Authentication and Policy

With HPE Aruba Networking Central, you can configure client roles with appropriate access rules while configuring a WLAN SSID. These client roles are assigned to user groups, which are mapped from the external identity server, while configuring user and client access policy for users.

For more information about configuring user roles and associated access rules, and configuring user and client access policies, see the following topics:

- Configuring Cloud Authentication and Policy Server in a WLAN Network
- *Configuring User Roles for Instant AP Clients* in HPE Aruba Networking Central Help Center

You can create user roles while configuring the WLAN SSID by selecting **Role Based** security level from the **Security Level** slider in the **Access** tab. For more information, see Configuring Cloud Authentication and Policy Server in a WLAN Network.

For more information about Cloud Authentication and Policy implementation, see the following topics:

- Supported Devices and Operating Systems
- Supported Deployment Types
- Prerequisites
- Configuring Cloud Authentication and Policy Server in a WLAN Network
- Configuring Cloud Authentication and Policy
- Updating Cloud Authentication and Policy
- Provisioning Clients
- Monitoring Cloud Authentication and Policy

Supported Devices and Operating Systems

This section lists all the HPE Aruba Networking devices and various client Operating Systems along with their versions that are required to configure user and client access policy.

Table 3: *Cloud Authentication and Policy Supported HPE Aruba Networking Devices* 5.23.

HPE Aruba Networking Device(s)	Minimum Supported Software Versions	Supported HPE Aruba Networking Device Models
Instant AP	Aruba Instant 8.6.0.x, 8.7.0.x, 8.8.0.x, 8.9.0.x, 8.10.0.x, and 8.11.0.x	▪ AP-2xx ▪ AP-3xx ▪ AP-50x ▪ AP-51x ▪ AP-53x ▪ AP-55x ▪ AP-56x ▪ AP-57x ▪ AP-58x ▪ AP-615 ▪ AP-635 ▪ AP-655 **NOTE:** The last supported release for AP-205 access points is Aruba Instant 6.5 release.
HPE Aruba Networking Wireless Operating System 10 AP	AOS-10.3.1.1	▪ AP-3xx ▪ AP-503H ▪ AP-504 ▪ AP-505 ▪ AP-505H ▪ AP-51x ▪ AP-53x ▪ AP-55x ▪ AP-56x ▪ AP-57x
	AOS-10.4.0.0	▪ AP-58x ▪ AP-635 ▪ AP-655
	AOS-10.5.0.0	▪ AP-503 5.23. ▪ AP-503R ▪ AP-605R ▪ AP-615
	AOS-10.6.0.0	▪ AP-634 ▪ AP-654

HPE Aruba Networking Device(s)	Minimum Supported Software Versions	Supported HPE Aruba Networking Device Models
AOS-CX	AOS-CX 10.10.xxxx **NOTE:** The minimum supported version for AOS-CX 8100 Switch series is 10.12.xxxx.	■ AOS-CX 4100i Switch Series ■ AOS-CX 6000 Switch Series ■ AOS-CX 6100 Switch Series ■ AOS-CX 6200 Switch Series ■ AOS-CX 6300 Switch Series ■ AOS-CX 6400 Switch Series ■ AOS-CX 8100 Switch Series ■ AOS-CX 8360 Switch Series
Gateway	AOS-10.3.1.1, AOS-10.4.0.0, and AOS-10.5.0.1	■ 7000 Series ■ 7200 Series ■ 9000 Series ■ 9100 Series ■ 9200 Series

Table 4: *Cloud Authentication and Policy Supported Client Operating System*

Client Operating Systems	Supported Versions
Windows	Windows 10 version 1803 and later
Windows Server	Windows Server 2016 and later
Android	Android 9 and later
macOS	macOS 10.13 and later
iOS	iOS 12.1 and later
ChromeOS	ChromeOS 115 and later

iOS 15.0 and iOS 15.1 versions are not supported because of a bug in iOS, which was fixed by Apple in the iOS 15.2 version.

Supported Deployment Types

With HPE Aruba Networking Central, you can deploy Cloud Authentication and Policy in wireless and wired modes. The Cloud Authentication and Policy Deployment Modes table lists the HPE Aruba Networking devices that must be available in HPE Aruba Networking Central to configure Cloud Authentication and Policy in wireless and wired modes.

- Cloud Authentication and Policy is supported for MSP customers. In the MSP mode, Cloud Authentication and Policy can be configured for MSP tenants. For more information, see Configuring Cloud Authentication and Policy .
- Cloud Authentication and Policy is supported for overlay deployment mode when not using MPSK.

Table 5: *Cloud Authentication and Policy Deployment Modes*

Deployment Mode	Traffic Forwarding Mode	HPE Aruba Networking Device (s) Connected to HPE Aruba Networking Central	Supported version(s)
Wireless	Bridge	Instant AP	Aruba Instant 8.10
			AOS-10.x
	Tunnel	HPE Aruba Networking AP	AOS-10.4
	Mixed	HPE Aruba Networking Gateway	AOS-10.5
Wired	Bridge	AOS-CX	AOS-10.10
		Instant AP	AOS-10.x

Prerequisites

Cloud Authentication and Policy allows you to create user and client access policies for users and client devices from HPE Aruba Networking Central.

The following are the prerequisites for configuring the user access policy and client access policy:

- Ensure that you have created a device group containing at least one HPE Aruba Networking AP. You can onboard HPE Aruba Networking APs, 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
- For more information on how to assign APs to device groups, see *HPE Aruba Networking Central Help Center*.
- Ensure that you have configured WLAN SSIDs for clients. For more information about configuring client SSID, see Configuring Cloud Authentication and Policy Server in a WLAN Network.
- Ensure that you have configured user roles with appropriate access rules that are applicable for Cloud Authentication and Policy. For more information about user roles, access rules, and, configuring user roles and associated access rules, see the following topics:
  - Configuring ACLs for Deep Packet Inspection in *HPE Aruba Networking Central Help Center*
  - Configuring User Roles for Instant AP Clients in *HPE Aruba Networking Central Help Center*
- Ensure the Client Profiles and Client Tags are available in your HPE Aruba Networking Central account. Optionally, create custom tags in addition to the system tags for client devices. For more information about adding Tags, see Managing Tags.

While configuring **Client Access Policy**, the client device **Tags** appear in the drop-down list under **Client Profile Tags** column of the **Client Profile Tag to Client Role Mapping** table.

- Ensure to obtain the external cloud identity store details. Cloud Authentication and Policy currently supports Google Workspace, Microsoft Entra ID, and Okta Workforce Identity Cloud. For more information, see Cloud Identity Store.

Caveats

This section describes the caveats to be noted when using Cloud Authentication and Policy in HPE Aruba Networking Central.

- Browser-based and App-based Onboarding
- WLAN SSID and Client Role Configuration
- Non-Passpoint Device
- Other Caveats

Browser-based and App-based Onboarding

The following are caveats that appear during the browser-based and app-based onboarding:

- The coexistence of browser-based and app-based onboarding for the same wireless network is not supported. When a network profile is provisioned multiple times from the same provisioning URL on a device via browser-based onboarding and app-based onboarding methods, the configured profile is not treated as two separate network profiles and is overwritten. The OS overrides the network configuration because it uses domain names and profile names to identify and update the configuration.

  In the same way, deleting a network profile manually or from the HPE Aruba Networking Onboard app, completely removes the network profile from the device.
- Onboarding is not supported for user email IDs longer than 64 characters. Create email aliases for the email IDs with more than 64 characters. For more information on creating email aliases, see Creating email alias in Microsoft Entra ID and Creating email alias in Google Workspace. Currently, this is a limitation and it will be fixed in a future release.
- Oppo and Realme devices are not supported with Cloud Authentication and Policy. The OS crashes on these devices after installation of network profiles. To fix this issue, users need to perform a factory reset which can lead to loss of data. This issue has been reported to the OEM vendors.

I. Browser-based Onboarding

The following are caveats and workarounds categorized under Android and Windows OS platforms:

Android

a. Android devices display one of the following behaviors after successful onboarding:
   - The device displays both the organization name and SSID configured by the admin in the list of available wireless networks (under Settings > Wi-Fi) and connects to the organization name enterprise wireless network.

- The device displays only the SSID and when the user taps the SSID, it prompts the user to enter credentials to connect to the enterprise network. OEM's partial Passpoint implementation causes this behavior and prevents the device from connecting to the network.

b. On Realme Narzo 30 5G (model RMX3242) devices running on Android 11, the browser-based provisioning capability is disabled because the device crashes continuously after a network profile is installed using browser-based provisioning. You must reset the device to factory settings to recover the device. This issue might have been caused by some OEM customizations in the operating system for the Passpoint Wi-Fi feature.

Windows

When trying to reinstall an existing network profile on a Windows device, the WLAN network profile, root CA, and client certificates are overwritten. Due to operating system's UI issue, Windows devices display duplicate network profiles in **Add or remove provisioning package** settings, but the network profile gets updated in the background.

II. App-based Onboarding

The following are caveats and workarounds categorized under Android, Windows, and Linux OS platforms:

Android

a. On Samsung devices running Android 11 and One UI version 3.1, when HPE Aruba Networking Onboard app is added into the deep sleep list by the operating system, the network profile is automatically removed from the device. It prevents the device from connecting to the wireless network. This issue has been reported to Samsung for further analysis. To avoid removing the network profiles, complete the following steps:
   - Add the HPE Aruba Networking Onboard app in the list of Never Sleeping Apps under Battery > Background Usage Limits > Never Sleeping Apps.
   - Remove the app in the list of Deep Sleeping Apps under Battery > Background Usage Limits > Deep Sleeping Apps. If the network profile is removed by operating system, perform the onboarding process again or refresh the network profile in HPE Aruba Networking Onboard app. For more information on refreshing network profile, refer App-based Onboarding.

b. The Android devices displays one of the following behaviors after successful onboarding:
   - The device displays both the organization name and SSID configured by the admin in the list of available wireless networks (under Settings > Wi-Fi) and connects to the organization name enterprise wireless network.
   - The device displays only the SSID configured by the admin and connects to the enterprise wireless network. This behavior is due to Passpoint feature being unsupported by the Original Equipment Manufacturer (OEM).
   - The device displays only the SSID and when user taps the SSID, it prompts the user to enter credentials to connect to the enterprise network. OEM's partial Passpoint implementation causes this behavior and prevents the device from connecting to the network. This will be addressed in future releases.

Windows

a. When users onboard two domains with the same organization name in HPE Aruba Networking Onboard app, two network profile cards are displayed with the same

organization name. The devices cannot connect to either of the onboarded network profiles. Before installing the new network profile, HPE Aruba Networking recommends to delete the inactive network profile when users roam between the commonly named domains.

b. When multiple users share a device:
   - If one of the user deletes the network profile from the system, the profile is deleted for all other users. This limitation is due to an operating system API and the issue has been reported to Microsoft Support.
   - If one of the user refreshes the network profile, the other users who are using the same network profile are unable to connect to the network. When other users try to connect using the same network profile, the client requests for a certificate to sign in and connect. In some cases, the refresh profile action might open the provisioning URL in a browser and force you to reinstall the network profile. This issue has been reported to Microsoft Support for further analysis.
   - It is recommended that you sign out of the shared device or exit the HPE Aruba Networking Onboard app after using it, as the next user using the same device may experience issues with the user interface when they log in with their credentials.
   - It is recommended that you uninstall the HPE Aruba Networking Onboard app version 1.0 before upgrading the app to version 1.1 because the certificates and network profiles (user AppData) installed with version 1.0 will not be deleted for users who are not logged in. This also ensures that the app registry keys are cleared or wiped from the system, which was observed to affect the provisioning flows for users who are not logged in. For more information about uninstalling the HPE Aruba Networking Onboard app, see App-based Onboarding.

c. Due to a design limitation in the HPE Aruba Networking Onboard app version 1.0, an existing version 1.1 user can install version 1.0 on top of version 1.1. This can result in an unexpected application behavior and is not recommended.

d. After onboarding the Windows client for a wired network, if a user connects to the Windows device through remote desktop connection, then the network connection for the provisioned network fails.

e. HPE Aruba Networking Onboard fails to provision a wired or dual profile when a mobile device is connected to a laptop using USB tethering. The workaround for this issue is to unplug the USB tethering device and redo provisioning.

Linux OS

When the HPE Aruba Networking Onboard app is installed and uninstalled several times using the Software Center, the app is seen to be installed multiple times.

WLAN SSID and Client Role Configuration

- Before you delete an SSID, ensure that it is not used in the user or client access policy as part of the Cloud Authentication and Policy configuration. If you delete an SSID associated with a user or client access policy, the policy will not work as expected. For more information about configuring a user access policy, see Configuring User Access Policy.
- If you modify the name of the WLAN SSID in the WLAN configuration, the WLAN SSID name will not be auto-updated in the Cloud Authentication and Policy user access policy. You must set the WLAN SSID to the updated name in the Cloud Authentication and Policy user access policy. For more information about configuring a user access policy, see Configuring User Access Policy.

- Before you delete a client role, ensure that it is not used in user and client access policies as part of the Cloud Authentication and Policy configuration. If you delete a client role associated with a user or client access policy, the policy will not work as expected. For more information about configuring a client access policy, see Client Access Policy.

Non-Passpoint Device

In a non-passpoint device, the device will connect to the default SSID name (which is configured by the admin under the user access policy) instead of the passpoint friendly name or organization name.

The following are the behaviors observed in Android devices along with recommendations for non-passpoint devices:

- **Behavior**: The device prompts for user credentials after successful provisioning upon manually selecting the provisioned network SSID from the WiFi picker list.

  Recommendation: Allow the device to detect and connect to the network automatically. If SSID name is tagged with **Available via HPE Aruba Networking Onboard**, you will be able to manually connect by selecting this SSID.

- **Behavior**: The device disconnects from a network if it switches from a provisioned network to a non-provisioned network. It may not immediately fallback to the provisioned network.

  Recommendation: Disable and enable the WiFi to connect the device to the provisioned network.

- **Behavior**: In the event of any change in the configuration about SSID on the policy side, the existing provisioned devices may fail to identify and connect to the new SSID.

  Recommendation: You will be able to connect to the older SSID provided it is still active. If you want to connect to the updated SSID, you must perform a profile refresh from the HPE Aruba Networking Onboard app.

- **Behavior**: The device will not be able to connect to an SSID that is updated with a new name as it is provisioned to connect to the SSID prior to its update.

  Recommendation: You must refresh the profile from the HPE Aruba Networking Onboard App after which the device will start connecting to the updated SSID.

- **Behavior**: The connection status to the provisioned base SSID on Vivo and Oppo devices may not be visible from the WiFi picker list, but will be visible on the main Android Settings page.

  Recommendation: This is a limitation for few vendors and this will not impact the connectivity.

- **Behavior**: If a device is manually disconnected from the network, it does not auto connect to the SSID for a duration of 24 hours although the device is in the network range or if the network is removed and added by the App.

  Recommendation: Disable and enable the WiFi, to connect to the network.

Other Caveats

The following are some of the various caveats observed in Cloud Authentication:

Dynamic Authorization

A client disconnect is invoked when a tag is added, changed, or deleted, and if the endpoint session is still alive. The delete tag action does not disconnect a session if the tag was created less than an hour to prevent frequent disconnection.

CHAP Disabled for Wired Configuration

The Challenge-Handshake Authentication Protocol (CHAP) mode is not supported by the Cloud Authentication RADIUS server. In HPE Aruba Networking Central UI, MAC authentication is restricted to the Password Authentication Protocol (PAP) mode as CHAP mode of authentication is not supported.

Authentication and Session Tracker

In some cases, multiple session records for an ongoing session are reported in the Access Tracker. Except for the original session record, most of these session records appear for a shorter duration, are irrelevant, and should be ignored. The original session record reflects the correct parameters for the ongoing session.

Authorization of External User Identities

Authorization of user accounts integrated with Google Workspace as an external identity source is not supported.

For Microsoft Entra ID, ensure to use the basic user group in the User Groups to Client Role Mapping.

Nested Groups

Cloud Authentication and Policy does not support nested groups. You can define your policy through one of the following:

a. Flatten the group to form a single group with all members.

b. Add individual subgroups as separate rules in the user policy.

c. Use the 'Unspecified' rule to assign a common role for all users.

Hidden SSID is not Supported

The HPE Aruba Networking Onboard Application does not support provisioning of hidden SSID network.

iOS Client Setup for Captive Portal with Google Identity Store

While using iPhone and iPad devices to connect to the Captive Portal with Google as the identity Store, the embedded user agent on an iOS is no longer permitted to make an OAuth authorization request to Google. Due to this, the authorization for the captive portal login must be done through a browser.

User Group Search Caveats

When searching for a user group in Google Workspace, the following conditions are observed:

- Special characters in a search term such as *, $, #, and so on are ignored.

  For example, if the search term is "#Count", the search is performed only for the term "Count".

- Search term matches only the prefix of the user group name.

  For example, for a user group "Engineering Director", if the search term is "Eng", it matches the user group whereas, the search term "Director" fails to match the user group.

Old Certificates on ChromeOS

ChromeOS does not remove old certificates from the device, when profile refresh/delete/re-onboarding operations are performed via the HPE Aruba Networking Onboard App. Although, on restarting the device, the old certificates disappear. This is a bug in ChromeOS and has been reported to Google.

Send Logs Option Failure

The **Send Logs** option fails when it is used with the default Gmail App on ChromeOS. Install Gmail from Google Play Store and then click **Send Logs** from the HPE Aruba Networking Onboard App, ChromeOS displays the Gmail App to share the logs.

Configuring Cloud Authentication and Policy Server in a WLAN Network

The Cloud Authentication and Policy server in a WLAN network must be configured in HPE Aruba Networking Central, to provide seamless wireless network connection to the end-users and client device. With HPE Aruba Networking Central, you can configure the Cloud Authentication and Policy server at various security levels in the **Security** tab.

To configure Cloud Authentication and Policy server in a WLAN network, complete the following steps:

1. In the WebUI, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
   A list of APs is displayed in the List view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click the **WLANs** tab.
   The WLANs details page is displayed.
5. In the **WLANs** tab, click **+ Add SSID**.
   The Create a New Network page is displayed.
6. In the **General** tab, enter a name in the **Name (SSID)** text-box.
7. Select a check box to specify the band at which the network transmits radio signals in the **Band**. You can set the band to **2.4 GHz**, **5 GHz**, or **6 GHz**.
8. Under **Advanced Settings**, configure the advanced settings parameters for an SSID. For more information, see *Table 1: Advanced Settings Parameters* in *Configuring Wireless Network Profiles on Instant APs* section in HPE Aruba Networking Central Help Center.

Hidden SSID is not supported for Cloud Authentication and Policy.

9. Click **Next**.
10. Under **VLANs**, configure the VLAN settings for an SSID. For more information, see Configuring VLAN Settings for Wireless Network in *Configuring Wireless Network Profiles on Instant APs* section in HPE Aruba Networking Central Help Center.
11. Click **Next**.
12. In the **Security** tab, select one of the following security level:
    - Setting up 802.1X network access:
      - Select **Enterprise** in the **Security Level** slider and then enter values for the following parameters:

a. **Key Management**—Select an encryption key from the drop-down list.
b. **Primary Server**—Select **CloudAuth** from the drop-down list.

WPA3-Enterprise (GCM 256) and WPA3-Enterprise (CNSA) encryption keys are not supported with CloudAuth as most of the client devices do not support these two modes.

- Setting up MAC authentication network access:
  - Select **Personal** in the **Security Level** slider and then specify the following parameters:
    a. **Key Management**—Select an encryption key from the drop-down list.

In the **Key Management** drop-down list, only **WPA2-Personal**, **WPA3-Personal**, and **Both (WPA2 & WPA)** encryption keys are supported. For more information on WPA2/WPA3 modes, see Support for WPA2/WPA3 Mode.

    b. **Passphrase Format**—Select **8-63 chars**or **64 chars** passphrase format from the drop-down list.
    c. **Passphrase**—Specify a passphrase in the text-box.
    d. **Retype**—Retype the passphrase to confirm in the text-box.
    e. Expand the **Advanced Settings** accordion and specify the following parameters:
       i. **MAC Authentication**—Enable the toggle switch to allow MAC authentication.

If **MAC Authentication** toggle switch is disabled, **Primary Server** to select **CloudAuth** will not be available.

       ii. **Primary Server**—Select **CloudAuth** from the drop-down list.
- Setting up MAC authentication network access (**Open** or **Enhanced Open** Key Management):
  - Select **Open** in the **Security Level** slider and then specify the following parameters:
    a. **Key Management**—Select an encryption key **Open** or **Enhanced Open** from the drop-down list.
    b. Expand the **Advanced Settings** accordion and specify the following parameters:
       i. **MAC Authentication**—Enable the toggle switch to allow MAC authentication.

If **MAC Authentication** toggle switch is disabled, **Primary Server** to select **CloudAuth** will not be available.

       ii. **Primary Server**—Select **CloudAuth** from the drop-down list.
  - For more information on advanced settings, see *Configuring Security Settings for Wireless Network* in *Configuring Wireless Network Profiles on Instant APs* section in HPE Aruba Networking Central Help Center.

13. Click **Next**.
14. Under **Access**, configure the access settings for an SSID. For more information, see *Configuring ACLs for User Access to a Wireless Network* in *Configuring Wireless Network Profiles on Instant APs* section in HPE Aruba Networking Central Help Center.

Only Role-Based and Unrestricted access levels are used for Cloud Authentication and Policy. Network based access is not used in Cloud Authentication and Policy.

15. Click **Next**.

    The **Summary** tab displays all the settings configured in the **General**, **VLANs**, **Security**, and **Access** tabs.
16. Click **Finish**.

Support for WPA2/WPA3 Mode

After configuring WLAN, the administrator can switch between the following Wi-Fi Protected Access (WPA) modes without requiring user to reprovision:

- WPA2
- WPA3-Enterprise (CCM 128) with Transition Enabled
- WPA3-Enterprise (CCM 128) with Transition Disabled

These WPA modes are supported for the following operating systems and the HPE Aruba Networking Onboard app versions:

Table 6: *Operating Systems and HPE Aruba Networking Onboard App Versions*

Operating Systems	Supported App Versions
Windows 10/11	1.4.5
Android	1.4.4
Ubuntu	1.4.3
iOS	1.4.0
macOS	1.4.7
ChromeOS	1.4.4

If there is a change in the network configuration, then the connected clients can experience network disruptions.

Configuring Cloud Authentication and Policy Server in a Wired Network

The Cloud Authentication and Policy server in a wired network authenticates the end-users and client device to provide access to the network. With HPE Aruba Networking Central, you can configure the Cloud Authentication and Policy server at **MAC Authentication** security level in the **Security** tab.

To configure Cloud Authentication and Policy server in a wired network, complete the following steps:

1. In the WebUI, set the filter to a group containing at least one AP.

   The dashboard context for the group is displayed.

2. Under **Manage**, click **Devices > Access Points**.
   A list of APs is displayed in the List view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click the **Interfaces** tab.
   The Interfaces page is displayed.

This tab is displayed only if **Show Advanced** is selected.

5. Click the **Wired** accordion.
6. To create a new wired profile, click **+ Add Port Profile**.
   The Create a New Network page is displayed.
7. In the **General** tab, configure the general settings parameters for a wired profile. Under **Advanced Settings**, configure the advanced settings parameters for a wired profile. For more information, see *Configuring General Network Profile Settings* in *Configuring Ethernet Port Profiles on Instant APs* section in HPE Aruba Networking Central Help Center.
8. Click **Next**.
9. Under **VLANs**, configure the VLAN settings for a wired profile. For more information, see *Configuring VLAN Network Profile Settings* in *Configuring Ethernet Port Profiles on Instant APs* section in HPE Aruba Networking Central Help Center.
10. Click **Next**.
11. In the **Security** tab, Select **MAC Authentication** in the **Security Level** slider and specify the following parameters:
    - **Port Type Trusted**—By default the **Port Type Trusted** is disabled. Make sure that the Port Type Trusted toggle switch is disabled.

If the **Port Type Trusted** toggle switch is enabled, the **Primary Server** field will not display.

    - **Primary Server**—Select **CloudAuth** from the drop-down list.
    - **Reauth Interval**—Specify the **Reauth Interval** in **Advance Settings** section, at which all associated, and authenticated clients must be re-authenticated.
12. Click **Next**.
13. Under **Access**, configure the access settings for a wired profile. For more information, see *Configuring Access Settings* in *Configuring Ethernet Port Profiles on Instant APs* section in HPE Aruba Networking Central Help Center.

Only Role-Based and Unrestricted access level users uses Cloud Authentication and Policy. Network-based access is not operational for Cloud Authentication and Policy.

14. Click **Next**.
    The **Summary** tab displays all the settings configured in the **General**, **VLANs**, **Security**, and **Access** tabs.
15. Click **Finish**.

Cloud Identity Store

Cloud Authentication and Policy allows users to connect to enterprise Wi-Fi networks securely and access HPE Aruba Networking Central. For enterprise users, HPE Aruba Networking Central allows network administrators to centrally configure and manage users and user groups. HPE Aruba Networking Central also allows administrators to select an external cloud identity store, such as Microsoft Entra ID, Google Workspace, or Okta Workforce Identity Cloud to authenticate users before providing them the right level of network access.

In HPE Aruba Networking Central, administrators can configure user policies based on the user groups defined in the following identity stores:

- Microsoft Entra ID
- Google Workspace
- Okta Workforce Identity Cloud

Microsoft Entra ID

Entra ID is Microsoft's cloud-based identity and access management service, which helps an organization's employees to sign-in and access internal and external apps on their corporate network and intranet. Administrators use Entra ID to control access to apps and app resources, based on the organizations' business requirements.

In HPE Aruba Networking Central, administrators can configure user policies based on the user groups defined in the Entra ID identity store. When creating a user policy, the network administrator must provide the information listed in Getting Information from Microsoft Entra ID.

When the administrator deletes or suspends a user from Microsoft Entra ID, the Cloud Authentication and Policy application receives a notification about the event. The application revokes any certificates provisioned to the user and disconnects any active sessions for the user. This change is reflected within a short span of time.

In addition, if a user is removed from a group for which he is currently authorized against, the user is disconnected and forced to re-authenticate.

To register Cloud Authentication and Policy, get API permissions, and create client secret ID, see the following topics:

- Configuring Microsoft Entra ID in Cloud Authentication
- APIs for Microsoft Entra ID

Getting Information from Microsoft Entra ID

To configure Entra ID in the Cloud Authentication and Policy app, you will need the following information:

- Client ID
- Client Secret
- Tenant ID

To get the client information, complete the following steps:

1. Open the URL *https://portal.azure.com/#home* to access the Entra ID portal.
2. Navigate to the **Entra Services** section and click **More services**.
   The **All services** page is displayed.
3. Select **Microsoft Entra ID**.

The Microsoft Entra ID page appears.

4. From the left navigation pane, click **App registrations** and select **Owned Applications** tab.
5. Click the application name under the **Display name** column.
   You can view the **Client ID**, **Tenant ID**, **Client Credentials** and other details.
6. Click **Client Credentials** to generate a new client secret for the application.

Client secrets are created by the administrator and have an expiration date. Ensure to periodically renew your client secret and update the user policy to avoid authentication failures.

Configuring Microsoft Entra ID in Cloud Authentication

To integrate Microsoft Entra ID with Cloud Authentication and Policy application from Entra ID, do the following:

1. Register Cloud Authentication and Policy Application in Entra ID Portal
2. Configure API Permissions for Cloud Authentication and Policy Application
3. Configure Client Secret ID for Cloud Authentication and Policy Application

Register Cloud Authentication and Policy Application in Entra ID Portal

Register the Cloud Authentication and Policy application inEntra ID to authenticate with the Microsoft identity platform endpoint. This configuration allows the Cloud Authentication and Policy application to call Microsoft Graph APIs to authorize users during authentication.

For instructions, see Register an application with the Microsoft identity platform.

In the **Redirect URI** section, add **OAuth** and **Reply URLs** of the **Cloud Guest** server. The reply URL must be in the *https://<cloud guest server>/oauth/reply* format.

For more information about Cloud Guest server URLs, see **Cloud Guest Server Domains for Guest Access Service** in *Opening Firewall Ports for Device Communication* section under *Getting Started with HPE Aruba Networking Central*.

For more information on Cloud Authentication and Policy application in Entra ID portal, see Create an Entra ID application and service principal that can access resources in the Entra ID documentation.

Configure API Permissions for Cloud Authentication and Policy Application

After registering the application, you must configure the following API permissions to call APIs:

- Directory.Read.All
- Group.Read.All
- User.Read
- User.Read.All

In the Entra ID portal, for the registered Cloud Authentication and Policy application, ensure that the API permission type is selected as **Application permissions** in the **API permissions** > **Add a permission** > **Microsoft Graph**.

For more information, see **Introduction to permissions and consent** section under Permissions and access in the Microsoft Entra ID portal.

After adding the API permissions, ensure to grant admin consent for all API permissions. To do this, select **Grant admin consent** in the **API Permissions** page. You must have administrator rights to grant admin consent.

For more information on configuring API permissions for Cloud Authentication and Policy application, see Configure a client application to access a web API in the Entra ID documentation.

Configure Client Secret ID for Cloud Authentication and Policy Application

The client secret is a string value and is used to identify the Cloud Authentication and Policy application when requesting an access token from the Microsoft identity platform token endpoint. Access token is used in the Microsoft Graph API to get information about users.

For more information, see Add a client secret.

The **Value** and **Secret ID** are generated for the client. Ensure to note down these values to use in the Cloud Authentication and Policy application. This secret value is never displayed again after you leave this page.

For more information on configuring the client value and secret ID for Cloud Authentication and Policy application, see Create a client secret in the Entra ID documentation.

APIs for Microsoft Entra ID

The following APIs are used by Cloud Authentication and Policy to authorize users in Microsoft Entra ID:

- **`GET https://graph.microsoft.com/v1.0/users/{id | userPrincipalName}`**
- **`GET https://graph.microsoft.com/v1.0/users/{id | userPrincipalName}/memberOf`**

Google Workspace

Google Workspace includes collaboration tools from Google like Gmail, Calendar, Meet, Chat, Drive, Docs, Sheets, Slides, Forms, and Sites. Organizations that use Google Workspace manage their organization's data, users, and apps from a single portal.

In HPE Aruba Networking Central, administrators can configure user policies based on the user groups defined in the Google Workspace identity store. When creating a user policy, the network administrator must provide the information listed in Getting Information from Google Workspace.

When the administrator deletes or suspends a user from Google Workspace, Cloud Authentication application receives a notification about the event. The application revokes any certificates provisioned to the user and disconnects any active sessions for the user. This change is reflected within a short span of time.

To register Cloud Authentication in Google Workspace, see the following topics:

- Configuring Google Workspace in Cloud Authentication
- Providing Access to Google Workspace Instance

Getting Information from Google Workspace

To configure Google Workspace in the Cloud Authentication and Policy application, you will need the following information:

- Customer ID
- Domain
- Client ID
- Client Secret
- JSON file

Get Customer ID and Domain Information

To get the **Customer ID** and **Domain** information, complete the following steps:

1. Open the URL *https://admin.google.com* to access the Google Admin Console.
2. Log in using Google admin credentials.
   The **Google Admin** dashboard is displayed.
3. From the left navigation pane, select **Account** > **Account settings**.
   The **Account Settings** page is displayed.

Ensure to note the **Customer ID** displayed in the **Profile** section.

4. From the left navigation pane, select **Domains** > **Manage Domains**.
   The **Manage Domains** table is displayed.
   Ensure to note the primary domain name.

Get Client ID and Client Secret

To get the **Client ID** and **Client Secret**, complete the following steps:

1. Open the *https://console.cloud.google.com/* URL to access the Google Cloud Platform.
2. Log in using Google administrator credentials.
   The **Google Cloud Platform** dashboard is displayed.
3. Select the project created for Cloud Authentication and Policy application.
4. From the left navigation pane, select **APIs & Services** > **Credentials**.
   The Credentials page is displayed.
5. In the **OAuth 2.0 Client IDs** section, click the client name.
   The Client ID for Web application page is displayed.
6. Note down the **Client ID** and **Client Secret**.

To generate and download the JSON file, see Creating a Service Account.

Now you have the required information to configure Google Workspace in the Cloud Authentication and Policy application.

Configuring Google Workspace in Cloud Authentication

This section describes the steps to be performed in the Google Workspace administration and developer console to register the Cloud Authentication and Policy application and provide access to the Google Workspace instance.

To integrate Google Workspace with the Cloud Authentication and Policy application and fetch user's attributes from Google Workspace, complete the following steps:

1. **Get the Customer ID and Domain Information**

To configure Google Workspace in the Cloud Authentication and Policy application, get the customer ID and domain information from the Google Admin Console. For instructions, see Get Customer ID and Domain Information.

For more information on getting customer ID and domain information from the Google Admin Console, see **Find your customer ID** and **Access your Google Workspace domain settings** in the Google Workspace documentation.

2. **Create a Project in Google Cloud Platform**

Create a new project for Cloud Authentication and Policy to authenticate the application with Google Cloud Platform. Enable the Admin SDK API to view and manage users and groups in Google Workspace.

To create a new project in Google Cloud Platform, you must have administrator rights.

For instructions, see Create a project and enable the API.

Configuring OAuth Consent Screen

Configure **OAuth consent screen** to register the application. After you get an authorization from Google, you can access and manage the user data.

For more information, see Configure the OAuth consent screen.

Configuring the OAuth consent screen is a pre-requisite for creating the OAuth Client ID.

Creating Credentials

The Google Workspace Admin API and Cloud Authentication and Policy application integration requires credentials to authenticate the Google Workspace Admin API.

On the **Credentials** page, you can create the **OAuth Client ID** and **Service Account**.

Creating OAuth Client ID

The client ID is used to identify the Cloud Authentication and Policy application by Google's OAuth servers.

In the **Authorized redirect URIs** section, click **ADD URI** to add **OAuth** and **Reply URLs** of the **Cloud Guest** server. The reply URL must be in the *https://<cloud guest server>/oauth/reply* format.

For more information about Cloud Guest server URLs, see **Cloud Guest Server Domains for Guest Access Service** in *Opening Firewall Ports for Device Communication* section under *Getting Started with HPE Aruba Networking Central*.

For more information on creating credentials in the Google Cloud Platform, see **Setting up OAuth 2.0** in the Google Cloud Platform Console documentation.

Creating a Service Account

Create a service account to enable server-to-server, application-level authentication between the Cloud Authentication and Policy application and Google Workspace. The service account allows the Cloud Authentication and Policy application to make API calls by using the service account's credentials to request user data from Google Workspace.

- For more information on creating a service account in the Google Cloud Platform, see **Create a service account** in the Google Workspace documentation.
- Ensure to note the Unique ID as this will be used to enable the Google Workspace domain-wide-delegation.
- Ensure to upload the JSON file after configuring Google Workspace in cloud authentication.

Providing Access to Google Workspace Instance

Cloud Authentication and Policy application requires access to Google Workspace instance (customer instance) to retrieve the user data.

To provide access to Google Workspace, complete the following steps in the **Google Admin Console**:

1. Open the *https://admin.google.com* URL to access the Google Admin Console.
2. Log in using Google admin credentials.
   The **Google Admin** dashboard is displayed.
3. Select **Enable Google Workspace domain-wide-delegation** for the service account.
4. Enter the following comma separated **Oauth scopes**:
   - https://www.googleapis.com/auth/admin.directory.user.readonly
   - https://www.googleapis.com/auth/admin.directory.group.readonly

For more information on enabling Google Workspace domain-wide-delegation and add Oauth scopes, see **Control API access with domain-wide delegation** Google Workspace documentation.

On successful authorization, the Cloud Authentication and Policy application is authorized to retrieve the user group membership, and role information from the **Google Workspace**.

An invalid Client Secret will only show up as an authentication error when connecting to network.

APIs for Google Workspace

The following APIs are used by Cloud Authentication and Policy to authorize users in Google Workspace:

- `GET https://admin.googleapis.com/admin/directory/v1/users`
- `GET https://admin.googleapis.com/admin/directory/v1/groups?userKey={userKey}`

Providing Access to Google Workspace Instance

Cloud Authentication and Policy application requires access to Google Workspace instance (customer instance) to retrieve the user data.

To provide access to Google Workspace, complete the following steps in the **Google Admin Console**:

1. Open the *https://admin.google.com* URL to access the Google Admin Console.
2. Log in using Google admin credentials.
   The **Google Admin** dashboard is displayed.
3. Select **Enable Google Workspace domain-wide-delegation** for the service account.

4. Enter the following comma separated **Oauth scopes**:
   - https://www.googleapis.com/auth/admin.directory.user.readonly
   - https://www.googleapis.com/auth/admin.directory.group.readonly

For more information on enabling Google Workspace domain-wide-delegation and add Oauth scopes, see **Control API access with domain-wide delegation** Google Workspace documentation.

On successful authorization, the Cloud Authentication and Policy application is authorized to retrieve the user group membership, and role information from the **Google Workspace**.

APIs for Google Workspace

The following APIs are used by Cloud Authentication and Policy to authorize users in Google Workspace:

- **`GET https://admin.googleapis.com/admin/directory/v1/users`**
- **`GET https://admin.googleapis.com/admin/directory/v1/groups?userKey={userKey}`**

Okta Workforce Identity Cloud

Okta Workforce Identity Cloud is an identity and access management solution which enables organizations to authenticate and authorize user access across apps and devices. It offers single sign-on (SSO), multi-factor authentication (MFA), and identity verification.

Configuring Captive Portal with Okta is currently not supported.

In HPE Aruba Networking Central, administrators can configure user policies based on the user groups defined in the Okta Workforce Identity Cloud identity store.

When creating a user policy, the network administrator must provide the information listed in Getting Information from Okta Workforce Identity Cloud.

When the administrator deletes or suspends a user from Okta Workforce Identity Cloud, the Cloud Auth application receives a notification about the event. The application revokes any certificates provisioned to the user and disconnects any active sessions for the user. This change is reflected within a short span of time.

If a user is removed from a group for which the user is currently authorized, the user is disconnected and will have to re-authenticate again.

To configure Okta Workforce Identity Cloud and for more information about the APIs used, see:

- Configuring Okta Workforce Identity Cloud
- APIs for Okta Workforce Identity Cloud

Getting Information from Okta Workforce Identity Cloud

To configure Okta in the Cloud Auth application, you will need the following credentials:

- Okta Domain
- Client ID
- Client Secret
- Service Client ID
- Service Client Secret

Okta Workforce Identity Cloud Credentials

You can obtain the Okta domain from the Okta Workforce Identity Cloud Administration Console. For more information, see https://developer.okta.com/docs/guides/find-your-domain/main/.

To obtain the Client ID and Client Secret, you must first install the Cloud Auth OIDC application. For more information, see Configuring Okta Workforce Identity Cloud.

1. Log in to the **Okta Workforce Identity Cloud** administration console.
2. Navigate to the **Applications** tab and click **Applications**.
3. Select the **Cloud Auth OIDC** application.
4. Select **Sign On**.
5. In the **OpenID Connect** section, copy the **Client ID** and **Client Secret**.

The Service Client ID and Service Client Secret is obtained from the Cloud Auth API Service application. For more information, see Configuring Okta Workforce Identity Cloud.

1. Log in to the **Okta Workforce Identity Cloud** administration console.
2. Navigate to the **Applications** tab and click **API Service Integrations**.
3. Select the **Cloud Auth API Service** application.
4. In the **Client Credentials** section, copy the **Client ID** as the **Service Client ID**.
5. If the **Service Client Secret** is not copied during the time of installation or if a new client secret is needed, use the **Generate new secret** link and copy the **Service Client Secret**.

Configuring Okta Workforce Identity Cloud

This section describes the steps to be performed in the Okta Workforce Identity Cloud administration to register the Cloud Auth application and provide access to the Okta Workforce Identity Cloud instance.

To configure Okta Workforce Identity Cloud as an identity provider, you must install the following applications:

- Configuring Okta Workforce Identity Cloud
- Cloud Auth API Service

Cloud Auth OIDC

To install the **Cloud Auth OIDC** application, complete the following steps:

1. Log in to the **Okta Workforce Identity Cloud** administration console.
2. Navigate to the **Applications** tab and click **Applications**.
3. Click **Browse App Catalog**.
4. Select **OIDC** in the **Functionality** section.
5. Search for **Cloud Auth OIDC** and select the **Cloud Auth OIDC** application.
6. Select **Add Integration** and click **Done.**
7. Select **Sign On**.
8. In the **Settings** section select **Edit**.
9. Scroll down to the **Advanced Sign-on Settings**.
10. Copy the Redirect URI obtained from the user access policy and paste it in the **Redirect URI** field which is located above the help text. For more information, see Copy Redirect URI.

11. In the **Credentials Details** section, for **Application username format**, select **Email**.
12. Click **Save**.

For the Cloud Auth OIDC application to authenticate a user, the user must be assigned the application. For more information about how users are assigned to applications, see https://help.okta.com/en-us/content/topics/users-groups-profiles/usgp-assign-apps.htm.

Cloud Auth API Service

To install the **Cloud Auth API Service** application, complete the following steps:

1. Log in to the **Okta Workforce Identity Cloud** administration console.
2. Navigate to the **Applications** tab and click **Applications**.
3. Click **Browse App Catalog**.
4. Select **API** in the Functionality section.
5. Search for **Cloud Auth API Service** and select the **Cloud Auth API Service** application.
6. Select **Add Integration**.
7. Select **Install & Authorize**.
   The **Client Secret** is displayed. Copy this as the **Service Client Secret**.
8. Click **Done**.
   The **Client ID** is displayed.

APIs for Okta Workforce Identity Cloud

The following Okta core APIs are used by Cloud Auth to authorize users in Okta Workforce Identity Cloud:

- **GET /api/v1/users/${userId}**
- **GET /api/v1/users/${userId}/groups**
- **GET /api/v1/groups**

Rate Limiting

The Okta Core APIs are subject to rate limiting set by Okta, which is of consequence for two of the above APIs used in the Cloud Auth authorization flow:

- GET /api/v1/users/${userId}
- GET /api/v1/users/${userId}/groups

As a result of rate limiting, Cloud Auth restricts the authorization rate to match the Okta rate limits so that user authentications do not fail because a rate limit has been exceeded.

To communicate when user authentications may be affected by rate limits, Cloud Auth provides the following audit trail entries:

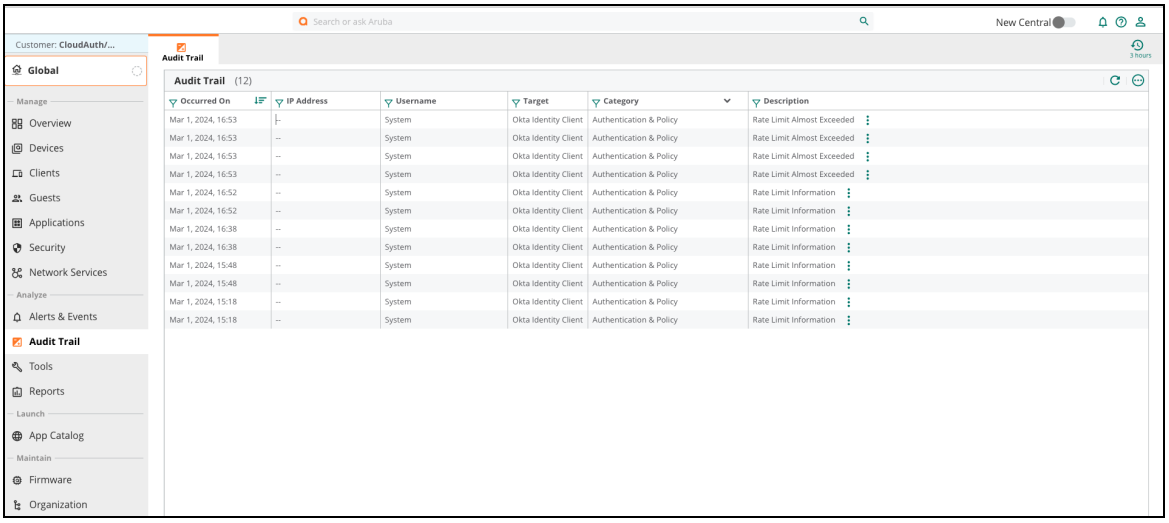
- Rate Limit Information: Indicates the rate limit for a particular API. For example, 1000 requests per minute for the GET /api/v1/users/${userId}. This audit entry does not mean that a rate limit has been exceeded.
- Rate Limit Almost Exceeded: Indicates that 95% of the rate limit for a particular API has been used.
- Rate Limit Exceeded: Indicates that the rate limit for a particular API has been exceeded.

The following are examples of each of the above audit entries that can be seen in the Central Audit Trail:

Occurred On	IP Address	Username	Target	Category	Description
Mar 1, 2024, 16:55		System	Okta Identity Client	Authentication & Policy	Rate Limit Exceeded
Mar 1, 2024, 16:53		System	Okta Identity Client	Authentication & Policy	Rate Limit Almost Exceeded
Mar 1, 2024, 16:38		System	Okta Identity Client	Authentication & Policy	Rate Limit Information

If the “Rate Limit Almost Exceeded” or “Rate Limit Exceeded” audits are seen frequently, HPE Aruba Networking recommends that your Okta Organization Administrator contact Okta support or sales about requesting a rate limit exception for the APIs listed in the above audit entries. For more information about rate limit exceptions, see https://developer.okta.com/docs/reference/rl-best-practices/#request-rate-limit-exceptions.

Figure 2 *Audit Trail*



Okta Rate Limits

In general, the rate limit for a particular API is measured in the number of API requests per minute. If, for example, within a minute the number of requests exceeds the rate limit, no more requests are allowed until the rate limit is reset at the end of the minute. For more information about Okta rate limits, see https://developer.okta.com/docs/reference/rate-limits/.

Monitoring Okta Rate Limit Usage

The audit trail entries mentioned above helps monitor the rate limit usage by the Cloud Auth API Service application, which is the endpoint for the Okta Core APIs used by Cloud Auth. However, rate limit usage by all applications across an Okta organization can be monitored from the Okta Administration Console, including usage by both the Cloud Auth API Service and Cloud Auth OIDC applications. For more information about monitoring rate limits, see https://developer.okta.com/docs/reference/rl-dashboard/.

Configuring Cloud Authentication and Policy

HPE Aruba Networking Central allows you to configure Cloud Authentication and Policy for your network to support different types of users and different deployment modes.

Cloud Authentication and Policy is supported in the MSP mode. The MSP administrator can perform the following functions:

- View dashboards, debug, troubleshoot authentication for each tenant and delete configuration on one tenant if required.
- Login and configure SSIDs for different groups with CloudAuth as the RadSec server.

To configure Cloud Authentication and Policy for MSP tenants, see Configuring User Access Policy.

For more information about updating user access policy and client access policy, see the following sections:

- Configuring User Access Policy
- Client Access Policy

Configuring User Access Policy

A default user access policy is configured by Cloud Authentication. To view the user access policy, complete the following steps:

1. In the WebUI, set the filter to **Global**.
   The global dashboard is displayed.
2. Click **Security > Authentication & Policy**.
3. Click the **Config** icon.
   The **Policies** page is displayed with the user and client access policies.

- The default policies are already configured and there is no need to configure the identity provider.
- Admin must configure the identity provider to use the user-managed MPSK. Only the admin-managed MPSK (named MPSK) will work without configuring the identity provider. For more information, see Editing User Access Policy.

Editing User Access Policy

The administrator can configure user policies by linking user groups, client tags, and client roles.

With the dual layer user policy, the administrator can configure user policies based on group membership and client tags. Earlier, the cloud authentication policies were based on only group memberships. Users will now be able to configure advanced user policies by incorporating the tags from Client Insights into user access policy decisions.

To configure a user access policy, complete the following steps:

1. In the **User Access Policy** card, in the **Policies** page, click the **Edit** icon.
   The **User Authentication** page appears.
2. Complete the following steps to configure an identity provider:

- To configure **Microsoft Entra ID** as your identity provider:
  a. Select **Microsoft Entra ID** from the **Identity Provider** drop-down list.

If you had configured Google Workspace as your identity provider, a **Confirm Change** pop-up window is displayed when you select Microsoft Entra ID. Click **Confirm** to proceed.

  b. Enter the following parameters:
    - **Tenant ID**—The tenant ID that is used by Cloud Authentication and Policy application when it communicates with the Microsoft Entra ID.
    - **Client ID**—The client ID that is used to identify the Cloud Authentication and Policy application with Microsoft Entra ID.
    - **Client Secret**—The client secret that is used to identify the Cloud Authentication and Policy application when requesting an access token from the Microsoft identity platform token endpoint. Access token is used in the Microsoft Graph API to get information about users.

- To configure **Google Workspace** as your identity server, do the following:
  a. Select **Google Workspace** from the **Identity Provider** drop-down list.

If you had configured Microsoft Entra ID as your identity provider, a **Confirm Change** pop-up window is displayed when you select Google Workspace. Click **Confirm** to proceed.

  b. Configure the following parameters:
    - **Customer ID**—The customer ID that is used to identify the Cloud Authentication and Policy application with Google Workspace.
    - **Domain**—The domain name that is used to identify the domain of your organization on Google Workspace.
    - **Administrator Email**—The administrator email ID that is associated with the Google Workspace account.
    - **Client ID (Open ID)**—The client ID that is used to identify Cloud Authentication and Policy application on Google Workspace.
    - **Client Secret**—The client secret that is used to identify the Cloud Authentication and Policy application while authenticating with authorization server.

      The client secret is shared only between the Cloud Authentication and Policy application and the authorization server.
    - **Credentials File**—The credentials file contains a private key for the service account. Drag and drop the credentials file, or click **browse** and navigate to the credentials file on your file system, and then click **Open**.

You must save the credentials file in the JSON format while configuring Google Workspace identity server. For more information, see Google Workspace.

- To configure Okta Workforce Identity Cloud as your identity server, do the following:
  a. Select **Okta Workforce Identity Cloud** from the **Identity Provider** drop-down list.
  b. Configure the following parameters:
     - **Okta Domain**—The **Okta domain** that is used by Cloud Authentication and Policy application when it communicates with Okta Workforce Identity Cloud.
     - **Client ID**—The client ID that is used to identify Cloud Authentication and Policy application to the Cloud Auth OIDC application.
     - **Client Secret**—The client secret that is used to identify Cloud Authentication and Policy application while authenticating with the authorization server. The client secret is shared only between the Cloud Authentication and Policy application and the authorization server.
     - **Service Client ID**—The API service client ID that is used to identify Cloud Authentication and Policy application to the Cloud Auth API Services application.
     - **Service Client Secret**—The API service client secret that is used to identify the Cloud Authentication and Policy application while authenticating with the authorization server.

- To set up the identity store in Microsoft Entra ID or Google Workspace console, you have to provide the redirect URI. This is the endpoint URL of the cloud guest server. To get the URI, click the **Copy Redirect URI** button. This action will instantly copy the URI on to your dashboard and the button label will change to **URI Copied**. You can then proceed with setting up the identity store.
- For Okta Workforce Identity Cloud identity provider, the redirect URI needs to be configured during the installation of the Cloud Auth OIDC application.

3. Click **Connect**.
   If the connection is successful, the **Connect** button changes to **Connected Successfully** ✓. The **User Group**, **Client Tag**, **Client Role** as well as the **Network Profile** sections, are displayed. Admin can map a **User Group** to a **Client Tag** and a **Client Role**.
   By default, the user group is set as **unspecified**, the client tag as **Any**, and the client role as **Deny**. Administrators can change the **Deny** role and use any other role that can grant the user with access to the network.
   Any device that attempts to connect to the network with user group as unspecified and client role as deny will be denied access to the network.
4. To add a new row in the **User Groups to Client Role Mapping** table, do the following:
   a. Click the **+** icon.
      A new row is added in the **User Groups to Client Role Mapping** table.
   b. Select a user group from the **User Group** drop-down list.

The values in this drop-down list are mapped to the user groups that are created or configured on the identity provider's server.

c. Select a client tag from the **Client Tag** drop-down list. The system tags as well as user defined tags from Client Insights are listed in this drop-down.

If a user group to client tag and client role mapping is specified as Any, then tags are ignored for this rule. In this case, during policy evaluation, only the user group is checked for the user connecting to the network. When client tags are added in the rules and matched, then the rules are evaluated in the order in which they appear in the table, from top to bottom.

d. Select a corresponding client role from the **Client Role** drop-down list.

e. Repeat steps **a** to **d** to add rows and map the user group with the client tag and client role.

- A same user group can be mapped to different client tags and different client roles.
- Client Role drop-down list displays only those roles that are configured at the group level using Configuring Cloud Authentication and Policy Server in a WLAN Network. That is, Client Role drop-down list does not display the roles that are configured at device level.
- Client Role must be created for all wired and wireless configurations including those on APs, Gateways, and Switches. This will ensure that Cloud Authentication and Policy is applied globally across wired and wireless networks.
- If you delete a client role associated with a user access policy, the user access policy will not work as expected.

5. In the **Network Profile** section, do the following:

a. In the **Organization name** field, enter the organization name.

- This is the user-friendly name that is displayed as Wi-Fi connection name on client-devices based on the device support.
- This field is pre-populated with the organization name that is registered with HPE Aruba Networking Central. Based on the organization name you have provided, the **HPE Aruba Networking Onboardmobile app preview** shows how the organization name will appear in the corresponding HPE Aruba Networking Onboard mobile app.

b. Select WLAN SSID from the **WLAN for Non-passpoint clients** drop-down list. The purpose of this field is to use the selected SSID for Non-Passpoint devices using Client App. This is the SSID created in AP's WLAN configuration. For more information, see Configuring Cloud Authentication and Policy Server in a WLAN Network.

- The **WLAN for Non-passpoint clients** drop-down displays only enterprise SSIDs. As enterprise SSIDs with Cloud Auth as AAA server are applicable to the Client App (HPE Aruba Networking Onboard App), only the enterprise SSIDs are displayed in the drop-down. This list consists of only those WLAN SSIDs that are configured at a group level using Configuring Cloud Authentication and Policy Server in a WLAN Network. That is, WLAN for Non-passpoint clients drop-down list does not display the WLAN SSIDs that are configured at the device level.
- If you delete the selected WLAN SSID from the WLAN configuration, the user access policy will not work as expected.

6. Click **SAVE** to save the user policy.
7. Click the **User Access Policy** accordion to view the summary of the newly created user access policy along with the newly generated onboarding URL.

   For onboarding and provisioning client devices, you must copy the onboarding URL and share the same with the end-users.

NOTE

For the wired client device access, after upgrade to HPE Aruba Networking Central 2.5.6, save the User Access Policy. Once the policy is saved, you must install the network profile on the wired client device using HPE Aruba Networking Onboard App version 1.3 and onwards.

Manage MPSK

The Manage MPSK link will only be visible after creating a user policy. For more information, see Managing MPSK Network.

Deleting User Access Policy

To delete a user access policy, click the icon in the **User Access Policy** section and click **Confirm** in the **Confirm Delete** window.

Client Access Policy 5.23.

With HPE Aruba Networking Central, you can create access policies for different client devices in wireless and wired (AOS-CX) modes that access the enterprise network. Client access policy uses the MAC address of the client for creating client access policy. Client devices can include VOIP phones, printers, laptops, desktop computers, mobile phones, tablets, and so on.

Client tags defined in the **Clients** > **Clients Profile** page are used to identify the device type or category. You can use the system-defined tags or create custom client tags in the **Clients Profile** page. Cloud Authentication and Policy supports **Unprofiled** tag, which helps you to allow a new client to access the enterprise network that does not have any client tags associated in HPE Aruba Networking Central.

For more information, see the following topics:

- Configuring Client Access Policy
- Dynamic Authorization
- Manage MAC Registrations
- Allow All MAC Addresses

Configuring Client Access Policy

To configure Client Access Policy, complete the following steps:

1. In the WebUI, set the filter to **Global**.
   The global dashboard is displayed.
2. Click **Security > Authentication & Policy** and click **Config** icon.
   The **Policies** page is displayed.
3. Click **Setup** in the **Client Access Policy** section.
   The **MAC Authentication** page is displayed.
4. In the **Allowed MAC Addresses** table, perform one of the following steps to add MAC addresses:
   - Click the **Upload CSV File** icon in the **Allowed MAC Addresses** table.
     The Upload CSV File dialog box appears.
     a. In the **Upload CSV File** dialog box, drag and drop the CSV file, or click **browse** to locate the CSV file and click **UPLOAD**.
        The CSV file is uploaded. The **Allowed MAC Addresses** table is updated with the MAC addresses from the CSV file. A status box displays a message about the upload and shows if there are any errors. A link to download the error report is also available.

   NOTE: The CSV file must contain MAC address and the corresponding client-name of the devices that needs to be added.

   or

   - Click the **Add New Row +** icon and do the following:
     a. In **Add MAC based client**dialog box, prompt, enter the **MAC address** of the device and the **Client Name**.
     b. Click **Save**. The new MAC address is added and appears in the table.

NOTE: You can click the icon to download all the entries in the **Allowed MAC Addresses** table onto a CSV file.

5. To add a new row in the **Client Profile Tag to Client Role Mapping** table, do the following:
   a. Select a client tag from the drop-down list under **Client Profile Tag**.

NOTE:
- The values that appear in this drop-down list are mapped to system tags and user tags available in HPE Aruba Networking Central. For more information about adding Tags, see Managing Tags.
- As part of the default policy mapping, the **Unspecified** client tag is now available. Users who do not belong to any of the existing client tag will be categorized as Unspecified. You can assign a role from the **Client Role** drop-down to the unspecified client tag.

   b. Select a corresponding client role for the user group from the drop-down list under **Client Role**.
   c. To create a new row in the **Client Profile Tag to Client Role Mapping** table, click the **+** icon and repeat steps **a** and **b**.

- Client Role drop-down list displays roles that are created in the WLAN configuration. For more information, see Configuring User Roles for Instant AP Clients in HPE Aruba Networking Central Help Center.
- Client Role must be created for all wired and wireless configurations including those on APs, Gatewayss and Switches. This will ensure that Cloud Authentication and Policy is applied globally across wired and wireless networks.
- If you delete a client role associated with a client access policy, the client access policy will not work as expected.
- After 2.5.6 upgrade, **Unspecified** will be introduced replacing **Unprofiled** in the role mapping table. However, policies will continue to have the **Unprofiled** behavior until the policy is re-saved by the network administrator, once it is saved it will have the **Unspecified** behavior.

- After the upgrade, when the admin wants to make changes to the policy and save it again, it will be necessary for the Admin to select a valid role for **Unspecified**. Otherwise, the policy cannot be saved.
- **Unprofiled** will be visible in the policy summary screen, but once the policy is saved and **Unspecified** has a valid role, **Unprofiled** will not be applicable anymore and it will be removed from the UI.
- Deny role is not available for client profile tags as it is necessary for the ClearPass Device Insights to have visibility of those clients in order to profile and assign all the applicable tags. You can use a role with the least privileges for the **Unspecified** client profile tag.

6. Click **Save**.
7. Click the **Client Access Policy** accordion to view the newly created client access policy.

Deleting Client Access Policy

To delete a client access policy, click the icon in the **Client Access Policy** section and click **Confirm** in the **Confirm Delete** window.

Dynamic Authorization

When a client connects for the first time, ClearPass Device Insight (CPDI) tags for the client are not available. For this initial connection, the client role that is configured for the “Unprofiled” Client Profile tag is used to enforce network access. CPDI notifies the Cloud Authentication service in the event tags for client changes. This can be triggered when tags are available after initial profiling or for incremental changes to tags later due to various factors. In such an event, the Cloud Authentication service triggers a session disconnect.

When the client reconnects, the client role based on the updated tags as configured by Admin are used to enforce network access. If the Client Profile tag is not configured to match one of the tags assigned to the client, then the client role mapped to the “Unprofiled” Client Profile tag will be used to enforce network access.

For more information about Client Profiles and client tags, see the following topics:

- Clients Profile section in HPE Aruba Networking Central Help Center
- Managing Tags in HPE Aruba Networking Central Help Center

Manage MAC Registrations

Cloud Authentication and Policy enables administrators to register new MAC addresses and upload up to 50,000 MAC registrations using the Client Access Policy.

Devices with these registered MAC addresses can connect to the network after authentication and are assigned roles according to the client tags. For more information about client tags, see Client Access Policy.

The following operations can be performed for MAC addresses:

1. Adding MAC Addresses
2. Sorting and Searching MAC Addresses
3. Uploading MAC Addresses
4. Exporting to CSV
5. Modifying MAC Addresses

Adding MAC Addresses

This topic describes the steps for adding MAC addresses.

Prerequisites

Ensure that a client policy exists. For more information on how to configure the client access policy, see Configuring Client Access Policy.

To add a MAC address, complete the following steps:

1. In the WebUI, set the filter to **Global**.
   The global dashboard is displayed.
2. Click **Security > Authentication & Policy** and click the **Config** icon.
   The **Policies** page is displayed.

NOTE

The **Manage MAC Registration** link is enabled only if a client policy is present.

3. Click **Manage MAC Registration**.
   The MAC Registration page is displayed.
4. Click the **Add New Row** + icon to add a MAC address in the **Allowed MAC Addresses** table.
   The **Add MAC based client** dialog box appears.
5. Enter the **MAC address**, the **Client Name** (optional), and click **SAVE**.
   The MAC address is added successfully.

NOTE

- The formats supported for MAC address are—MAC address separated by colon or hyphen or MAC address with no special characters.
  For example: 01:23:45:67:89:A or 01-23-45-67-89-AB or 0123456789AB.
- Ensure that **Client Name** does not contain colon.

Sorting and Searching MAC Addresses

This topic describes the steps for sorting and searching MAC addresses.

Prerequisites

Ensure that a client policy exists. For more information on how to configure the client access policy, see Configuring Client Access Policy.

To sort MAC addresses, complete the following steps:

1. Mouse hover on the **MAC Address** and **Client Name** header row in the **Allowed MAC Addresses** table.

   An arrow appears next to these two headings.

2. Click the arrow.

   The entries under these columns are sorted in the ascending or descending order.

To search MAC addresses, complete the following steps:

1. Click the **Search** icon in the **Allowed MAC Addresses** table.
2. In the search field, type the text to search a MAC Address or a Client Name.

   The **Allowed MAC Addresses** table displays the matched output based on the text in the search field.

NOTE

You can search a MAC address by entering it in upper or lower case using the following patterns FF:FC:E9:27:B7:11 or FF-FC-E9-27-B7-11

Uploading MAC Addresses

The **Upload CSV File** icon in the **Allowed MAC Addresses** table allows users to upload MAC addresses into HPE Aruba Networking Central. After a CSV file is uploaded, the content of the file is added to the list of existing MAC addresses. Only one file can be uploaded at a time.

Prerequisites

Ensure that a client policy exists. For more information on how to configure the client access policy, see Configuring Client Access Policy.

To upload MAC addresses, perform the following steps:

1. Click the **Upload CSV file** icon in the **Allowed MAC Addresses** table.

   The **Upload CSV file** pop-up window appears.

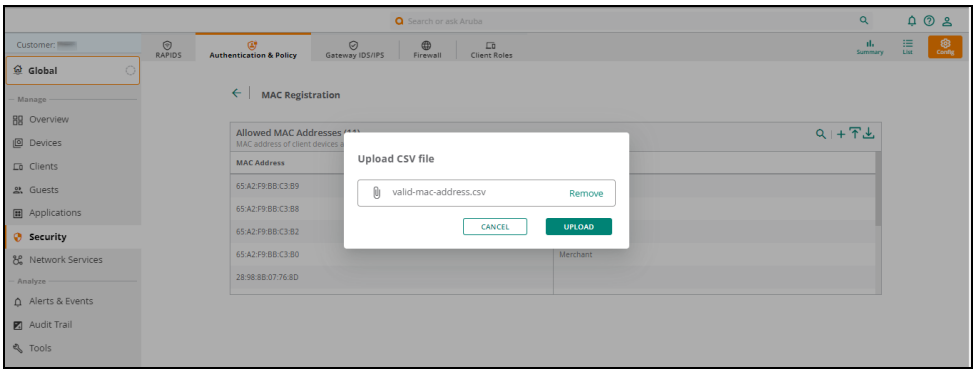
NOTE

- Client Name is optional in the CSV file.
- Maximum limit of the CSV file is 10 MB.

2. Drag and drop the CSV file, or click browse to locate the file.
3. Select the file and click **UPLOAD**.

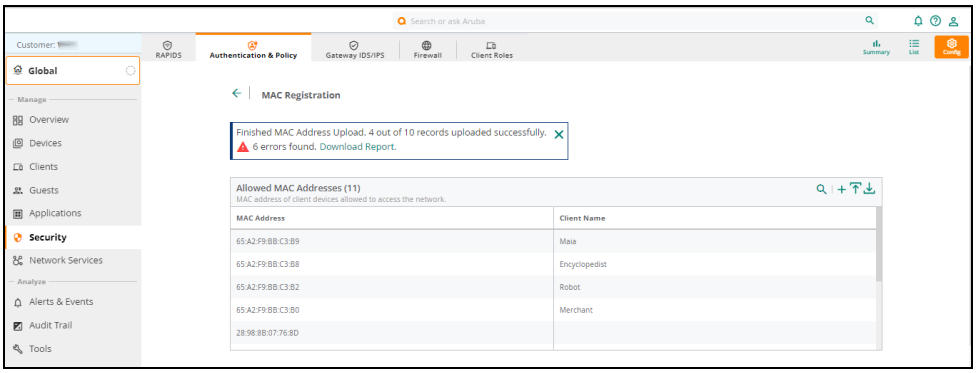
   The CSV file is uploaded and the newly added MAC addresses are displayed in the table.

   The upload summary is displayed in the status box above the table. For more information on the different states of the upload status, see Upload Status.



- The progress of the file upload is displayed in the message box.
- The total number of MAC addresses uploaded is displayed within parenthesis next to the **Allowed Mac Addresses**.
- When a file upload is in progress, you cannot upload or download files and add new MAC registrations.
- File uploads may take some time depending on the file size. Navigating from the screen or closing the browser will not interrupt the upload.

4. If the uploaded file contains an error, a message is displayed in the status box along with a link to download the error report. Click **Download Report**.



The report is downloaded to the **Downloads** folder.

5. Click **CLOSE** to dismiss the status box.

Upload Status

The following table describes the different states of the file upload status:

State	Description
In Progress	Appears when a file upload is in progress. It contains information about the total and pending number of records to be uploaded. You cannot abort the upload while it is in progress.
Successful	Appears after a file upload is successful. It contains information about the total count of uploaded records. Administrator can dismiss the status box in this state.

State	Description
Stalled	Appears if a file upload has been stalled for some time and will not proceed further. The uploaded and total number of records is displayed. When stalled, the user can start over by re-uploading the CSV file. Records that already exist will be overwritten.
Error	Appears if an upload contains records, which failed to upload. The upload continues and tries to upload all possible records. Records with errors will be listed in the report at the end of the process. The status box displays the number of failed, uploaded, and total records. A link to download the error report is available. The report provides an error for each individual failed record.

Exporting to CSV

The **Export to CSV** icon enables you to export a report in the CSV file format.

In the **Allowed MAC Addresses** table click the **Export to CSV** icon. The MAC Registration file is downloaded and appears in the downloads folder.

- A comma-separated value (CSV) file is a text file that has a specific format which allows data to be saved in a tabular format.
- If a search parameter is specified in the search text box and administrator clicks the **Export to CSV file** icon, then all MAC addresses that match the search parameter are downloaded.
- If the MAC Address and Client Name fields are sorted in ascending or descending order and administrator clicks the **Export to CSV file** icon, then only those MAC addresses matching the sort criteria are downloaded.

Modifying MAC Addresses

This section describes the steps for editing and deleting a MAC address and a client name.

Prerequisites

Ensure that a client policy exists. For more information on how to configure the client access policy, see Configuring Client Access Policy.

Editing MAC Registration

To edit an existing MAC-based client, complete the following steps:

1. In the **Allowed MAC Addresses** table, mouse hover on the row that you want to modify and click the **Edit Row** icon.
   The **Edit MAC-based Client** dialog box appears.
2. Modify the **Client Name** and click **SAVE**.
   The Client Name is updated in the table.

Ensure that the Client Name does not contain a colon.

Deleting MAC Registration

To delete an existing MAC-based client, complete the following steps:

1. In the **Allowed MAC Addresses** table, mouse hover on the row that you want to delete and click the **Delete Row** icon.
   The **Delete MAC Address** confirmation dialog box appears.
2. Click **CONFIRM** to delete the specific MAC Address row.
   The MAC address is deleted from the table.

NOTE

- On deleting the client policy, all MAC addresses will also be deleted.
- You cannot delete the client policy when a MAC address upload is in progress.

Allow All MAC Addresses

In the client access policy page, the administrator can enable the **Allow All MAC Addresses** option through which MAC addresses can get automatically registered and are visible on the UI. Only clients with registered MAC addresses can connect to the network.

For more information on enabling and disabling automatic registration of all MAC addresses, see the following topics:

- Enabling Automatic Registration of All MAC Addresses
- Disabling Automatic Registration of MAC Addresses

Enabling Automatic Registration of All MAC Addresses

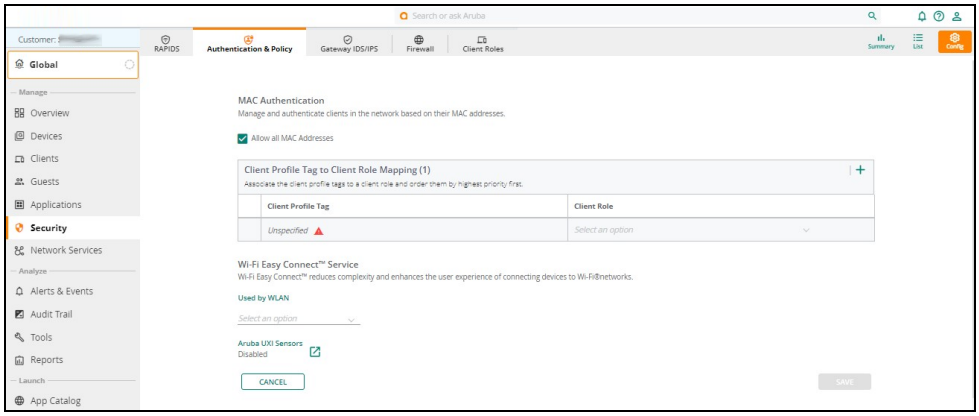
This topic describes the steps for enabling automatic registration of all MAC addresses.

Prerequisites

Ensure that a client policy exists. For more information on how to configure the client access policy, see Configuring Client Access Policy.

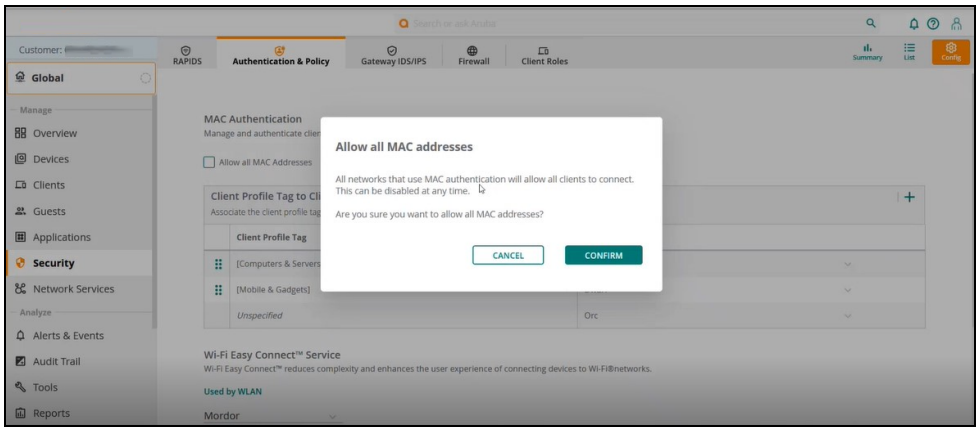
1. In the WebUI, set the filter to **Global**.
   The global dashboard is displayed.
2. Click **Security > Authentication & Policy** and click the **Config** icon.
   The **Policies** page is displayed.
3. Click the **Edit Policy** icon.
   The MAC Authentication page is displayed.
4. Navigate to the top of the MAC Authentication page and select the **Allow All MAC Addresses** check box.

Figure 3 *Allow All MAC Addresses*



The **Allow All MAC Addresses** confirmation dialog box is displayed.

5. Click **CONFIRM > SAVE**.



The policies page appears with an alert—**Allow all MAC addresses is enabled** under the Client Access Policy card. This warning will continue to appear as long as all MAC addresses are enabled. All networks that use MAC authentication will allow all clients to connect to the network.

After authenticating a device, the MAC address of the device will be added in the **Allowed MAC Addresses** table.

Disabling Automatic Registration of MAC Addresses

The administrator can disable automatic registration of MAC addresses by disabling the **Allow All MAC Addresses** option In the client access policy page.

Prerequisites

Ensure that a client policy exists. For more information on how to configure the client access policy, see Configuring Client Access Policy.

To disable MAC addresses, complete the following steps:

1. In the WebUI, set the filter to **Global**.
   The global dashboard is displayed.
2. Click **Security > Authentication & Policy** and click the **Config** icon.
   The **Policies** page is displayed.
3. Click the **Edit Policy** icon.

The MAC Authentication page is displayed.

4. In the MAC Authentication page, clear the **Allow All MAC Addresses** check box.

   Only clients with registered MAC address will be able to connect.

   Clients that are previously connected will be retained as the client is registered and the MAC address appears in the **Allowed MAC Addresses** table.

If you delete the client access policy, all registered MAC addresses will also be deleted. This includes MAC addresses registered through allow all registrations as well.

Revoke Client Certificates

Users can revoke certificates for their devices if the certificates are valid. Client certificates are valid for a specific period. Administrators or end-users can revoke certificates within the validity period.

End-users can revoke their device's certificates using the self-service portal. Administrators can revoke certificates for a specific user device through HPE Aruba Networking Central. Also, certificates are automatically revoked when the user is disabled or deleted from the Identity Store.

For a windows client, the revocation check might fail due to port 80 being blocked. This results in provisioning failure of the windows client.

For information on how to revoke certificates, see the following topics:

- Revoking Using Self-Service Portal
- Revoking Using HPE Aruba Networking Central
- Automatic Revocation

Revoking Using Self-Service Portal

Ensure you have the onboarding URL shared by the network administrator. For more information, see Onboarding Wired and Wireless Devices.

To revoke certificates using the self-service portal, perform the following steps:

1. In a web browser paste the onboarding URL into the address bar and press the **Enter** key.

   The onboarding portal is displayed.

2. Click **Manage my network credentials**.

   A **Sign in** page appears.

3. Click **Sign in for Provisioning**.

   The **Self-Service** page appears which lists the **Network Credentials**.

4. Type your username and password to login to the **Self-Service** portal.

   The **Self-Service** portal displays a list of network credentials issued to you on your devices.

5. Click the check box to revoke the specific credential and click **Revoke**.

   A confirmation message appears in a pop-up window to confirm the revoke action.

6. Click **Revoke**.

   The devices using these credentials will be disconnected from the associated network and will be denied access.

For a device to gain access to the network again, you will need to provision it with a new network profile. For more information, see Provisioning Clients.

Revoking Using HPE Aruba Networking Central

To revoke certificates using HPE Aruba Networking Central, perform the following steps:

1. In the **Aruba Central** app, set the filter to **Global**.
   The global dashboard is displayed.
2. Under **Manage**, click **Security > Authentication & Policy**.
3. Click the **List** icon and click the **Access Requests** tab.
   The **Access Requests** tab displays a table of successful and failed access requests for users and client devices.
4. Select the appropriate username and the client device for certificate revocation.
   The **Details View** page is displayed. The **Summary** and **Authorization** cards displays the device details. The **Certificate Expiration** field displays the certificate validity.

NOTE

- If the certificate is valid, the certificate expiration date is displayed along with the **Revoke** icon.
- If the certificate has expired, the certificate expired date is displayed.
- If the certificate is revoked, only the revoked date is displayed.

5. Click the Revoke icon under the **Certificate Expiration** date.
   The **Revoke Certificate** confirmation dialog box appears.
6. Click **REVOKE**.
   The client certificate is revoked and the **Certificate Expiration** displays the certificate revoked date.

Automatic Revocation

Cloud Authentication and Policy has a provision to revoke profiles and certificates of deleted users and disabled users in Microsoft Entra ID and suspended users in Google Workspace so that they do not automatically connect to the network.

When an user's account is deleted on the Identity Store, the client devices connected to the network are disconnected and their profiles or certificates are automatically revoked.

After the client devices are disconnected, the user's session will end. When the devices try to reconnect to the network, the request will be rejected due to revocation of the client's certificate. The **CLIENTS** page in HPE Aruba Networking Central will display the client **Status** as **Offline**.

To view the status of the client devices, do the following:

1. In the **Aruba Central** app, set the filter to to a device, site, label, or **Global**.
   The global dashboard is displayed.
2. Under **Manage**, click **Clients**.
   The **CLIENTS** page displays the status of the client devices.

Configuring Wired Port on an AP or IAP

The Cloud Authentication and Policy server in a wired network authenticates the end-users and client device to provide a seamless access to the network. With HPE Aruba Networking Central, you can configure the Cloud Authentication and Policy server at **802.1X Authentication** security level in the **Security** tab.

To configure a wired interface, complete the following steps:

1. In the WebUI, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
   A list of APs is displayed in the List view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click the **Interfaces** tab.

This tab is displayed only if **Show Advanced** is selected.

5. Click the **Wired** accordion.
6. To create a new wired port profile, click **+ Add Port Profile**.
   The Create a New Network page is displayed.
7. In the **General** tab, configure the general settings parameters for a wired profile.
   - Type the **Name** for the port profile.
   - In the **ports** drop-down, specify the ports.
8. Under **Advanced Settings**, configure the advanced settings parameters for a wired profile. For more information, see *Table1: Advanced Settings Parameters* in *Configuring Wireless Network Profiles on IAPs* section in the HPE Aruba Networking CentralOnline Help.
9. Click **Next**.
10. Under **VLANs**, configure the VLAN settings for a wired profile. For more information, see *Configuring VLAN Settings for Wireless Network* in *Configuring Wireless Network Profiles on IAPs* section in the HPE Aruba Networking CentralOnline Help.
11. Click **Next**.
12. In the **Security** tab, Select **802.1X Authentication** in the **Security Level** slider and specify the following parameters:
    - **Port Type Trusted**— Ensure to turn off the **Port Type Trusted** toggle switch.

If the **Port Type Trusted** toggle switch is turned on, the **Primary Server** field is not displayed.

    - **Primary Server**—Select **CloudAuth** as the primary server from the drop-down list.
    - **MAC Authentication**—By default the **MAC Authentication** is disabled.
13. Under **Access**, select **Role Based** to configure the access settings for a wired profile. For more information, see *Configuring ACLs for User Access to a Wireless Network* in *Configuring Wireless Network Profiles on Instant APs* section in HPE Aruba Networking Central Help Center.

Only Role-Based and Unrestricted access levels are used for Cloud Authentication and Policy. Network based access is not used in Cloud Authentication and Policy.

14. Click **Next**.

    The **Summary** tab displays all the settings configured in the **General**, **VLANs**, **Security**, and **Access** tabs.
15. Click **Finish**.

    A success message is displayed.
16. Click **OK**.
17. Click the **Configuration Audit** tab in the dashboard.

    The Configuration Status displays the IAP status.
18. Proceed to configure a user policy. For more information, see Configuring User Access Policy.

AOS-CX Support for Cloud Authentication and Policy

Cloud Authentication and Policy supports AOS-CX switch to manage network access.

Cloud Authentication and Policy is only supported for AOS-CX devices with firmware 10.10 or later versions. If a device with firmware version 10.09 or earlier is added to a CloudAuth-enabled group and is then upgraded to firmware 10.10 or later versions, then the CloudAuth configuration will not be pushed to the device, unless CloudAuth is disabled and re-enabled for the group.

For more information about configuring AOS-CX switch for Cloud Authentication and Policy, see the following topics:

1. Configure User Access Policy
2. Configure Client Access Policy
3. Configuring Cloud Authentication and Policy on AOS-CX
4. Configure Client Roles

Configure User Access Policy

Ensure to configure the Identity store, User Group, and the Client Role. For more information, see Configuring User Access Policy. After configuring the user access policy, you must onboard and provision the client devices. To do this, see Provisioning Clients.

Configure Client Access Policy

Ensure client device MAC addresses are added to the Allowed MAC Addresses list under the Client Access Policy. For more information, see Configuring Client Access Policy.

To configure Cloud Authentication and Policy on AOS-CX, complete the following steps:

After the HPE Aruba Networking Central upgrade to 2.5.6, for the wired client device access to function, users must edit and save the User Access Policy post the upgrade. After the policy is saved, users seeking wired access can re-provision their wired clients using the HPE Aruba Networking Onboard App 1.3 or later versions. This will ensure that the wired network profile is configured on the clients. The client devices can now connect to the AOS-CX ports enabled for 802.1x or MAC Authentications to get Cloud Authentication and Policy driven access.

Configure Client Roles

For information on configuring client roles, see Configuring Client Roles for AOS-CX in HPE Aruba Networking Central Help Center.

In deployments where network devices like APs, IAPs, and Gateways, other than AOS-CX switches are also deployed, the Client Roles defined specifically in AOS-CX configurations will have lower precedence and as a result will not show up in the Cloud Authentication and Policy Configurations. To overcome this limitation, you must maintain the same role names across all device types in such deployments.

Configuring Cloud Authentication and Policy on AOS-CX

To configure Cloud Authentication and Policy on AOS-CX, complete the following steps:

1. In the WebUI, set the filter to a group or a device containing at least one switch.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Switches**
   A list of switches is displayed in the List view.
3. Click the **Config** icon.
   The **Configuration Status** page for the switches is displayed.
4. Under **Security**, click **Authentication Servers**.
5. In the **Server Groups** window, click the edit icon for **Cloud Auth**.
   The **Edit Cloud Auth** window appears.
6. Enable the Cloud Auth toggle button and click **Save**.
7. Navigate to the **Configuration Status** page and in the **Security** card click **Authentication**.
   The **Authentication** page is displayed.
8. In the 802.1X Authentication card, select **Cloud Auth** from the **Server Group** drop-down list.
9. For enabling MAC Authentication, in the **MAC Authentication** card, select Password Authentication Protocol (**PAP**) mode and select **Cloud Auth** from the **Server Group** drop-down list.

The Challenge-Handshake Authentication Protocol (CHAP) mode of authentication is not supported for the Cloud Auth Server Group.

10. In the Ports table, select the port for which you want to configure authentication, and click the edit icon.
    The **Edit Port** card appears.
    From the **Authentication** drop-down list, choose 802.1X or MAC method for authentication.
11. Click **Apply**. The authentication parameters are displayed in the Ports table.
12. Click **Save**.
    An update successful message is displayed. The configuration is pushed to the switch once CloudAuth is enabled. This will help in troubleshooting on the switch.

Wi-Fi Easy Connect for UXI Sensors

Wi-Fi Easy Connect uses Device Provisioning Protocol (DPP) which is a provisioning protocol certified by Wi-Fi Alliance. With Wi-Fi Easy Connect, Wi-Fi enabled devices can easily and securely be provisioned. HPE Aruba Networking User Experience Insight (UXI) devices support Wi-Fi Easy Connect and can be deployed and onboarded easily and securely.

For more information about configuring DPP, see the following topics:

- Integrating UXI sensors with HPE Aruba Networking Central
- Enable DPP
- Configuring DPP
- Supported Models, Modes, and Devices

Integrating UXI sensors with HPE Aruba Networking Central

Ensure to integrate the UXI sensors with HPE Aruba Networking Central before you configure DPP.

Perform the following steps:

1. In the WebUI, set the filter to **Global**.
   The dashboard context is displayed.
2. Under **Maintain** click **Organization > Platform Integration**.
   The Platform Integration page is displayed.
3. In the **API Gateway** card, click **Rest API**.
4. In the API Gateway page, click **System Apps and Tokens** tab.
5. Click the **+Add Apps and Tokens** icon.
   The **NEW TOKEN** pop-up window is displayed.
6. Enter an **APPLICATION NAME** to easily identify where the token is being used and click **Generate**.
7. Once the token is generated, copy the Client ID and Client Secret to any text editor such as, Notepad or BBEdit.
8. Navigate to the **Token List** table and click on **Download Token** to download and save the **JSON** file.
9. Navigate to the **APIs** tab and note down the URL listed under Documentation.
10. Log in to the UXI Dashboard (https://dashboard.capenetworks.com/login).
11. Navigate to **Settings > Account > Integrations**.
12. Click on **Link Central Account**.
13. The **Add HPE Aruba Networking Central** page is displayed.

    Enter the following parameters:

    1. **Central Client ID** - Enter the Client ID (as noted in step 7).
    2. **Secret** - Enter the client secret (as noted in step 7).
    3. **Token** - Click **Choose a file** to upload the JSON file obtained from the Central dashboard.
    4. **Server Type** - Choose **Cloud**.
    5. **Cluster URL** - In the Central dashboard, navigate to the **APIs** tab, copy the FQDN portion of the URL listed under **Documentation** and paste this in the Cluster URL text field.
       For example, if the URL listed is https://apigw-sanjose.arubalive.cloud.hpe.com/swagger/apps/nms/, you must paste https://apigw-sanjose.arubalive.cloud.hpe.com in the Cluster URL text field.
    6. Click **Add**.

    The UXI and HPE Aruba Networking Central accounts are synced and is displayed on the UXI Dashboard.

Enabling DPP in WLAN

To enable DPP in WLAN, see *Enabling DPP in WLAN SSID Profile* under *Device Provisioning Protocol* section in HPE Aruba Networking Central Help Center.

Enabling DPP Provisioning in Radio Profile

To enable DPP provisioning in the Radio Profile, see *Enabling DPP Provisioning in Radio Profile* under *Device Provisioning Protocol* section in HPE Aruba Networking Central Help Center.

Configure DPP in Cloud Authentication and Policy

To configure DPP, a Client Access Policy must be created. For more information, see Client Access Policy.

Complete the following procedure:

1. In the WebUI, set the filter to **Global**.
   The global dashboard is displayed.
2. Click **Security > Authentication & Policy**.
3. Click the **Config** icon.
4. Click **Setup** in the **Client Access Policy** section.
   The client policy page appears.
5. Navigate to the **Wi-Fi Easy Connect Service**.
6. From the **Used by WLAN** drop-down, select the WLAN used by DPP.
7. Click **Save**.
   A DPP policy is created.
8. Click the **Client Access Policy** accordion.
   The drop-down will display the **Wi Fi Easy Connect service** with the DPP WLAN and will show the **HPE Aruba Networking UXI sensors** as enabled.

Supported AP models and AOS version

UXI sensors supports all AP models except AP-1xx and AP-6xx. It supports AOS version 10.4 and onwards.

Supported Deployment mode

UXI sensors are supported only in the underlay mode.

Supported UXI Sensor models

The following UXI devices are supported:

- UX-G6 (Wi-Fi Only) - R7H75A
- UX-G6C (With Cellular) - R7H76A

Enable DPP

To enable DPP, see the following topics:

Enable DPP in WLAN

To enable DPP in WLAN, see *Enabling DPP in WLAN SSID Profile* under *Device Provisioning Protocol* section in HPE Aruba Networking Central Help Center.

Enable DPP Provisioning in Radio Profile

To enable DPP provisioning in the Radio Profile, see *Enabling DPP Provisioning in Radio Profile* under *Device Provisioning Protocol* section in HPE Aruba Networking Central Help Center.

Configuring DPP

Prerequisites

Ensure that a client policy exists. For more information on how to configure the client access policy, see Configuring Client Access Policy.

To configure DPP, complete the following steps:

1. In the WebUI, set the filter to **Global**.
   The global dashboard is displayed.
2. Click **Security > Authentication & Policy**.
3. Click the **Config** icon.
4. Click **Setup** in the **Client Access Policy** section.
   The client policy page appears.
5. Navigate to the **Wi-Fi Easy Connect Service**.
6. From the **Used by WLAN** drop-down, select the WLAN used by DPP.
7. Click **Save**.
   A DPP policy is created.
8. Click the **Client Access Policy** accordion.
   The drop-down will display the **Wi Fi Easy Connect service** with the DPP WLAN and will show the **HPE Aruba Networking UXI sensors** as enabled.

Supported Models, Modes, and Devices

The following are the list of supported models, modes, and devices for UXI sensors:

- UXI sensors supports all AP models except AP-1xx and AP-6xx. It supports AOS version 10.4 and onwards.
- UXI sensors are supported only in the underlay mode.
- UXI devices UX-G6 (Wi-Fi Only) - R7H75A and UX-G6C (With Cellular) - R7H76A are supported

MPSK Support

Cloud Authentication supports Multi Pre-Shared Key (MPSK).

A Multi Pre-Shared Key (MPSK) is the network password that a user or device uses to connect to the network in HPE Aruba Networking Central. MPSK can be unique for an individual user or admin created entity. The behavior is identical to a normal PSK network other than multiple keys that exist on the same SSID, which allow different authorizations to be applied when using the Cloud Authentication functionality.

Cloud Authentication requires AOS-10.4 and above software versions to support the MPSK feature.

MPSK passwords are generated using the following options:

- **Passphrase**—is an unpredictable string or sequence of words that is longer than a traditional password. For example: "bleak tinker avenge lively".
- **Random password**—is similar to a traditional password that is auto-generated using a combination of letters and numbers. For example: "kdcc8mht".

Pre-Shared Keys (PSKs) can be assigned in two ways:

- User Managed MPSK
- Admin Managed MPSK

- A maximum of 5000 MPSKs are supported in the foundation license. This applies to all the user managed, admin managed, and enabled MPSKs across all networks.
- Users can connect multiple devices with a single MPSK, without pre-registering their devices.

User Managed MPSK

These PSKs are specific to the user in the identity store and are auto-generated when the user signs in to the MPSK portal with their credentials. End-users can connect multiple devices with this MPSK.

Admin Managed MPSK

This is also referred to as **Named MPSK**. PSKs are auto-generated when the admin creates a named MPSK entry. Admin can share this with one or more users or use it to configure multiple devices.

For more information, see Named MPSK.

User Workflow

This section describes the workflow for user managed MPSK and admin managed MPSK.

User Managed MPSK

1. Navigate to the password portal.
2. Sign-in using identity store credentials.
3. Connect one or more clients to the MPSK network using the displayed password.

Named MPSK

The admin shares MPSK passwords shown in the Named MPSK table with users. Users can use the shared MPSK passwords to connect one or more clients.

MPSK Pre-configuration

Ensure that a user policy is created. For more information about creating a user policy, see Configuring User Access Policy.

To create an SSID with MPSK support, complete the following steps:

1. In the WebUI, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.

2. Under **Manage**, click **Devices > Access Points**.

   A list of APs is displayed in the List view.
3. Click the **Config** icon.

   The tabs to configure the APs are displayed.
4. Click the **WLANs** tab.

   The WLANs details page is displayed.
5. In the **WLANs** tab, click **+ Add SSID**.

   The **Create a New Network** page is displayed.
6. In the **General** tab, enter a name in the **Name (SSID)** text-box. Under **Advanced Settings**, configure the advanced settings parameters for an SSID. For more information, see *Table 1: Advanced Settings Parameters* in *Configuring Wireless Network Profiles on IAPs* section in the HPE Aruba Networking Central Online Help.
7. Click **Next**.
8. Under **VLANs**, configure the VLAN settings for an SSID. For more information, see *Configuring VLAN Settings for Wireless Network* in *Configuring Wireless Network Profiles on IAPs* section in the HPE Aruba Networking Central Online Help.
9. Click **Next**.
10. In the **Security** tab, select the following:
    - **Security Level**—Select **Personal** in the **Security Level** slider. The authentication options applicable to the personalized network are displayed.
    - **Key Management**—Select **MPSK-AES** as the encryption key from the drop-down list. This option supports multiple PSKs simultaneously on a single SSID.
    - **Primary Server**—Select **Cloud Auth** from the drop-down list to authenticate through a Cloud Identity provider.
11. Click **Next**.
12. In the **Access** tab, configure the access settings for an SSID. For more information, see *Configuring ACLs for User Access to a Wireless Network* in *Configuring Wireless Network Profiles on Instant APs* section in HPE Aruba Networking Central Online Help.

Only Role-Based and Unrestricted access levels are used for Cloud Authentication.

13. If **Role-based** access control is selected:
    - Under **Role**, select an existing role for which you want to apply the access rules, or click **New** and add the required role. To add a new access rule, click **Add Rule** under **Access Rules For Selected Roles**.
    - In the **Access rules** pop-up window, select the **Rule Type**, choose a **Service** option, and specify the **Action** and **Destination** from the drop-down list and click **OK**.

The default role with the same name as the network is automatically defined for each network. Default roles cannot be modified or deleted.

14. Click **Next**.

    The **Summary** tab displays all the settings configured in the **General**, **VLANs**, **Security**, and **Access** tabs.

15. Click **Finish**.
    The MPSK SSID is configured successfully.

Configuring MPSK Network

To configure an MPSK network, complete the following steps:

1. In the WebUI, set the filter to **Global**.
   The global dashboard is displayed.
2. Click **Security > Authentication & Policy**.
3. Click the **Config** icon.
   The **Policies** page is displayed.

If an user policy is already created, the **Manage MPSK** link is visible in the User Access Policy section.

4. Click **Manage MPSK**.
   The **MPSK Management** screen appears. You can add new MPSK networks, configure, or delete existing MPSK networks.
5. Click the **Add MPSK Network** icon.
6. Select an MPSK SSID from the **WLAN** drop-down list and click **SAVE**.
   The MPSK network is configured and the **Password Portal** is enabled.
   Administrators can share the password portal with end-users. End-users can use this portal to generate and retrieve their personal MPSKs.

Managing MPSK Network

To modify or update an existing MPSK network, complete the following steps:

1. In the MPSK Management page, navigate to the MPSK network section and click the configuration icon.
   The **MPSK Configuration** screen appears.
2. Modify the MPSK attributes and click **Save**.
   The MPSK configuration is updated.

Changing MPSK Type

To change the MPSK type, complete the following steps:

1. Select the desired option from the **MPSK Type** drop-down list. By default, **Passphrase** is selected.
2. Select **Reset** from the pop-up under the MPSK column.
   The MPSK is reset according to the selected MPSK Type.

- Changing the MPSK type does not impact connected devices and existing user MPSKs. It can be used as is.
- The MPSK password reset is applicable only for named MPSKs.

Deleting MPSK Network

To delete an existing MPSK network, complete the following steps:

1. Click the **Delete** icon in the MPSK network section.
   The **Delete MPSK Network** confirmation box appears with the following note:

NOTE

Deleting an MPSK network will delete all named and user managed MPSKs. No clients will be able to connect to the network. The connected clients will remain connected until they try to re-authenticate. Delete the corresponding WLAN to disconnect all connected clients.

2. Click **CONFIRM**.
   The selected MPSK Network is deleted.
3. Delete the SSID from WLAN configuration.
   The SSID is deleted.

Named MPSK

The Admin Managed MPSK is also referred to as **Named MPSK**.

Prerequisite: Ensure to create an MPSK network before using the named MPSK feature. For more information, see Configuring MPSK Network.

For more information about adding, uploading, and managing named MPSKs, see the following topics:

- Adding Named MPSK
- Uploading Named MPSK
- Managing Named MPSK
- Exporting to CSV Format

Adding Named MPSK

NOTE

In the MPSK Management page, hover over the information icon under the **MPSK Usage**. A pop-up displays the number of MPSKs allocated per SSID, the MPSK limit, and the remaining number of MPSKs. MPSK entries can be added, but cannot exceed the remaining number of MPSKs.

To add a named MPSK to an MPSK network, complete the following steps:

1. In the MPSK Management page, click the configure icon.
   The **MPSK Configuration** screen appears.
2. Click the **Add New Row** icon in the **Named MPSK** table.
   The **Add Named MPSK** dialog box appears.
3. Enter an MPSK **Name** and select a **Client Role** from the drop-down list and click **SAVE**.
   An MPSK password is created that can be used to connect to the network.

NOTE

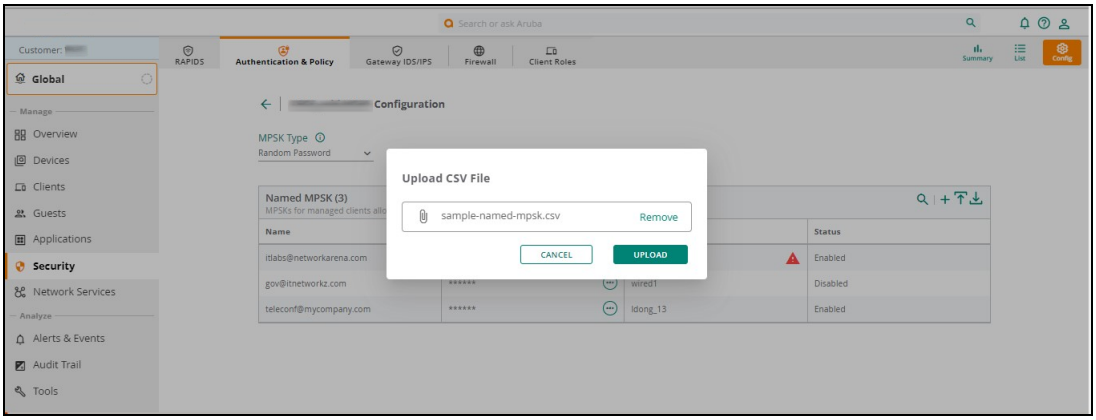
MPSK name must be in the User Principal Name (UPN) format. For example: confroom@mycompany.com.

Uploading Named MPSK

The **Upload CSV File** icon in the Named MPSK table allows the user to upload named MPSKs into HPE Aruba Networking Central. After a named MPSK file is uploaded, the content of the file is added to the list of existing named MPSKs. Only one file can be uploaded at a time.

To upload a named MPSK file, complete the following steps:

1. Click the **Upload CSV File** icon In the **Named MPSK** table.
   The **Upload CSV File** pop-up window appears.
2. Drag and drop the file or click browse to locate the file.
3. Select the file and click **UPLOAD**.
   The named MPSK file is uploaded and the successfully added MPSKs are displayed in the **Named MPSK** table.
   The upload summary is displayed in the status above the table and the individual errors can be downloaded from the link in the summary box. For more information on the different states of the upload status, see Upload Status.

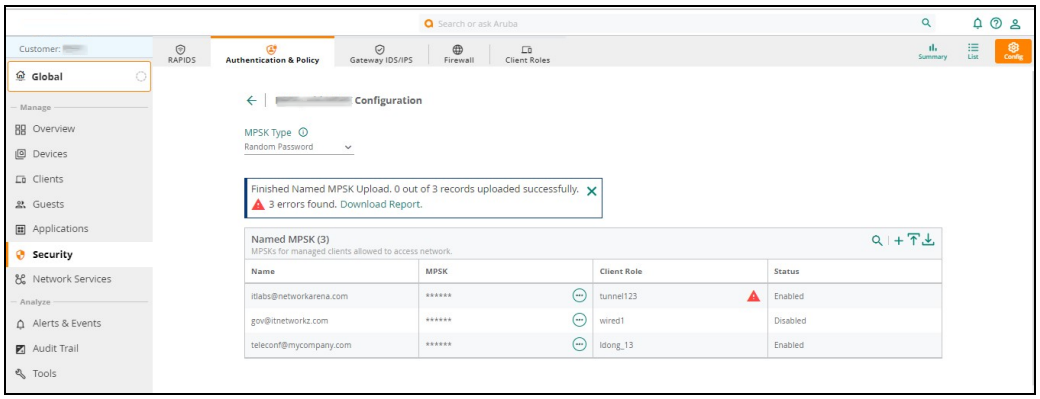


NOTE

During an ongoing upload the following operations are forbidden and will display an error:

- Another MPSK file cannot be uploaded from another SSID. The upload button will be disabled and a message is displayed indicating that the upload is in progress.
- An MPSK file cannot be downloaded for that SSID. The download button will be disabled for that SSID. However, MPSKs for other SSIDs can be downloaded.
- The particular MPSK SSID cannot be deleted. When you click the delete icon, an error message is displayed.
- When an upload is in progress, user policy cannot be deleted. If an attempt is made to delete the policy, an error message is displayed.

4. If the uploaded file contains an error, click the **Download Report** link to download the error file.



The report is downloaded to the **Downloads** folder. The error report is available only if there are errors in the uploaded MPSK file.

5. Click **Close** to dismiss the status box.

Upload Status

The following table describes the state of the named MPSK file upload status:

State	Description
In Progress	Appears when the file upload is in progress. The total and pending number of records to be uploaded is displayed.
Successful	Appears after the upload is complete. Total count of uploaded records is displayed.
Error	Appears if an upload contains records, which failed to upload. The status box displays the number of failed, uploaded, and total records. A link to download the error report is available. The report provides an error for each individual failed record.
Stalled	Appears if an upload has been stalled for some time and will not proceed further. The uploaded and total number of records is displayed. When stalled, the user can start over by re-uploading the CSV file. Records that already exist will be overwritten but it will not generate a new PSK for those records.
In progress for another SSID	Appears if an upload is ongoing for another SSID. The status box will show up for all other SSIDs indicating the upload in-progress and the name of the SSID.

Exporting to CSV Format

The **Export to CSV** option enables you to export a report in the CSV file format.

NOTE

A comma-separated value (CSV) file is a text file that has a specific format which allows data to be saved in a tabular format.

To export a report, complete the following steps:

1. In the **Named MPSK** table click the **Export to CSV** icon.
   The **Export to CSV** pop-up window appears.
2. Click **EXPORT**.

The CSV file is downloaded in the CSV format. The downloaded file displays records under the MPSK Name, Client Role, and Status fields.

3. Select the **Include MPSKs** check box and click **Export**.
   This will include the MPSKs in the CSV file.

Only administrators can export the file in the CSV format and include MPSKs. All other users can only download the file.

Managing Named MPSK

This section describes the steps for editing, deleting, and managing passwords for a named MPSK.

Editing Named MPSK, Updating Roles, and Status

To edit an existing named MPSK, complete the following steps:

1. In the **Named MPSK** table, click the **Edit** icon.
   The **Edit Named MPSK** dialog box appears and the MPSKs for the specific network are listed in the **Named MPSK** table.
2. Modify the MPSK name and click **SAVE**.
   The MPSK name is updated. This change will not impact the connected clients.
3. Click the **Client Role** drop-down and choose a client role.

Changing the **Client Role** will not impact the connected clients. The new client role will apply to future authentications.

4. To enable or disable a named MPSK, move the slider.
   The status gets updated.

If an MPSK is disabled, existing user sessions are terminated and the MPSK password is no longer valid. All clients connected using that PSK will be disconnected. This will also lead to a drop in the MPSK usage count.

5. Click **SAVE**.
   The changes are updated.
6. To search for an MPSK use the search icon. Enter an MPSK name in the search field.
   The Named MPSK table highlights the matched output based on the text in the search field.
   You can also sort the MPSKs by **Name**, **Client Role**, and **Status**.

Deleting Named MPSK

To delete an existing named MPSK, complete the following steps:

1. In the **Named MPSK** table, hover over the MPSK row you want to delete.
   The delete icon appears.
2. Click the **Delete** icon.

The **Delete Named MPSK** confirmation box appears.

3. Click **CONFIRM**.

   The named MPSK row is deleted, the connected clients are disconnected, and the password is no longer valid.

Managing Named MPSK Passwords

To manage named MPSK passwords, complete the following steps:

1. In the **Named MPSK** table, under the MPSK column click the icon.

   A pop-up appears with the options to **Copy to Clipboard**, **Reveal/Hide**, and **Reset** the generated MPSK.

2. Select the **Reveal/Hide** option to view or hide the MSPK.

   The MPSK generated is based on the MPSK type. If the MPSK type is Passphrase, the password is also in the Passphrase format.

3. Select **Reset** from the pop-up under the **MPSK** column to reset the password.

   The MPSK password is reset according to the MPSK type.

When the password is reset or revoked, all clients connected using that MPSK will be disconnected and will need to authenticate with a new password.

Configure Captive Portal

Cloud Authentication and Policy supports the captive portal which authenticates end users based on their Identity Store credentials.

To configure the captive portal, do the following:

1. Configure the user policy. For more information, see Configuring User Access Policy.
2. Creating Splash Pages
3. Creating SSID for Captive Portal
4. Connecting to Captive Portal

Creating Splash Pages

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.

If the administrator wants to change the identity store for captive portal, a new splash page must be created with that identity store, and the admin must update the SSID configuration to use that splash page.

1. In the WebUI, set the filter to a device or a group.

   The corresponding dashboard is displayed.

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

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

3. Click **Add Profile +** icon to create a splash page.
   The **NEW SPLASH PAGE** pane is displayed.
4. In the **Configuration** tab, enter the following details:
   - **Name**—Enter a unique name to identify the splash profile.

If you attempt to enter an existing splash profile name, HPE Aruba Networking Central displays a message stating that **Splash page with this name exists**.

   - **Type**—Select **Authenticated** to provide a secure network access to the guest users and visitors.
   - **Username/Password**—Enable this option as an authentication method for Cloud Authentication and Policy.
   - **Use HPE Aruba Networking Central Authentication & Policy**—Enable this option to allow captive portal to use HPE Aruba Networking Central authentication policy.
   - **Authentication Success Behavior**—This is optional. Enable this option to specify a method for redirecting users after a successful authentication. Select one of the following options:
     - **Redirect to Original URL**—When selected, upon successful authentication, the user is redirected to the URL that was originally requested.
     - **Redirect URL**—Specify a redirect URL if you want to override the original request of users and redirect them to another URL.
   - **Authentication Failure Message**—This is optional. Enter the authentication failure message text string returned by the server when the user authentication fails.
   - **Enable MAC Caching**—Select this parameter to bypass captive portal during re-authentication. To use this feature, you must configure the client policy. For more information, see Configuring Client Access Policy.

When users first login via captive portal, their MAC addresses are cached. Subsequent logins will use MAC authentication and bypass the captive portal. The cache lifetime of the MAC address is same as the session timeout after which user will have to re-authenticate using captive portal.

5. Click **Next**.
6. Click **Next** in the **Customization** tab and click **Finish** in the **Localization** tab.
   The Splash Page is configured.

- All other fields in the **Configuration** tab are not supported.
- Captive Portal sessions will end in 8 hours and require re-authentication.

Creating SSID for Captive Portal

To create an SSID for the captive portal, complete the following steps:

1. In the WebUI, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.

2. Under **Manage**, click **Devices > Access Points**.

   A list of APs is displayed in the List view.
3. Click the **Config** icon.

   The tab to configure the APs are displayed.
4. Click the **WLANs** tab.
5. In the **WLANs** tab, click **+ Add SSID**.

   The Create a New Network page is displayed.
6. In the **General** tab, enter a name in the **Name (SSID)** text-box.
7. Click **Next**.
8. Under **VLANs**, configure the VLAN settings for an SSID. For more information, see Configuring VLAN Settings for Wireless Network.
9. Click **Next**.
10. In the **Security** tab, select **Visitors** in the **Security Level** slider.
11. Under **Access Network**, enter values for the following parameters:
    a. **Type**—Select **Cloud Guest** from the drop-down.
    b. **Guest Captive Portal Profile—Select** the splash page profile name from the drop-down.
12. Click **Next**.
13. In the **Access** tab, configure the access settings for an SSID. Select the Role-based configuration and confirm that an appropriate role is configured. For more information, see Configuring ACLs for User Access to a Wireless Network.
14. Click **Next**.

    The **Summary** tab displays all the settings configured in the **General**, **VLANs**, **Security**, and **Access** tab.
15. Click **Finish**.

    The SSID for the captive portal is created successfully.

    The client can connect to this SSID after authenticating with user name and password. After the user logs in successfully, the captive portal role is assigned to the client.

Connecting to Captive Portal

For iOS devices, if a user policy is set up with Google workspace, then captive portal authentication must be done through a web browser. For more information, see Caveats.

Google and iOS Clients

Perform the following steps as a one-time configuration when connecting to an SSID at the first instance:

1. Connect to the network you want to join.
2. On your device, tap **Settings > Wi-Fi**.
3. Select **Info** next to the network that you want to join,
4. Turn off **Auto-Join** and **Auto-login**.
5. Open a browser and navigate to any http URL.
6. After the sign-in page reopens, you can choose to sign in with your Google Account.

7. After a successful sign-in, you will be able to use the Internet.
   For all subsequent connections to the network, repeat steps 5 through 7.

Other Configurations

1. Connect to the network for Captive Portal.
2. Sign-in with your identity store credentials when prompted.
3. After a successful sign-in, you will be able to connect to the network.
   For all subsequent connections to the network, follow steps 5 through 7.

Configuring Wired Port Profile on an AP or IAP using Cloud Guest

The Cloud Authentication and Policy server supports Captive Portal based authentication using Cloud Guest for users and devices connected through AP or IAP wired ports.

To configure a wired port profile on an AP or IAP, complete the following steps:

1. In the WebUI, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
   A list of APs is displayed in the list view.
3. Click the **Config** icon.
   The tab to configure the APs is displayed.
4. Click the **Interfaces** tab.
   The Interfaces page is displayed.

This tab is displayed only if **Show Advanced** is selected.

5. Click the **Wired** accordion.
6. To create a new wired port profile, click **+ Add Port Profile**.
   The Create a New Network page is displayed.
7. In the **General** tab, configure the general settings parameters for a wired profile.
   - Type the **Name** for the port profile.
   - In the **ports** drop-down list, specify the ports.
8. Under **Advanced Settings**, configure the advanced settings parameters for a wired profile. For more information, see *Table1: Advanced Settings Parameters* in *Configuring Wireless Network Profiles on IAPs* section in HPE Aruba Networking Central Online Help.
9. Click **Next**.
10. To configure the VLAN settings, complete the following steps in the **VLANs** tab:
    1. **Mode**—Select **Access** mode from the drop-down list
    2. **Client IP Assignment**—Select **Instant AP assigned**
    3. **Client VLAN Assignment**—Select **Custom**
    4. **Access VLAN**—Select a VLAN setting from the drop-down list
11. Click **Next**.

12. In the **Security** tab, set the **Security Level** sliding bar to **Visitors** and configure the following parameters:
    - **Type—Select** Cloud Guest from the drop-down list.
    - **Guest Captive Portal Port Profile**—Select the cloud guest profile from the drop-down list.

Ensure that a guest splash page (Guests ->Splash Pages) is configured with Cloud Authentication and Policy or a social login.

13. Click **Next**.
14. Under **Access**, select **Role Based** to configure the access settings for a wired profile. For more information, see *Configuring ACLs for User Access to a Wireless Network* in *Configuring Wireless Network Profiles on Instant APs* section in HPE Aruba Networking Central Help Center.

Only Role-Based and Unrestricted access levels are used for Cloud Authentication and Policy. Network based access is not used in Cloud Authentication and Policy.

15. Click **Next**.

    The **Summary** tab appears with all the settings configured in the **General**, **VLANs**, **Security**, and **Access** tabs.
16. Click **Finish**.

    A success message is displayed. The wired port profile is configured.
17. Click **OK**.
18. Proceed to connect your client devices to the configured AP or IAP wired port.

Cloud Authentication and Policy for Branch Gateways

Cloud Authentication and Policy supports wired authentication for clients connecting to Branch Gateways. Cloud Authentication and Policy can be enabled to perform 802.1X, MAC, or Cloud Guest authentication.

Configuring Cloud Authentication and Policy Using 802.1x or MAC Authentication

1. In the WebUI, set the filter to a Branch Gateway group.

   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices**, and then click **Gateways**.

   A list of gateways is displayed in the **List** view.
3. Click **Config**.

   The configuration page is displayed for the selected group.
4. Ensure you are in the **Basic Mode**.
5. Click **Policies** > **Roles**.
6. Click the **+** icon to add a user role in the **Roles** table.
7. Click the **+** icon in the **Role Assignment** table. The **Role Assignment** pop-up appears.
8. Select a VLAN ID from the **VLAN ID** drop-down list to which this role must be applied.

9. Select a role from the **Initial role** drop-down list. This role is the default user role that is assigned to the clients connecting through this VLAN.
10. From the Authentication drop-down, select one of the following options:
    - **Corporate Authentication**—choose this for Dot1x and MAC auth authentication type.
    - **Cloud Guest**—choose this for captive portal (via splash page) based authentication type.
11. Select the **Default authenticated role** from the drop-down list.
12. Select one of the following authentication modes:
    - **MAC authentication**—Select this check box to ensure that the Gateway ports configured under this VLAN are enabled to perform MAC Authentication. Based on the authentication status (Success or Failure), appropriate roles (server provided, default, or initial role) are applied.
    - **802.1X authentication**—Select this check box to ensure that the Gateway ports configured under this VLAN are enabled to perform 802.1X Authentication. Based on the authentication status (Success or Failure), appropriate roles (server provided, default, or initial role) are applied. You can also enable MAC authentication to allow clients to complete 802.1X authentication when MAC authentication fails and vice-versa.
13. Enable the **Cloud Auth** toggle switch.

    This creates the Cloud Authentication and Policy server and is assigned to its server group. These servers are mapped in the AAA profiles and used for authentications based on the authentication type (MAC or 802.1x) set in the role assignment profile.
14. Click **Save** in the Role Assignment window and click **Save Settings**.

    The settings are saved.

Configuring Cloud Authentication and Policy for Branch Gateways using Cloud Guest

You can enable Cloud Authentication and Policy for Branch Gateways using Cloud Guest.

To do this, complete the following steps:

1. In the WebUI, set the filter to a Branch Gateway group.

   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices**>**Gateways**.

   A list of gateways is displayed in the **List** view.
3. Click **Config**.

   The configuration page is displayed for the selected group.
4. Ensure you are in the **Basic Mode**.
5. Click **Policies** > **Roles**.
6. Click the **+** icon to add a user role in the **Roles** table.
7. Click the **+** icon in the **Role Assignment** table.

   The **Role Assignment** pop-up appears.
8. From the VLAN ID drop-down list, select a VLAN ID to which this role must be applied,
9. From the Authentication drop-down list, select the authentication type as **Cloud Guest**.

   The **Initial role** is auto-populated. There is no option to set the initial role.

10. Select the **Guest Captive Portal Profile** from the drop-down list.

Ensure that a guest splash page (Guests ->Splash Pages) is configured with Cloud Authentication and Policy or a social login.

11. Select the **Default guest role** from the drop-down list.
12. To update the detailed configuration settings, see the Advanced mode configurations:
    - Roles - contains initial role configuration (guest redirect role)
    - Auth Servers - Authentication Servers and Server Groups
    - Role Assignments (AAA Profile) - Authentication profile
    - L3 Authentication - Captive Portal Authentication Profile
13. Click **Save** in the Role Assignment window.
    The settings are saved and the **Role Assignment** table is updated with the configured values.

Updating Cloud Authentication and Policy

You can edit the existing user access policy and client access policy based on your requirements, which can include changing the identity server, adding new user roles, adding new client MAC addresses and so on.

If you modify the name of WLAN SSID in the WLAN configuration, the updated name will not be auto-updated in the user access policy. You must set the WLAN SSID to the updated name in the user access policy.

For more information about updating user access policy and client access policy, see the following sections:

- Updating User Access Policy
- Updating Client Access Policy

Updating User Access Policy

You can update the user access policy to change the following details:

- Configure a new identity provider.
- Add, modify, or delete a user group and client-role mappings
- Edit organization's network profile, which includes changing default WLAN SSID and the organization name.

To update the user access policy, complete the following steps:

1. In the WebUI, set the filter to **Global**.
   The global dashboard is displayed.
2. Click **Security > Authentication & Policy**.
3. Click the **Config** icon.
4. In the **User Access Policy** section, click the Edit icon to edit an external identity server.

5. Click the Delete icon in the **User Authentication** section to delete the existing identity provider, and do one of the following:

NOTE

A **Confirm Delete** pop-up window is displayed to confirm the delete action. Click **Confirm** to proceed.

   - To configure **Google Workspace** or **Microsoft Entra ID** or **Okta Workforce Identity Cloud** as your identity server, see step 5 in Configuring User Access Policy.

6. To create, edit, and delete the user group to client role mapping, do one of the following:
   - To create a new row in the **User Groups to Client Role Mapping** table, click the **+** icon, and do the following:
     1. Select a user group from the drop-down list under **User Group**.

NOTE

The values in this drop-down list are mapped to the user groups that you have created or configured in the identity provider's server.

     2. Select the corresponding client role for the user group from the drop-down list under **Client Role**.

NOTE

- Client Role drop-down list displays roles that are created in the WLAN configuration.
- If you delete a client role associated with a user access policy, the user access policy will not work as expected.

   - To edit a user group to client role mapping, do the following:
     1. Select a user group from the drop-down list under **User Group**.
     2. Select the corresponding client role for the user group from the drop-down list under **Client Role**.
   - To delete a user group to client role mapping, hover on the specific row and click the icon.
7. To edit the **Network Profile** section, do the following:
   - In the **Organization name** field, enter the organization name.
   - Select WLAN SSID from the **Connect users to WLAN** drop-down list. This WLAN SSID will be set as the default SSID for your network.

NOTE

If you delete the selected WLAN SSID from the WLAN configuration, the user access policy will not work as expected.

8. Click **Save** to save changes, or click **Cancel**.
9. Click **User Access Policy** accordion to view the updated client access policy.

External Identity Server Reconfiguration

Deleting an identity store will also delete the configuration related to the user group and roles mapping. This will impact the wired and wireless networks for dot1x, MPSK, and captive portal using this policy. Authentications for these networks will also fail.

When a new identity store is added, perform the following actions:

User Policy

Add one or more user groups to role mapping. For more information, see External Identity Server Reconfiguration in this section.

Dot1x

Redeploy user profile in the client application. For more information, see App-based Onboarding.

MPSK

Inform users to fetch new MPSK passwords from portal. For more information, see MPSK Support.

Captive Portal

Create a new captive portal splash page for all groups using this user policy. For more information, see Configure Captive Portal.

Ensure to update all the wired and wireless network configurations to use the new splash page.

AP

For changing splash page for wireless SSID in IAP, refer to **Create SSID for Captive Portal** in Configure Captive Portal.

Updating Client Access Policy

You can update the client access policy to change the following details:

- Add new MAC addresses and client names of devices that will be accessing the network
- Modify or delete the existing MAC addresses
- Add new client profile tags and client role mappings to enable access for new client devices

To update client access policy, complete the following steps:

1. In the WebUI, set the filter to **Global**.
   The global dashboard is displayed.
2. Click **Security > Authentication & Policy**.
3. Click the **Config** icon.
4. Click the icon in the **Client Access Policy** section.
5. To update MAC address details in the **Allowed MAC Addresses** table, do one of the following:
   - Click the icon to upload the CSV file in **Allowed MAC Addresses** table and do the following:

The CSV file must contain MAC address and the corresponding device-name of the devices that needs to be added.

     1. In **Upload CSV file** prompt, drag and drop the CSV file, or click **browse** and navigate to the CSV file on your file system, and then click **Open**. The file name is displayed and the **ADD** button is enabled.
     2. Click **ADD**.
   - To edit a row in the **Allowed MAC Addresses** table, select the row you want to edit and click the icon, and do the following:

NOTE

If you know the MAC address of a client, click on the icon and enter the MAC address with the ":" delimiter to view the corresponding row in the **Allowed MAC Addresses** table.

1. In the **Add MAC based client** prompt, enter the MAC address of the device and the corresponding client name in the **MAC Address** and **Client Name** fields, respectively.
2. Click **Save**.

- To create a new row in the **User Groups to Client Role Mapping** table, click the **+** icon, and do the following:
  1. On the **Add MAC based client** prompt, enter the MAC address of the device and the corresponding client name in the **MAC Address** and **Client Name** fields.
  2. Click **Save**.

NOTE

Click icon to download all the entries in the **Allowed MAC Addresses** table onto a CSV file.

6. To update one or more client-profile tag to client-role mapping, do the following:
   - Select a client tag from the drop-down list under **Client Profile Tag**.
   - Select the corresponding client role for the user group from the drop-down list under **Client Role**.

NOTE

- Client Role drop-down list displays roles that are created in the WLAN configuration.
- If you delete a client role associated with a client access policy, the client access policy will not work as expected.

   - To create a new row, click **+** icon located at the top-right corner of the **Client Profile Tag to Client Role Mapping** table and repeat steps **a** and **b**.
7. Click **Save**.
8. Click the **Client Access Policy** accordion to view the updated client access policy.

Provisioning Clients

With HPE Aruba Networking Central, administrators can configure a single Cloud Authentication and Policy that implies for both users and client devices. Administrators can configure separate user policy and client policy as part of configuring Cloud Authentication and Policy.

For more information about the workflows to provision users and client devices, see the following sections:

- Provisioning Wired and Wireless Devices
- Onboarding Wired and Wireless Devices

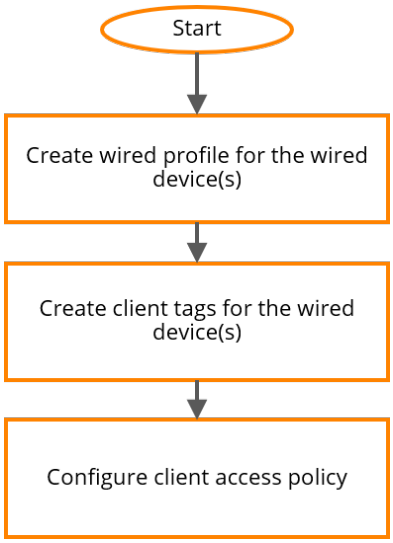
Provisioning Wired and Wireless Devices 5.23.

With HPE Aruba Networking Central, you can provision various wired and wireless devices using their MAC addresses to access enterprise WLAN networks. Client devices can include IoT devices, medical devices, printers, smart devices, gaming consoles, and so on. With HPE Aruba Networking ClearPass Device Insight, network and security administrators can discover, add devices, monitor, and automatically classify new and existing devices that connect to a network.

Cloud auth tenants are provisioned using the EC-384 bit certificates which ensure secure authentication.

With Cloud Authentication and Policy, administrators can provision wired and wireless clients by creating a client access policy to provision devices on the enterprise networks. We recommend you to assign a tag for a device before creating a client access policy. For more information about tags, see Configuring Cloud Authentication and Policy

The following workflow shows the steps required to provision wired and wireless devices using Cloud Authentication and Policy.

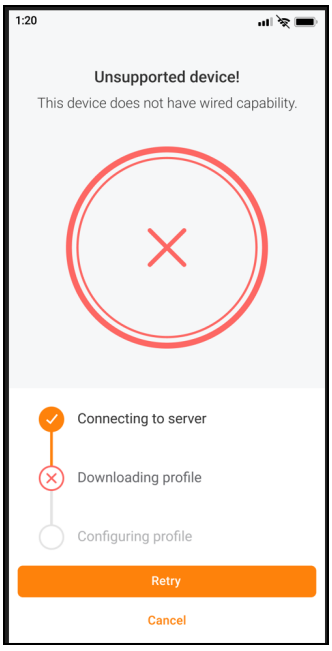


Prerequisites for Provisioning Wired and Wireless Devices

Ensure to complete the following prerequisites before provisioning wired and wireless devices.

- Configure a wired profile with **CloudAuth** as the authentication server. For more information about configuring wired SSID, see Configuring Cloud Authentication and Policy Server in a Wired Network.
- Client Profiles and Client Tags must be available in your HPE Aruba Networking Central account. Optionally, create custom tags in addition to the system tags for client devices. For more information about adding Tags, see *Managing Tags* in HPE Aruba Networking Central Help Center.
- Configure necessary client roles that are applicable for creating client access policy in Cloud Authentication and Policy. For more information about user roles and configuring user roles, see *Configuring User Roles for Instant AP Clients* in HPE Aruba Networking Central Help Center.

On devices that do not support a wired interface, if you try to provision wired-only profiles using the HPE Aruba Networking Onboard app, an unsupported device error message appears.

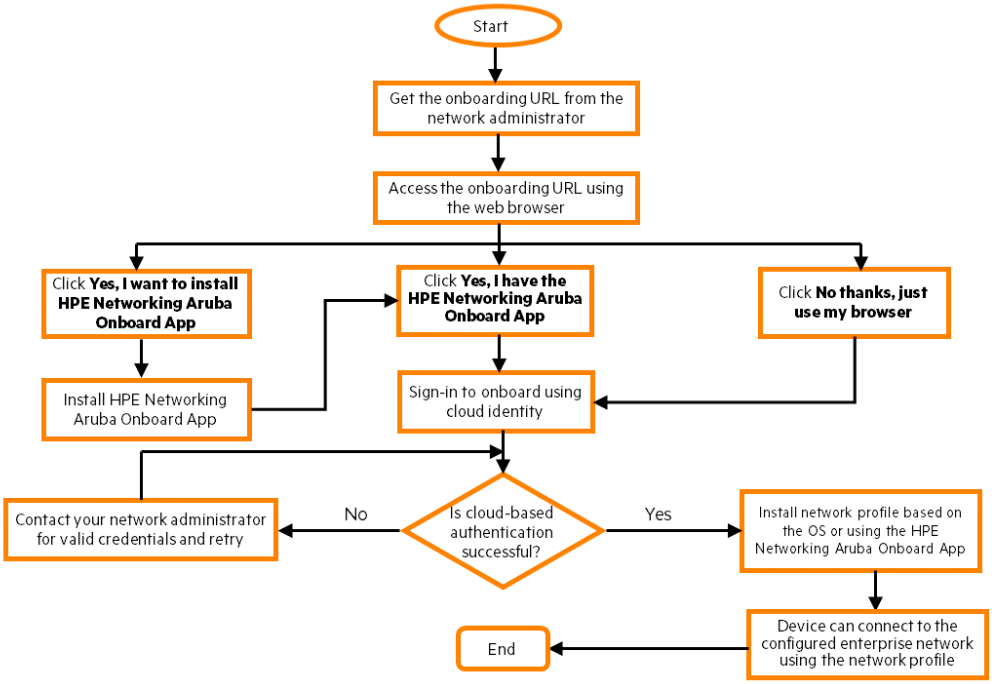


Onboarding Wired and Wireless Devices

This section describes the procedure about onboarding wired and wireless devices.

Cloud Authentication policies in *HPE Aruba Networking Central* define a set of rules and authorize users and devices to access networks. Users can authenticate through cloud identity providers like Microsoft Entra ID or Google Workspace or Okta Workforce Identity Cloud, and download network profiles to access enterprise wireless network. After downloading the network profiles, your devices can connect automatically to the enterprise wireless network.

The following workflow shows the steps required to connect wired and wireless devices to the network using Cloud Authentication and Policy.



Onboarding Workflow

The onboarding workflow for wired and wireless devices includes the following steps:

1. **Accessing the onboarding URL**

   Network administrators share the on-boarding URL and Cloud Authentication and Policy usernames to you through email or a text message. Access the URL using a web browser on your laptop or mobile device.

2. **Onboarding the Client Device**

   Onboarding enables the device to connect to the enterprise network through authenticated network profiles. You can onboard your device in two ways:

   - **Browser-based Onboarding**—Browser-based onboarding helps you to install network profiles using a web browser.
   - **App-based Onboarding**—App-based onboarding helps you to install network profiles using the HPE Aruba Networking Onboard app on your devices. App-based onboarding has the following advantages over browser-based onboarding.
     - Easy installation and configuration of network profiles for accessing networks.
     - Refresh and delete the network profiles.
     - Manage certificates and troubleshoot issues using logs.
     - Onboard Android devices that do not support Passpoint or Hotspot 2.0.
     - Easily accessible to all types of users, those who rely on keyboard navigation or screen readers, including those who are colorblind or have temporary/permanent/situational disabilities.

Ensure to use the HPE Aruba Networking Onboard app to quickly connect your devices to the network.

3. **Authentication using Cloud Authentication and Policy**

   Users should authenticate their identity using Cloud Identity providers such as Microsoft Entra ID or Google Workspace or Okta Workforce Identity Cloud to install the network profiles on their devices. Cloud auth supports the TLSv1.3 to securely authenticate clients. For more information on the supported OS versions, see Supported OS versions for TLSv1.3

4. **Installing and Managing Network Profile**

   Install and manage network profiles on your devices using the HPE Aruba Networking Onboard app or using a web browser.

Supported Operating Systems

The following operating systems support both browser-based onboarding and app-based onboarding:

- Windows 10 version 1803 or later versions
- Windows Server 2016 or later versions (supports only app-based onboarding)
- Android 9 or later versions
- macOS 10.13 or later versions
- iOS 12.1 or later versions
- ChromeOS 115 or later versions (supports only app-based onboarding)

NOTE

The iOS 15.0 and iOS 15.1 versions are not supported because of a bug in iOS. The iOS 15.2 version is supported.

Supported OS versions for TLSv1.3

- Windows 11
- Ubuntu 23.10
- macOS 14.0
- Selected Android devices (like Google Pixel) starting from Android 10

Prerequisites for Onboarding

- Ensure that you have the on-boarding URL shared by the network administrator. The onboarding URL is used to connect your device to wireless network using Cloud Auth. You should also obtain your Microsoft Entra ID or Google Workspace or Okta Workforce Identity Cloud credentials from your network administrator to authenticate using the URL.
- On Windows devices, ensure that the Wi-Fi adapter is enabled to install the network profiles and connect to the network.
- Ensure that the Hotspot 2.0 or Passpoint feature is enabled on your Android device.

NOTE

To enable the settings on Android devices, Go to Settings > Connections > Wi-Fi > Advanced > Passpoint or Hotspot 2.0. The location of the Hotspot 2.0 or Passpoint settings may differ slightly among devices.

- For better UI rendering experience on laptop devices, ensure the screen resolution is 1920x1080 (Full HD/1080p).

App-based Onboarding

App-based onboarding enables the client to seamlessly connect to the wireless or wired network.

HPE Aruba Networking Onboard App

To connect your devices to enterprise wireless networks using network profiles, you must install the HPE Aruba Networking Onboard app. With the HPE Aruba Networking Onboard app you can download and configure your network profile.

NOTE

- For all operating systems, only users with administrator privileges can install or uninstall the HPE Aruba Networking Onboard app.
- After the app is installed by an administrator, an user without administrator privileges can also use the app for provisioning.
- On Windows and Android platforms, HPE Aruba Networking Onboard App also supports devices which do not support Passpoint networks.

Installing HPE Aruba Networking Onboard App on Windows

To install the app on Windows, complete the following steps:

1. Access the on-boarding URL shared by the network administrator.
2. Select **Yes, I want to install HPE Aruba Networking Onboard**.
3. Click **Download for Windows**.
4. Double-click the .exe file.
   The **Welcome to the HPE Aruba Networking Onboard Setup** page is displayed.
5. Click **Next**.
   The **End User License Agreement** page is displayed.
   Review the agreement before you proceed to install the HPE Aruba Networking Onboard App.
6. Click **I agree**.
7. Click **Close** after the installation is complete.

NOTE

The HPE Aruba Networking Onboard App can be installed silently by using a `/s` command line parameter.

Installing HPE Aruba Networking Onboard App on an Android Device

To install the app on an Android device, complete the following steps:

1. Access the on-boarding URL shared by the network administrator.
2. Select **Yes, I want to install HPE Aruba Networking Onboard**.
3. Select the option **Get it on Google Play Store** and click **Install**.
   Follow the on-screen instructions to complete the installation.

NOTE

- On Samsung devices running Android 11 and One UI version 3.1, the HPE Aruba Networking Onboard app can be added into the deep sleep list by the OS and the network profile is automatically removed from the device. To avoid removing network profiles, add the app in the list of never sleeping apps. For more information, see Caveats.
- App-based provisioning is not supported on Oppo and Realme devices.

Installing HPE Aruba Networking Onboard App on iOS

To install the app on an iOS device, complete the following steps:

1. Access the on-boarding URL shared by the network administrator.
2. Select **Yes, I want to install HPE Aruba Networking Onboard**.
3. Click **Download on the App Store** and select **GET**.
   Follow the on-screen instructions to complete the installation.

Installing HPE Aruba Networking Onboard App on macOS

To install the app on a macOS device, complete the following steps:

1. Access the on-boarding URL shared by the network administrator.
2. Select **Yes, I want to install HPE Aruba Networking Onboard**.

3. Double-click the downloaded.pkg file and follow the on-screen instructions to complete the installation.

Installing HPE Aruba Networking Onboard App on Linux OS

To install the HPE Aruba Networking Onboard app on Linux OS, complete the following steps:

1. Access the on-boarding URL shared by the network administrator.
2. Select **Yes, I want to install HPE Aruba Networking Onboard**.
3. Click **Download for Linux**.

   The file is downloaded into your local folder.
4. Choose one of the following options to install the app.
   - Command line terminal — use the standard deb installer tools like apt, dpkg and execute the following command:

     Example: `sudo apt install -f ~/Downloads/ArubaOnboard_1.0.0-xxxxxx_amd64.deb`

Ensure to have sudo access for installation.

   - Software center (UI) — complete the following steps:
     - Double click the .deb package.

       The package opens in the Software Center.
     - Click **Install**.

       The HPE Aruba Networking Onboard app is installed.

Due to few installer issues with the software center, HPE Aruba Networking recommends to use the command line terminal method to install the HPE Aruba Networking Onboard app. For more information, see Caveats.

Installing HPE Aruba Networking Onboard App on ChromeOS

To install the app on chromeOS, complete the following steps:

1. Access the on-boarding URL shared by the network administrator.
2. Select **Yes, I want to install HPE Aruba Networking Onboard**
3. Select the option **Get it on Google Play Store** and click **Install**.

   Follow the on-screen instructions to complete the installation.

Automatic Network Profile Refresh

The network profiles and certificates installed by the HPE Aruba Networking Onboard app have a validity period. The app triggers an automatic network profile refresh before the expiration of the validity period. The app triggers an auto-refresh when the installed profile has about 20% of the validity remaining as part of the network profile. The app continues to auto-refresh at regular intervals till the profile expires.

OS limitations for each platform

Table 7: *Profile Refresh limitations for Operating Systems*

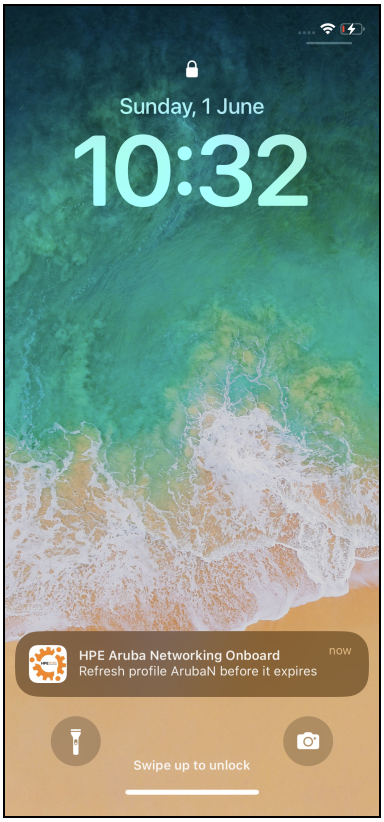
Operating System	Limitation
Android	Automatic network profile refresh is not supported due to OS limitation. User must manually refresh the network profile before it expires. For more information, see Automatic Network Profile Refresh.
iOS	Profile installed using app version prior to 1.4 will not be selected for auto refresh. User must manually refresh for these profiles.

NOTE

On Windows network profiles are refreshed automatically. On macOS, user needs to perform a manual Network Profile refresh through a notification.

Notification alert for iOS users

When the network profiles and certificates are due to expire, the HPE Aruba Networking Onboard app displays a notification alert—**Refresh profile before it expires**.



Connecting your Device to the Network

Accessing a wireless network through your devices allows you to connect to the network. Connecting to an enterprise network requires installing network profiles in the HPE Aruba Networking Onboard app. The app downloads and configures the network profile on your device to connect to an enterprise wireless network.

To connect your device to the network, complete the following steps:

1. Access the on-boarding URL shared by the network administrator.
2. Click **Yes, I have the HPE Aruba Networking Onboard app**.
3. Click **Sign in for Provisioning**.
4. Sign in using the Cloud Identity configured by the network administrator.

   To connect using your Microsoft Entra ID or Google Workspace or Okta Workforce Identity Cloud account, complete the following steps:
   a. Enter the username.
   b. Click **Next**.
   c. Enter the password.
   d. Click **Sign in**.
5. Click **Install using HPE Aruba Networking Onboard app** to install the network profile.

   The HPE Aruba Networking Onboard app is displayed after installing the network profile.
6. On the desktop, click **Open HPE Aruba Networking Onboard**.
7. In the HPE Aruba Networking Onboard app, click **Set up network profile**.

   The **HPE Aruba Networking Onboard** app onboards and installs the profile in your device in the following steps.
   a. Connects to the server.
   b. Downloads the network profile.
   c. Configures the network profile.

   After the app completes the onboarding workflow, a successful profile configuration message is displayed.

After onboarding is complete, the device is ready to connect to the configured network. The device must be in the vicinity of the configured network and should not be already connected to any other network.

Users already connected to a wireless network can manually switch to the newly configured network available in the Wi-Fi list. At times, this manual switching might not work on mobile devices. In such situations user can either try to disconnect from the already connected network or disable / enable the Wi-Fi connection.

When creating a user access policy, the network administrator can provide a personalized name for the **Organization name** for the network profile. Instead of the SSID name, the HPE Aruba Networking Onboard app displays this name in network profiles.
On iOS and ChromeOS, the SSID name is displayed in the list of available wireless networks. On Windows devices, organization names are tagged to the SSID names and displayed in the list of available networks. In few occurrences, the Android devices displays the **Organization name** after few seconds in the available wireless network of the device.

Provisioning of passpoint networks is not supported on Linux OS due to the OS limitation. Only traditional provisioning method of configuring 802.11x SSID profiles is possible.

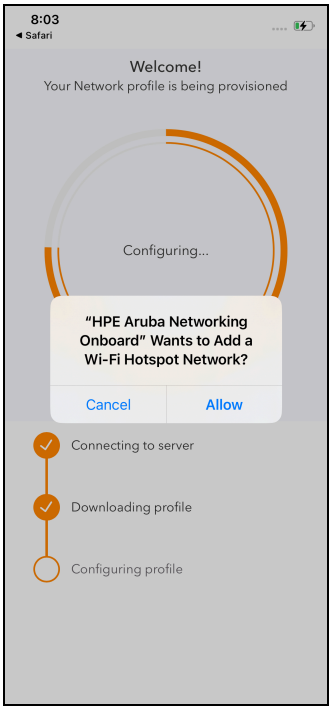
Additional User Action

During installation of the network profile or network connection, user consent is required as shown for the following OS platforms:

On **macOS**:

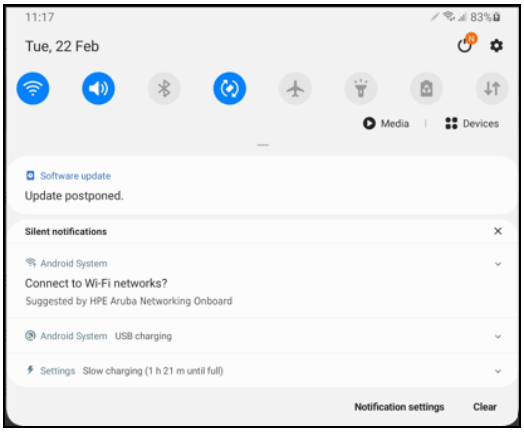
- **Profile/MDM wants to make changes**
  - If Touch ID is configured on your device, tap the Touch ID sensor or click **Use Password** to proceed.
  - If Touch ID is not supported on your device, enter the device password to proceed.
- **Profiles (Certificates) trying to trust a certificate from a user configuration profile**
  - If Touch ID is configured on your device, tap the Touch ID sensor or click **Use Password** to proceed.
  - If Touch ID is not supported on your device, enter the device password to proceed.

On **iOS**: a security warning is displayed to add a Wi-Fi hotspot network. Tap **Allow** to proceed.



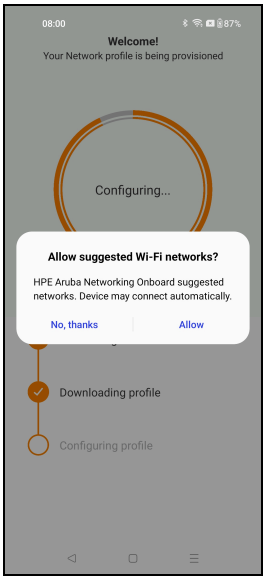
On **Android 10 devices**: users will have to accept the notification shown by the system when the device comes in the range of the network SSID after provisioning. This occurs on Android 10 OS on devices that do not support Passpoint.

Figure 4 *Notification*



On Android11 devices

While installing the network profile for the first time, a security warning is displayed to allow the Wi-Fi network. Tap **Allow** to proceed.

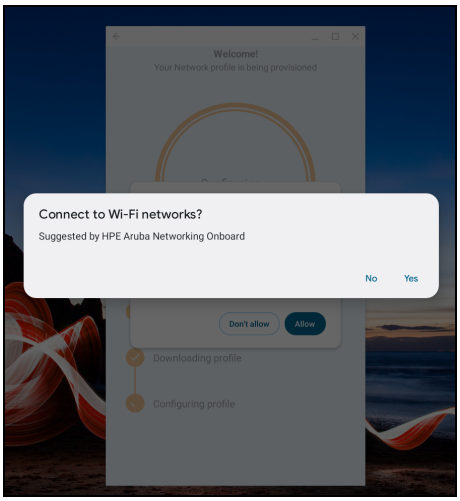


NOTE

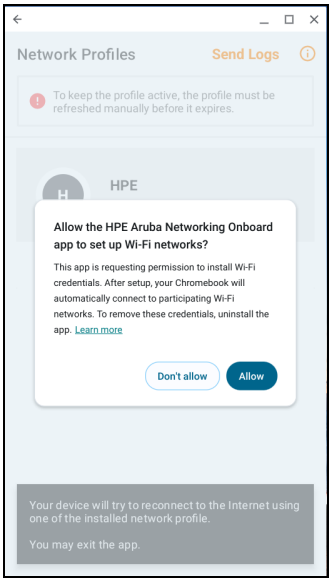
On **Android** devices that do not support passpoint, if the OS Wi-Fi picker does not display organization name (Passpoint friendly name) then the device can connect to the default SSID name (which is configured by the Admin under user access policy).

On ChromeOS

While installing the network profile for the first time, ChromeOS displays two consent dialogues as shown below. Tap **Yes** to proceed.



When you refresh the network profile, ChromeOS displays the following consent dialogue. Tap **Allow** to proceed.



Managing Network Profiles

You can add one or more network profiles in the HPE Aruba Networking Onboard app. Use the following options to manage the network profiles in the app.

Checking Validity of a Network Profile

The validity of the network profile is displayed on the network profile card within the App.

Refreshing Expired Profiles

To replace expired profiles in the HPE Aruba Networking Onboard app, complete one of the following steps:

- For Windows/macOS/Linux OS, right-click the network profile card and click **Refresh**.
- For Android or iOS devices, on the network profile card, swipe from right to left and select **Refresh**.

NOTE

- Users with Windows devices that do not support Wi-Fi CERTIFIED Passpoint™ solution cannot install network profiles either through browser-based or app-based onboarding methods.

Deleting a Network Profile

To delete network profiles installed by the client App, complete one the following steps:

- For Windows/macOS/Linux OS, right-click the network profile card and click **Delete**.
- For Android or iOS devices, on the network profile card, swipe from right to left and select **Delete**. Ensure to enable the wireless interface before deleting a profile.

NOTE

- Windows users must ensure to enable the wireless interface before deleting a profile.
- When a device is shared by multiple users and if one of the users deletes their profile then the wired profile of the non-active user is also deleted.
- If a user manually deletes network profiles installed by the client app, the HPE Aruba Networking Onboard app continues to display the network profile card even though the system is unable to utilize the network profile. The user can click the Refresh button to use the network profile or click the Delete button to delete the network profile.

Troubleshooting and Sending Error Logs

To troubleshoot and send the error logs in the network profile installed on the HPE Aruba Networking Onboard app, complete one of the following steps:

- For Windows/macOS/Linux OS, click **Send Logs**.

  The HPE Aruba Networking Onboard app adds the error log files and opens the default email client to send the log files to the administrator.

NOTE

If an email client is not configured on your device, the message to save the logs as a .zip file is displayed. Click **OK** to save and send the logs later.

- For Android or iOS devices, tap **Send Logs**.

  The HPE Aruba Networking Onboard app provides a variety of share options for the device to send logs to the administrator.

Uninstalling HPE Aruba Networking Onboard App

Upon uninstalling the HPE Aruba Networking Onboard app, the certificates and network profiles associated with enterprise wireless networks are removed.

Uninstalling the app on an Android/Chrome OS/iOS Device

To uninstall the app on any of these devices, follow the standard procedure.

NOTE

Uninstalling the HPE Aruba Networking Onboard app on an Android 9 device will not remove the network profiles and certificates from the device.

Uninstalling the app on macOS

To uninstall the HPE Aruba Networking Onboard app on macOS, complete one of the following steps:

- Run the **Aruba Onboard Uninstaller.app** from the location **/Library/Application Support/ArubaOnboard/**. In this method, the app removes the configured wireless network credentials and all app data from the device.
- Delete the HPE Aruba Networking Onboard app from **/Applications** folder or drag and drop to the Trash. In this method, the app removes it from Applications folder but does not remove the configured wireless network credentials, few app components, and app data from the device.

Uninstalling the app on Linux OS

To uninstall the HPE Aruba Networking Onboard app on Linux OS, execute the following commands using admin or root privileges:

```
apt remove aruba-onboard
apt purge aruba-onboard
```

Uninstalling the app on Windows

Use the standard procedure to uninstall the app on Windows.

Users only with administrative privilege can uninstall the app.

Upgrading HPE Aruba Networking Onboard App

The HPE Aruba Networking Onboard app periodically checks for updated versions. When the updated version of the HPE Aruba Networking Onboard app is available, the application automatically upgrades in the background without any user intervention.

The auto-check and auto-upgrade is applicable only for desktop platforms such as Microsoft Windows (App version 1.1 onward), macOS (App version 1.4 onward) and Linux OS.

Manually Upgrading HPE Aruba Networking Onboard App on Windows

Manual upgrade is only applicable if you are using Windows OS. For instance, from version 1.0 to version 1.1. Users with administrator privileges only can upgrade the application.

- Ensure to uninstall the HPE Aruba Networking Onboard app version 1.0 before attempting to upgrade to 1.1. For more information, see Manually Upgrading HPE Aruba Networking Onboard App on Windows.
- From the HPE Aruba Networking Onboard app version 1.1 onwards, the update occurs automatically without user intervention and there is no disruption in the use of existing profiles or network connectivity.

To upgrade the app on Windows, complete the following steps:

1. Access the on-boarding URL shared by the network administrator.
2. Select **Yes, I want to install HPE Aruba Networking Onboard**.
3. Select **Download for Windows**.

4. Double-click the .exe file.

   A pop-up window opens and prompts you to confirm the upgrade.

5. Click **OK**.

   The **Welcome to the HPE Aruba Networking Onboard Setup** page is displayed.

6. Click **Next**.

   The **End User License Agreement** page is displayed.

7. Click **I agree** to compete the HPE Aruba Networking Onboard app upgrade.

8. Click **Close**.

   You must manually launch the upgraded app and any existing network profiles will be automatically migrated.

Third Party Software Licenses

The HPE Aruba Networking Onboard uses OpenSource components which can be downloaded from https://myenterpriselicense.hpe.com/cwp-ui/dashboard/software. For more information, see notices information for the third-party components used by HPE Aruba Networking Onboard.

Browser-based Onboarding

Browser-based onboarding enables the device to download network profiles through a web browser. It connects to the enterprise wireless network through network profiles and Cloud Authentication and Policy authentication.

To connect the device to the enterprise wireless network, complete the following steps:

1. Access the onboarding URL shared by the network administrator.

- To access the onboarding URL, you should use the Google Chrome or Mozila Firefox browsers for mobile devices running Android. HPE Aruba Networking recommends the Safari browser for devices running iOS and macOS.
- Web-based provisioning is not supported on Oppo and Realme devices.

2. Select **No thanks, just use my browser**.
3. Click **Sign in for Provisioning**.
4. Sign in using the cloud identity configured by the network administrator.
   - To connect using your Microsoft Entra ID or Google Workspace or Okta Workforce Identity Cloud account, use the following steps:
     1. Enter the username.
     2. Click **Next**.
     3. Enter the password.
     4. Click **Sign in**.
5. To download the network profile to your device, complete one of the following steps:
   - On Windows laptop, select **Install on Windows**.
   - On Android mobile device, select **Install on Android**.
   - On macOS and iOS devices, select **Install on Apple**.

   The network profile file is downloaded to your device.

6. Install the downloaded network profile on your device.

Windows devices do not allow non-admin users to install Passpoint network profiles through web-based onboarding.

Once onboarding is complete, devices that support Passpoint are automatically connected to the enterprise wireless network if they are not connected to another wireless network and in proximity of Passpoint network.

Users who are already connected to a wireless network can switch into the newly configured wireless network manually by tapping the configured network on the list of available networks or they can disconnect from the existing wireless network. It allows the device to automatically connect to the newly configured network. In few occurrences, the Android devices displays the organization name after few seconds in the available wireless network of the device. If your iOS device is not able to connect to the newly configured network, forget the connected network or retry connecting again after few seconds.

Monitoring Cloud Authentication and Policy

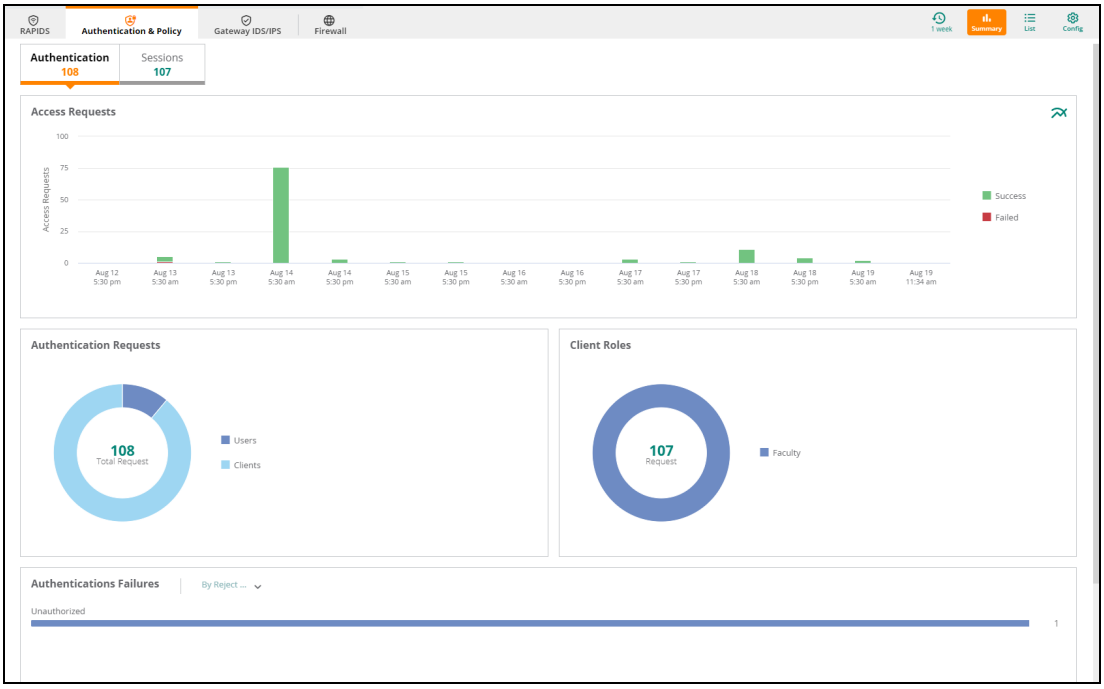
The **Authentication & Policy** dashboard provides all the details about authentication requests from users, and session details of client devices that are connected to the APs managed by HPE Aruba Networking Central. It enables the network administrators in decision making processes by representing authentication and session details in form of charts and tables. However, the **Authentication & Policy** dashboard represents authentication requests from users and session details using the following tabs.

Only for client MAC addresses that are added (or registered) in the **Allowed MAC Addresses** table in the client access policy, the MAC authentication failures are recorded and reported in the charts and Access list table. For more information about configuring new client MAC addresses, see Updating Client Access Policy.

- **Authentication** tab: The Authentication tab includes charts and tables that provide detailed information about all the users and client devices connected to the AP through Cloud Identity authentication.
- **Sessions** tab: The Sessions tab includes charts and tables that provide detailed session related information about all the client devices connected to the AP through Cloud Identity authentication.

Figure 5 shows the **Authentication** and **Sessions** tab in the **Authentication & Policy** dashboard:

Figure 5 *Monitoring Page*



Data Filters

The different data filters allow you to screen and customize the authentication and sessions related data that are displayed on the charts.

Time Filter

The time filter allows you to set a time range to display authentication and sessions related data in the charts and list. You can set the filter to any of the following time ranges:

- **3 Hours**—The charts display the Cloud Authentication and Policy details for the past three hours.
- **1 Day**—The chart displays the Cloud Authentication and Policy details for the current day.
- **1 Week**—The chart displays the Cloud Authentication and Policy details for the current week.
- **1 Month**—The chart displays the Cloud Authentication and Policy details for the current month.
- **3 Months**—The chart displays the Cloud Authentication and Policy details for the past three months.

For more information about different monitoring dashboards, see the following topics:

- Viewing Authentication Summary
- Viewing Sessions Summary
- Access Requests
- Viewing Sessions List

Viewing Authentication Summary

The **Authentication** tab provides charts to represent the number of Cloud Identity authentication requests and access requests made by users, and client devices associated with different client roles.

To view the Authentication summary page, complete the following steps:

1. In the WebUI, set the filter to **Global**.
   The global dashboard is displayed.
2. Under **Manage**, click **Security > Authentication & Policy**.
3. To view the **Authentication** summary page, click the **Summary** icon and click **Authentication**.
   The authentication summary page is displayed.

NOTE

To set the charts to show data for a specific duration, use the options in the time range filter. By default, the data is displayed for a duration of 3 hours. To view the graphs for different durations, click the time filter icon and select a time range of your choice.

Authentication Summary Charts

The **Authentication** summary charts page displays the following charts:

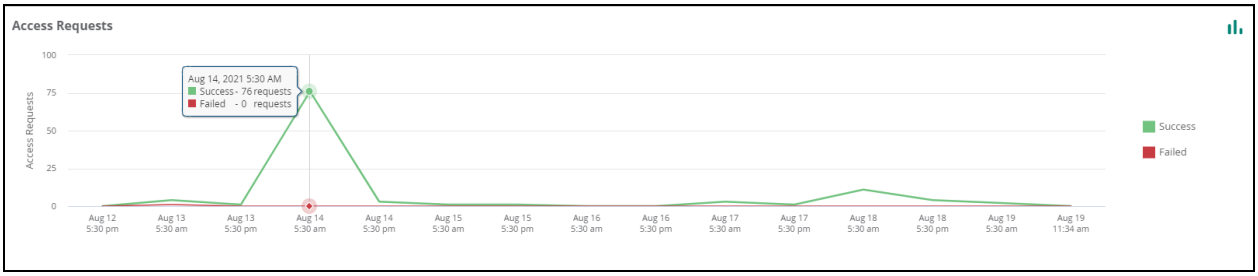
- Access Requests Charts
- Authentication Requests Chart
- Client Roles Chart
- Authentication Failures Chart

Access Requests Charts

HPE Aruba Networking Central provides two different chart options to view the access request data, that is, line chart and the bar chart. Click and icons to toggle between line chart and bar chart.

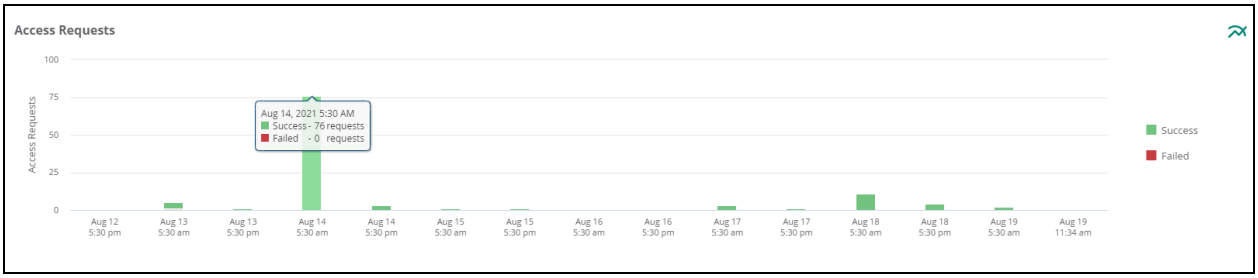
- **Access Requests** line chart—The data points on the chart display the number of access requests that were made in a selected duration, which are grouped by a specific set of dates. When you hover over a data point, it displays the number of successful and failed access requests on a particular date. Click a region on the line connecting data points, or click on a data point to view the details in the **Access Request** List. For more information, see Access Requests.

  Figure 6 *Access Requests Line Chart*



- **Access Requests** bar chart—The stacked vertical bars display the number of access requests that were made in a selected duration, which are grouped by specific set of dates. When you hover over a stacked vertical bar, it displays the number of successful and failed access requests on a particular date. Click a region on the stacked vertical bar to view the details in the **Access Request** List. For more information, see Access Requests.

Figure 7 *Access Requests Bar Chart*



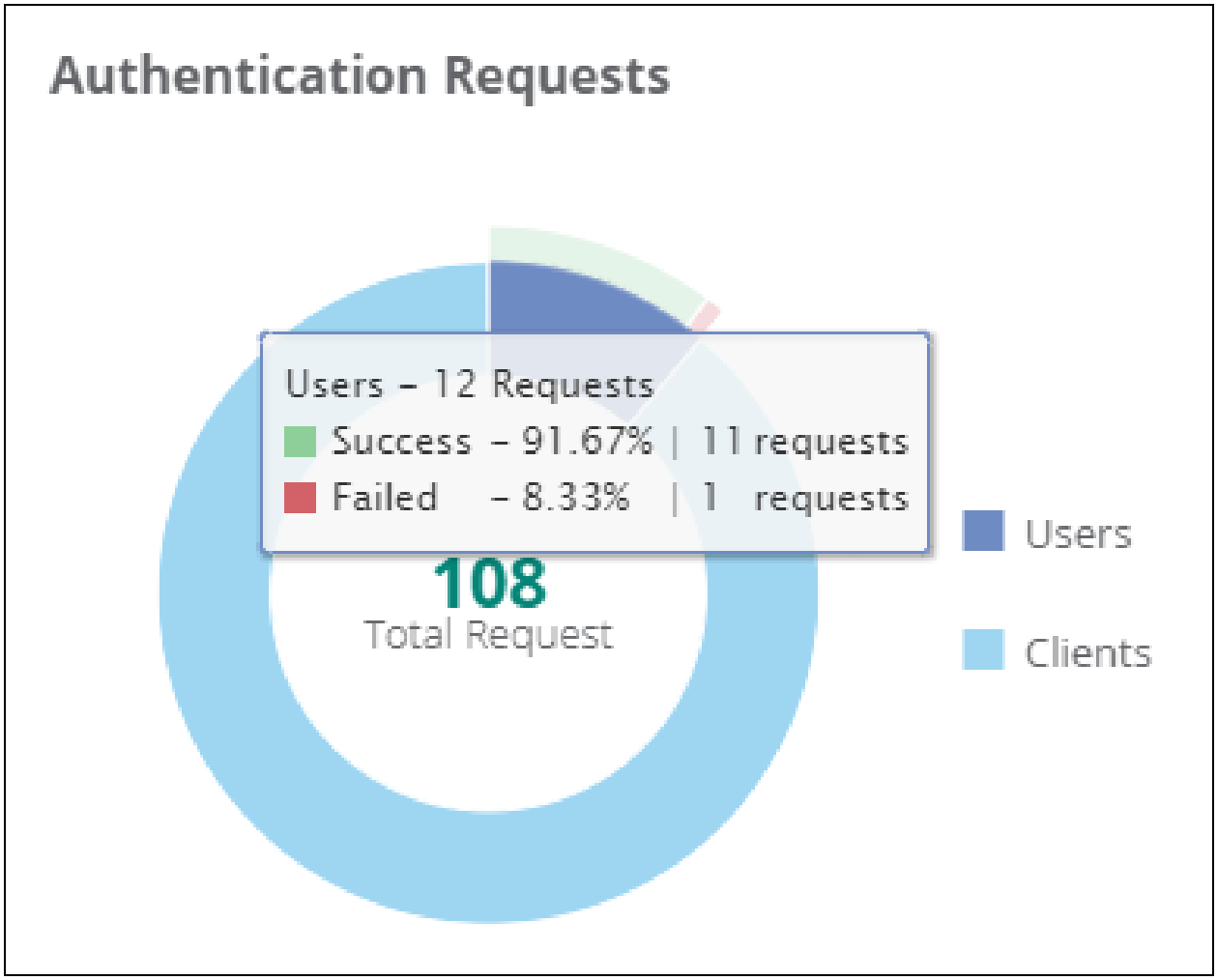
- A legend is displayed next to the **Access Requests** chart. When you click a legend, the associated portion of the chart is shown or hidden for a selected duration. For example, when you click **Success**, the chart shows or hides the number of successful access requests. By default, the chart displays the total number of access requests made in a selected duration.

Authentication Requests Chart

The center of this chart displays the grand total number of authentication requests received in a selected duration. When you hover over the different regions on the chart, each region displays the total number of authentication requests received from users and client devices. It also displays how many authentication requests were successful and how many of them failed. Click a region on the stacked vertical bar to view the details in the **Access Request** List.

A legend is displayed next to the **Authentication Requests** chart. When you click a legend, the associated portion of the chart is shown or hidden for a selected duration. For example, when you click **User-Based**, the associated portion of the chart shows or hides the total number of access requests that were made by **Users**. By default, the chart displays the total number of all the authentication requests.

Figure 8 *Authentication Requests Pie Chart*

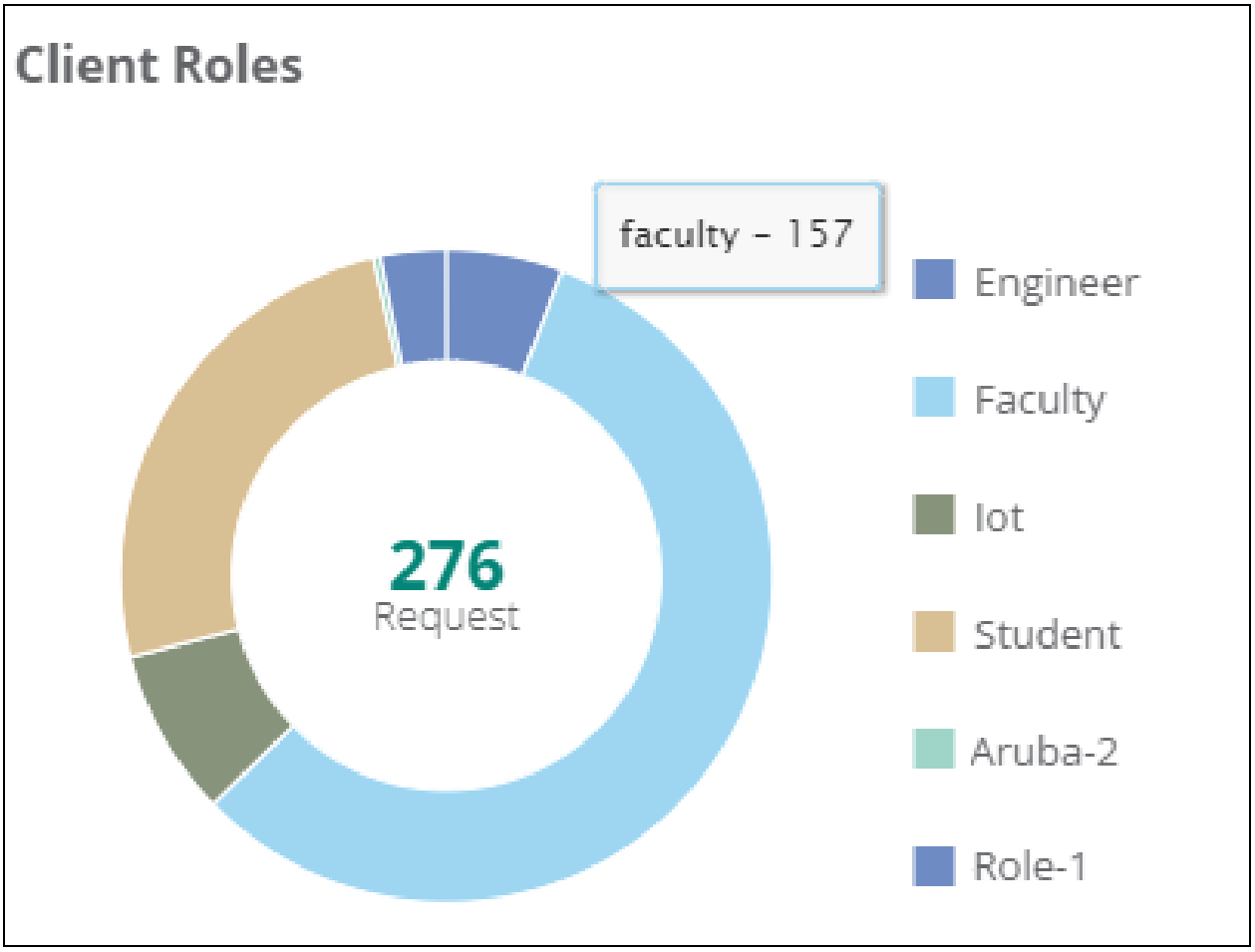


Client Roles Chart

The center of this chart displays the grand total number of client roles who raised authentication requests for a selected duration. When you hover over the different regions on the chart, each region displays the total number of authentication requests received from each client role. Click a region on the stacked vertical bar to view the details in the **Access Request** List. For more information, see Access Requests.

A legend is displayed next to the **Client Roles** chart. When you click a legend, the associated portion of the chart is shown or hidden for the selected duration. For example, when you click **Engineer**, the associated portion of the chart shows or hides all the authentication requests raised by the **Engineer** client role. By default, the chart displays the total number of authentication requests made by all the client roles.

Figure 9 *Client Roles Pie Chart*

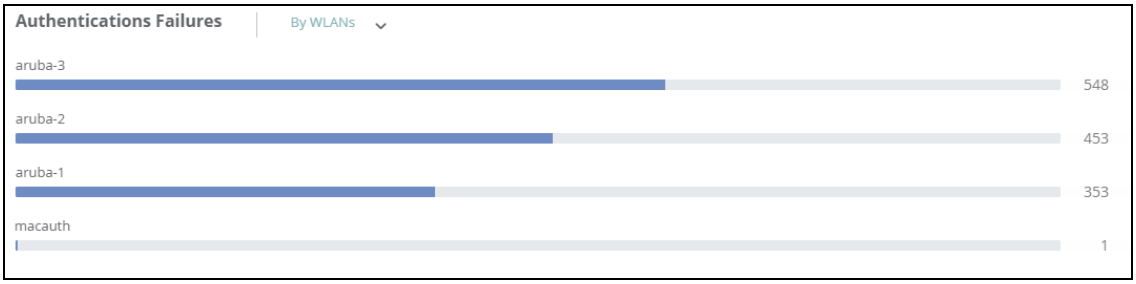


Authentication Failures Chart

This chart displays the failures based on the following **Authentication Failures** filter.

- **By WLANs**—When you select this filter, the chart displays the number of failed authentications requests per WLAN SSID.

  Figure 10 *Authentication Failures WLAN*

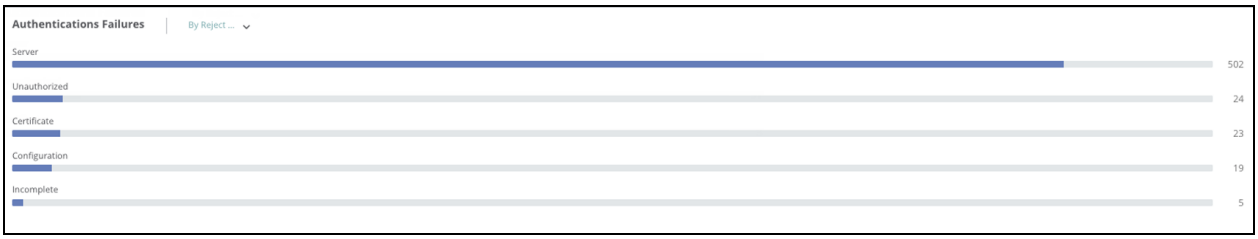


- **By Policy**—When you select this filter, the chart displays the number of failed authentications requests per Cloud Authentication and Policy.

Figure 11 *Authentication Failures By Policy*

- **By Reject Reason**—When you select this filter, the chart displays the number of failed authentications requests per Reject Reason.

Figure 12 *Authentication Failures Reject Reason*



Viewing Sessions Summary

The **Sessions** charts display metrics related to Cloud Identity sessions that help the administrator in decision making process. These metrics include number of active sessions, MAC address (MAC ID randomized and non randomized), duration of each session, and the data usage during each session within a selected duration. This information is useful to monitor the number of active sessions, data usage, and session-duration details per user or per client device.

To view the **Sessions** summary page, complete the following steps:

1. In the WebUI, set the filter to **Global**.
   The global dashboard is displayed.
2. Under **Manage**, click **Security > Authentication & Policy**.
3. To view the **Sessions** summary page, click the **Summary** icon and click **Sessions**.
   The sessions summary page is displayed.

NOTE

To set the charts to show data for specific duration, use the options in the time range filter. By default, the data is displayed for a duration of 3 hours. To view the graphs for different durations, click the time filter icon and select a time range of your choice.

Sessions Summary Charts

The **Sessions** summary charts page displays the following charts:

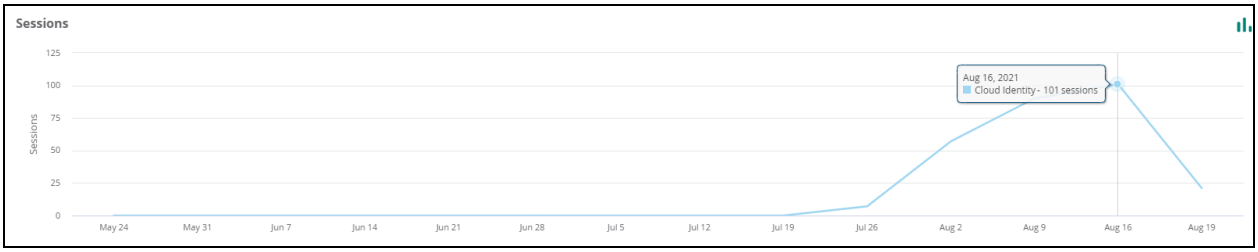
- Sessions Charts
- MAC ID Randomized Chart
- Sessions by Duration Chart
- Usage Chart

Sessions Charts

HPE Aruba Networking Central provides two different chart options to view the sessions data, that is, line chart and the bar chart. Click and icons to toggle between line chart and bar chart.

- **Sessions** line chart—The data points on the chart display the number of successful sessions in a selected duration, which are grouped by a specific set of dates. When you hover over a data point, it displays the number of successful sessions on a particular date. Click a region on the line connecting data points, or click on a data point to view the details in the **Sessions** List. For more information, see Viewing Sessions List.

  Figure 13 *Sessions Line Chart*



- **Sessions** bar chart—The stacked vertical bars display the number of successful sessions in a selected duration, which are grouped by a specific set of dates. When you hover over a stacked vertical bar, it displays the number of successful sessions on a particular date. Click a region on the stacked vertical bar to view the details in the **Sessions** List. For more information, see Viewing Sessions List.

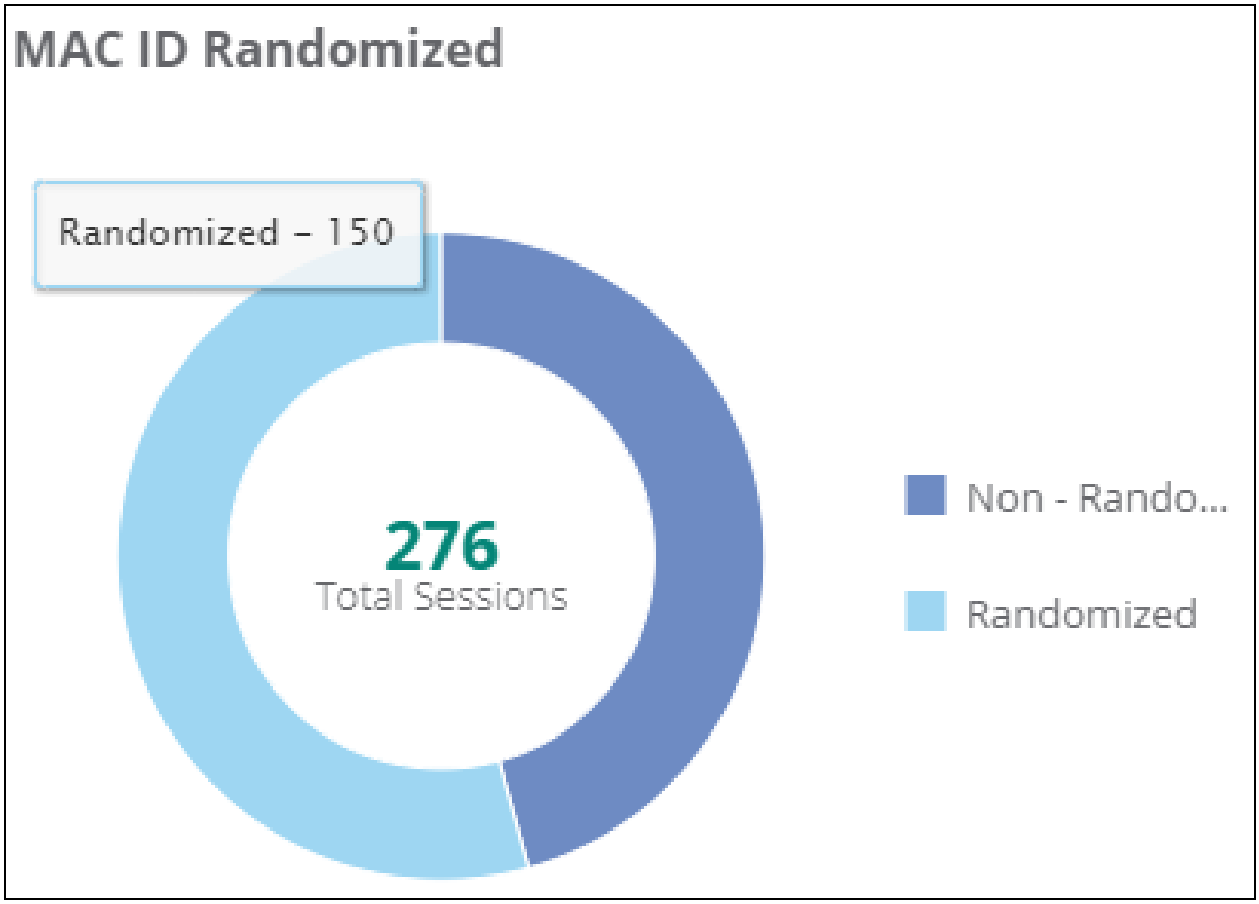
  Figure 14 *Sessions Bar Chart*

MAC ID Randomized Chart

The center of the chart displays the grand total number of client MAC addresses that were connected to the network in a selected duration. When you hover over different regions on the chart, each region displays the total number of client MAC addresses that were connected to the network for that selected region. Click a region on the chart to view the details in the **Sessions** List. For more information, see Viewing Sessions List.

A legend is displayed next to the **MAC ID Randomized** chart. When you click a legend, the associated portion of the chart is shown or hidden. For example, when you click **Randomized**, the associated portion shows or hides the number of **Randomized** client MAC addresses. By default, the chart displays the total number of client MAC addresses that were connected in the selected duration.

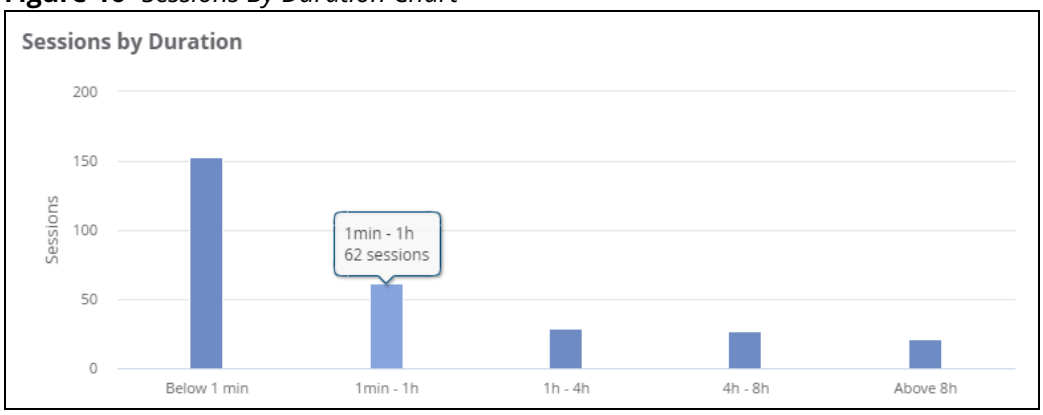
Figure 15 *MAC ID Randomized Pie Chart*



Sessions by Duration Chart

The stacked vertical bars display the number of active sessions for a specific duration, which are grouped by time intervals. When you hover over a stacked vertical bar, it displays the number of active sessions in a particular time interval.

Figure 16 *Sessions By Duration Chart*

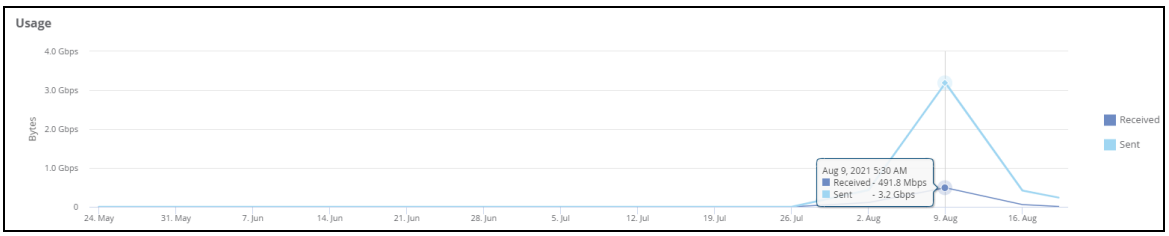


Usage Chart

The data points on the chart display the total amount of data that was transmitted (in Bytes) over the network in the selected duration. When you hover over a data point, it displays the amount of data that was sent and received on a particular date. Click a region on the line connecting data points, or click on

a data point to view the amount of data transmitted in a selected duration in the **Sessions** List. For more information, see Viewing Sessions List.

Figure 17 *Usage Chart*



Access Requests

The **Access Requests** tab consists of a table that lists all the details of access requests made by users based on the associated client roles. In addition to displaying the details of all the access requests, the **Access Requests** tab displays successful access-requests and failed access-requests using the following sub-tabs:

- **Success** tab—Success tab consists of a table that lists all the details of access requests that are accepted by AP.
- **Failed** tab—Failed tab consists of a table that lists all the details of incomplete and rejected access requests.

Viewing Access Requests List

To view the **Access Requests** list, complete the following steps:

1. In the WebUI, set the filter to **Global**.
   The global dashboard is displayed.
2. Under **Manage**, click **Security > Authentication & Policy**.
3. To view the **Access Requests** table, click the **List** icon and click the **Access Requests** tab.
   The **Access Requests** table is displayed with the following information:
   - **Username**—Name of the user that was used for authentication.
   - **Status**—Status of the connection request.
   - **Client Role**—Role of the client device.
   - **Access Device Name**—Name of the AP.
   - **Date and Time**—The date and time of the network access request.
   - **Error**—Displays the error message.
   - **Authorization Source**—The source of the authentication request.
   - **Authentication Type**—The authentication type of the client device.
   - **Connection**—The type of connection (wired or wireless).
   - **MAC**—The MAC address of the client device.
   - **MAC Randomized**—A boolean value that indicates if the MAC address is randomized or not.
   - **SSID**—The SSID to which the client device is connecting to.
   - **NAD IP**—The IP address of the AP.
   - **NAD MAC**—The MAC address of the AP.
   - **Carrier**—The name of the SIM provider.

- **Policy Type**—The type of Cloud Authentication and Policy (user access policy or client access policy).
- **User Groups**—The user group that a user belongs to, that is defined in the identity store.

Click the icon and select the columns that you want to display in the table. To reset the columns, click the icon and select **Reset to default**.

Click the **Export as CSV** icon to download the data in the CSV file format. All columns are exported irrespective of the current selected columns. If you change the time range or filter the data using the column headers, similar data will be exported in the CSV file. Filters like time range such as 1 day, 1 month, or 3 months are also applicable. The **Export as CSV** icon will not be visible for read-only users. The maximum download limit is 25000 records. Administrators can use NBAPI's to fetch data for more records.

In the **Access Requests** table, use the filter and the sort icons to filter and sort the threats data.

Viewing Access Requests Details

The **Access Requests** tab consists of a table that lists all the details of access requests made by users on the APs managed by HPE Aruba Networking Central.

To view the **Access Requests** list, complete the following steps:

1. In the WebUI, set the filter to **Global**.
   The global dashboard is displayed.
2. Under **Manage**, click **Security > Authentication & Policy**.
3. Click the **List** icon.
   The Access Requests table is displayed.
4. In **Access Requests** table, click on any row to open the **Details View** tab.
   The **Details View** tab is displayed. This tab displays the access-request related information. For more information, see Access Requests Information.

Access Requests Information

This topic describes the following sections:

- Summary
- Authorization
- Request
- Response

Summary

The **Summary** section displays all the user and client device related information received from the access request.

The **Summary** section provides the following information:

- **Username**—The user-account name that was used to raise an access request.
- **Date and Time**—The date and time of the network access request.
- **Access Device Name**—Name of the AP.
- **MAC Address**—The MAC address of the client device.

- **Client IP**—The IP address of the client device.
- **Access Device IP**—The IP address of the AP.
- **Request ID**—The request ID of the user access request.
- **Access Policy**—The Cloud Authentication and Policy name used to raise an access request.
- **Client Role**—The role name associated with the client device.
- **Access Status**—Status of the access request.
- **Identity Store**—Name of the external identity store configured in the user access policy.
- **Error**—Displays the error message. The error can be one of the following values:
  - **Unauthorized**—This value is displayed if the RADIUS request is successful, but the user was rejected by authorization service (either internal or external) due to invalid credentials.
  - **Invalid Certificate**—This value is displayed if the EAP SSL handshake was not completed due to certificate issues.
  - **Unsupported configuration**—This value is displayed if an attempt was made to perform an authentication that was not configured for the network.
  - **Internal Server Error**—This value is displayed if the authentication fails due to an internal server error.
  - **Unexpected Client Data**—This value is displayed if the client has sent unexpected data that was not identified by the server.

Authorization

The **Authorization** section displays all the user information related to the external identity server that was configured in the user access policy.

The **Authorization** section provides the following information:

- **Authorization Source**—The name of the external identity store.
- **User Group**—The user-group name to which the user is assigned in the external identity server.
- **Department**—The department name to which the user is assigned in the external identity server.
- **User Principal Name**—The name of the user that is mentioned in the external identity server.
- **Given Name**—The user-account name that is mentioned in the external identity server.
- **Connection type**—The connection type that was used to raise an access request.
- **MAC Randomized**—A boolean value that indicates if the MAC address is randomized or not.

Request

The **Request** section displays all the user information used by the AP. It also includes details of the AP that processed the access request.

The **Request** section provides the following information:

- **MAC Address**—The MAC address of the client device.
- **SSID**—The SSID used by the client device to connect with the network.
- **Username**—Name of the user that was used for authentication.
- **NAD IP Address**—The IP address of the AP.
- **NAD Name**—Name of the AP.
- **AP Group**—Name of the device group that contains the AP.
- **Device Type**—The type of client device.
- **EAP Type**—The type of EAP that was used for authenticating access request.

Response

The **Response** section displays all the information related to the response sent by AP after authenticating the access request.

The **Response** section provides the following information:

- **Authentication Status**—The authentication status of the access request after AP authentication.
- **Authorization Status**—The authorization status of the access request after AP authentication.
- **Client Role**—The role name associated with the client device.

Viewing Sessions List

The **Sessions** tab consists of a table that lists all the active and terminated sessions after the authentication request.

To view the **Sessions** list, complete the following steps:

1. In the WebUI, set the filter to **Global**.
   The global dashboard is displayed.
2. Under **Manage**, click **Security > Authentication & Policy**.
3. To view the **Sessions** table, click the **List** icon and click the **Sessions** tab.
   The **Sessions** table is displayed with the following information:
   - **Username**—Name of the user that was used for authentication.
   - **Access Device Name**—Name of the client device.
   - **Start Date and Time**—The date and time the user or device logged in.
   - **End Date and Time**—The date and time the user or device logged out.
   - **Duration**—The duration of a user or device that was active on the network.
   - **Authorization Source**—The source of the authentication request.
   - **Authentication Type**—The authentication type of the client device.
   - **Connection**—The type of connection (wired or wireless) used by the user or client to connect with the network.
   - **MAC**—The MAC address of the client device.
   - **MAC Randomized**—A boolean value that indicates if the MAC address is randomized or not.
   - **SSID**—The SSID used by the client device to connect with the network.
   - **NAD IP**—The IP address of the AP.
   - **Input Bytes**—The amount of data uploaded by the user to network.
   - **Output Bytes**—The amount of data downloaded by the user from the network.
   - **Closed**—A boolean value that indicates the connection status.

NOTE

Click the icon and select the columns you want to display in the table. To reset the columns, click the icon and select **Reset to default**.

In the **Access Requests** table, use the filter and sort icons to filter and sort the threats data.

Click the **Export as CSV** icon to download the data in the CSV file format. All columns will get exported irrespective of the selected columns. If you change the time range or filter the data using the column headers, similar data will be exported in the CSV file. Filters like time range such as 1 day, 1 month, or 3 months are also applicable. The **Export as CSV** icon will not be visible for read-only users. The maximum download limit is 25000 records. Administrators can use NBAPI's to fetch data for more records.

Client Security

When a client device is authenticated, Cloud Authentication and Policy is assigned to the device, and the policy is enforced when the client device accesses the network. The AAA page displays the authentication, accounting, and authorization information of the client.

To view the AAA page, complete the following steps:

1. In the WebUI, set the filter to a device, site, label, or **Global**.
2. Under **Manage**, click **Clients**.
3. Select a client in the **Client Name** column.
4. Under **Manage**, click **Security**.
5. Click the **AAA** tab to view the authentication, accounting, and authorization information of the client.

Cloud Authentication and Policy Details

Following are the authentication, accounting, and authorization details of a client authenticated by Cloud Authentication and Policy.

Authentication

The authentication information includes:

Table 8: *Client Authentication Information*

Condition	Value
Authentication request time	The time at which the authentication request was raised.
Status	The status of authentication.
Username	The username used for authentication.
Request Type	The authentication request type.
Access Policy	The access policy used for authentication.
Reject Reason	The reason for rejecting authentication request.
Role	The role of the user.

Authorization

The authorization information includes:

Table 9: *Client Authorization Information*

Condition	Value
Group	The list of user groups from the cloud identity provider.
Department	The department of the user as per the cloud identity provider.
Identity Store	The cloud identity provider name (Entra ID or Google or Okta Workforce Identity Cloud).

Condition	Value
Mobile Operator	The name of the carrier. For example: AT&T, Verizon, and so on. **NOTE:** This field is applicable only for the Air Pass request.

The **Group**, **Department**, and **Identity Store** fields do not show any information for the Client Access Policy request (MAC-Auth).

Accounting

The accounting information includes:

Table 10: *Client Accounting Information*

Condition	Value
Start time	The start time of a session.
End time	The end time of a session.
Duration	The duration of a session.
Bytes transferred	The total number of bytes transferred during a session.

Cloud Authentication and Policy FAQs

How do I create a policy as an administrator for multiple users and client devices?

You can create user access policy and client access policy for users and clients using the procedures mentioned in Configuring Cloud Authentication and Policy Before you create user access policy and client access policy, you must complete all the prerequisites mentioned in Prerequisites.

How do I add or update user groups or client role mapping in the user access policy?

You can update user groups and client role mapping by performing one of the following:

- To add one or more user groups in the existing user access policy, you must create new mappings for user groups and client roles in the user access policy.

The values in this drop-down list are mapped to the user groups that are created or configured on the identity provider's server.

- To change user groups, you must update the existing user groups and associated client roles in the user access policy.

For more information, see Updating User Access Policy.

How do I change the organization name and see the preview that appears on the HPE Aruba Networking Onboard app?

You can change the organization name in the **Network Profile** section, when creating or updating the user access policy. The **HPE Aruba Networking Onboard mobile app preview** section displays how the organization name will appear on the **HPE Aruba Networking Onboard** app.

For more information, see Configuring User Access Policy.

How do I update the user access policy when a user switches between user groups?

User groups are obtained from cloud identity stores like Google Workspace or Entra ID or Okta Workforce Identity Cloud, and the user can change groups within the identity stores. Hence, you must update the user access policy to include the modified user groups to provide appropriate network access. For more information, see Updating User Access Policy.

How do I update user groups when a user leaves the organization?

Since the policy is based on user groups, there is no need to update the user access policy when the user leaves an organization. However, to prevent the user from accessing the organization network, you must deactivate the user account in the identity store used by your organization.

For more information, see Updating User Access Policy.

How do I update a policy to change the default WLAN SSID that the users connect to?

In the **Network Profile** section, you can select a different WLAN SSID from the **Connect users to WLAN** drop-down list.

For more information, see Updating User Access Policy.

How do I configure Google Workspace for Cloud Authentication?

To integrate Google Workspace with the Cloud Authentication and Policy application, and fetch user attributes from Google Workspace, complete the following steps:

1. Create a project in Google APIs.
2. Provide access to Google Workspace instance.

For more information, see Google Workspace.

How do I configure Microsoft Entra ID for Cloud Authentication?

To integrate Entra ID with Cloud Authentication and Policy application, and fetch user attributes from Entra ID, complete the following steps:

1. Register the Cloud Authentication and Policy application on the Entra ID portal.
2. Configure API permissions for the Cloud Authentication and Policy application.
3. Configure Client Secret ID for the Cloud Authentication and Policy application.

For more information, seeMicrosoft Entra ID.

What roles are used when creating the Cloud Authentication and Policy?

Client roles, which are defined in the WLAN configuration for IAPs are used when configuring Cloud Authentication and Policy.

For more information, see Cloud Authentication and Policy Overview.

How do I create a policy to block users who are violating the user access policy?

While creating a user access policy, you must place most restricted user group(s) in the topmost row of the **User Groups to Client Mapping** table in **User Access Policy** section. For example, if you have a policy to block user or user groups consuming larger bandwidth, you must place that policy in the topmost row of the user group to client role mapping table.

For more information, see Client Access Policy.

What are the WLAN access levels that Cloud Authentication and Policy support?

Cloud Authentication and Policy is supported for **Role Based** and **Unrestricted** access levels.

How do I add headless device(s) that are not defined in HPE Aruba Networking Central using client tags?

While configuring client access policy, you must select **Unprofiled** client tag from the drop-down list under **Client Profile Tag**.

For more information, see Client Access Policy.

Can I upload client information from an external file?

Yes, while configuring client access policy, you can upload the client information from a CSV file. The CSV file must contain the client's MAC address and the corresponding name of the client.

For more information, see Client Access Policy.

Sample content from a CSV file:

```
MAC Address,Client Name
01:23:45:67:89:AB,Client Laptop1
12:34:56:78:90:BC,Client Laptop2
```

I do not have Passpoint or Hotspot 2.0 on my mobile device. Can I connect it to an enterprise wireless network?

Yes, as long as the mobile device meets the minimum supported operating system requirements.

For more information, Supported Devices and Operating Systems.

How do I get the onboarding URL for the HPE Aruba Networking Onboard app?

You must obtain the on-boarding URL and credentials from the network administrator. For further assistance, contact your network administrator.

How can I connect the client to an wireless network without using the HPE Aruba Networking Onboard app?

You can use browser-based onboarding to download network profiles and connect to the wireless network.

For more information, see Browser-based Onboarding.

Can I delete a network profile from the HPE Aruba Networking Onboard app?

Yes, you can delete or add network profiles in the HPE Aruba Networking Onboard app. For more information, see App-based Onboarding.

Does Cloud Authentication and Policy support wired interfaces?

Cloud Authentication and Policy supports 802.1X, captive portal, and MAC authentication on wired interfaces.

Does the HPE Aruba Networking Onboard app use OpenSource components?

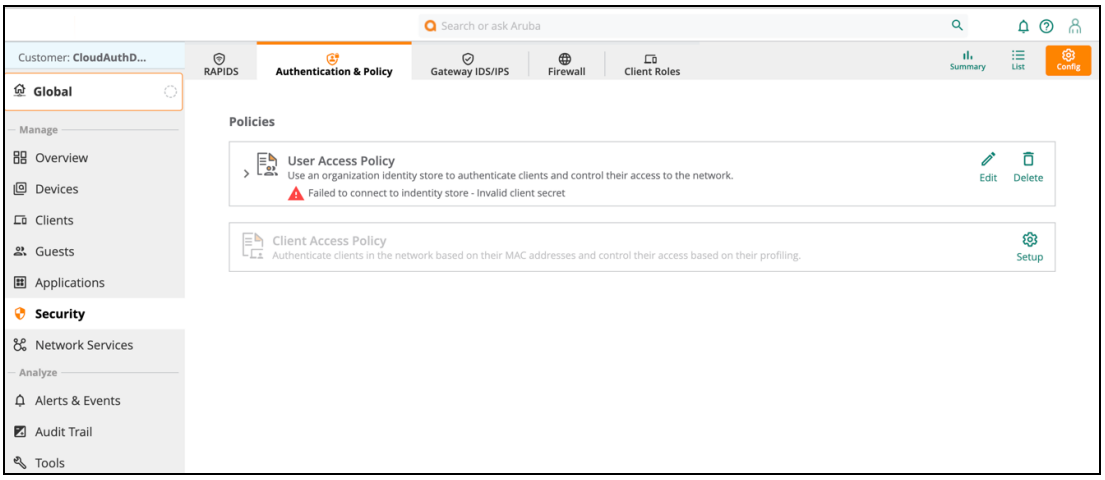
Yes, the HPE Aruba Networking Onboard uses OpenSource components which can be downloaded from https://myenterpriselicense.hpe.com/cwp-ui/dashboard/software.

For more information, see notices information for the third-party components used by HPE Aruba Networking Onboard.

How can I successfully connect to Cloud Authentication and Policy without authorization failures?

To avoid authorization failures, the administrator must verify the validity of credentials for the external identity store by checking the **Authentication & Policy** tab. If the credentials are not valid, an error will be shown in that tab. These errors might occur if the credentials have expired or changed in the identity store. To update your credentials, edit the Identity Store configuration.

The following figure shows a snapshot of the authorization error:



Can I upload an Admin Managed MPSK file more than once? What happens if the file has entries with an existing MPSK name?

Yes, you can upload an Admin Managed MPSK file more than once. If there are no changes in the file, the upload will have the same result as the initial upload and no records will be updated. If there are changes in the file, records will be matched based on the MPSK name and updated accordingly, except for the MPSK password that will remain unchanged.

You can upload a file that has entries with an existing MPSK name. If the entry has a different role or status than the existing MPSK, then the entry will get updated while the existing MPSK password will remain unchanged. For more information, see MPSK Support.

What happens if an MPSK name is repeated in an Admin Managed MPSK file?

Only the first instance of the MPSK name is applied whereas the other rows will generate an error.