

Cloud Authentication and Policy Feature Guide



a Hewlett Packard
Enterprise company

Copyright Information

© Copyright 2022 Hewlett Packard Enterprise Development LP.

Open Source Code

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

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

Contents	3
About This Document	5
Intended Audience	5
Conventions	5
Terminology Change	7
Contacting Support	7
Cloud Authentication and Policy Overview	8
Cloud Authentication and Policy Architecture	8
Roles Applicable for Configuring Cloud Authentication and Policy	9
Supported Devices and Operating Systems	10
Supported Deployment Types	11
Prerequisites for Configuring Cloud Authentication and Policy	11
Cloud Authentication and Policy Caveats	12
Configuring Cloud Authentication and Policy Server in a WLAN Network	16
Configuring Cloud Authentication and Policy Server in a Wired Network	18
Cloud Identity	20
Configuring Microsoft Azure Active Directory for Cloud Authentication	20
Configuring Google Workspace for Cloud Authentication	22
Configuring Cloud Authentication and Policy	25
Configuring User Access Policy	25
Configuring Client Access Policy	28
Revoking Client Certificates	30
Configuring Wired Port on an AP or IAP	31
Configuring AOS-CX for Cloud Authentication and Policy	33
Configuring Wi-Fi Easy Connect for UXI Sensors	34
Configuring Unbound MPSK	36
Updating Cloud Authentication and Policy	40
Updating User Access Policy	40
Updating Client Access Policy	41
Provisioning Clients	43
Provisioning Wired Devices using Cloud Authentication and Policy	43
Onboarding Wired and Wireless Devices using Cloud Authentication and Policy	44
Onboarding Workflow	45
App-based Onboarding	46
Browser-based Onboarding	52
Monitoring Cloud Authentication and Policy	54
Data Filters	54
Authentication Summary Charts	55
Sessions Summary Charts	59
Viewing Access Request List	62
Viewing Access Request Details	63
Viewing Sessions List	65
Client Security	66
Cloud Authentication and Policy FAQs	68
How do I create a policy as an administrator for multiple users and client devices?	68
How do I add or update user groups or client role mapping in the user access policy?	68
How do I change the organization name and see the preview that appears on the Aruba	68

Onboard app?	
How do I update the user access policy when a user switches between user groups?	68
How do I update user groups when a user leaves the organization?	69
How do I update a policy to change the default WLAN SSID that the users connect to?	69
How do I configure Google Workspace for Cloud Authentication?	69
How do I configure Azure Active Directory for Cloud Authentication?	69
What roles are used when creating the Cloud Authentication and Policy?	69
How do I create a policy to block users who are violating the user access policy?	70
What are the WLAN access levels that Cloud Authentication and Policy support?	70
How do I add headless device(s) that are not defined in Aruba Central using client tags?	70
Can I upload client information from an external file?	70
I do not have Passpoint or Hotspot 2.0 on my mobile device. Can I connect it to an enterprise wireless network?	70
How do I get the onboarding URL for the Aruba Onboard app?	70
How can I connect the client to an wireless network without using the Aruba Onboard app?	70
Can I delete a network profile from the Aruba Onboard app?	71
Does Cloud Authentication and Policy support wired SSID?	71
Does the Aruba Onboard app use OpenSource components?	71
How can I successfully connect to Cloud Authentication and Policy without authorization failures?	71

This document describes the Aruba Cloud Authentication and Policy and provides detailed instructions for setting up, configuring, and updating Cloud Authentication along with provisioning devices and monitoring authentication requests from Aruba Central.

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

The following informational icons are used throughout this guide:



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



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



Indicates a risk of personal injury or death.

Terminology Change

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

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

Contacting Support

Table 2: *Contact Information*

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

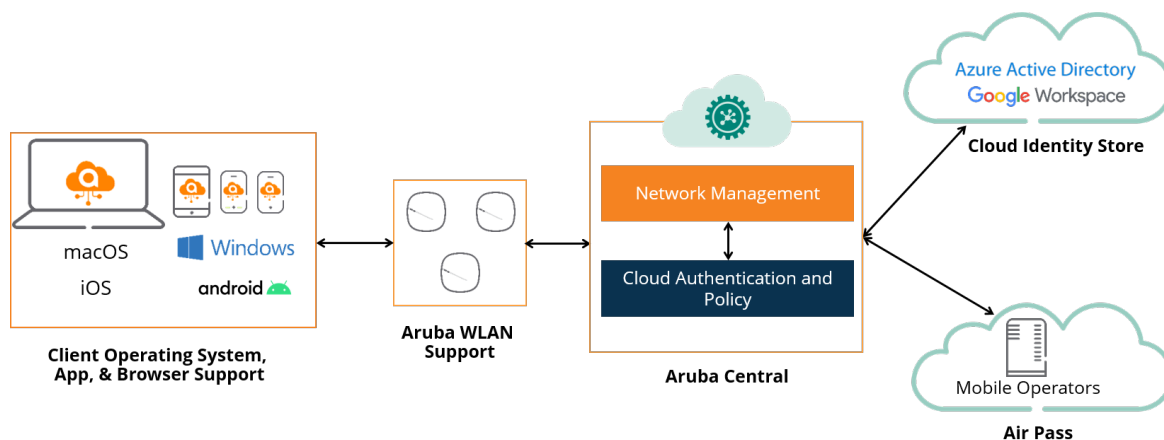
Cloud Authentication and Policy allows you to configure user and client access policies that provide a secured, cloud-based network access control (NAC). In Aruba Central, you can configure these policies and provide an on-boarding URL for the network users to connect to the network. As the users attempt 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 Aruba Central. User groups must be predefined in the cloud identity stores, from cloud providers like Google Workspace or Microsoft Azure Active Directory (Azure AD). Client roles can be defined in the Aruba 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 Aruba 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 Aruba Devices:** Based on the client access policy in the Cloud Authentication and Policy configuration, the Aruba devices that are managed through Aruba 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 Aruba devices. You can also use the Aruba Onboard app to connect the clients to the network.

- **Cloud Authentication and Policy:** With Aruba Central, administrator can configure separate user policy and client policy as part of configuring user and client access policy. This flexibility of configuring independent user and client access policies allows the administrator to configure security levels at both user and client level. For more information about configuring user and client access policy, see [Configuring Cloud Authentication and Policy](#)
- **Cloud Identity Store:** Aruba 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 Aruba 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. Cloud Authentication and Policy retrieves and validates all the necessary attributes from the identity providers before enforcing role-based access policies associated with the user groups. Currently, Cloud Authentication and Policy supports two external identity providers, that is, Google Workspace and Microsoft Azure AD.
For more information about configuring Google Workspace and Microsoft Azure AD, see the following topics:
 - [Configuring Google Workspace for Cloud Authentication](#)
 - [Configuring Microsoft Azure Active Directory for Cloud Authentication](#)

Roles Applicable for Configuring Cloud Authentication and Policy

With Aruba 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 Aruba 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 for Configuring Cloud Authentication and Policy](#)
- [Configuring the 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 Aruba 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 Aruba Devices*

Aruba Device(s)	Supported versions	Supported Aruba Device Models
Instant AP	Aruba Instant 8.6.0.x, 8.7.0.x, 8.8.0.x, and 8.9.0.x	<ul style="list-style-type: none">■ AP-2xx■ AP-3xx■ AP-50x■ AP-51x■ AP-53x■ AP-55x■ AP-635
AP	AOS 10.2, AOS 10.3, and AOS 10.4	<ul style="list-style-type: none">■ AP-303P■ AP-318■ AP-325■ AP-34x■ AP-36x■ AP-37x■ AP-387■ AP-50x■ AP-51x■ AP-53x■ AP-635■ AP-655
	AOS 8.10 and AOS 8.11	<ul style="list-style-type: none">■ AP-615■ AP-655
AOS-CX	AOS 10.10	<ul style="list-style-type: none">■ 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 8360 Switch 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

Client Operating Systems	Supported Versions
macOS	macOS 10.13 and later
iOS	iOS 12.1 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 Aruba Central, you can deploy Cloud Authentication and Policy in wireless and wired modes. The [Cloud Authentication and Policy Deployment Modes](#) table lists the Aruba devices that must be available in Aruba 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](#).

Table 5: *Cloud Authentication and Policy Deployment Modes*

Deployment Mode	Aruba Device(s) Connected to Aruba Central	Supported version(s)
Wireless	Instant AP	Aruba Instant 8.10
	Aruba AP	AOS 10.4
Wired	AOS-CX	AOS 10.10



Cloud Authentication and Policy is not supported for overlay deployment mode.

Prerequisites for Configuring Cloud Authentication and Policy

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

Ensure to complete the following prerequisites before configuring the user access policy and client access policy for users and client devices.

- Ensure that you have created a device group containing at least one Aruba AP. You can onboard ArubaAPs, using the **Devices** option in HPE GreenLake platform. For more information, see the **Managing Devices** section in the HPE GreenLake Edge to Cloud Platform User Guide, using the following link - <https://www.arubanetworks.com/techdocs/central/latest/content/nms/intro-pages/related-info.htm>.

- For more information about how to assign APs to device groups, see *Aruba 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 *Aruba Central Help Center*
 - Configuring User Roles for Instant AP Clients in *Aruba Central Help Center*
- Ensure the Client Profiles and Client Tags are available in your Aruba Central account. Optionally, create custom tags in addition to the system tags for client devices. For more information about adding Tags, . For more information about adding Tags, see *Managing Tags in Aruba Central Help Center*.



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.

- You must obtain the external cloud identity store details. Cloud Authentication and Policy currently supports Aruba, Google Workspace, and Microsoft Azure AD.
For more information about configuring Google Workspace and Microsoft Azure AD, see the following topics:
 - [Configuring Google Workspace for Cloud Authentication](#)
 - [Configuring Microsoft Azure Active Directory for Cloud Authentication](#)

Cloud Authentication and Policy Caveats

The following sections provide details on the caveats to be noted when using Cloud Authentication and Policy in Aruba Central.

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 Aruba 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 Azure AD](#) and [Creating email alias in Google Workspace](#). Currently, this is a limitation and it will be fixed in a future release.

Browser-based Onboarding

The following section defines the caveats and workarounds for browser-based onboarding across different OS platforms.

Android

- 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 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.
- 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.

App-based Onboarding

The following section defines the caveats and workarounds for app-based onboarding across different OS platforms.

Android

- On Samsung devices running Android 11 and One UI version 3.1, when Aruba 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:
 1. Add the Aruba Onboard app in the list of Never Sleeping Apps under Battery > Background Usage Limits > Never Sleeping Apps.
 2. 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 Aruba Onboard app. For more information on refreshing network profile, refer [Managing Network Profiles](#).
- 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

- When users onboard two domains with the same organization name in Aruba 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, Aruba recommends to delete the inactive network profile when users roam between the commonly named domains.
- 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 for some reason, 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 Aruba 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 Aruba 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 Aruba Onboard app, see [Uninstalling the Aruba Onboard App](#).
- Due to a design limitation in the Aruba 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 behaviour and is not recommended.

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 [Configuring Client Access Policy](#).

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.

Non-Passpoint Device Support for Android Onboarding App

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 Aruba 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 configuration w.r.t 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 Aruba 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 Aruba 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.

CHAP Disabled for Wired Configuration

The Challenge-Handshake Authentication Protocol (CHAP) mode is not supported by the Cloud Authentication RADIUS server. In Aruba 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 is not Supported

Authorization of user accounts that are integrated with Microsoft Azure AD and Google Workspace as an external identity source is currently not supported.

For more information, see [External Identities in Azure Active Directory](#).



For Azure AD, ensure to use the basic user group in the User Groups to Client Role Mapping. Nested groups in Azure AD are not supported.

Hidden SSID is not Supported

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

Configuring Cloud Authentication and Policy Server in a WLAN Network

The Cloud Authentication and Policy server in a WLAN network must be configured in Aruba Central, to provide seamless wireless network connection to the end-users and client device. With Aruba 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 **Aruba Central** app, 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 Instant APs* section in Aruba Central Help Center.



Hidden SSID is not supported for Cloud Authentication and Policy.

7. Click **Next**.
8. Under **WLANs**, 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 Aruba Central Help Center.
9. Click **Next**.
10. 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.

- 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.

- 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 Aruba Central Help Center.

11. Click **Next**.

12. 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 Aruba 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.

13. Click **Next**.

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

14. Click **Finish**.

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 a seamless access to the network. With Aruba 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 **Aruba Central** app, 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.



NOTE

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 Aruba 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 Aruba 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 the **Port Type Trusted** toggle switch is disabled.



NOTE

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

- **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 Aruba 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**.

Cloud Authentication and Policy allows users to connect to enterprise Wi-Fi networks securely and access Aruba Central. For enterprise users, Aruba Central allows network administrators to centrally configure and manage users and user groups. Aruba Central also allows administrators to select an external cloud identity store, such as Microsoft Azure Active Directory (Azure AD) or Google Workspace, to authenticate users before providing them the right level of network access.

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

- [Configuring Microsoft Azure Active Directory for Cloud Authentication](#)
- [Configuring Google Workspace for Cloud Authentication](#)

Configuring Microsoft Azure Active Directory for Cloud Authentication

Azure AD 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 Azure AD to control access to apps and app resources, based on the organizations' business requirements.

In Aruba Central, administrators can configure user policies based on the user groups defined in the Azure AD identity store. When creating a user policy, a network administrator must provide information such as tenant ID, client ID, and client secret from Azure AD.

Cloud Authentication and Policy fetches and validates all the necessary user attributes such as user's group membership, department, and title, from the identity store before enforcing role-based access policies.



When the administrator changes the group membership of a user, or deletes or disables a user in Azure AD, the change gets synchronized with Cloud Auth by the daily full sync. The full synchronization runs daily once in every 24 hours. This can take up to 24 hours for the changes to get reflected.

Getting the Client Information from Microsoft Azure AD

To get the client information for configuring a user policy, complete the following steps:

1. Open the <https://portal.azure.com/#home> URL to access Azure portal.
The Microsoft Azure portal is displayed.
2. From **Azure Services** section, select **Azure Active Directory**.
The **Active Directory** page is displayed.
3. From the left navigation, click **App registrations**.
4. Click the **Owned Applications** tab.
5. Click the application name to see the details such as Client ID, Tenant ID, and Client Secret.

To register the Cloud Authentication and Policy application, get API permissions, and create client secret ID, refer to the following topics.

Configuring Cloud Authentication and Policy Application in Microsoft Azure AD

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

- Registering the Cloud Authentication and Policy application in Azure AD portal
- Configuring API permissions for Cloud Authentication and Policy application
- Configuring Client Secret ID for Cloud Authentication and Policy application

Registering Cloud Authentication and Policy Application in Azure AD Portal

Register the Cloud Authentication and Policy application in Azure AD to authenticate with the Microsoft identity platform endpoint. This authentication is required to configure the Cloud Authentication and Policy application and get a token from the Microsoft identity platform endpoint. This configuration allows the Cloud Authentication and Policy application to call Microsoft Graph to fetch the required user data.

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 in Aruba Central Help Center.

Configure API Permissions for Cloud Authentication and Policy Application

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



In the Azure 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**.

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

For instructions, see the **Request the permissions in the app registration portal** section in the [Permissions and consent in the Microsoft identity platform](#) page.



After adding the API permissions, you must grant the admin consent for all API permissions that you have added. Click the **Grant admin consent** option on **API Permissions** screen to consent to the API permissions. You must have the administrator rights to the directory to grant admin consent.

Configure Client Secret ID for Cloud Authentication and Policy Application

The client secret is a string value and it 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 instructions, 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. To see **Tenant ID** for the Cloud Authentication and Policy application, select **Properties** from the left navigation. Ensure to note down the tenant ID to use it in the Cloud Authentication and Policy application.

Configuring Google Workspace for Cloud Authentication

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

In Aruba Central, administrators can configure user policies based on the user roles defined in the identity store. When a user policy is created, a network administrator must provide information such as client ID and client secret from Google Workspace.

Cloud Authentication and Policy fetches and validates all the necessary user attributes such as user's group membership, department, and title from the identity store before enforcing role-based access policies.



When the administrator deletes or disables a user from Google Workspace, Cloud Auth receives a notification about the event. This change gets reflected within a short span of time. When the administrator changes a user's group membership, the change is synchronized by the daily synchronization. This can take up to 24 hours to get reflected.

Getting the Required Information from Google Workspace

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

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

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

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. From the left menu, select **Account > Account settings**.
The Account Settings page is displayed.
4. Note down the **Customer ID** that is displayed in the **Profile** section.
5. From the left menu, select **Domains > Manage Domains**.
The **Manage domains** table is displayed.
6. Note down the primary domain name.

To get the **Client ID**, **Client Secret**, and download the **JSON** file, 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 menu, 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 from this page.
7. Click **Download JSON**.
The JSON file is downloaded.
8. From the credentials page, copy the **Client ID**, **Client Secret**, and download the credentials JSON file.

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

To register the Cloud Authentication and Policy application in Google Workspace, see the following topics.

Configuring Cloud Authentication and Policy Application in Google Workspace

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:

- Get the customer ID and domain details from the Google Admin Console.
- Create a project in Google Cloud Platform.
- Provide access to Google Workspace instance.

Get the Customer ID and Domain Information from the Google Admin Console

To configure the Google Workspace in the Cloud Authentication and Policy application, get the client and domain information from the Google Admin Console. For instructions, see [To get the Customer ID and Domain information, complete the following steps:](#)

Creating a Project and Enabling the Admin SDK API 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 the users and groups in the 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 instructions, see [Configure the OAuth consent screen](#).

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. For instructions, see [Setting up OAuth 2.0](#).

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 in Aruba Central Help Center.

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 instructions, see [Create a service account with domain-wide delegation of authority](#).

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,`
 - `https://www.googleapis.com/auth/admin.directory.user.readonly,`
 - `https://www.googleapis.com/auth/admin.directory.user.security,`
 - `https://www.googleapis.com/auth/admin.directory.group,`
 - `https://www.googleapis.com/auth/admin.directory.group.readonly,`
 - `https://www.googleapis.com/auth/admin.directory.group.member,`
 - `https://www.googleapis.com/auth/admin.directory.group.member.readonly,`
 - `https://www.googleapis.com/auth/admin.directory.rolemanagement,`
 - `https://www.googleapis.com/auth/admin.directory.rolemanagement.readonly,`
 - `https://www.googleapis.com/auth/cloud-platform`

For instructions, see [Set up domain-wide delegation for a client](#).

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

Removed **Configuring Webhook Notifications** section as per CDA-2664, applicable to both 255 and 256 - Sandhya

Aruba 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](#)
- [Configuring Client Access Policy](#)

Configuring User Access Policy

With Aruba Central, you can create user access policies in wireless and wired (AOS-CX) modes to define network locations that can be accessed by end users in an enterprise network.

To configure user access policy, complete the following steps:

1. In the **Aruba Central** app, 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 **User Access Policy** section.
5. To configure an external identity server, do one of the following:
 - To configure **Microsoft Azure AD** as your identity server, do the following:
 - a. Select **Microsoft Azure AD** 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 Azure AD. Click **Confirm** to proceed.

- b. Configure the following parameters:
 - **Tenant ID**—The tenant ID that is used by Cloud Authentication and Policy application when it communicates with the Microsoft Azure AD.
 - **Client ID**—The client ID that is used to identify the Cloud Authentication and Policy application with Microsoft Azure AD.
 - **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.

c. Click **Connect**.

If the connection is successful with your **Microsoft Azure AD** account, you can see the following changes:

- The **Connect** button is changed to **Connected Successfully ✓**.
- The **User Groups to Client Role Mapping** table and the **Network Profile** section are displayed.

■ 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 Azure AD 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 [Configuring Google Workspace for Cloud Authentication](#).

c. Click **Connect**.

If the connection is successful with your **Google Workspace** account, you can see the following changes:

- The **Connect** button is changed to **Connected Successfully ✓**.
- The **User Groups to Client Role Mapping** table and the **Network Profile** section are displayed.



To set up the identity store in Microsoft Azure AD console 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.

6. To add a new row in the **User Groups to Client Role Mapping** table, do the following:
 - a. Select a user group from the drop-down list under **User Group**.



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

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



-
- 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.
 - If you delete a client role associated with a user access policy, the user access policy will not work as expected.
-

- c. To create a new row in the **User Groups to Client Role Mapping** table, click the **+** icon and repeat steps **a** and **b**.



As part of the default policy mapping, the **Unspecified** user group is now available. Users who are not part of any of the existing user group, will be categorized as Unspecified user group. You can assign a role or deny access from the **Client Role** drop-down to the Unspecified user group.

7. 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 Aruba Central. Based on the organization name you have provided, the **Aruba Onboard mobile app preview** shows how the organization name will appear in the corresponding Aruba Onboard mobile app.
-

- b. Select WLAN SSID from the **Connect users to WLAN** 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 **Connect users to WLAN** drop-down displays only enterprise SSIDs. As enterprise SSIDs with Cloud Auth as AAA server are applicable to the Client App (Aruba 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, Connect users to WLAN drop-down list does not display the WLAN SSIDs that are configured at device level.
- If you delete the selected WLAN SSID from the WLAN configuration, the user access policy will not work as expected.

8. Click **Save**.

9. Click the **User Access Policy** accordion to view 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 .



For the wired client device access, after upgrade to Aruba 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 Aruba Onboard App version 1.3 and onwards.

Viewing User Access Policy

To view a user access policy, click the **User Access Policy** accordion.

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.

Configuring Client Access Policy

With Aruba 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 Aruba Central.

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 Aruba Central Help Center
- Managing Tags in Aruba Central Help Center

To configure Client Access Policy, complete the following steps:

1. In the **Aruba Central** app, 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.
5. To add a new row 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:
 - a. 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 appears and the **ADD** button is enabled.



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

- b. Click **ADD**.
- To create a new row in the in the **Allowed MAC Addresses** table, click the **+** icon, and do the following:
 - a. In **Add MAC based client** prompt, enter the MAC address of the device in the **MAC Address** field and the client name in the **Client Name** field.
 - b. Click **Save**.



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

6. 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**.



-
- The values that appear in this drop-down list are mapped to system tags and user tags available in Aruba Central. . For more information about adding Tags, see Managing Tags section in Aruba Central Help Center.
 - 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 Aruba Central Help Center](#).
- 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.

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

Viewing Client Access Policy

To view a client access policy, click the **Client Access Policy** accordion.

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.

Revoking Client Certificates

End-users can use the Self-Service portal for revoking certificates for a specific client.

Ensure you have the onboarding URL shared by the network administrator. For more information, see [Onboarding Wired and Wireless Devices using Cloud Authentication and Policy](#).

Perform the following steps to revoke the client certificates:

1. Ensure you have the onboarding URL.
2. In a web browser paste the onboarding URL into the address bar and press the **Enter** key.
The onboarding portal is displayed.
3. Click **Manage my network credentials**.
A **Sign in** page appears.
4. Click **Sign in for Provisioning**.
The **Self Service** page appears which lists the **Network Credentials**.

5. 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.
6. 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.
7. 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](#).

Automatically Revoke Client Profiles and Certificates

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

When a 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.

The **CLIENTS** page in **Aruba Central** will display the client **Status** as **Offline**.

To view the status of the client devices complete the following steps:

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

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.

To view the **Access Requests** list, complete 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. To view the **Access Requests** table, click the **List** icon and click the **Access Requests** tab.
The **Access Requests** table is displayed which lists the details of the client devices in the network.
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.
4. Click the Username in the **Access Requests** table.
The user's device details is displayed in the **Details View** page.
Under **Summary**, the **Error** field displays the reason as **Certificate revoked**.

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 Aruba 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 **Aruba Central** app, 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 *Table 1: Advanced Settings Parameters in Configuring Wireless Network Profiles on IAPs* section in the Aruba 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 Aruba 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 Aruba 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](#).

Configuring AOS-CX for Cloud Authentication and Policy

[Cloud Authentication and Policy Overview](#) 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.

To configure AOS-CX switch support for Cloud Authentication and Policy, do the following:

1. Configure User Access Policy
2. Configure Client Access Policy
3. Configure 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](#).

Configure Cloud Authentication and Policy on AOS-CX

1. In the **Aruba Central** app, 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.



After the Aruba 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 Aruba 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 Aruba 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 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. Aruba User Experience Insight (UXI) devices support Wi-Fi Easy Connect and can be deployed and onboarded easily and securely.

Prerequisites

The following are the prerequisites for configuring DPP:

Integrate UXI sensors with Aruba Central

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

Perform the following steps:

1. In the **Aruba Central** app, 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 Aruba 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 Aruba 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 Aruba 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 Aruba Central Help Center.

Configure DPP in Cloud Authentication and Policy

To configure DPP, a Client Access Policy must be created. For more information, see [Configuring Client Access Policy](#).

Complete the following procedure:

1. In the **Aruba Central** app, 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 **Aruba 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

Configuring Unbound MPSK

The Cloud Authentication and Policy server enables unbound Multi Pre-Shared Key (MPSK) in a WLAN network in Aruba Central, to provide seamless wireless network connection to the end-users and client devices. With Aruba Central, you can configure MPSK at the **Personal** security level in the **Security** tab.



-
- A maximum of 1000 MPSK keys are supported.
 - Cloud Authentication and Policy requires AOS 10.4 software for implementation of the unbound MPSK feature.
-

To configure MPSK, complete the following steps:

1. In the **Aruba Central** app, 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 Aruba CentralOnline 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 Aruba CentralOnline Help.
9. Click **Next**.
10. In the **Security** tab, select the following:
 - 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 Aruba Central Help Center.



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

13. If the **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** from the drop-down, 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. The 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**.

A success message that the MPSK SSID is configured is displayed.

Add MPSK SSIDs to User Policy

With Aruba Central, you can add the MPSK SSID to the user policy. To do this, complete the following steps:

1. In the **Aruba Central** app, 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 **User Access Policy** section.



The **Setup** is available only for a first time configuration. For subsequent configurations, click **Edit**.

5. To configure an external identity server, see [Configuring User Access Policy](#).
6. To map the user group to the client role, in the **User Groups to Client Role Mapping** table, do the following:
 - a. From the **User Group** drop-down list select a user group.



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

- b. From the **Client Role** drop-down list select the corresponding client role for the user group.



-
- Client Role drop-down list displays only those roles that are configured at group level in the WLAN configuration. That is, Client Role drop-down list does not display the roles that are configured at device level.
 - If you delete a client role associated with a user access policy, the user access policy will not work as expected.
-

- c. To create a new row in the **User Groups to Client Role Mapping** table, click the + icon and repeat steps **a** and **b**.
7. To enable the MPSK network, configure the WLANs for MPSK access in the **WLAN to Password Portal Mapping** table under **Unbound MPSK**. Perform the following steps:
 - a. Select a WLAN from the **WLAN** drop-down list.
 - b. The **Password Portal URL** is auto generated once the configuration is saved.
Click **Save**.



To set up another MPSK, click on the + icon.

Password Portal URL

1. The **Password Portal URL** provides options to open the URL in a new tab or to copy the URL.
2. Click **Copy URL**.
The URL is copied.
3. For onboarding and provisioning client devices, copy the password portal URL and share this with end users. End users must use their account credentials to login to the Password Portal and obtain the generated password.



-
- After the user logs in, a unique MPSK password is generated and this must be used to connect the MPSK SSID.
 - The unique password is generated for each user and can be used to connect all the user's devices.
-

Change Password Policy

1. The **Password Policy** enables the administrator to control the kind of passwords generated for end users. There are two options, **Passphrase** and **Random password**. By default, the **Passphrase** option is selected as the Password Policy. This will generate a passphrase password in the password portal.
2. In the **User Access Policy** card, click **Edit** to change the password policy.
3. Navigate to the **Password Policy** column and choose the **Random Password** option from the drop-down and click **SAVE**. A random password is generated in the password portal.



The password policy change is applicable only to those users who do not already have a password.

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 **Aruba Central** app, 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:



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

- To configure **Google Workspace** or **Microsoft Azure AD** 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**.




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**.



- 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.



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.

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 **Aruba Central** app, 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:



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**.



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**.



- 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.

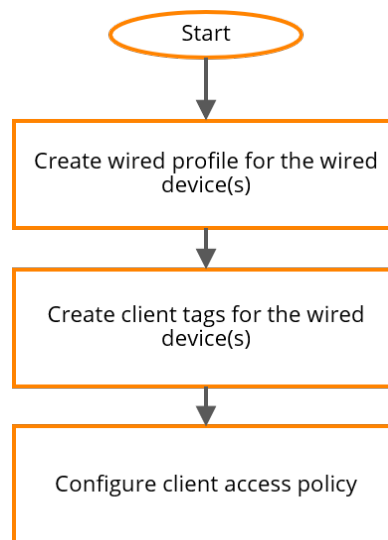
With Aruba Central, administrator can configure a single Cloud Authentication and Policy that implies for both users and client devices. With Aruba Central, administrator can configure separate user policy and client policy as part of configuring Cloud Authentication and Policy.

Provisioning Wired Devices using Cloud Authentication and Policy

With Aruba 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 Aruba ClearPass Device Insight, network and security administrators can discover, add devices, monitor, and automatically classify new and existing devices that connect to a network.

With Cloud Authentication and Policy, administrators can provision wired clients by creating a client access policy to provision devices on the enterprise networks. However, Aruba recommends 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 devices using Cloud Authentication and Policy.



Prerequisites for Provisioning Wired Devices

Before provisioning wired devices in a template group, ensure that the following prerequisites are completed:

- Ensure that you have configured 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](#)

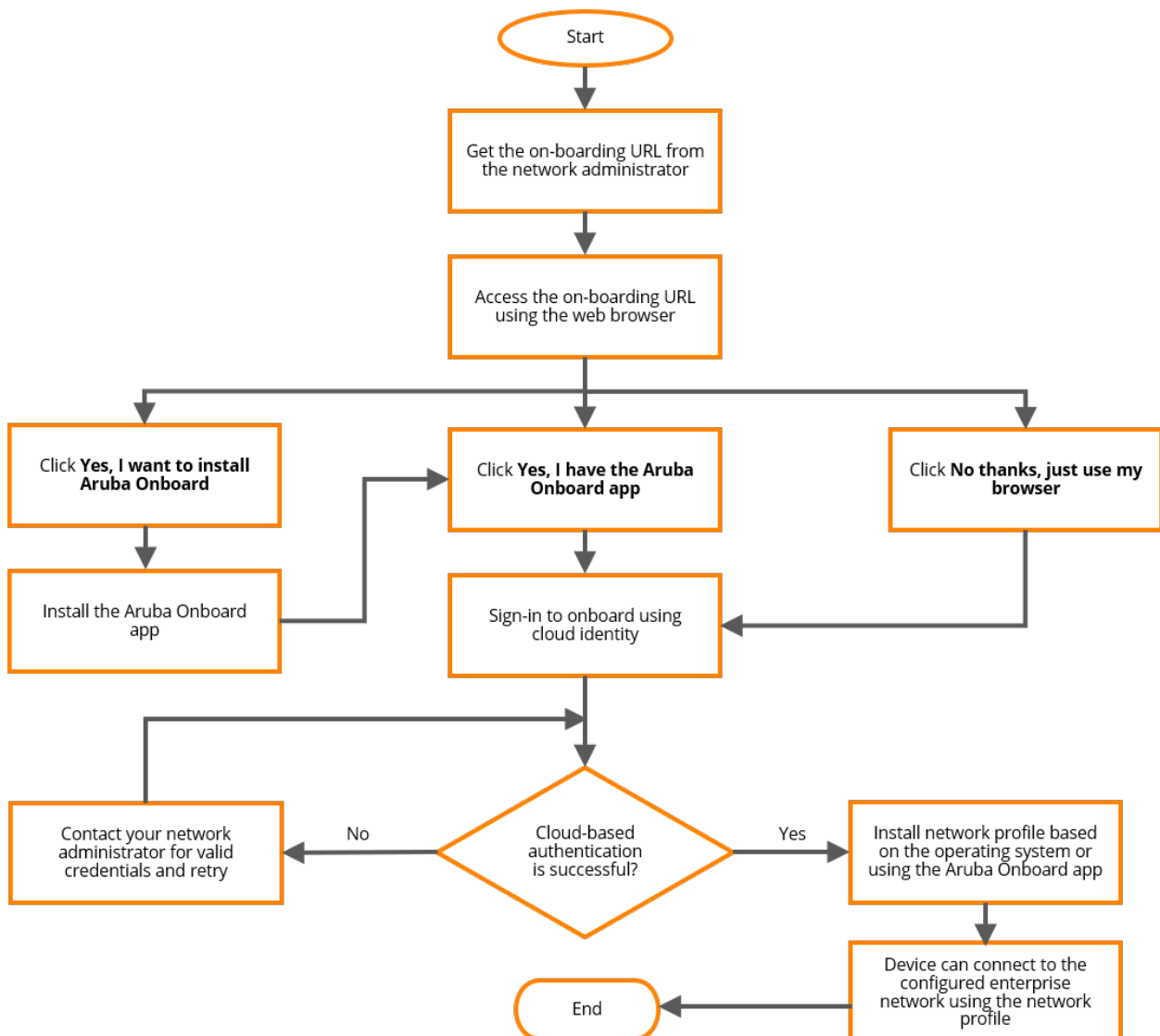
Wired Network.

- Ensure the Client Profiles and Client Tags are available in your Aruba 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 Aruba Central Help Center.
- Ensure that you have configured 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 Aruba Central Help Center.

Onboarding Wired and Wireless Devices using Cloud Authentication and Policy

Cloud Auth policies in Aruba Central define a set of rules and authorize users and devices to access networks. Users can authenticate through cloud identity providers like Microsoft Azure AD or Google Workspace, 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 on-boarding 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 Aruba 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



Aruba recommends using the Aruba 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 Azure AD or Google Workspace to install the network profiles on their devices.

4. Installing and Managing Network Profile

Install and manage network profiles on your devices using the Aruba 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



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.

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

Azure AD or Google Workspace 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.



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 device to connect to the enterprise wireless network through network profiles and Cloud Authentication and Policy authentication. With the Aruba Onboard app, you can download, install, and manage network profiles.

Installing the Aruba Onboard App

To connect your devices to enterprise wireless networks using network profiles, install the Aruba Onboard app. By installing the Aruba Onboard app, you are able to download and configure your network profile. With the Aruba Onboard app, you can also manage the network profiles by refreshing and deleting the network profiles.



-
- For Windows:
 - Only users with administrator privileges can install or uninstall the Aruba Onboard app.
 - Once the Aruba Onboard app is installed by an administrator, a user without administrator privileges can use the app for provisioning.
 - For macOS, only users with administrator privileges can install or uninstall the Aruba Onboard app.
 - For Linux OS, only users with administrator privileges can install or uninstall the Aruba Onboard app.
-

To install the app, complete the following steps:

1. Access the on-boarding URL shared by the network administrator.
2. Select **Yes, I want to install Aruba Onboard**.
3. To install the app, use one of the following options:
 - For Windows, do the following:
 - a. Click **Download for Windows**.
 - b. Double-click the .exe file.

The **Welcome to the Aruba Onboard Setup** page is displayed.
 - c. Click **Next**.

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

d. Click **I agree**.

e. Click **Close** to exit the setup window.

- For Linux, you can use the standard deb installer tools like apt, dpkg, or ubuntu software to install the Aruba Onboard app. Aruba recommends to install the Aruba Onboard app using the command line terminal.
- For an Android device, click the **Get it on Google Play Store** option and select **Install**. Follow the on-screen instructions to complete the installation.
- For an iOS device, click the **Download on the App Store** option and select **GET**. Follow the on-screen instructions to complete the installation.
- For macOS, double-click the downloaded.pkg file and follow the on-screen instructions to complete the installation.



On Samsung devices running Android 11 and One UI version 3.1, Aruba Onboard app may be added into the deep sleep list by the operating system and the network profile is automatically removed from the device. To avoid removing network profiles, add Aruba Onboard app in the list of never sleeping apps. For more information, refer [Cloud Authentication and Policy Caveats](#).

Connecting Device to the Network using Aruba Onboard App

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 Aruba Onboard app. The Aruba Onboard app downloads and configures the network profile on your device to connect to an enterprise wireless network.

To connect device to network, complete the following steps:

1. Access the on-boarding URL shared by the network administrator.
2. Click **Yes, I have the Aruba 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 Azure AD account, complete the following steps:
 1. Enter the username.
 2. Click **Next**.
 3. Enter the password.
 4. Click **Sign in**.
 - To connect using your Google Workspace account, complete the following steps:
 1. Enter the username.
 2. Click **Next**
 3. Enter the password.
 4. Click **Next**.
5. Click **Install using Aruba Onboard app** to install the network profile.
6. Click **Open Aruba Onboard**.

The Aruba Onboard app is displayed.



On Android devices, the Aruba Onboard app is displayed after installing the network profile.

7. In the Aruba Onboard app, click **Set up network profile**.

The **Aruba 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 has completed the onboarding workflow, the successful profile configuration message is displayed.

8. After installing the network profiles, the following security warnings are displayed based on the device's operating system:
 - On Windows, a security warning to install a certificate from a certification authority is displayed. Click **Yes** to proceed.

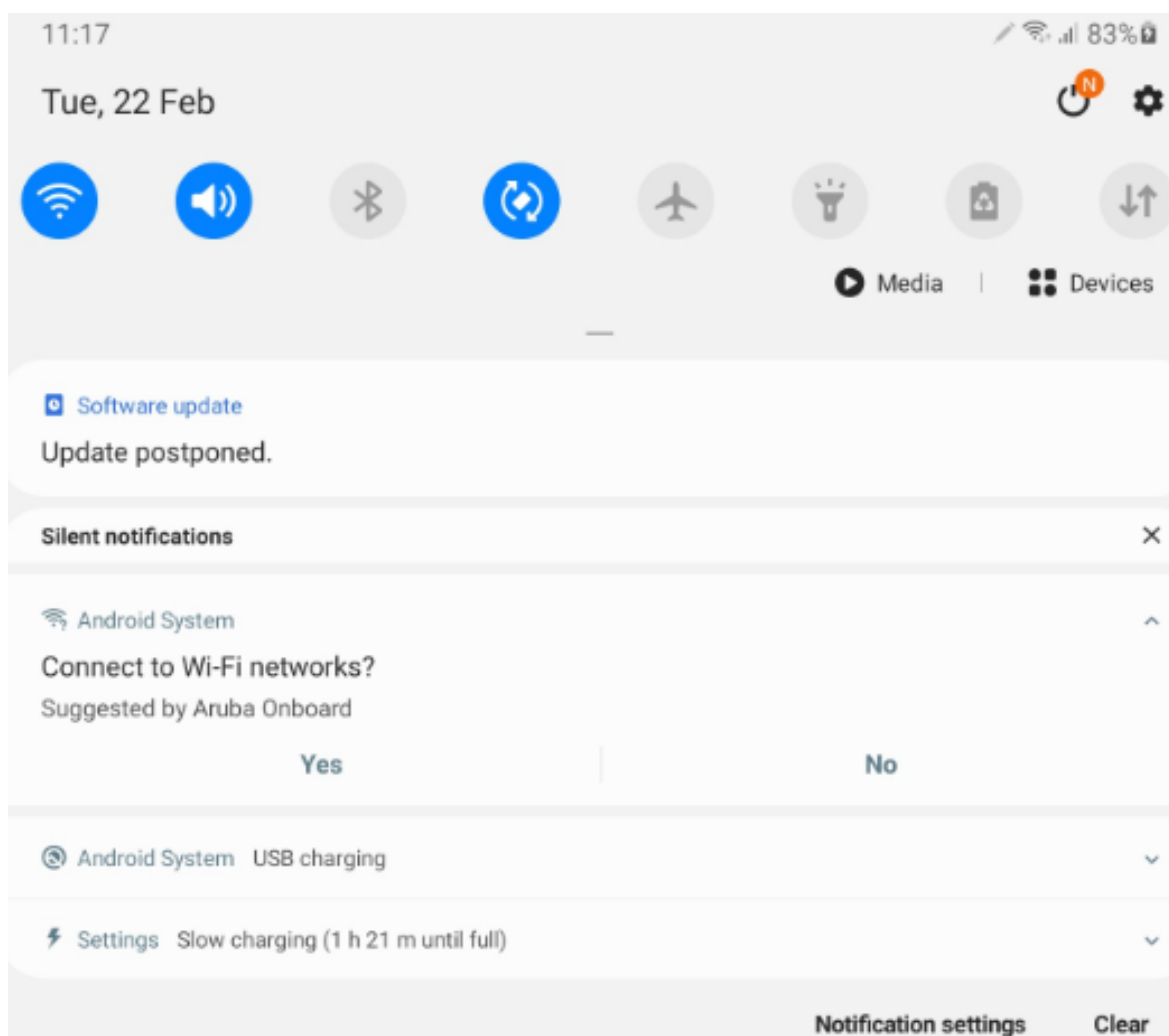


Users with Windows devices that do not support Wi-Fi CERTIFIED Passpoint™ solution cannot install network profiles either through browser-based or app-based onboarding methods.

- On Android 11 devices, the following security warning is displayed while installing network profile for the first time: **Allow Suggested Wifi Network**. Tap **Allow** to proceed.
- On macOS, the following security warnings are displayed:
 - **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 device password to proceed.
 - **Profiles (Certificates) is 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 device password to proceed.
- On iOS, the following security warning is displayed: **Add a Wi-Fi Hotspot Network?**. Tap **Allow** to proceed.
- On Android devices, 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).

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

Figure 2 Notification



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



When creating a user access policy, the network administrator can create a unique name for the network profile. Instead of the SSID name, the Aruba Onboard app displays this organization name in network profiles. On iOS, 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.



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. Users can also disconnect or forget all the existing wireless network in the vicinity. It allows the device to automatically connect to the newly configured network. 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.



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.

Managing Network Profiles

You can add one or more network profiles in the Aruba Onboard app.

You can manage the network profiles in the Aruba Onboard app using the following options:

- To check the validity of the network profile and replace expired certificates in the Aruba Onboard app, complete one of the following steps:
 - On laptops, right-click the network profile card, and click **Refresh**.
 - On mobile devices, on the network profile card, swipe from right to left and select **Refresh**.



After successful onboarding, if Windows devices are unable to connect to the configured network, click **Refresh** on the network profile card or contact your network administrator.

- To delete a network profile in the Aruba Onboard app, complete one of the following steps:
 - On laptops, right-click the network profile card, and click **Delete**.
 - On mobile devices, on the network profile card, swipe from right to left and select **Delete**. Prior to deleting a profile ensure that the Wireless interface is in the enabled state.



-
- Users with Windows devices must ensure that the wireless interface is in the enabled state prior to 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 the network profile installed by the Aruba Onboard app has been deleted manually from the system, the Aruba 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.
-

- To troubleshoot and send the error logs in the network profile installed on the Aruba Onboard app, complete one of the following steps:
- On laptops, click **Send Logs**. The Aruba Onboard app adds the error log files and opens the default email client to send the log files to the administrator.



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.

- On mobile devices, tap **Send Logs**. The Aruba Onboard app provides a variety of share options for the device to send logs to the administrator.

Automatic Network Profile Refresh

Network profiles and certificates installed by the Aruba Onboard app have a validity period. The Aruba Onboard app triggers an automatic network profile refresh before the expiry of the validity period. Aruba Onboard app will trigger an auto-refresh when the installed profile has approximately 20% of the validity remaining as part of the network profile. It continues retrying at regular intervals till the profile expires.

OS limitations for each platform

Table 6: Profile Refresh limitations for Operating Systems

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



1. Windows: Network profiles are refreshed automatically in the background.
2. macOS and iOS: A notification is displayed to the user to initiate Network profile refresh. Users have to tap or click the notification to trigger the network profile refresh.

Uninstalling the Aruba Onboard App

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



Uninstalling the Aruba Onboard app on Android 9 devices do not remove the network profiles and certificates from the device.

To uninstall Aruba Onboard app on macOS devices, 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 Aruba 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.

To uninstall the Aruba Onboard app on Linux devices, complete one of the following steps:

- Use the following commands:
`apt remove aruba-onboard`
`apt purge aruba-onboard`
- On the Aruba Onboard app, click the uninstall icon to remove the app.

Upgrading the Aruba Onboard App

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



- This upgrade is applicable only for desktop platforms Microsoft Windows (App version 1.1 onward) and macOS (App version 1.4 onward).
- The Aruba Onboard App automatically upgrades on Linux OS.

Manually upgrading the Aruba Onboard App for Windows

You need to manually upgrade the Aruba Onboard app from version 1.0 to version 1.1. Only users with administrator privileges can upgrade the application.



- When two or more users share a device, it is recommended that you uninstall the Aruba Onboard app version 1.0 before attempting to upgrade to 1.1. For more information, see [Uninstalling the Aruba Onboard App](#).
- In future releases, the update will occur automatically without user intervention and there will be no disruption in the use of existing profiles or network connectivity.

To upgrade the app, complete the following steps:

1. Access the on-boarding URL shared by the network administrator.
2. Select **Yes, I want to install Aruba 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 Aruba Onboard Setup** page is displayed.
6. Click **Next**.
The **End User License Agreement** page is displayed.
7. Click **I agree** to complete the Aruba 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 Aruba 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 Aruba 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 Mozilla Firefox browsers for mobile devices running Android. Aruba recommends the Safari browser for devices running iOS and macOS.

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 Azure AD or Google Workspace 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.



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

Chapter 7

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 Aruba 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.

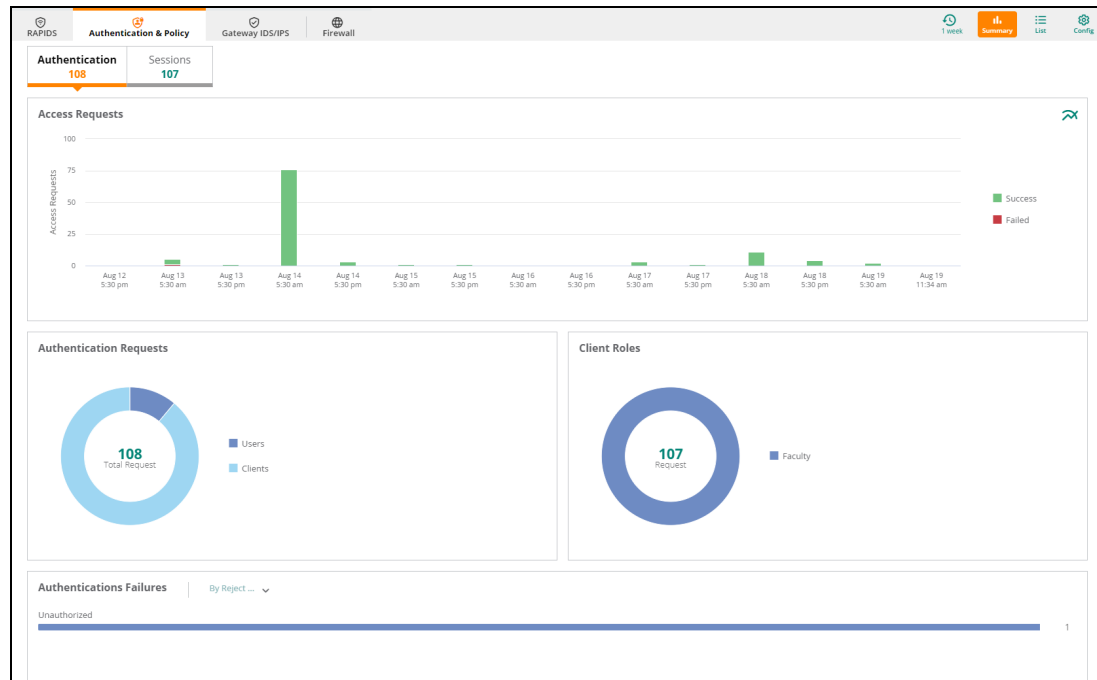


Only for client MAC addresses that are added (or registered) in the **Allowed MAC Addresses** table in the client access policy, the MAC authentication failures are recorded and reported in the charts and Access list table. For more information about configuring new client MAC addresses, see [Updating 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 3](#) shows the **Authentication** and **Sessions** tab in the **Authentication & Policy** dashboard:


Figure 3 *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:

- [Authentication Summary Charts](#)
- [Sessions Summary Charts](#)
- [Viewing Access Request List](#)
- [Viewing Sessions List](#)


Authentication Summary Charts

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 **Aruba Central** app, 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.



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.

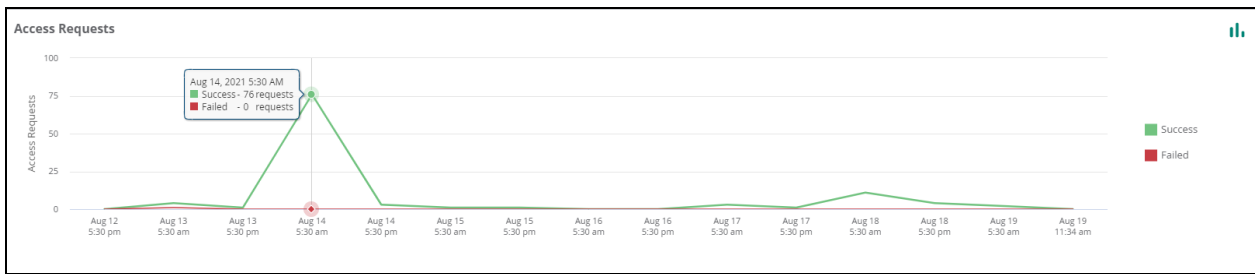
The **Authentication** summary page displays the following charts.

Access Requests Charts

Aruba 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.

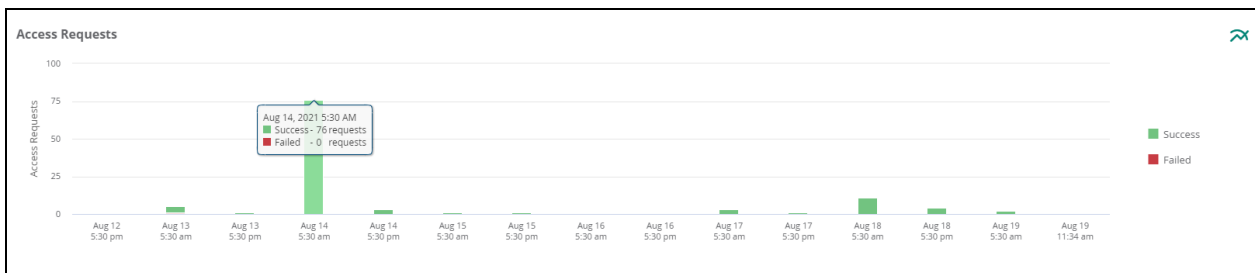
- **Access Requests** line chart—The data points on the chart display the number of access requests that were made in a selected duration, which are grouped by a specific set of dates. When you hover over a data point, it displays the number of successful and failed access requests on a particular date. 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 [Viewing Access Request List](#).

Figure 4 Access Requests Line Chart



- **Access Requests** bar chart—The stacked vertical bars display 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 [Viewing Access Request List](#).

Figure 5 Access Requests Bar Chart



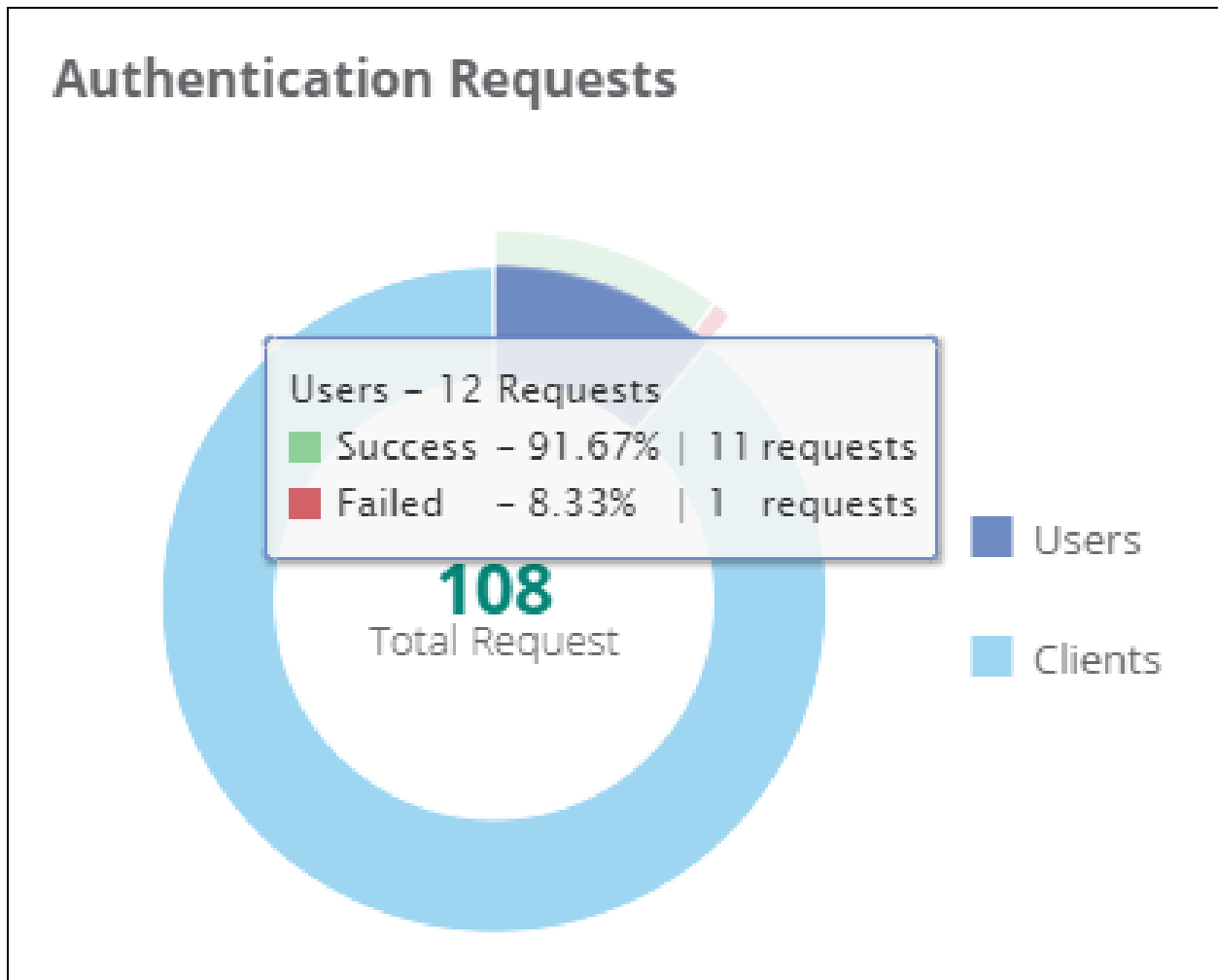
- A legend is displayed next to the **Access Requests** chart. When you click a legend, the associated portion of the chart is shown or hidden for a selected duration. For example, when you click **Success**, the chart shows or hides the number of successful access requests. By default, the chart displays 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 6 Authentication Requests Pie Chart

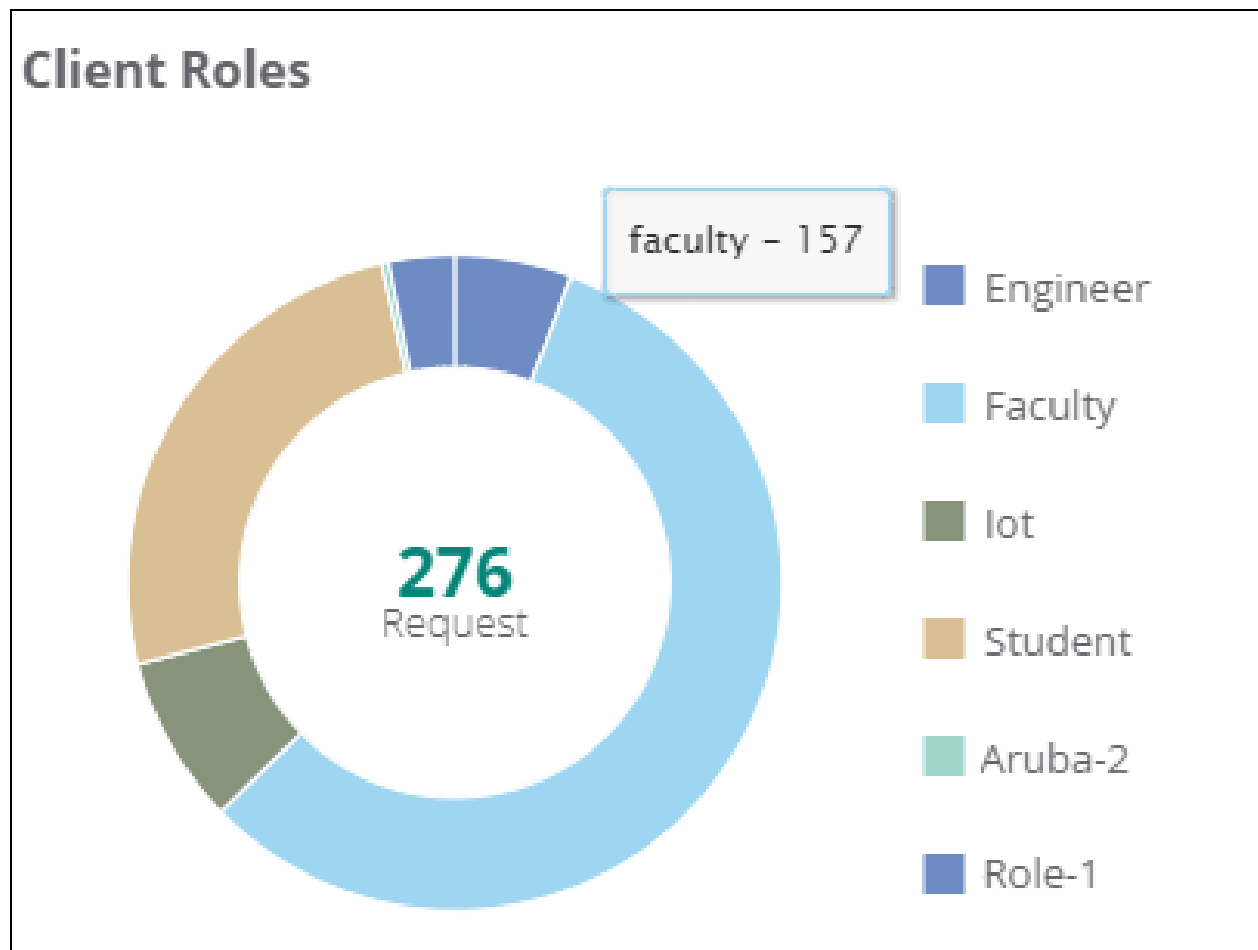


Client Roles Chart

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 [Viewing Access Request List](#).

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 7 *Client Roles Pie Chart*

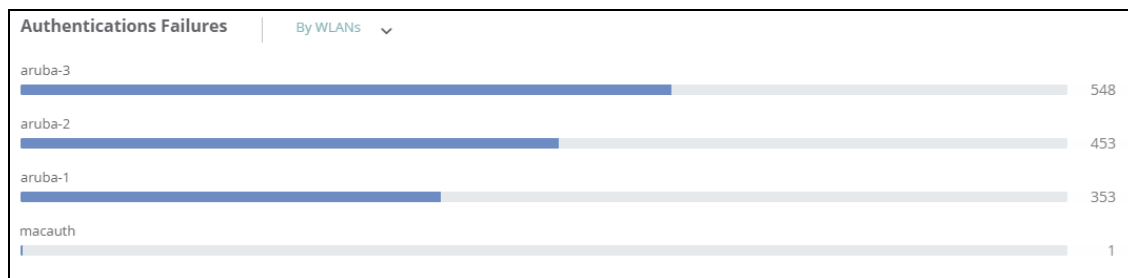


Authentication Failures Chart

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

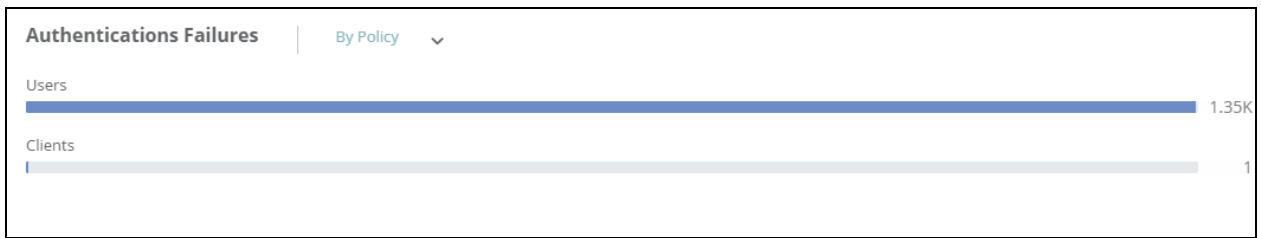
- **By WLANs**—When you select this filter, the chart displays the number of failed authentications requests per WLAN SSID.

Figure 8 *Authentication Failures WLAN*



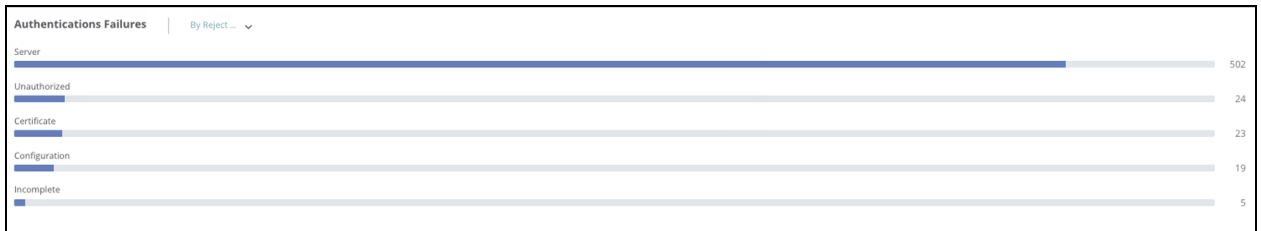
- **By Policy**—When you select this filter, the chart displays the number of failed authentications requests per Cloud Authentication and Policy.

Figure 9 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 10 Authentication Failures Reject Reason




Sessions Summary Charts

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 **Aruba Central** app, 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.



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.

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

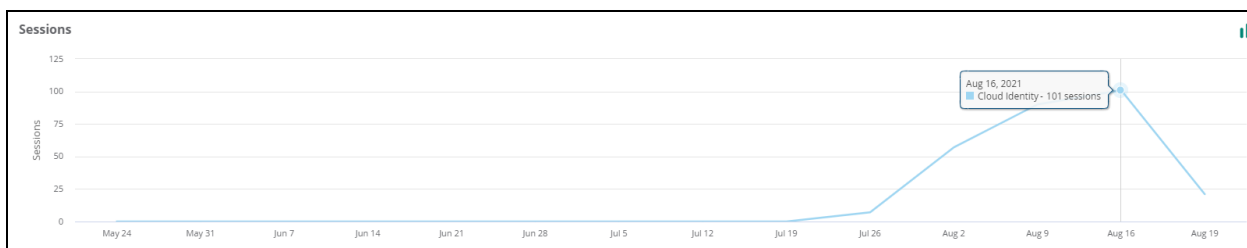
Sessions Charts

Aruba 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 11 *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 12 *Sessions Bar Chart*

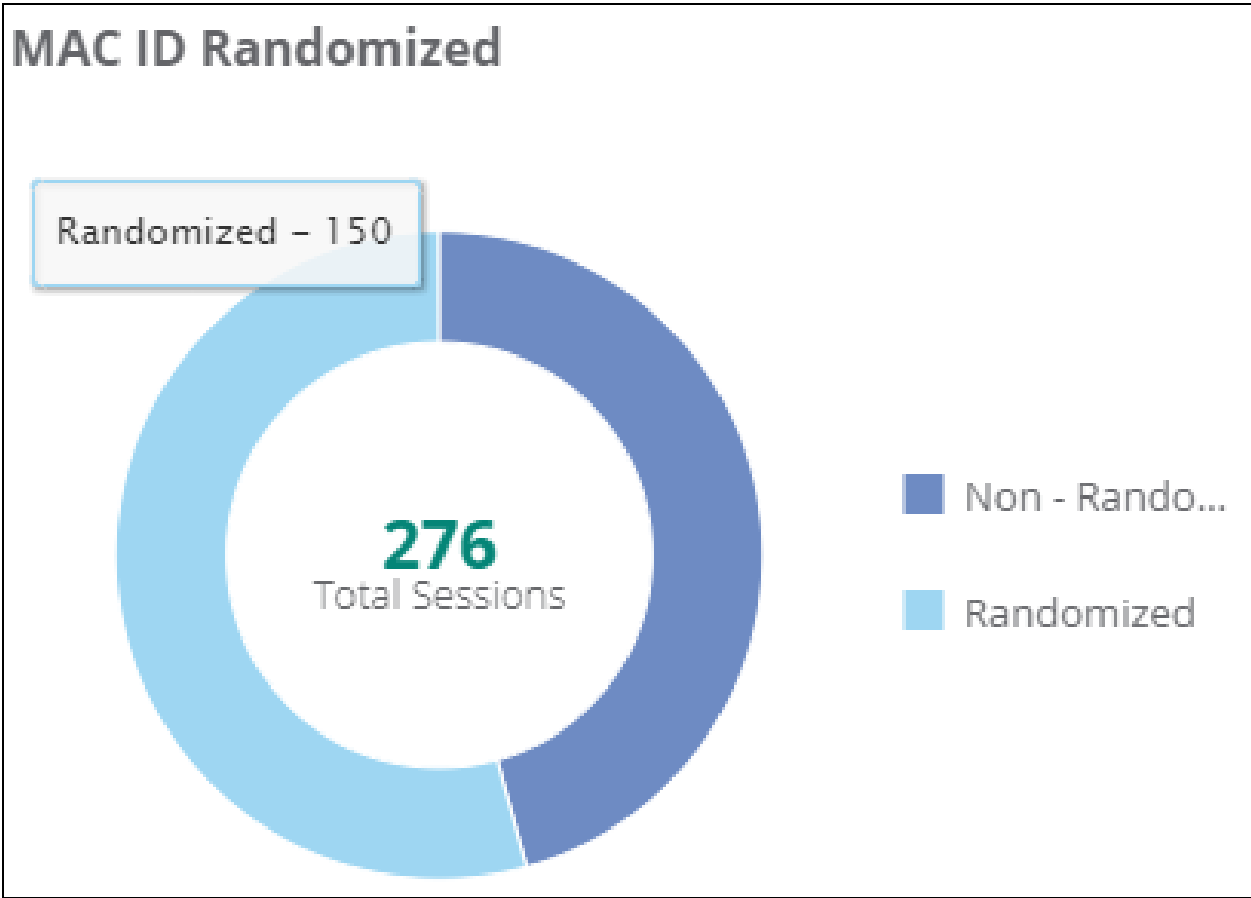


MAC ID Randomized Chart

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.

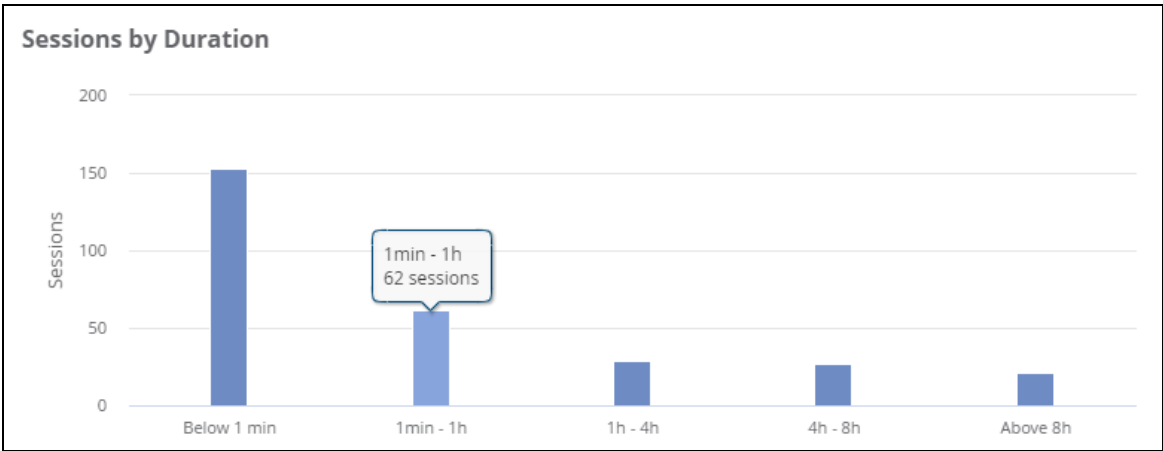
Figure 13 *MAC ID Randomized Pie Chart*



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 14 *Sessions By Duration Chart*

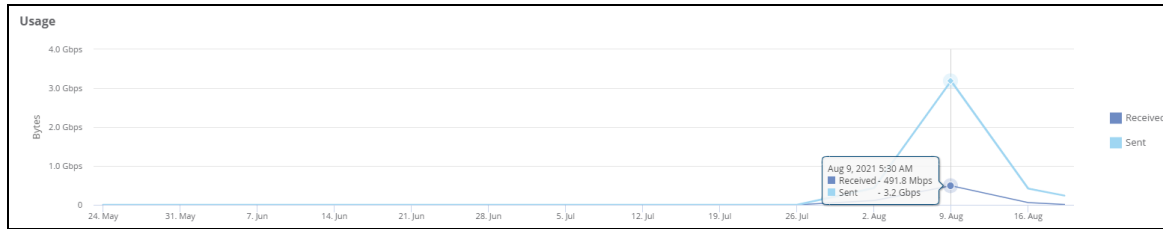


Usage Chart

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 15 *Usage Chart*



Viewing Access Request List

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.



To view the **Access Requests** list, complete 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. To view the **Access Requests** table, click the **List** icon and click the **Access Requests** tab.
The **Access Requests** table is displayed.

The **Access Requests** table provides 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 Request 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 Aruba Central.

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

1. 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.

The **Details View** tab displays the access-request related information in the following sections:

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 **Aruba Central** app, 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.

The Sessions table provides 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.

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.



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 **Aruba Central** app, 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 7: *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 8: *Client Authorization Information*

Condition	Value
Group	The list of user groups from the cloud identity provider.

Condition	Value
Department	The department of the user as per the cloud identity provider.
Identity Store	The cloud identity provider name (Azure or Google).
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 9: *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.

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 for Configuring Cloud Authentication and Policy](#).

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 Aruba Onboard app?

You can change the organization name in the **Network Profile** section, when creating or updating the user access policy. The **Aruba Onboard mobile app preview** section displays how the organization name will appear on the **Aruba 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 Azure AD, 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 [Configuring Google Workspace for Cloud Authentication](#).

How do I configure Azure Active Directory for Cloud Authentication?

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

1. Register the Cloud Authentication and Policy application on the Azure AD 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, see [Configuring Microsoft Azure Active Directory for Cloud Authentication](#).

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 [Configuring 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 Aruba 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 [Configuring 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 [Configuring 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, see [Supported Devices and Operating Systems](#).

How do I get the onboarding URL for the Aruba 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 Aruba 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 Aruba Onboard app?

Yes, you can delete or add network profiles in the Aruba Onboard app. For more information, see [Managing Network Profiles](#).

Does Cloud Authentication and Policy support wired SSID?

Currently, Cloud Authentication and Policy supports only WLAN SSIDs for creating user access policy and client access policy.

Does the Aruba Onboard app use OpenSource components?

Yes, the Aruba 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 Aruba 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:

