aruba
a Hewlett Packard Enterprise company

AT A GLANCE

CLOUD AUTHENTICATION & POLICY FOR ARUBA CENTRAL

Seamless cloud-based onboarding and secure role-based policy for users and devices

Company dynamics have changed in the past year, welcoming a wave of remote workers. However, unreliable access and poor security can disrupt business continuity plans and cause help desk calls to soar.

Applying consistent security controls and enabling seamless, cloud-based onboarding can help recreate an office-like experience from home. Aruba Central will release cloud authentication capabilities, extending its ability to provide a cloud-based, single pane-of-glass operational experience.

Aruba Central simplifies security controls by enabling cloud authentication & policies through an easy-to-use user interface and dashboard for monitoring and troubleshooting. End users are authenticated and provided authorizations for appropriate network access through fine-grained policies implemented in Aruba Central.

With privacy concerns rising, Aruba secures MAC-based authentications with ClearPass Device Insight through Aruba Central, collecting device information and working with the device profile to gain in depth visibility for better security than MAC addresses alone.

CLOUD IDENTITY

Aruba Cloud Identity allows end users to connect to Wi-Fi networks securely and automatically. The application integrates with the company's existing cloud identity server like Google Workspace or Azure Active Directory to authenticate the user's information and assign them the right level of network access. Frictionless Wi-Fi connectivity for known and new users, visibility into traffic patterns, and implementing fine-grained policies to control access is provided through Passpoint or ClearPass Device Insight.

KEY BENEFITS AND FEATURES

- Time-saving workflows to configure and manage onboarding, authorization, and authentication policies via the cloud
- Integration into common cloud identity stores such as Google Workspace and Azure Active Directory
- Simplified end-user experience using the client app (mobile, desktop, laptop) with support for broad range of devices
- Enhanced security with ClearPass Device Insight to secure MAC-based authentications and leveraging Passpoint technology
- Frictionless, automated onboarding for visitors using cellular subscription with Aruba Air Pass

END-USER DEVICE ONBOARDING

Devices used by staff can easily be configured for seamless connection to wireless networks. Managed through Aruba Central, end users are authenticated through the company's identity store with an enrollment link from the Passpoint Portal. Using company credentials to login, the information will be redirected to the Identity store for authentication.

Devices can also be configured using the client app, supporting macOS, Windows, iOS, and android. With the Enterprise Passpoint Profile installed on the device, anytime the user walks into range of the network, the device will automatically connect with the appropriate network access rules as configured by Admin through Aruba Central. The client app provides automatic renewals, requiring no additional onboarding steps and upkeep from the end user, while allowing Admin to change and update policies at any time.

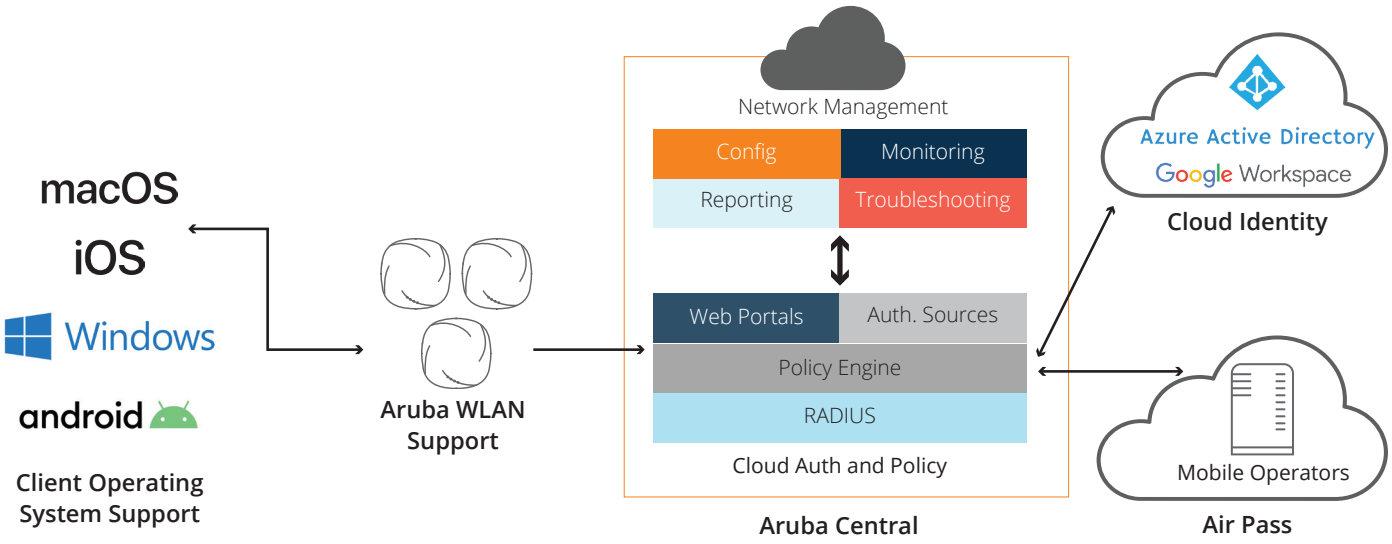

Figure 1: Cloud Authentication and Policy Overview

AUTOMATED ONBOARDING FOR GUESTS AND VISITORS

Aruba Air Pass is the industry's first seamless cellular roaming solution designed to unify enterprise and mobile network experiences. Air Pass is managed in Aruba Central, extending the 5G experience to the enterprise using Aruba Wi-Fi 6 technology. Air Pass uses prenegotiated agreements with MNOs powered by Passpoint, authorized in majority of mobile devices, to enable cellular roaming without hardware upgrades.

Air Pass gives guests and visitors an uninterrupted Wi-Fi experience in indoor venues with the added benefit of enterprise-grade security.

SUMMARY

Cloud authentication & policy for Aruba Central allows a seamless cloud-based onboarding solution. Enterprises will benefit from simplified workflows with secure role-based policies administered through ClearPass Device Insight or Passpoint, for users and devices to gain appropriate network access. End users experience is amplified with Aruba's client app, supporting broad range of devices and automatic renewals.

As organizations continue to adopt to remote workers, it's become evidently important to secure users and devices to ensure appropriate levels of access are provided for business continuity while increasing efficiency in admin approvals and policies.

RESOURCES

For more information, please refer to the following resources, or contact your Aruba sales representative:

- Aruba Central
- ClearPass Device Insight

AAG_CloudAuthentication&Policy_061621 a00115477enw