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 the past few years, welcoming an unprecedented volume of remote workers, as well as those working in hybrid environments. However, unreliable network access and new security concerns can disrupt business and cause help desk calls to soar.

Applying consistent security controls and ensuring users have seamless access to apps and data in the office, at home, and on the go is a critical mandate. Aruba Central simplifies this process for IT with Cloud Auth cloud-based Network Access Control (NAC), extending its ability to deliver a single point of visibility and control over all network infrastructure and related security services.

Featuring an easy-to-use interface and dashboard, Aruba Central makes it easy to onboard new clients, as well as to monitor and troubleshoot issues that prevent users from connecting to the network. End users are authenticated and provided authorizations for appropriate network access through fine-grained policies as configured by the administrator in Aruba Central.

With privacy concerns rising, Aruba Central leverages MAC-based authentications and AI-based Client Insights to capture and profile all devices on the network. Using this information provides IT with continuous, in-depth visibility into the behavior of all connected clients, enabling a stronger security posture than by using MAC addresses alone.

CLOUD IDENTITY

Cloud Auth on Aruba Central enables end users to connect to wired and wireless networks securely and automatically. The cloud-native security service integrates with a company's existing cloud identity store such as Google Workspace or Azure Active Directory to authenticate the user's information and assign them the right level of network access.

KEY BENEFITS AND FEATURES

- Time-saving workflows to configure and manage onboarding, authorization, and authentication policies for wired and wireless networks via the cloud
- Integration into common cloud identity stores such as Google Workspace and Azure Active Directory
- Enhanced ease of user onboarding with the use of Multi Pre-Shared Keys (MPSK), eliminating the need for pre-registration.
- Simplified end-user experience using a client app (mobile, desktop, laptop) with support for a broad range of devices
- Enhanced security with AI-based Client Insights to secure MAC-based authentications and by leveraging Passpoint technology
- Frictionless, automated onboarding for visitors using cellular subscription with Aruba Air Pass

AUTOMATED SECURITY AT SCALE FROM EDGE TO CLOUD

Cloud Auth is an integral part of Aruba Central NetConductor, which streamlines the adoption of identity-based access and simplifies IT operations by delivering advanced, cloud-native configuration, management, and security services, including intent-based policy automation and orchestration, and AI-based discovery and profiling of all connected clients.

To learn more, please refer to the Central NetConductor solution page.

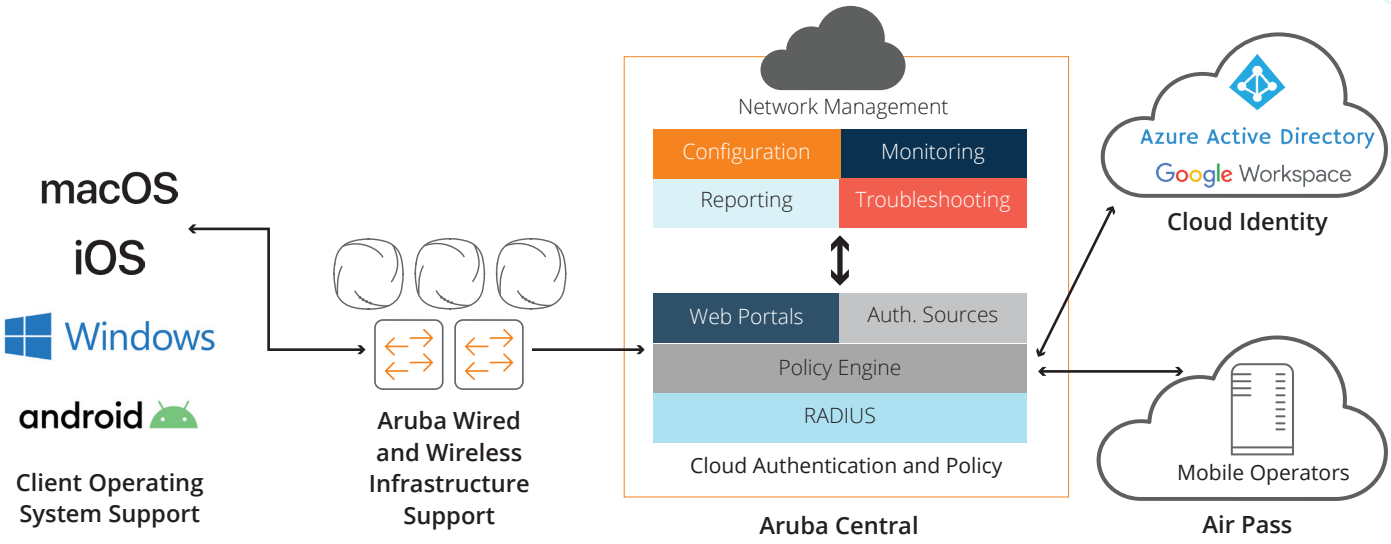

Figure 1: Cloud Auth service in Aruba Central provides a flexible, powerful framework for granting network access

END-USER DEVICE ONBOARDING

Employee devices can easily be configured for seamless connection to wired and wireless networks. Managed through Aruba Central, end users are authenticated through the company's cloud identity store with an enrollment link provided on Aruba Central. Using company credentials to log in, the user will be redirected to the identity store for authentication. Onboarding can be further simplified by leveraging Multi Pre-Shared Keys (MPSK). These are unique per-user passphrases that do not require device registration and can be used for more than one of the user's devices.

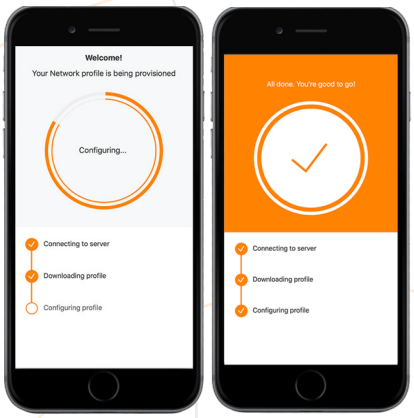

Figure 2: The Aruba Onboard client app provides a seamless way for end users to connect to corporate networks.

Client devices can be configured using Aruba Onboard, a client app that is supported on macOS, Windows, iOS, and Android operating systems. 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 the admin through Aruba Central. The client app provides automatic renewals, requiring no additional onboarding steps and upkeep from the end user, while allowing the admin to change and update policies at any time.

DYNAMIC MONITORING OF CLIENT ACCESS POLICY

Fine-grained access policies can be defined in Aruba Central based on the type of the client device. System-defined tags or custom tags are used to identify or logically group clients with similar characteristics. Cloud authentication enables stronger security posture by dynamically monitoring client tags and initiating a disconnect when a tag change is detected, ensuring that the client receives access policies that correspond to the new tag.

MONITORING AND TROUBLESHOOTING NETWORK CONNECTIVITY

The cloud authentication dashboard in Aruba Central provides granular visibility into authentication requests from users, as well as session details for clients that are connected to access points managed by Aruba Central.

From the authentication tab, the IT admin can see details on the number of successful and failed access requests within a select time range, and includes breakdowns of user versus client requests, client roles, and failure reasons (by SSID, policy, and reject reasons). The sessions tab displays metrics such as the number of active sessions, MAC addresses (randomized and non-randomized), duration of each session, and data usage during each session within a selected duration.

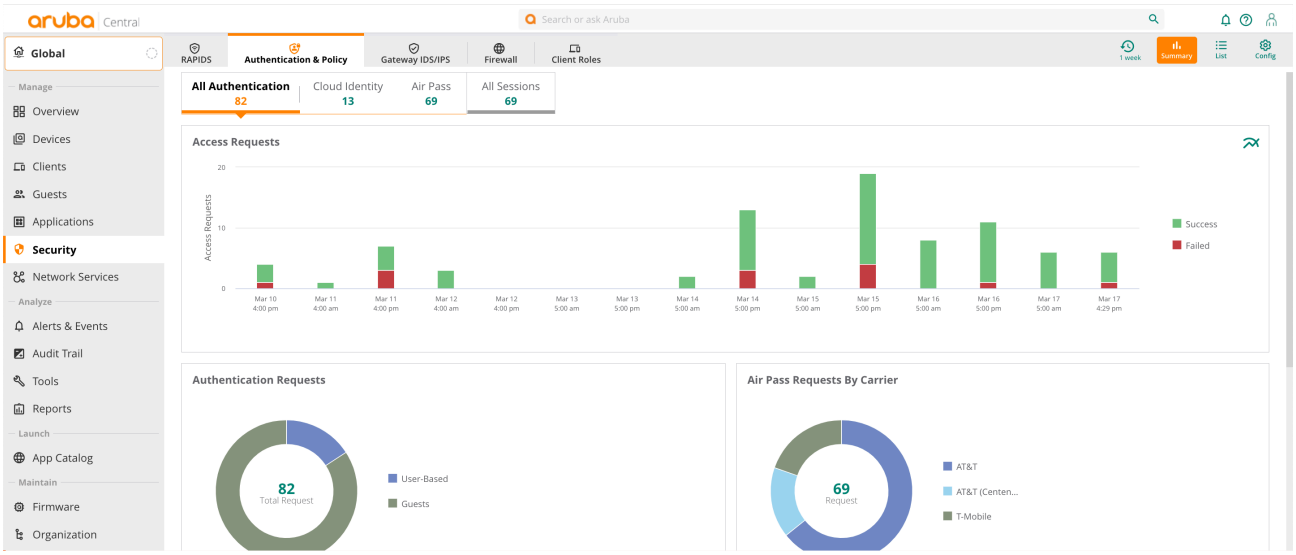

Figure 3: Visibility into all authentication requests and connected clients helps IT easily troubleshoot potential issues

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 technology. Air Pass uses pre-negotiated agreements with mobile network operators (MNOs) powered by Passpoint.

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

STREAMLINED ONBOARDING OF UXI SENSORS

Streamlined workflow for onboarding UXI sensors without manual intervention using secure and standardized Wi-Fi Easy Connect™, also known as Device Provisioning Protocol (DPP). Once a UXI sensor is registered, it can connect and onboard automatically based on configuration enabled by the administrator

***Air Pass is currently available in the U.S. only.**

SUMMARY

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

Cloud Auth on Aruba Central provides a seamless, cloud-based onboarding and NAC solution. Small and medium sized organizations with limited IT personnel will benefit from simplified workflows and secure role-based policies administered through Aruba Central to ensure users and devices have appropriate network access. End users experience is amplified with the Aruba Onboard client app, which supports a broad range of devices and enables seamless connectivity to the network using profiles that are automatically renewed on the user's behalf.

RESOURCES

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

Aruba Central

AI-powered Client Insights on Aruba Central

Central NetConductor

a Hewlett Packard Enterprise company

AAG_CloudAuthentication&Policy_RVK_092022 a00115477enw

Contact us at www.arubanetworks.com/contact