

atmosphere'22 BELGIUM

Cloud Authentication and Policy

Herman Robers – Aruba Systems Engineer EMEA

September 2022

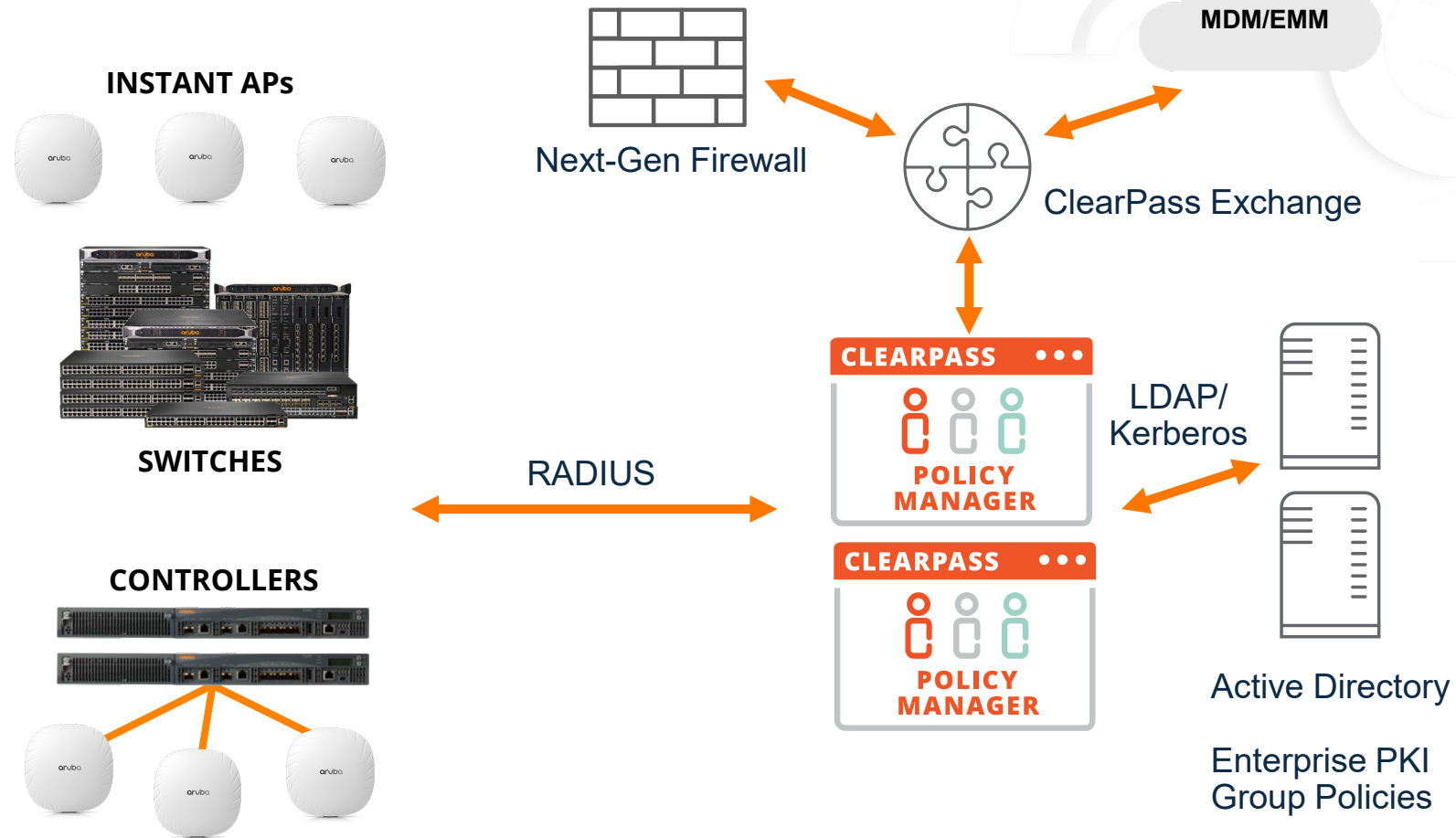
Agenda

- ❖ Authentication and the Cloud
- ❖ Cloud Identities – Overview & Authentication Workflow
- ❖ Cloud Authentication and Policy
- ❖ Demo – “Unbound” MPSK
- ❖ Summary

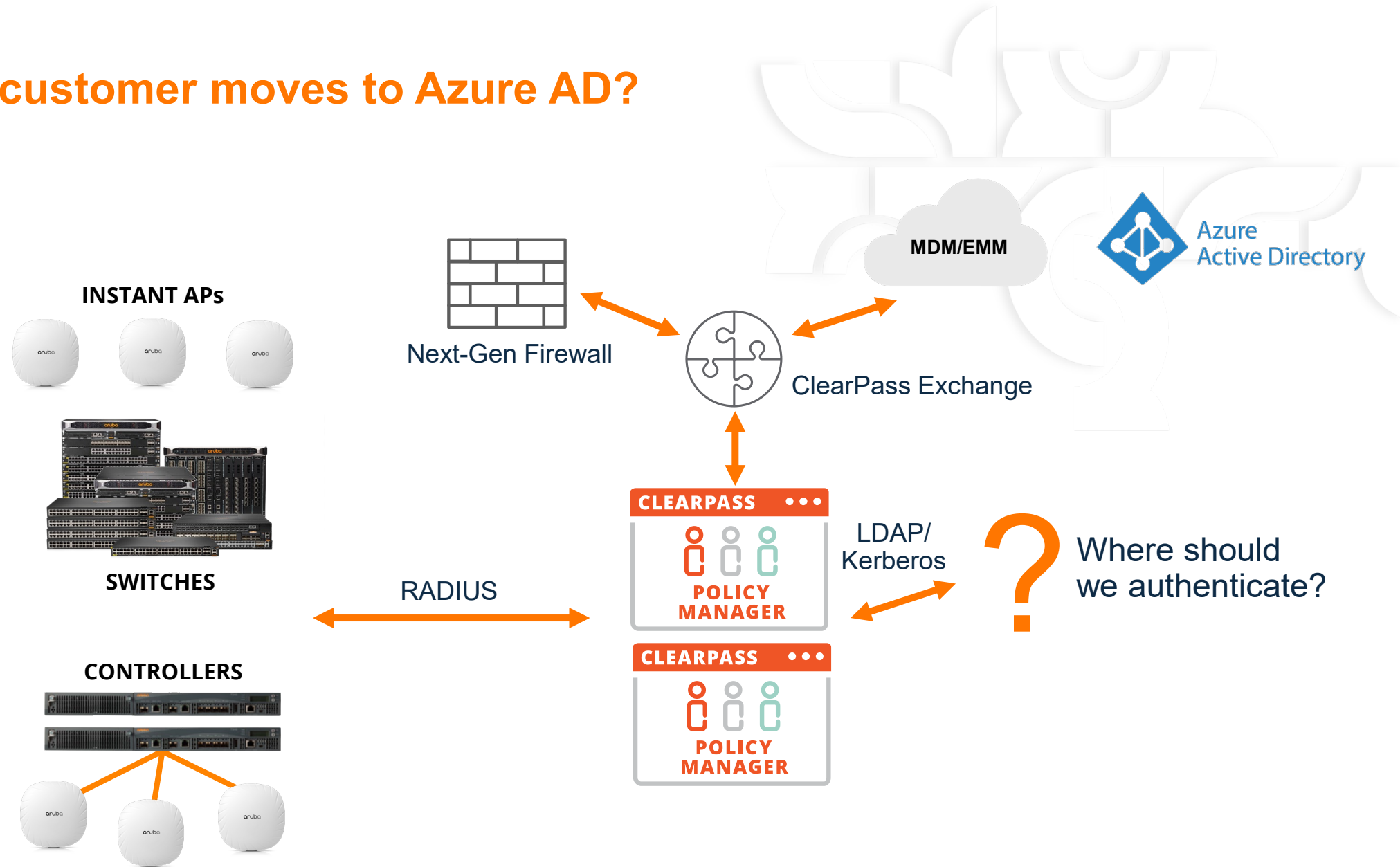
Authentication and the Cloud

When organizations go to the cloud

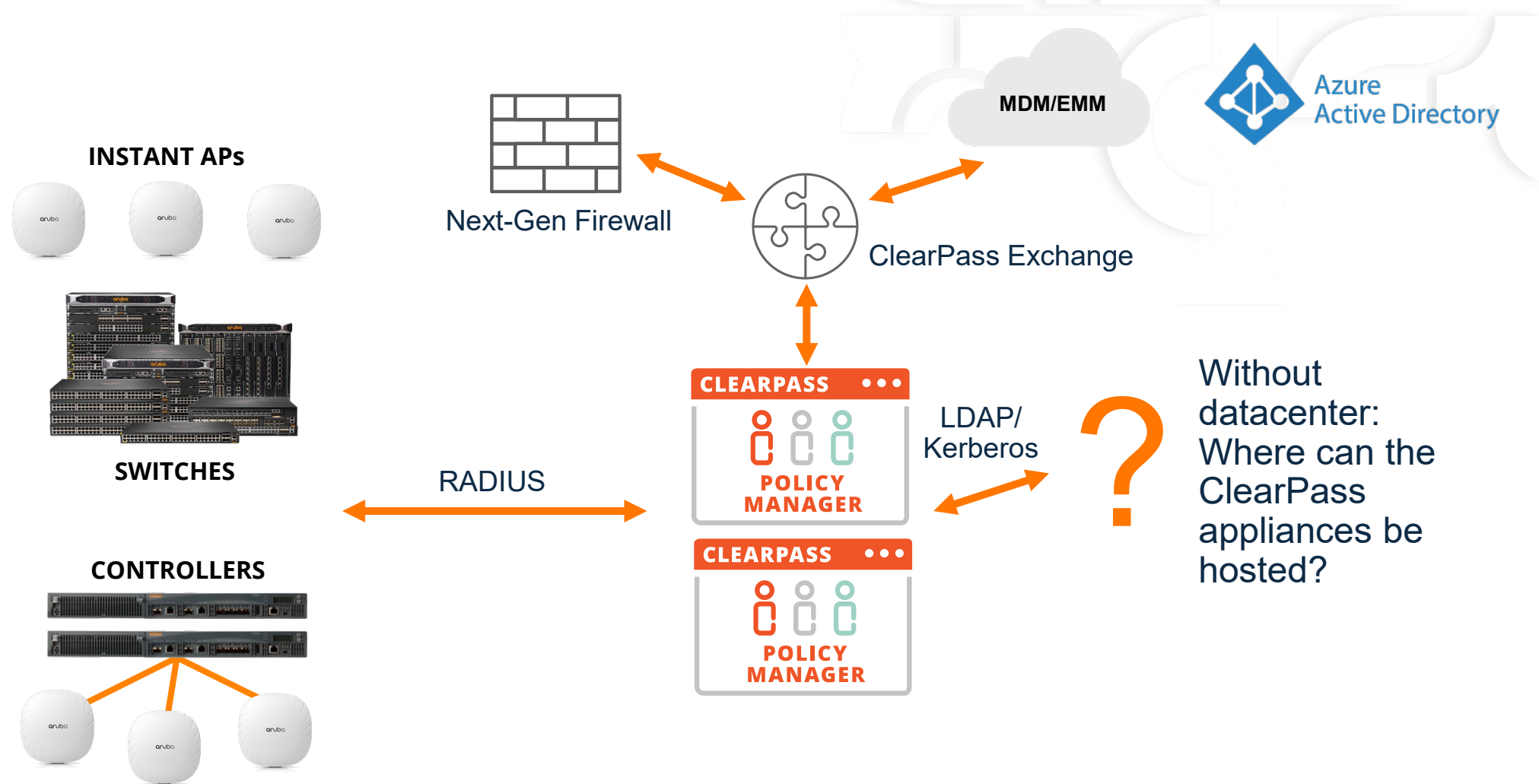
Traditional deployment (On-Premise)



What when customer moves to Azure AD?



What when customer removes datacenter and goes cloud hosted?



Authentication options in the cloud and on-premises

Identity Stores



In-the Cloud

Authentication Services



Cloud Guest



Cloud Auth

Runs on:



Aruba Central



Runs on:



SaaS

IaaS



On-premises

Virtualized



Hardware



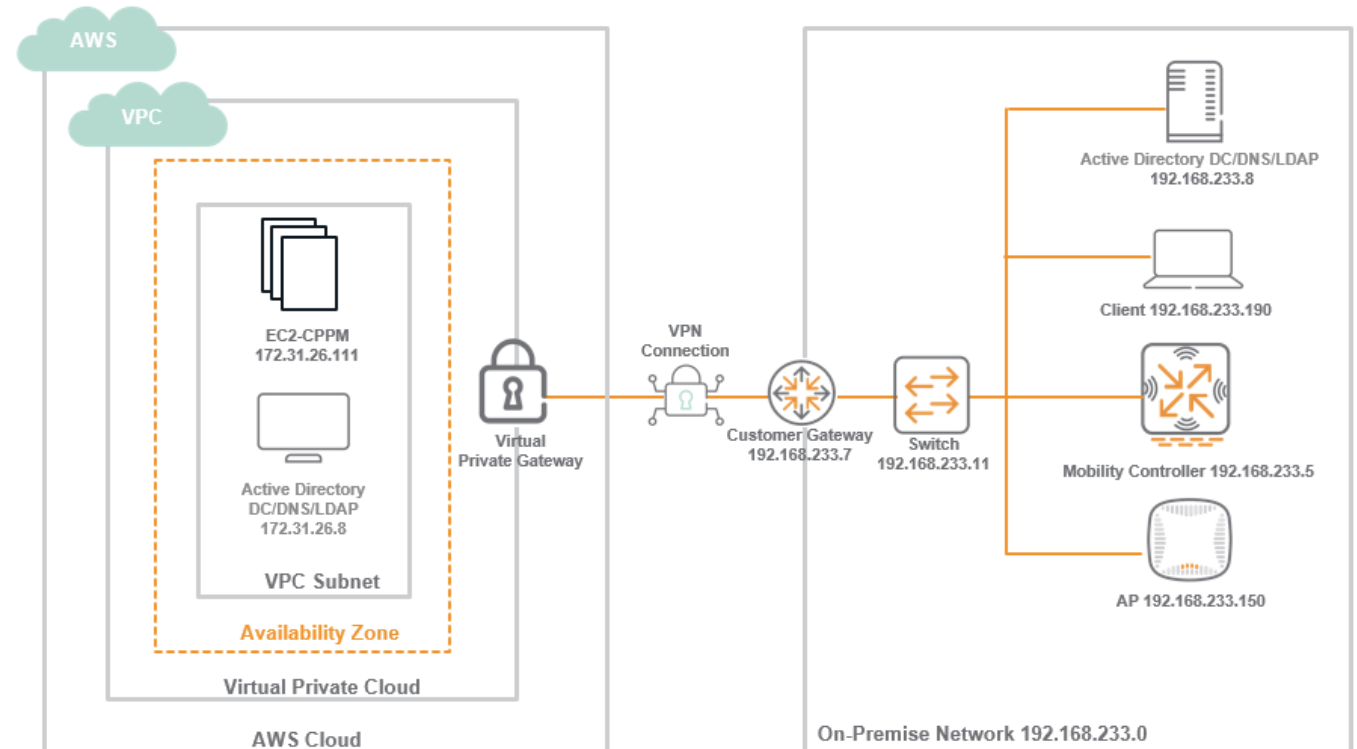
ClearPass in the Cloud

Options for ClearPass to run in and with the cloud

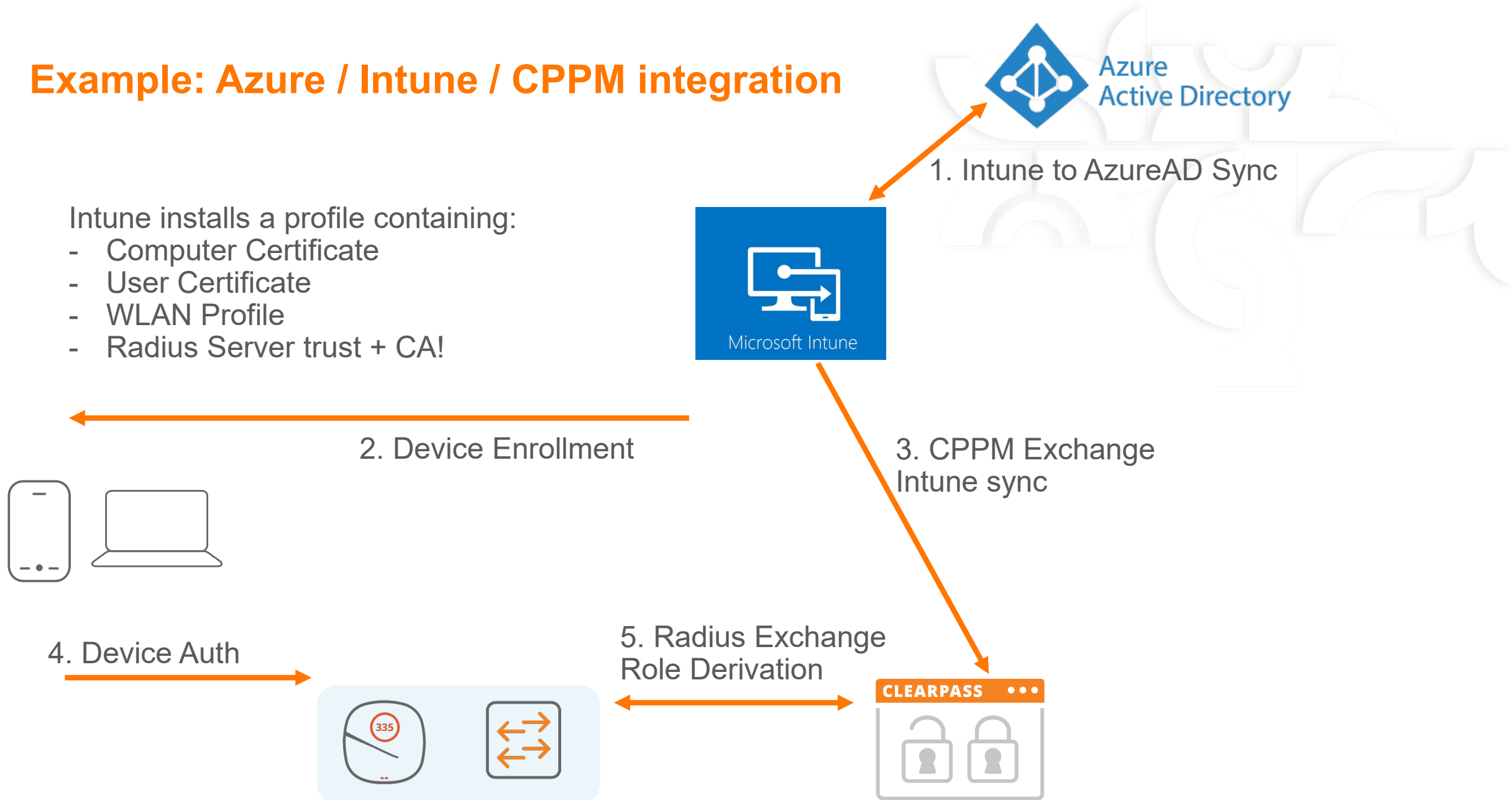
Running ClearPass in the cloud: AWS / Azure



- Runs in a Virtual Private Cloud (VPC)
- Same ClearPass as on-premise, it just runs in the cloud instead of in your datacenter
- Connectivity required between Branch and VPC. Normally part of cloud strategy already.
- Perfect match with Aruba EdgeConnect SD-Branch / Cloud Orchestrator.
- Freedom to cluster ClearPass between cloud and on-prem (publisher/subscriber)



Example: Azure / Intune / CPPM integration

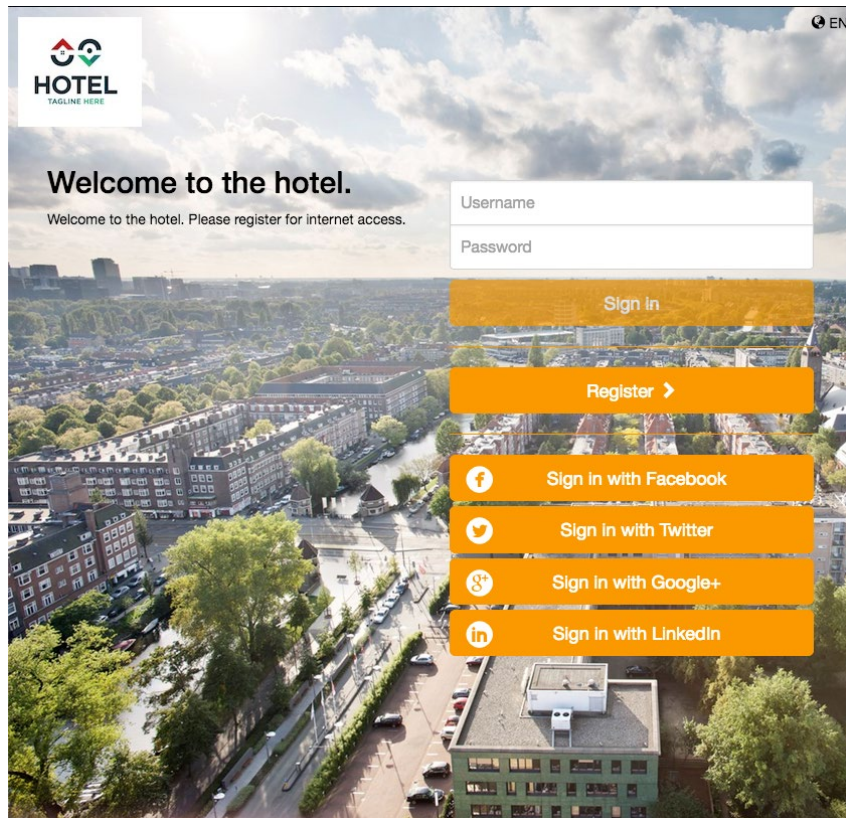


Cloud Guest Cloud Auth

Authentication options in Aruba
Central

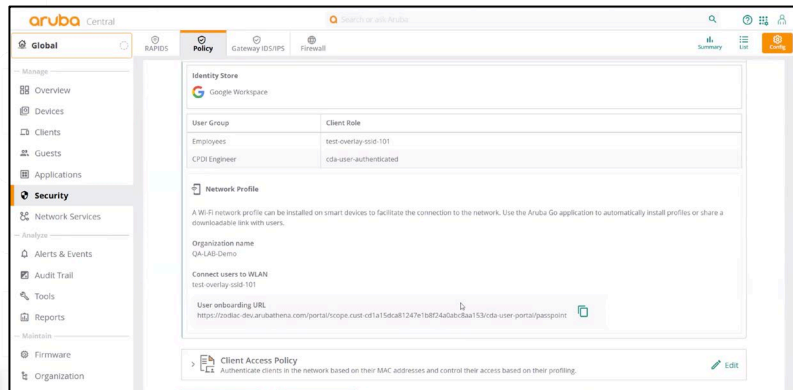
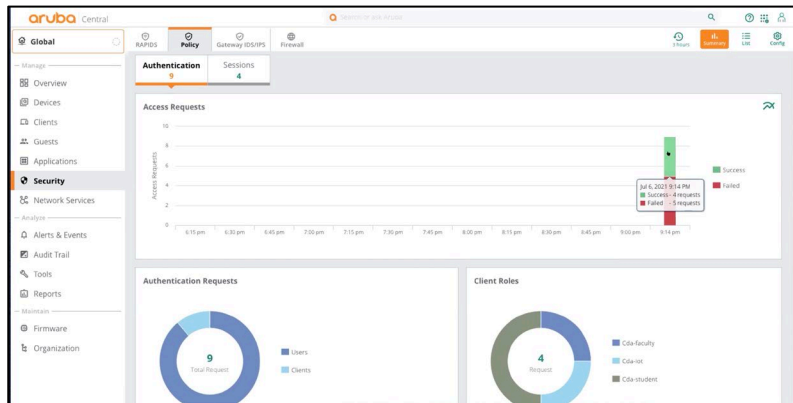
Central Cloud Guest

- Runs from Central
- Simple to deploy, no additional hardware
- Covered in the Foundation License
- WiFi4EU support (on EU clusters)



Cloud Authentication & Policy

—Seamless onboarding and secure role-based policy



Key Capabilities

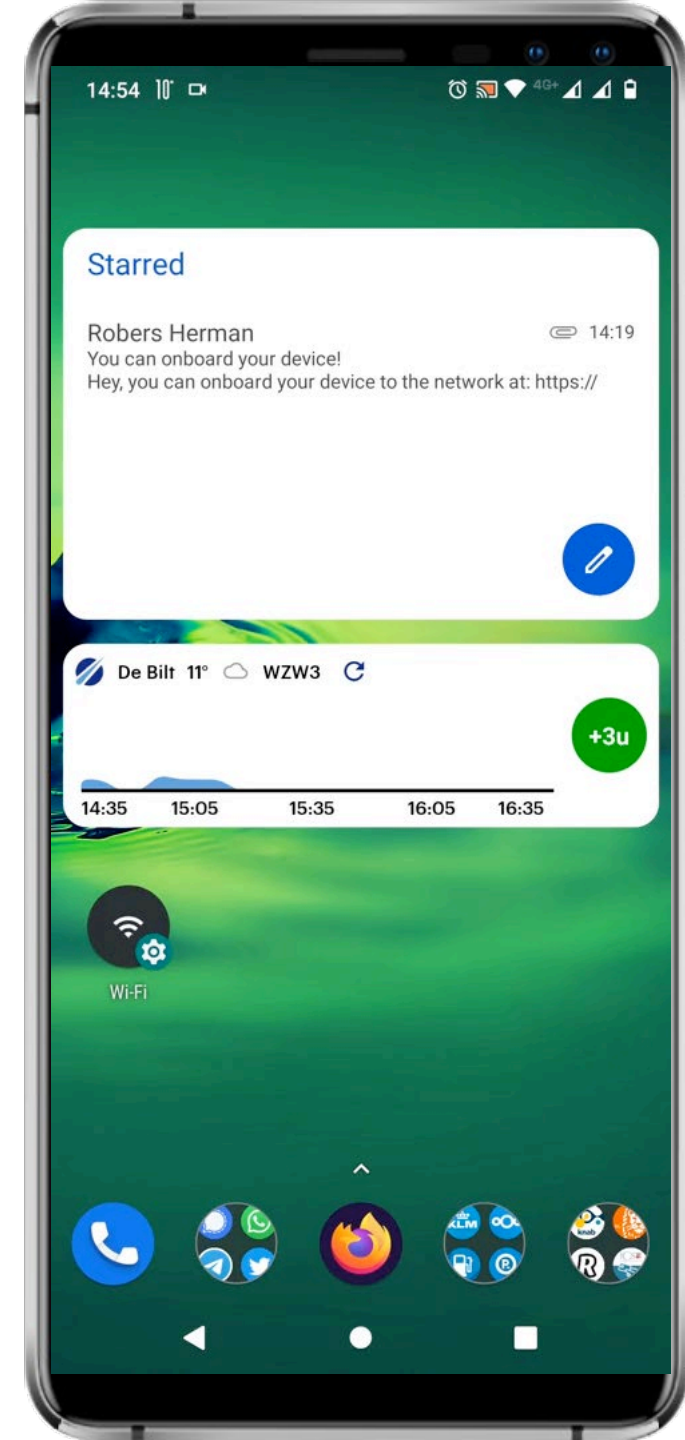
Simplified and efficient workflows to configure and manage onboarding

Visibility into authentication traffic patterns through dashboards

Authentication validated against cloud identity store granting access to Wi-Fi

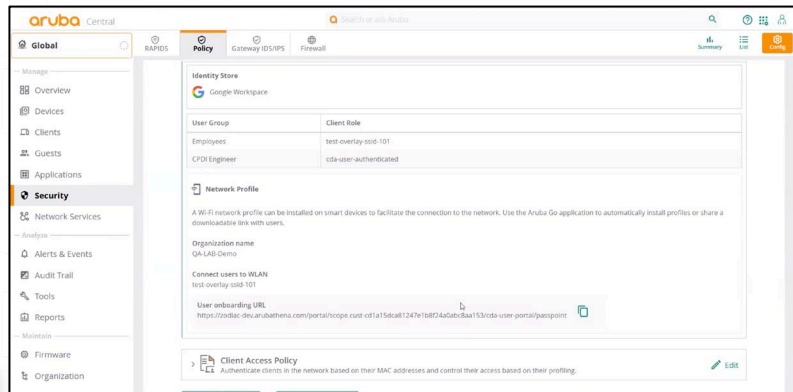
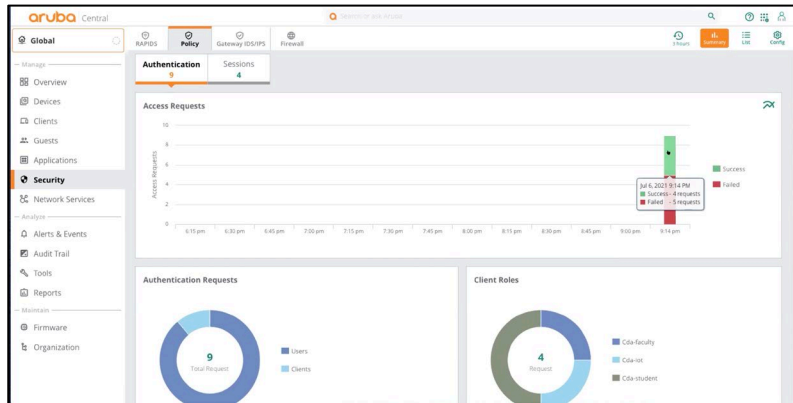
Authorization of users and their devices enforced using role-based policies

Simplified end-user experience with client app



Cloud Authentication & Policy

—Seamless onboarding and secure role-based policy



Key Capabilities

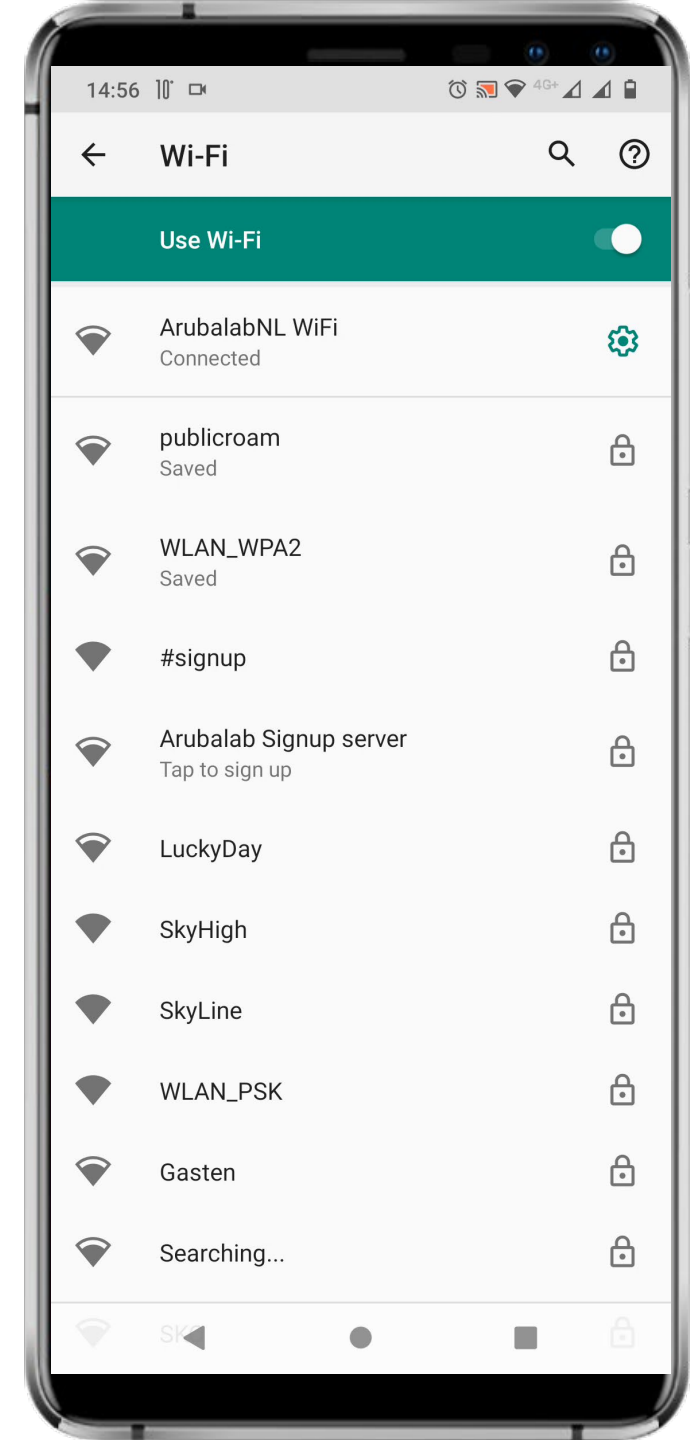
Simplified and efficient workflows to configure and manage onboarding

Visibility into authentication traffic patterns through dashboards

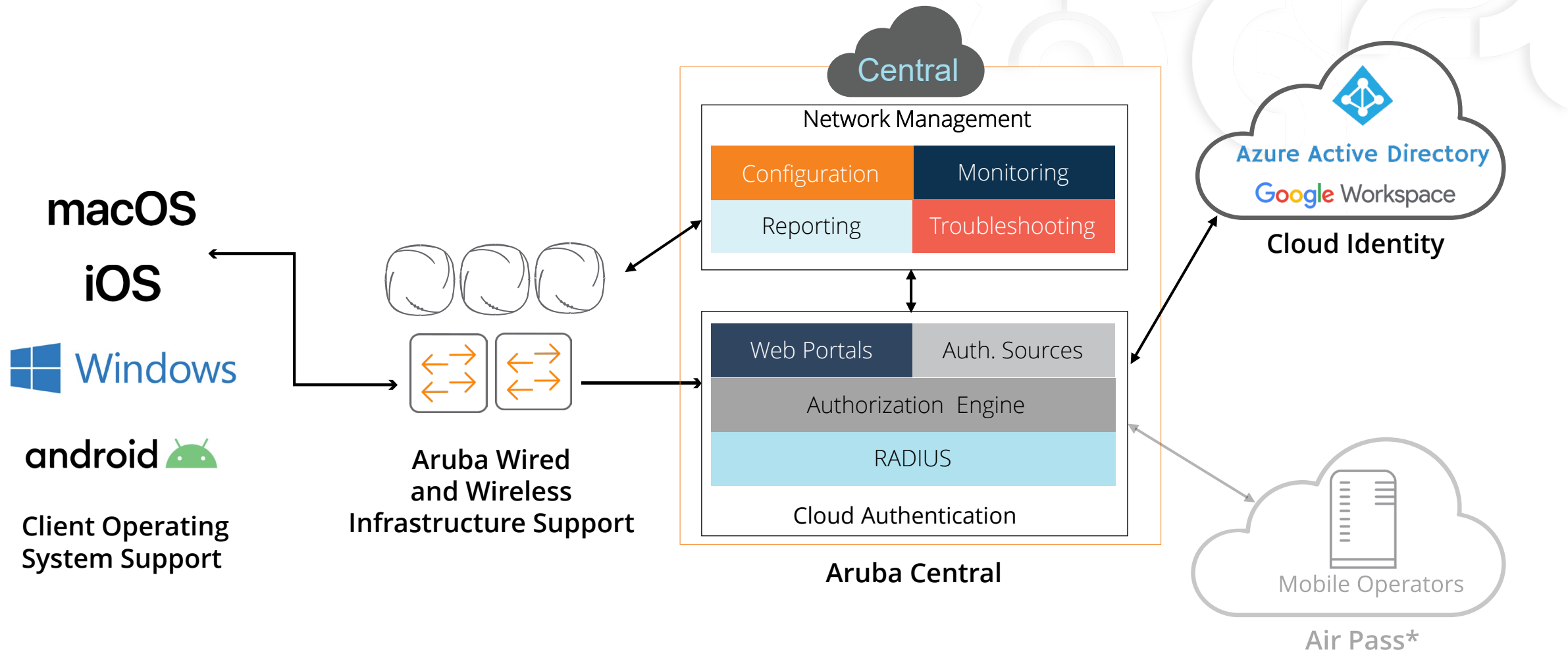
Authentication validated against cloud identity store granting access to Wi-Fi

Authorization of users and their devices enforced using role-based policies

Simplified end-user experience with client app



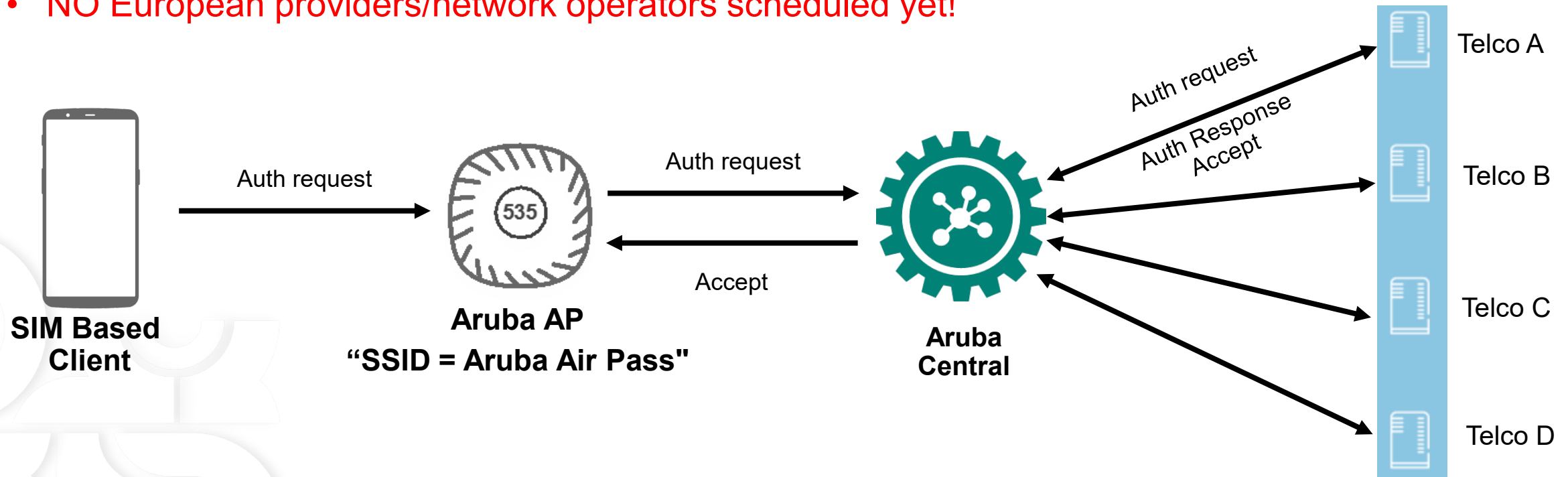
Cloud Authentication & Policy Overview



US Only: Air Pass - SIM: Authentication Overview

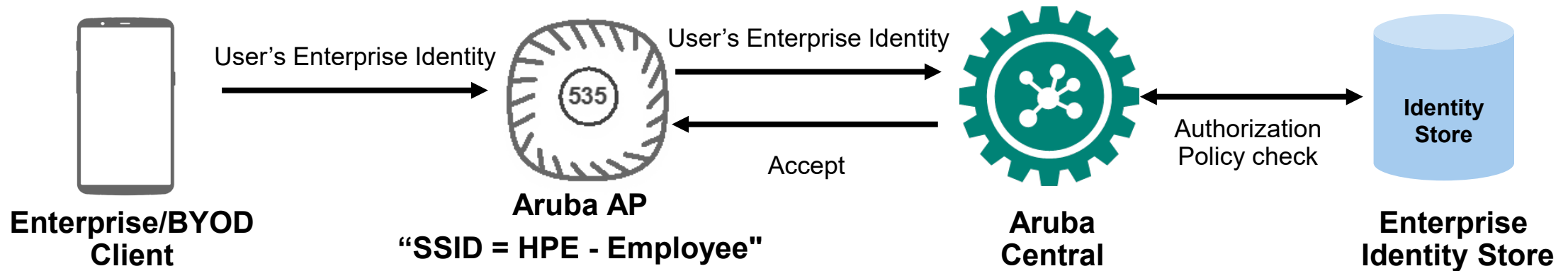
- MNOs provision a Passpoint profile on subscriber's devices
- Leverage subscriber's SIM identity to authenticate & provide Wi-Fi access
- Easy way for Guest Access as no client device configuration is needed
- **NO European providers/network operators scheduled yet!**

Currently only
in the US with
US providers



Cloud Identity – Authentication Overview

- User's device is configured for seamless connection to Enterprise wireless networks
- Device automatically associates to the network
- Uses Passpoint technology and secure TLS authentication



Cloud Authentication (Users)

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

The screenshot shows the Aruba Central web interface. The top navigation bar includes the Aruba logo, a search bar, and icons for notifications, help, and user profile. The main navigation menu on the left lists various sections: Global, Manage (Overview, Devices, Clients, Guests, Applications), Security (highlighted), Network Services, and Analyze (Alerts & Events, Audit Trail, Tools, Reports). The 'Authentication & Policy' section is active, displaying 'User Authentication' information. It states that an organization identity store is used to authenticate clients and control their access to the network. A status bar indicates 'Where is the user information stored?' with a Microsoft Azure AD connection icon. Below this, a table titled 'User Groups to Client Role Mapping (4)' shows the mapping of user groups to client roles.

User Group	Client Role
Contractors	contractor
IT Admins	byod
IoT Devices	iot-internet
Unspecified	unmatched-user

Key Capabilities

Simplified and efficient workflows to configure and manage onboarding

Authentication validated against cloud identity store granting access to Wi-Fi

Simplified end-user experience with client app



Cloud Authentication (Devices)

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

The screenshot displays the Aruba Central web interface. The top navigation bar includes the Aruba Central logo, a search bar, and icons for notifications, help, and user profile. The main navigation menu on the left lists various sections: Global, Manage (Overview, Devices, Clients, Guests, Applications), Security (highlighted), Network Services, Analyze (Alerts & Events, Audit Trail, Tools, Reports), Launch (App Catalog), and Maintain (Firmware). The main content area is titled 'Authentication & Policy' and contains two sections:

MAC Authentication
Manage and authenticate clients in the network based on their MAC addresses.

Allowed MAC Addresses (341)
MAC address of client devices allowed to access the network.

MAC Address	Client Name
FC:1D:43:2F:1D:71	iPad-van-Henny
F6:28:3F:D6:3C:8E	gw
F6:0B:52:22:B9:AB	gw
F4:CF:A2:F5:2B:52	openthermgw
F4:60:E2:D6:38:02	POCOPHONEF1-POCOPHON

Items per page: 5 | 1 - 5 of 341

Client Profile Tag to Client Role Mapping (3)
Associate the client profile tags to a client role and order them by highest priority first.

Client Profile Tag	Client Role
[IOT]	iot-local
[Computers & Servers]	byod
Unspecified	unmatched-device

Key Capabilities

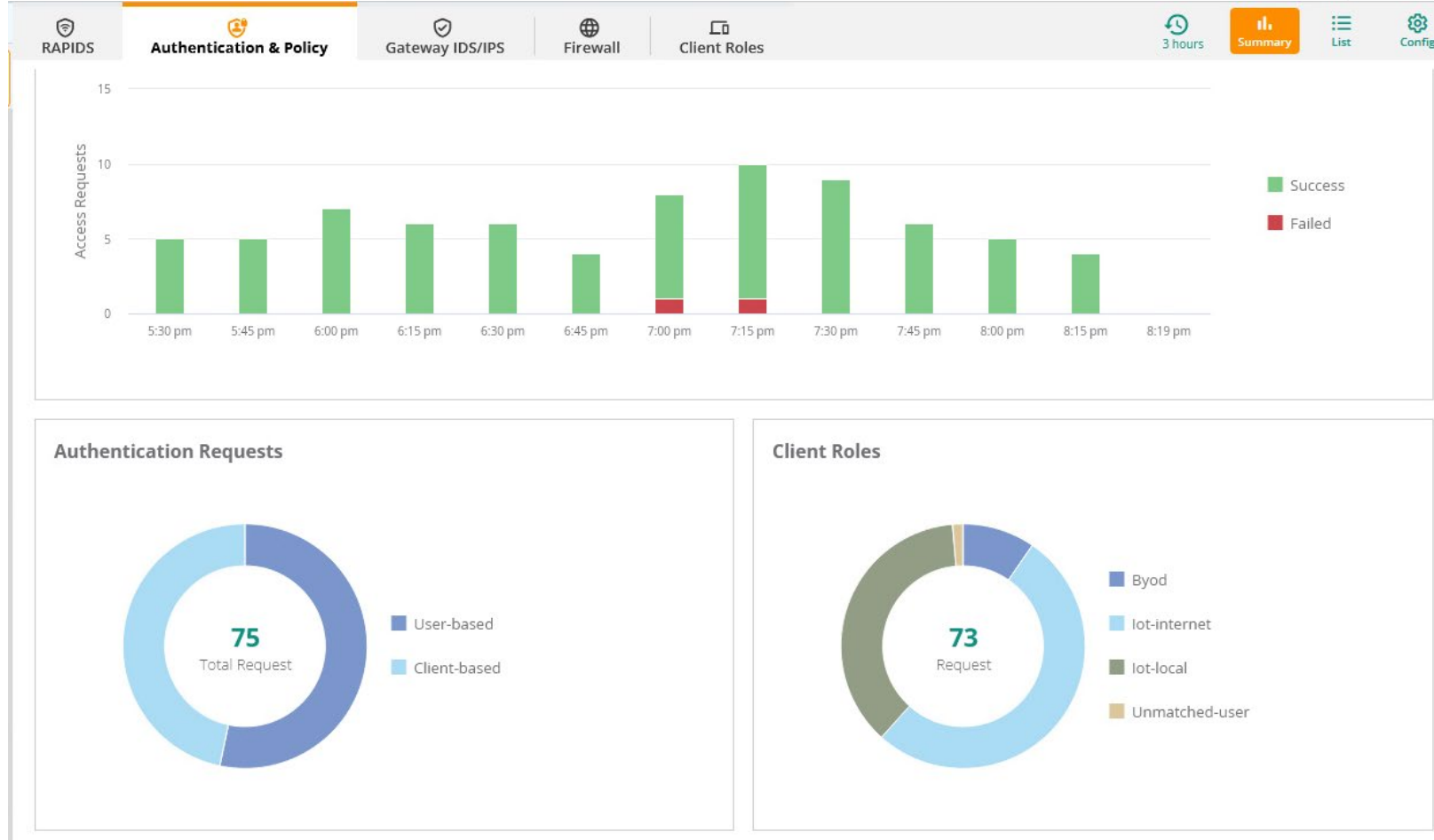
MAC Authentication

Assign network roles based on device-type

Based on Client Insight Device Classification

Cloud Authentication

– Visibility through Aruba Central



Key Capabilities

Visibility into authentication traffic patterns through dashboards

Authorization of users and their devices enforced using role-based policies



Cloud Authentication & Policy – Supported Features since Central 2.5.4

Feature	Supported?
802.1X/MAC Authentication	Yes
Guest Authentication Support (Cloud Guest)	Yes
Cloud Identity & Social Login Auth Sources	Yes
Device Provisioning for iOS, macOS, Windows, and Android operating systems	Yes
Basic Policy Support	Yes

Cloud Authentication & Policy – New features with Central 2.5.6*

Feature	Supported?
Unbound MPSK support	Yes
Wired support (Integration with AOS CX switches)	Yes
Auth revocation of specific devices belonging to an end-user	Yes
MSP Mode	Yes

“Unbound” MPSK - Demo

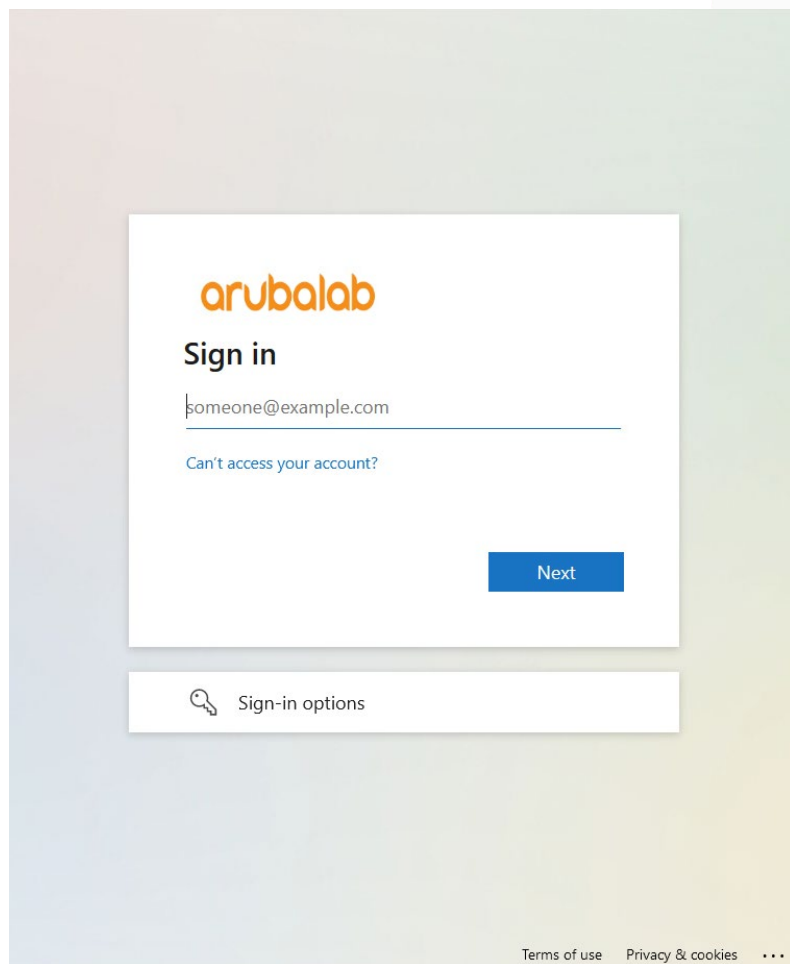
Will be new in Central 2.5.6

Unbound MPSK

What it is and Limitation

- Unbound MPSK
 - End users can create personal PSK
 - Just type the key on any of your devices to get access
 - Not tied to MAC pre-registration (ala ClearPass)
- Requires AOS 10.4
 - Changes are required to make this work in the AP code, not just in Cloud Auth
- Initially 1,500 unique keys per tenant
 - We expect to be able to go higher in future versions but do not know limits yet
- Does not support WPA3, only works with WPA2-PSK

Unbound MPSK User Experience




arubalab

Sign in

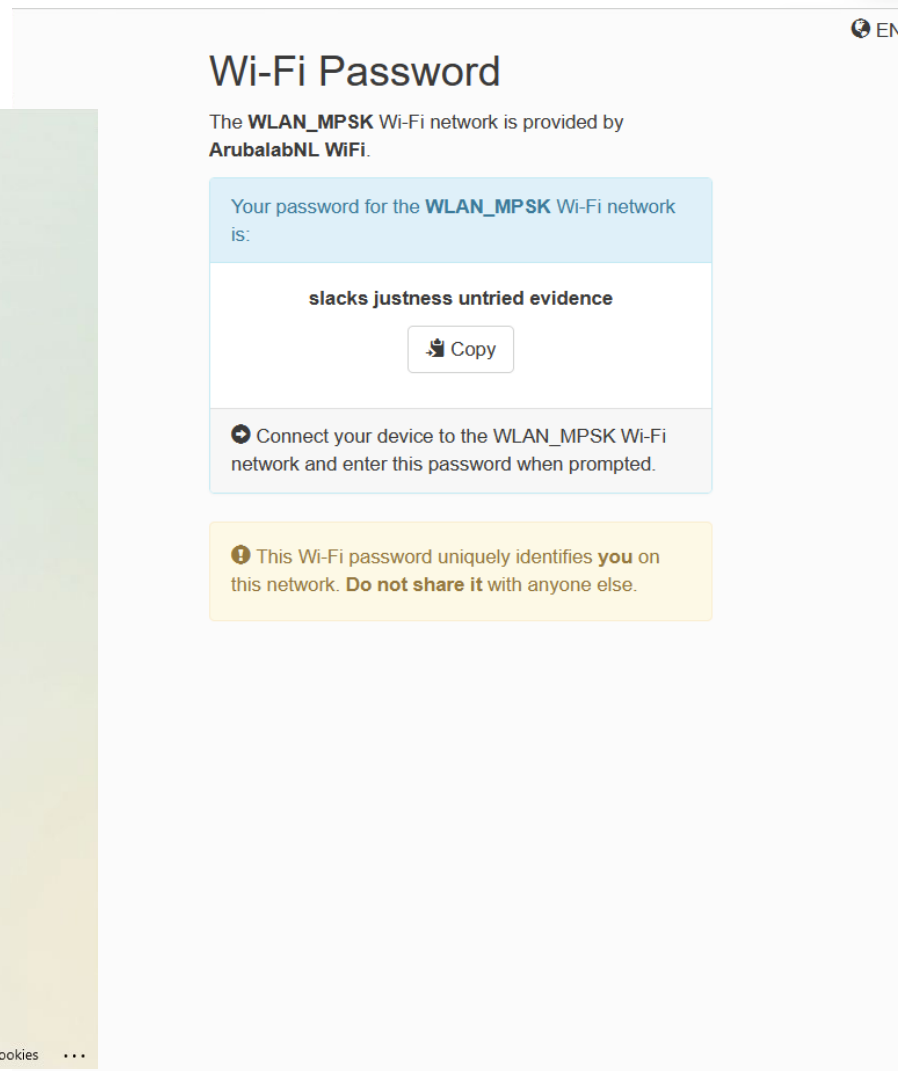
someone@example.com

[Can't access your account?](#)

Next

 Sign-in options

[Terms of use](#) [Privacy & cookies](#) ...




Wi-Fi Password

The **WLAN_MPSK** Wi-Fi network is provided by **ArubalabNL WiFi**.

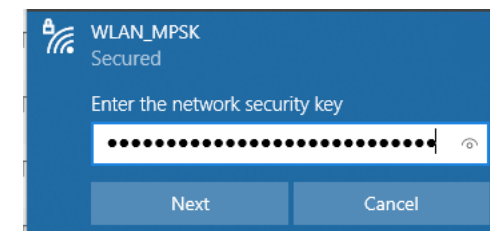
Your password for the **WLAN_MPSK** Wi-Fi network is:

slacks justness untried evidence

 Copy

➔ Connect your device to the **WLAN_MPSK** Wi-Fi network and enter this password when prompted.

⚠ This Wi-Fi password uniquely identifies **you** on this network. **Do not share it** with anyone else.



WLAN_MPSK
Secured

Enter the network security key

.....

Next Cancel

Aruba Central

← → ↺

https://internal-ui.central.arubanetworks.com/frontend/#/POLICIES/CONFIGURATION?nc=global

120%

☆

☰

Cloud Auth Onboard Cloud Auth MPSPK

HPE GreenLake

☰

aruba Central

Search or ask Aruba

🔍

🔔

?

👤

Customer: Herman Rob...

🛡️ RAPIDS

👤 Authentication & Policy

🛡️ Gateway IDS/IPS

🌐 Firewall

📄 Client Roles

📊 Summary

☰ List

⚙️ Config

🏠 Global

⌛

Manage

☰ Overview

🖼️ Devices

📁 Clients

👥 Guests

🔧 Applications

🛡️ Security

🔗 Network Services

Analyze

🔔 Alerts & Events

📄 Audit Trail

🔧 Tools

📊 Reports

Launch

Policies

> 📄 User Access Policy

Use an organization identity store to authenticate clients and control their access to the network.

✎ Edit

🗑️ Delete

📄 Client Access Policy

Authenticate clients in the network based on their MAC addresses and control their access based on their profiling.

⚙️ Setup

© Copyright 2022 Hewlett Packard Enterprise Development LP

Privacy

Terms of Use

Ad Choices & Cookies

Do Not Sell My Personal Information

Summary

When to use Cloud Auth, Cloud Guest, ClearPass

When to use what?

Cloud Auth, Cloud Guest, Central

- Basic authentication policies
- When all infrastructure devices are Aruba branded and managed by Central
- Azure Active Directory or Google Workspace as Identity store
- BYOD Scenario for users
- No authentication services on-premise required
- Unbound MPSK
- No additional cost: included in Foundation Central subscriptions

ClearPass

- Supports complex Enterprise Scenario
- On premises footprint for high availability
- Highly customizable
- Multi-vendor infrastructure
- Infrastructure (WLAN, Switching, etc) not managed by Central
- Can integrate with Azure AD, Google Workspace and more
- MDM / Intune Integration
- ClearPass Exchange integrations



atmosphere'22

BELGIUM

Thank you

herman.robbers@hpe.com
#hrwlan

September 2022

airheads COMMUNITY

Still not part of the Airheads Community?

Sign up today:
www.community.arubanetworks.com

