

Meraki Cloud-Delivered Network Access Control (NAC) for Modern Networks

cisco Live !

11 Nov 2025 *** | 1545h | Room 204 ***

Fred Chua
Solutions Engineer, Cisco

Session ID: BRKMER-1431

Cisco Webex App

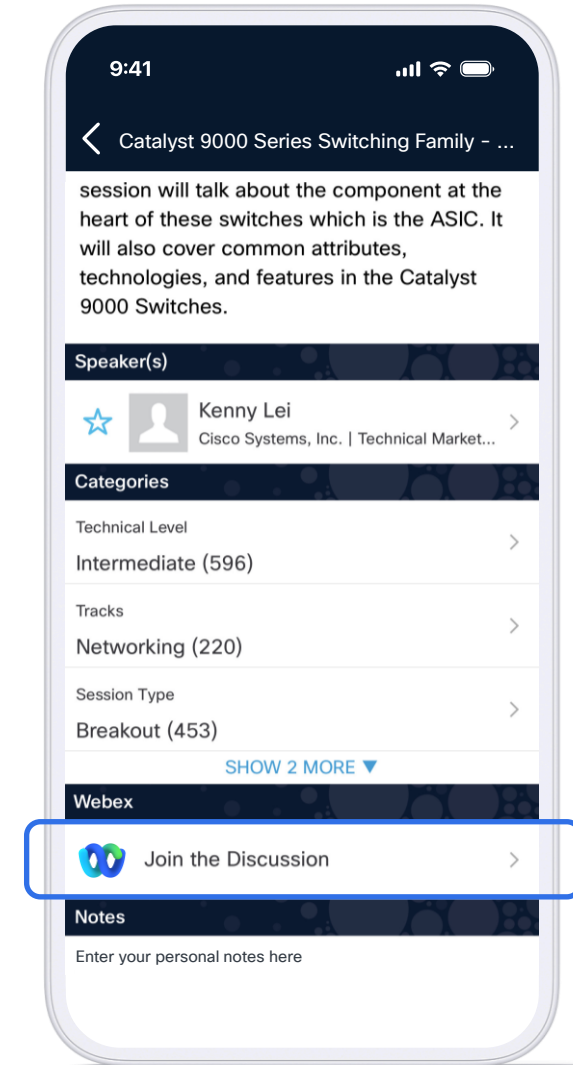
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until 14 November 2025.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKMER-1431>

Agenda

- 01 About Me
- 02 A Throwback: Network Security 101
- 03 Elements of Network Access Control
- 04 Our NAC Solution: from the Cloud
- 05 Beyond Authentication: Segmentation
- 06 Demo / Q&A

About Me

Self-proclaimed Geek, Tech Enthusiast, and Foodie

Family

- wife and two children

Passions

- Food, Travel, Technology

About Me

- I'm not shy, I am an introvert
- Not a fan of huge crowds, but have done a lot of public speaking
- I am willing to try anything out at least once

"I have no special talent. I am only passionately curious."

– Albert Einstein



Back to Basics: Network Security 101

Do you even NAC?



Words to make Bob (from IT) want to pull his hair out:

- I shared the Wi-Fi Password with my guest
- Can I plug my personal laptop here?
- I need to access the Top-Secret company app using my mobile device

Let's Set a Few Things Straight

802.1x??

EAP??

AAA?

RADIUS?

Certificates?

802.1x in a Single Image

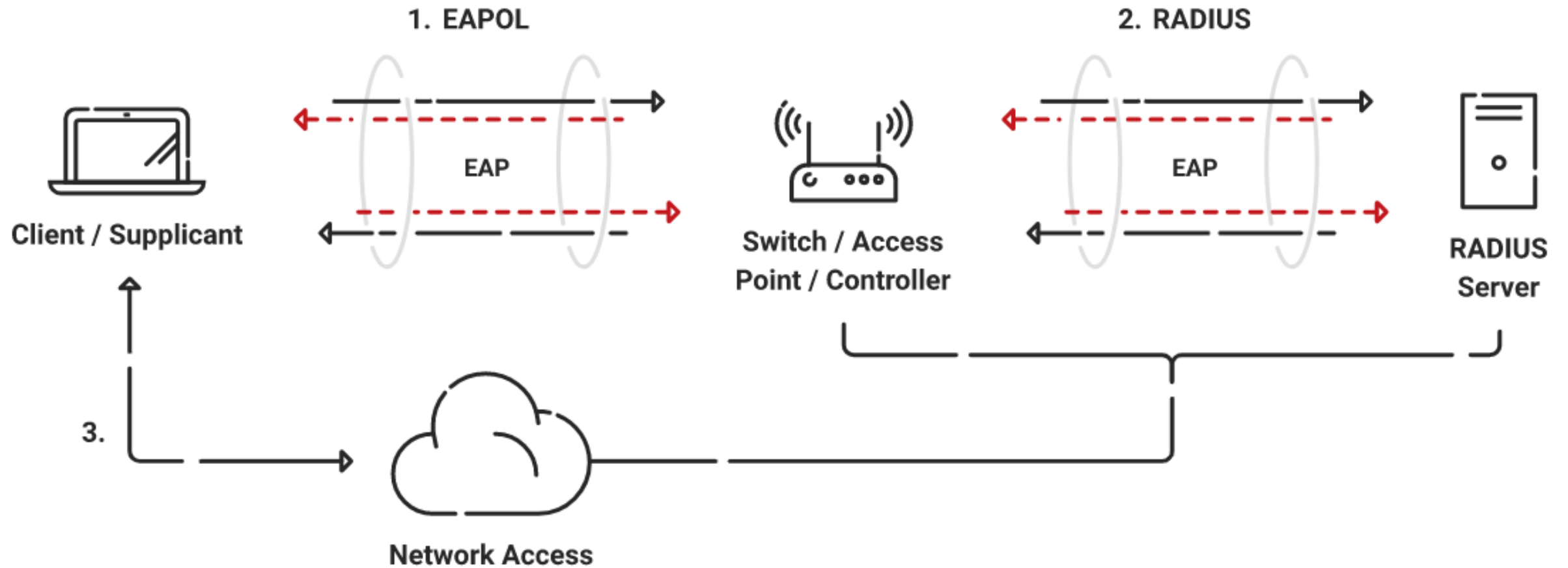


Image Source: <https://www.cloudradius.com/the-stages-of-802-1x-authentication/>

802.1x: The Bouncer of the Network



You shall not pass!

- The security checkpoint: Stops you at the gate to ask for credentials
- Defines the “how” in identifying yourself
- IEEE Standard for Port-based NAC
- Can use what you: know / have / are

EAP: The 'Secret' Handshake

- Think: 'Secret Handshake' to get in the club
- The 'how' in proving your identity
- An authentication *framework* that allows use of **different** authentication methods: EAP-MD5, PEAP, EAP-TLS, EAP-TTLS, TEAP...
- A specification (RFC 3748) for the **transport of authentication and authorization** mechanisms

Why EAP?

- ‘**Extensible**’ means it can be customized
- Versatile: used on wired, wireless, or VPN connections
- Provides strong, **mutual** authentication:
 - Supplicant $\leftrightarrow$ Authentication Server

RADIUS: The Security Front Desk



- Think: front desk security personnel, or RFID badge reader
- Provides **Authentication**, **Authorization**, and **Accounting** (**AAA**) services; acts like a ‘security broker’
- Client/Server Model for passing Authentication information
- Checks validity of your Identity

Certificate-Based Authentication

The Good, The Bad, and The Ugly

The Pros

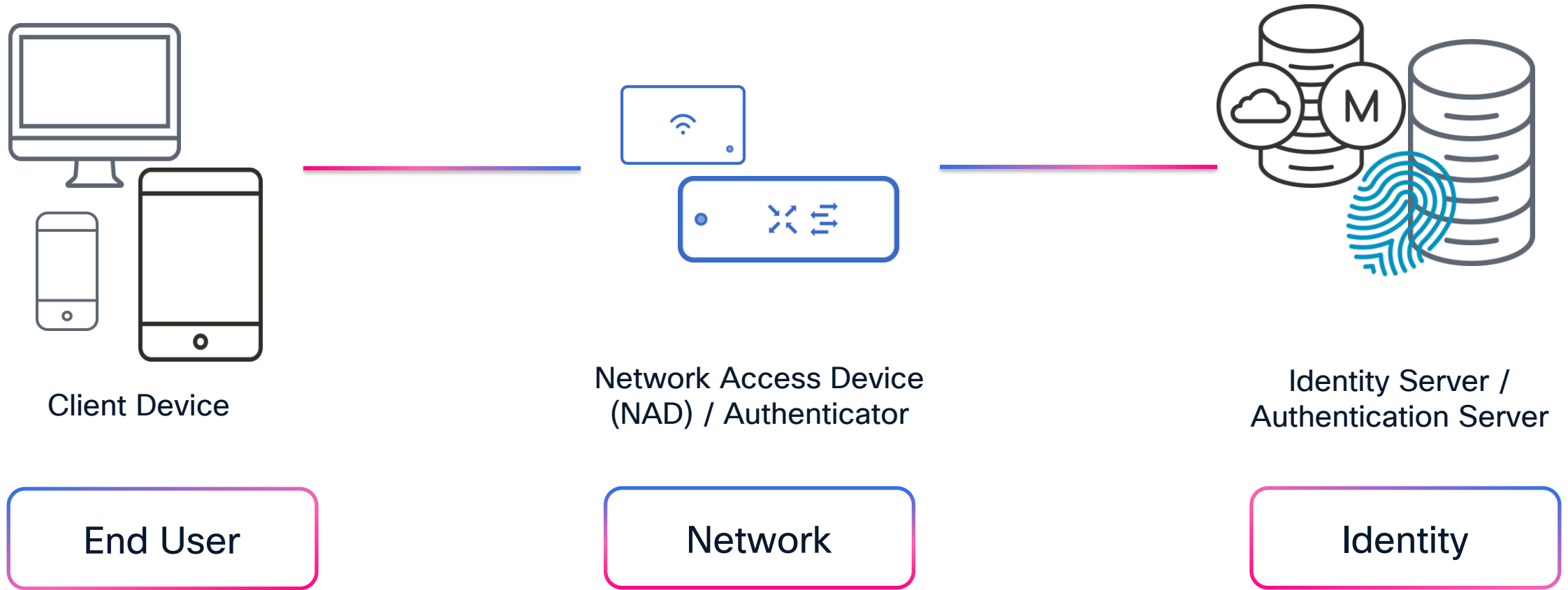
- Phishing resistant: no password, no problem
- Cert resides on the device, presented upon request
- Simple, convenient, and mutual authentication
- Makes SSO flows smoother, reduce authentication steps

The Cons

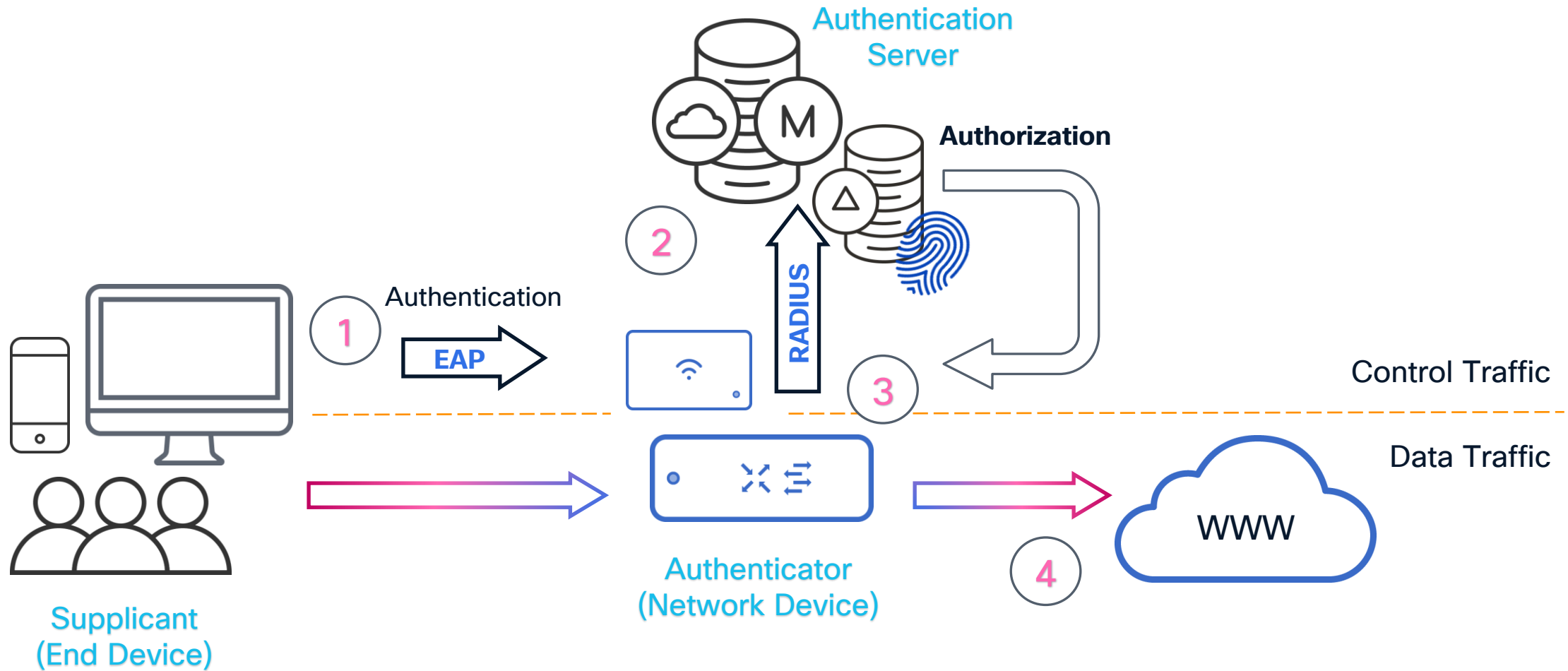
- Deploying requisite infrastructure may be complex and costly:
Public Key Infrastructure (PKI),
Certificate Authority (CA),
Certificate Management System (CMS)
- Ongoing operation must always be considered:
issuance, renewal, revocation
- Relies on a Unified Endpoint Management (UEM) system to deploy certificates and configure supplicants

Elements of Network Access Control

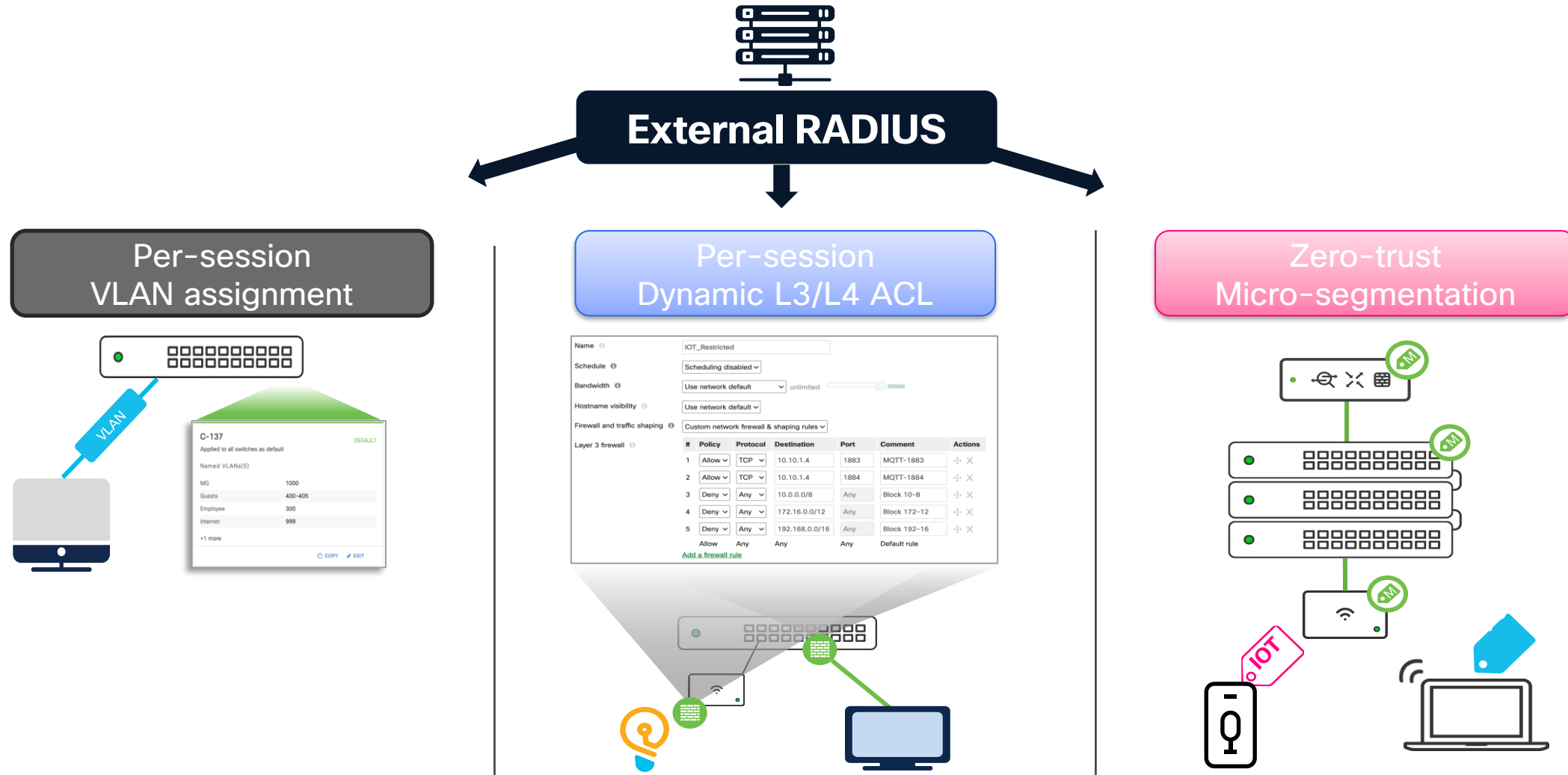
Basic Elements of a 'N' with 'AC'



Authentication and Traffic Flow



802.1X and RADIUS support was always in Meraki



So, why a Cloud-Delivered NAC?

- Centrally-managed AAA service and policy enforcement
- Less admin overhead: No added external RADIUS server required
- Tight integration with your Cloud-Managed Networking Dashboard and Cloud IdP
- Cisco Access Manager uses native Meraki management TLS tunnel for secure RADIUS transport over the Internet

**Our NAC Solution:
Straight from heaven
(aka the Cloud...)**

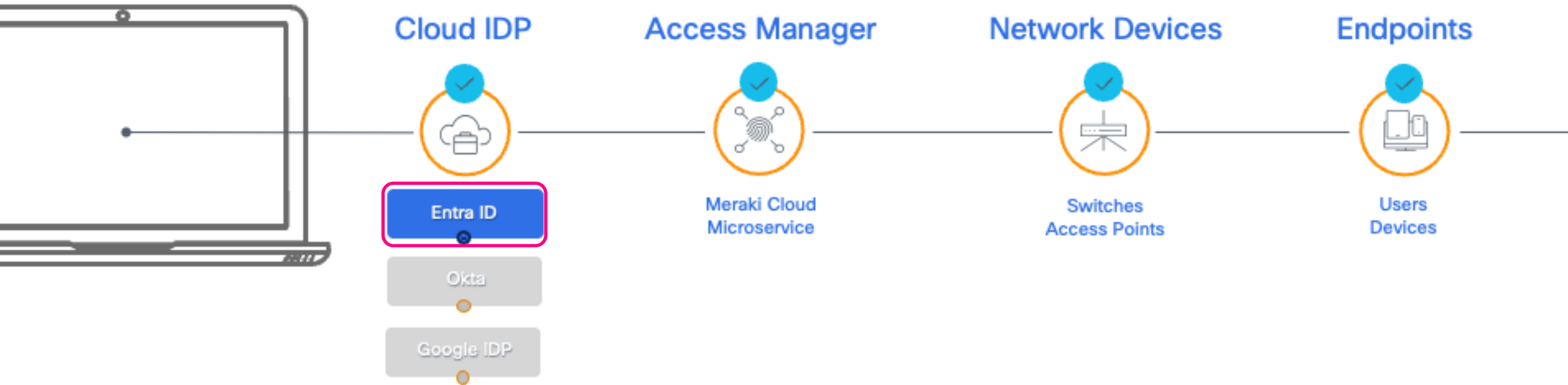


Built-in to Dashboard and Delivered from the Cloud

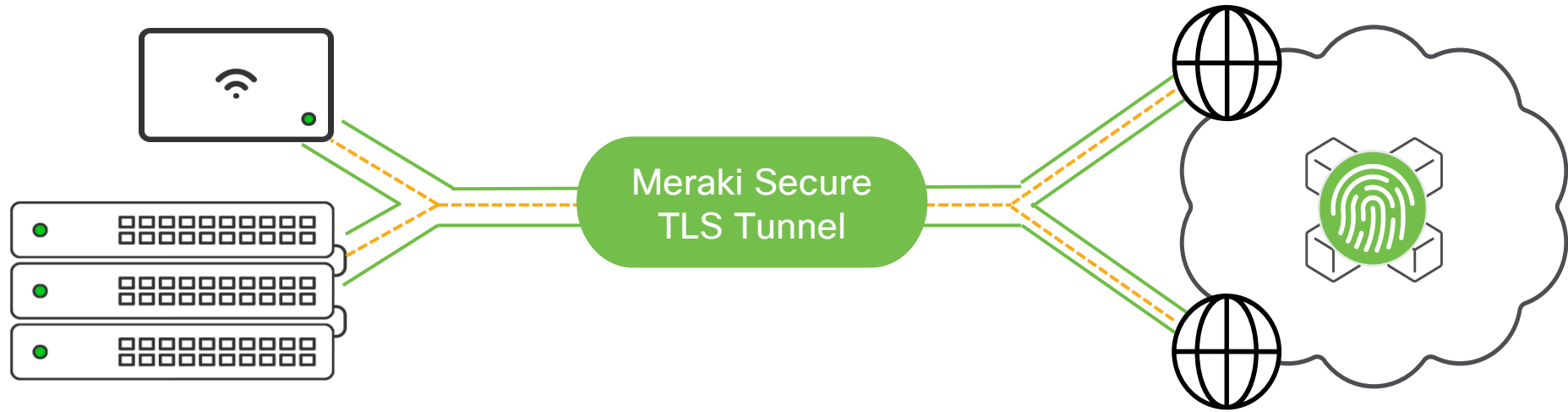
Org-wide 802.1x

EntraID as Identity Source (more IdP to follow)

Meraki Cloud as RADIUS



Under the Hood: how it all comes together



RADIUS Caching

Critical-auth/Fallback

Extended Local Auth
(Wireless)

In-geo primary & secondary
tunnel connectivity

Horizontal auto-scaling

In-geo termination

Entra ID sync and caching
for low latency response

Supported Authentication Methods (as of GA, today)



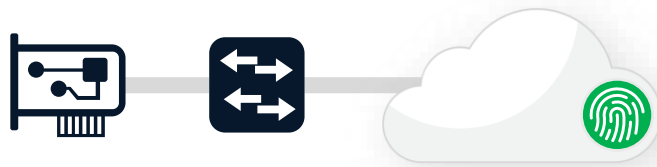
EAP-TLS Auth with Entra ID Lookup



EAP-TTLS Auth with Entra ID Lookup



Identity PSK for Wireless **IOT**



MAC Auth Bypass (MAB) for **IOT**

Cisco Access Manager (CAM) Licensing

Licensing

- CAM Advantage is a separate license from Meraki MR/MS licenses
- Orderable under the Meraki Co-Term, Meraki SUB & UNX Subscriptions & Networking EA
- Consumption is based on active, concurrent, endpoint sessions
- CAM license assigns Adaptive Policy SGT to sessions; Meraki Advantage device licenses required for enforcement

Trials

- 3 Months Trial
- Orderable using AM co-term SKUs
- Available for co-term orgs only not for subscription: meraki.cisco.com/form/trial/

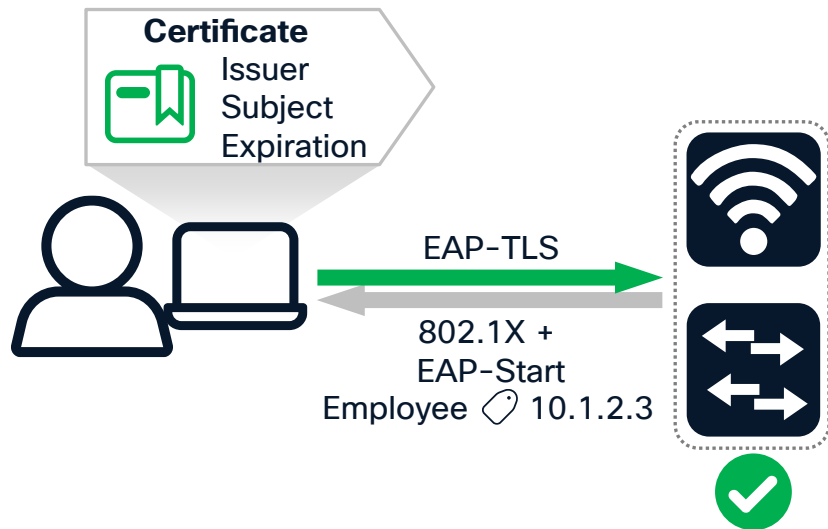
Promotions

- Customer gets 1 year off when purchasing Access Manager licenses for 3 years+
- Applicable for a la carte co-term & subscription offer, not for EA

Securing Corporate Managed Devices

EAP-TLS: Certificate Authentication + EntraIDLookup

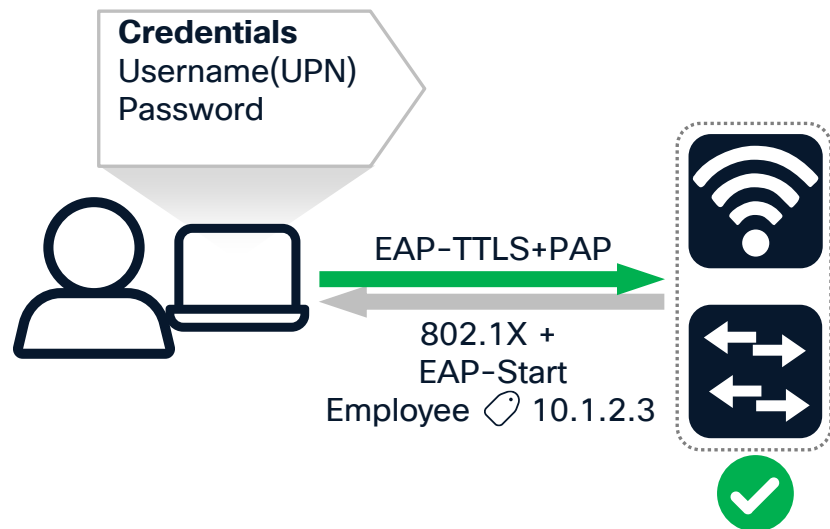
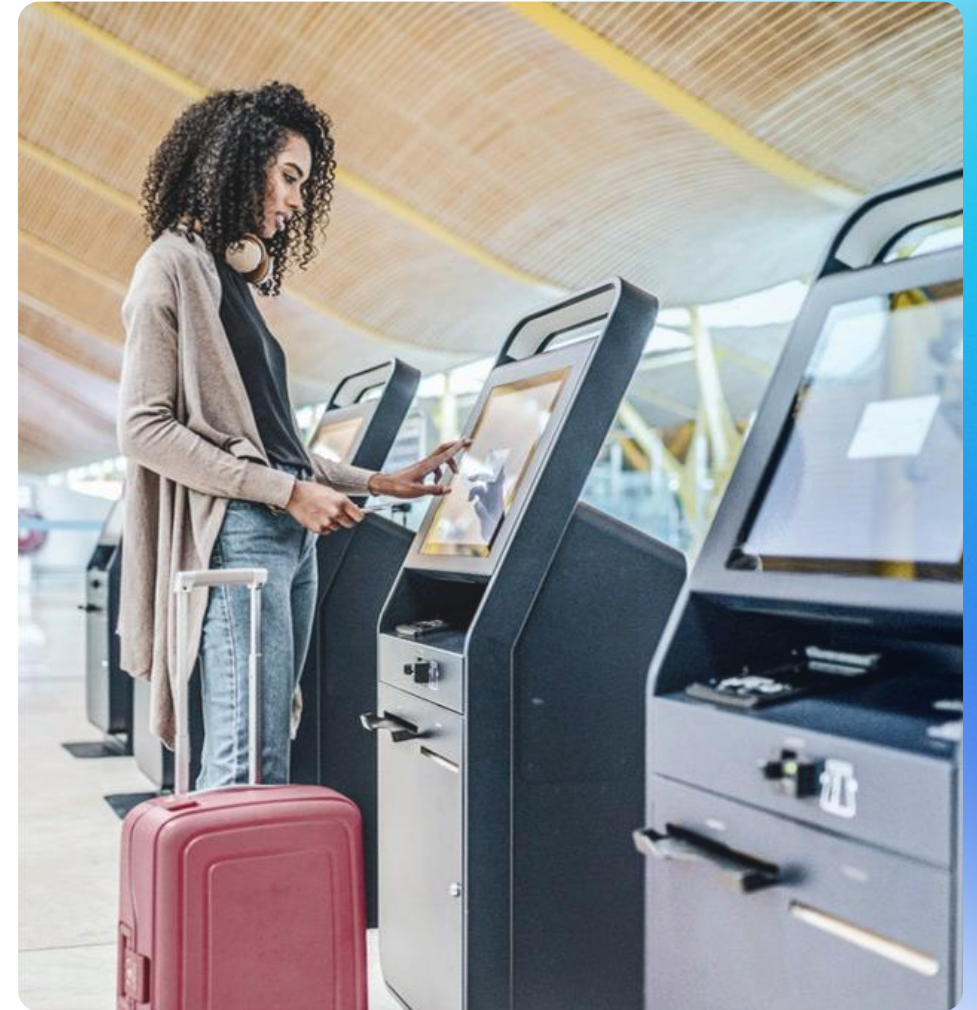
Highly recommended for endpoints that are managed by MDM/UEM.



Securing Managed (MDM/UEM) or Unmanaged (Guest) Devices **without PKI**

EAP-TTLS/PAP: Username/Password Auth + EntraID Lookup. Provision endpoints with eap.meraki.com certificate chain on endpoints for 802.1x configs.

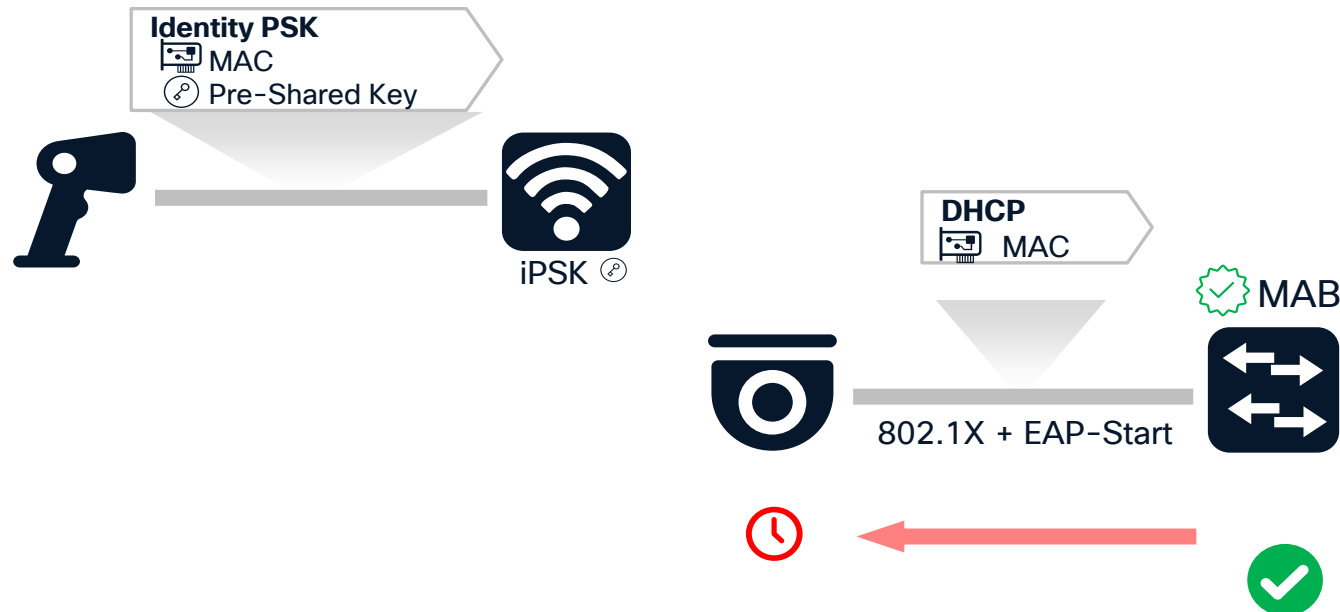
Transition into a Cloud NAC solution from existing on-prem NAC. Consider using **Cert-based** authentication for the **long-term**.



Securing IoT and Operational Technology (OT)

MAC Authentication Bypass (MAB) for wired/LAN or iPSK for wireless/WLAN.

Suitable for endpoints that are un-managed and do not support 802.1X like printers, cameras etc.



Demo:

Configure an SSID with Access Manager

Org Wide Users - Meraki Dashboard

n445.dashboard.meraki.com/o/t3b8Fd/manage/org_wide_users/

Meraki

Search

Global Overview

Organization
FC@Home

Network
HQ-Prod

Network-wide

Assurance

Wireless

Organization

Automation

Access Manager New

Find in Menu

The Cisco AI Assistant is now available! Use the AI Widget to launch this exciting new feature from the top-right corner of your dashboard. For additional information and examples, watch this [short video](#) or visit the [documentation](#).

Users

View IdP integrations Refresh

Summary

4 Users3 User groups

IdP Sources

1 Synced0 Not Synced

SyncConfigureCreate IdP

UsersUser Groups

SearchStatusIdP sourceUser groupChannelAdd User

	Username	Status	IdP source(s)	User group(s)	Channel(s)	Account update time
☐	kakashi.hatake@ichaicha.org	✔	CLAPJC2025-MAM-IdP	Hokage-sama		Oct 4 2025 03:03
☐	zoro.roronoa@strawhat.crew	✔	CLAPJC2025-MAM-IdP	Pirate Crews		Oct 4 2025 03:03
☐	levi.ackermann@surveycorps.mil	✔	CLAPJC2025-MAM-IdP	Squad Leaders		Oct 4 2025 03:03
☐	F Chua	✔	CLAPJC2025-MAM-IdP			Oct 4 2025 01:57

Rows per page101-4 of 41

© 2025 Cisco Systems, Inc.

Privacy policyTerms of service

Last login
1 day ago from 2401:d002:4907:d269:84b5:ffe9:58f5:a56e , Australia

Current session started
10 days ago

Data for FC@Home (organization ID: 1684825) is hosted in Asia-Pacific

Give your feedback

Demo: End Device Configuration (without MDM)

- Global Overview
- Organization
FC@Home
- Network
HQ-Prod
- Network-wide
- Assurance
- Wireless
- Organization
- Automation
- Access Manager New
- Find in Menu

New in Dashboard: Early Access: New Assurance-Focused Organization Summary Page - [Read more.](#)

The Cisco AI Assistant is now available! Use the AI Widget to launch this exciting new feature from the top-right corner of your dashboard. For additional information and examples, watch this [short video](#) or visit the [documentation](#).

Certificates ⓘ

EAP-TLS 0 RADSEC 0

Want an easier way to securely connects personal devices to business-critical resources without requiring an MDM profile to be installed? Learn more about [Meraki Trusted Access](#).

Custom certificate authority

Download RADIUS CA certificates



Upload certificates

This page is for you to manage certificates that are used to validate client certificates.

+ Upload CA certificates

What's Next?

We've so far covered the
Authentication side of AAA

How about **Authorization**...?
...and **segmentation**?

Your NAC fits into the
organization's
segmentation strategy

Rule

Group or Attribute

Issuer - Organization

Contains

Meraki

+ Add attribute

Attribute source 3

Select source

+ Add attribute source

Authorization

Access permission

Allow restricted access

☐ VLAN ID / name

☐ Voice domain

☒ Adaptive policy

Infrastructure

☐ Identity PSK

☐ Group policy

Cancel

Save

Demo:

Access Rules Configuration

Org Wide Users - Meraki Dashi

n994.dashboard.meraki.com/o/uoHSxd/manage/org_wide_users/

Search

Meraki

Global Overview

Organization
FC@Meraki

Network
HQLab-SM

Secure Connect

Systems Manager

Insight

Organization

Security New

Automation

Access Manager New

Find in Menu

This is a Cisco internal organization.

Users

View IdP integrations Refresh

Summary

3 Users0 User groups

IdP Sources

0 Synced

0 Not Synced

Sync

Configure

Create IdP

Users

User Groups

Search

Status

IdP source

User group

Channel

Add User

☐	Username	Status	IdP source(s)	User group(s)	Channel(s)	Account update time	
☐	frchua@outlook.com		Meraki		Client VPN	Sep 1 2025 02:26	
☐	fychua@gmail.com		Systems Manager		Self-service portalTrusted access	Jun 17 2025 11:52	
☐	frchua@cisco.com		Systems Manager		Self-service portalTrusted access	Sep 15 2023 02:38	

Rows per page

10

1-3 of 3

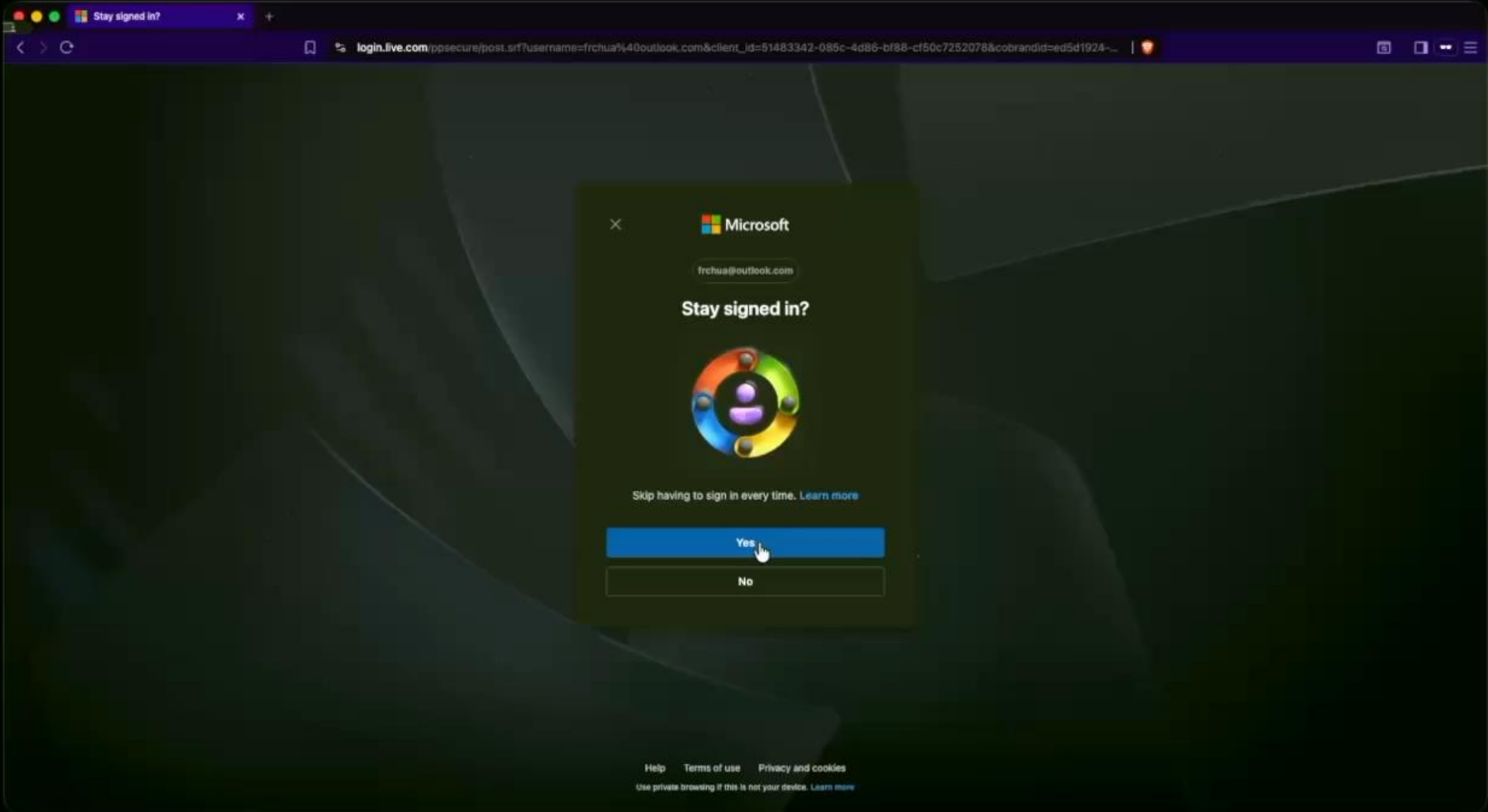
<1>

© 2025 Cisco Systems, Inc.

Privacy policyTerms of service

But Wait...
There's More!

Demo: EntraID Enterprise Application Configuration



Azure EntraID: Configuration Recap

1. Home > Manage > New 'Enterprise Application'
> [Create your own Application](#)
2. Set Permissions via Graph API:
 - Delegated: '[User.Read](#)'
 - Application: '[Directory.Read.All](#)' and '[User.Read.All](#)'
3. Generate 'Client Secret' Key
 - Home > App Registrations > {App Name}
 - Manage > Certificates & Secrets
 - Remember: Use the Client Secrets '[Value](#)'

Demo:

Configure IdP Integration on Dashboard

- Global Overview
- Organization
FC@Home
- Network
HQ-Prod
- Network-wide
- Assurance
- Wireless
- Organization
- Automation
- Access Manager New
- Find in Menu

Clients

View old version

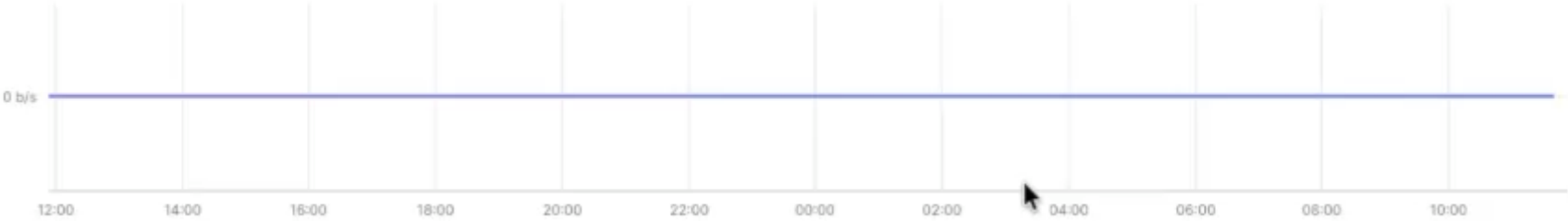
+ Add client

Usage and clients

All clients

Last day

Applications



Search for clients

Filters 0 results

Download

No data

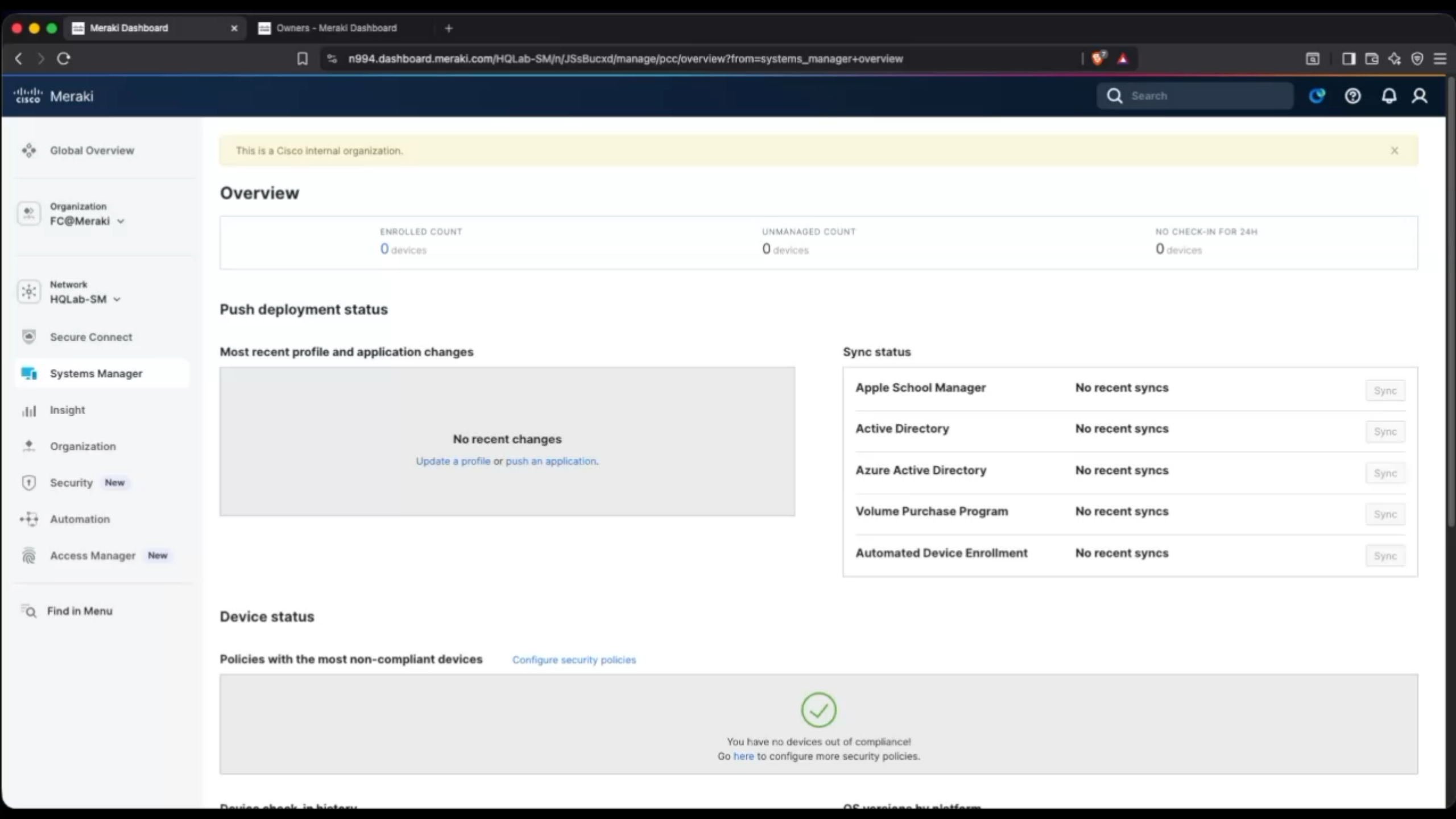
Access Manager: Integrating EntraID

1. Access Manager > Configure > Users
2. Copy from Entra:
 - Directory (Tenant) ID
 - Application (Client) ID
 - Client Secret 'Value'
3. Hit 'Save' then grab a coffee

Notes from my lab testing

1. Check if AirMarshal marks your SSID 'rogue'
2. Get the right 'Enterprise Application' type
3. Remember to add users manually if using Free EntraID instance

Bonus Demo: EAP-TLS using Systems Manager



Questions?

References: to get you started

Meraki Knowledge Base on Access Manager:

<https://documentation.meraki.com/Access Manager/Access Manager Configuration Guides>

<https://documentation.meraki.com/General Administration/Cross-Platform Content/Organization End Users>

Free Trial for Entra: (working as of 2025-Aug)

<https://www.microsoft.com/en-au/security/business/microsoft-entra-pricing>

Entra Enterprise Application Config Guide:

<https://learn.microsoft.com/en-gb/entra/identity/saas-apps/meraki-dashboard-tutorial>

References: Access Manager Public Resources



Access Manager Data Sheet cs.co/am-ds

Architecture And Example Use Cases

EAP-TLS Client Configuration

EAP-TLS Certificate Authentication with Entra ID Lookup

EAP-TTLS Client Configuration

EAP-TTLS/PAP User+Password Auth with Entra ID Lookup

MAB (MAC Auth Bypass) and iPSK for I/OT Endpoints

↗ Meraki Launchpad Instant Demo cs.co/mlp

↗ Access Manager Self-Guided Demo (Navattic)

↗ Cisco Meraki MS150 with AdP and Access Manager

▷ Meraki Minute | YouTube :

▷ Access Manager Playlist

▷ Meraki SM Playlist

Access Manager (NAC) Community cs.co/nac-community

!! Watch out for this session: BRKEWN-2047

Securing Wireless Networks with Cisco Identity Services Engine and Access Manager

Presented by:

Fletcher Joyce,
Solutions Engineer

Session ID: **BRKEWN-2047**

When: 12-Nov 1:00-2:30PM AEDT

Where: Room 210

Securing Wireless Networks with Cisco Identity Services Engine and Access Manager [BRKEWN-2047]



Schedule

Wednesday, Nov 12 | 1:00 PM - 2:30 PM AEDT | Room 210

Fletcher Joyce, Solutions Engineer, Cisco

Unlock the full potential of your Cisco Wireless Network with Cisco Identity Services Engine (ISE) or Meraki Access Manager integration. This session will guide you through the essentials of designing, deploying, and troubleshooting a secure wireless environment. Discover how to seamlessly integrate Catalyst and Meraki wireless solutions, efficiently manage network and wireless users, and enhance authentication processes. Dive into advanced topics such as network segmentation, Scalable Group Tags, and Adaptive Policy to strengthen your network security framework. Whether you're looking to secure users or endpoints, this session provides the insights and tools you need to build a robust and secure wireless network architecture.

Session Type: Breakout

Technical Level: Intermediate

Technology: Meraki, Security, Wireless and Mobility

Session Track: Networking

!! Watch out for this session: BRKEWN-2104

Understanding Wireless Security and the Implications for Secure Wireless Network Design

Presented by:

Mark Krischer,
Principal Wireless Architect

Session ID: **BRKEWN-2104**

When: 12-Nov 1:00-2:30PM AEDT
Where: Room 204 (this room)

Understanding Wireless Security and the Implications for Secure Wireless Network Design [BRKEWN-2104]



Schedule

Wednesday, Nov 12 | 1:00 PM - 2:30 PM AEDT | Room 204

Mark Krischer, Principal Solutions Engineer, Cisco

This session will explore secure wireless network design with a key focus on the latest Wi-Fi and WPA standards. Mobility brings unique challenges to network security, such as the need for strong authentication and support for secure fast roaming. Participants will learn how 802.11 addresses these requirements and will consider the changes WPA3 brings and the implications for wireless deployments. This session will also examine how Catalyst Center and Meraki Dashboard expand on the wireless security standards with rogue access point detection and location, and advanced wireless intrusion detection and prevention. The intent is to provide a deeper understanding of wireless security capabilities from the perspective of the attacks they defend against.

Session Type: Breakout

Technical Level: Intermediate

Technology: Security, Wireless and Mobility

Session Track: Networking

Shameless Plug: We have a Podcast!



Spotify



Apple
Podcast

If you find yourselves
enjoying this session,
please follow our
podcast:

Packet Party 🎉

Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: Insert preferred comms method

Thank you

CISCO Live !

