

Cisco Access Manager runs as a multi-tenant SaaS within the Meraki Dashboard used to verify users and endpoints. It offers a scalable way to ensure only authorized users and endpoints can access resources and enforces network access for users and endpoints based on user and endpoint identity, network and security context.

Benefits:

Deploy in minutes, not months: Access Manager is cloud-delivered and designed for speed. Integrated directly with the Meraki Dashboard, it allows you to create, manage, and enforce identity policies across your existing Meraki infrastructure.

Secure every connection: Authenticate users and devices using multiple methods including 802.1X with EAP-TLS or EAP-TTLS, identity PSK (iPSK), and MAC-based access.

Stop lateral movement automatically: Identity-based segmentation restricts each connection to only the resources it requires. By controlling traffic at the source, Access Manager helps contain breaches and prevent them from spreading.

Accelerate zero-trust adoption: Fuse identity, access control, and segmentation into your network fabric, providing a fast, practical path to full zero-trust security.

Reduce cost and complexity: Eliminate physical hardware, patch cycles, reducing operational burden and total cost of ownership.

Manage your security architecture from one Meraki Dashboard: Unify campus access, cloud security, and threat detection, giving IT teams visibility and control across the network from a single pane of glass.

Core Capabilities:

- Supported Authentication Methods:
 - EAP-TLS / EAP-TTLS:** Certs or User/Pass credentials for users and devices
 - iPSK (Identity PSK):** Per-endpoint group pre-shared keys for wireless clients
 - MAB (MAC Authentication Bypass):** For IoT and endpoints without 802.1X
- Provides strong, **seamless certificated based authentication** without requiring user interaction, enabling granular access control and micro-segmentation via TrustSec based on verified endpoints and user identity.
- Supports organizations that prefer or require **traditional credential-based authentication** by integrating with Microsoft Entra ID while still enabling identity-driven micro-segmentation and policy enforcement.
- Allows organizations to extend **identity-based access control** to IoT, OT and other un-managed endpoints based on endpoint MAC addresses or endpoint groups, optionally using Identity Pre-Shared Key (iPSK) for wireless endpoints for added security maintaining network segmentation and reducing risk.
- Provides **flexible authorizations options** from L2-L7 including Dynamic VLANs, ACLs, Group Policy and TrustSec based micro-segmentation.

FAQs:

Q: What identity providers are integrated?

A: It integrates natively with Microsoft Entra ID for user lookups, group memberships, and credential validation.

Q: Which network hardware is supported?

A: Supports all Cisco MS switches, cloud-configured Catalyst switches, MR access points, and Cisco Wireless (CW) access points.

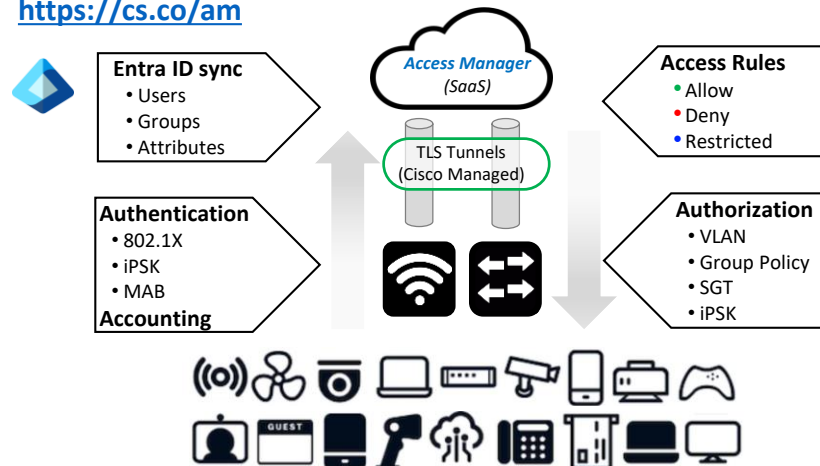
Q: How is Cisco Access Manager licensed?

A: Cisco Access Manager Advantage, which is purchased separately from base Meraki switch or access point licenses.

Q: How do you deploy Cisco Access Manager?

A: It is activated from the Meraki Dashboard utilizing existing cloud-based telemetry tunnels, requiring no firewall rule changes or appliance setup.

<https://cs.co/am>



Resources:

SalesResources	At-a-Glance	Video Channel 	FAQ
Ordering Guide	Solution Overview	Self Guided Demo	Roadmap
Data Sheet	Documentation	Entra ID Integration	Community
	Positioning Guide	Supported Devices	Public page