Cisco Access Manager

Get idenity-based zero trust security without the appliances, complexity or overhead of traditional access control solutions.

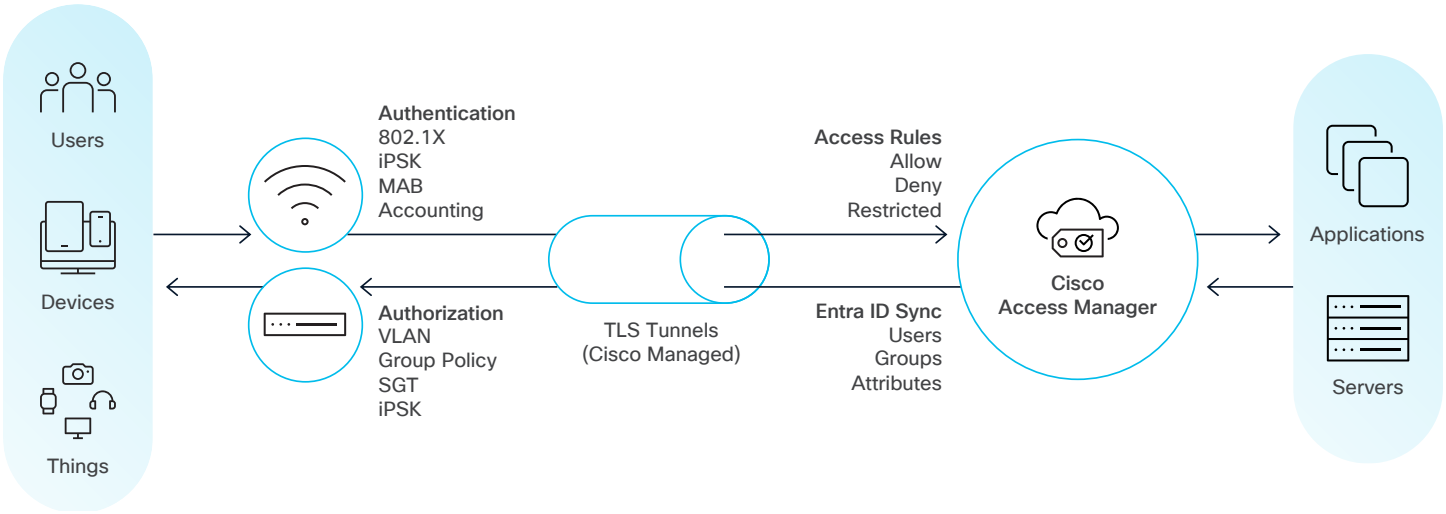
Overview

Cisco Access Manager delivered as a pure Software as a Service (SaaS) within the Cisco Meraki Dashboard makes identity a native attribute of your network, not a bolt-on system. Users and endpoints are verified once, but their identity travels with them across your entire network infrastructure, enforced automatically at every relevant point from campus to cloud.

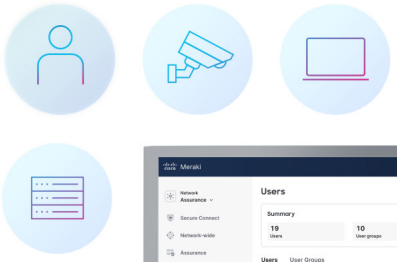
It offers a powerful, scalable, and flexible way to ensure only authorized users and endpoints can access your resources. It enables IT teams to effortlessly enforce and monitor network access for users and endpoints based on user identity, endpoint identity, network context, and identity and security context from external integrations like Microsoft Entra ID (formerly Azure AD).

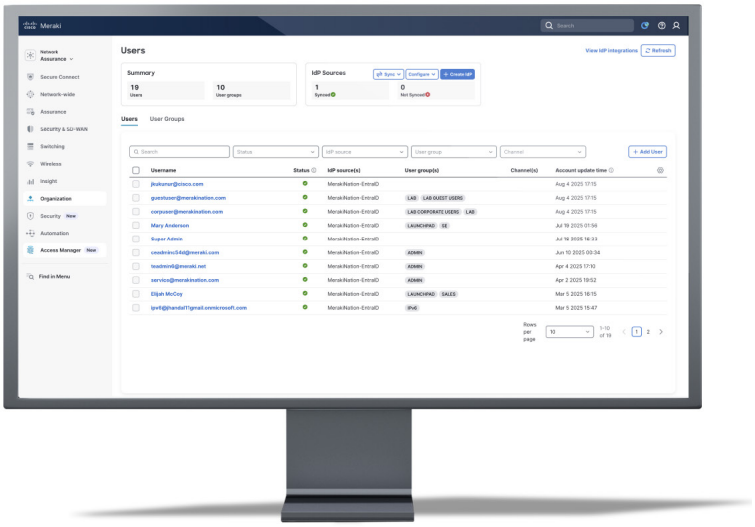
Key Benefits

- **Deploy identity-based access in minutes** using your existing Meraki infrastructure
- **Secure and protect** every user and device that connects to your network
- **Stop attackers' lateral movement** with identity-based segmentation
- **Meet zero trust requirements faster** with automated policy enforcement
- **Reduce costs and free IT resources** by eliminating on-prem hardware and maintenance cycles
- **Manage your end-to-end security architecture** in the Meraki Dashboard



Feature	Benefit
Certificate Authentication (EAP-TLS) for Managed Endpoints	Provides strong, seamless authentication without requiring user interaction, enabling granular access control and micro-segmentation via TrustSec based on verified device and user identity.
Username Password based Authentication (EAP-TTLS) for Managed Endpoints	Supports organizations that prefer or require traditional credential-based authentication by integrating with Microsoft EntraID while still enabling identity-driven micro-segmentation and policy enforcement.
MAC Authentication Bypass(MAB) for Unmanaged Endpoints	Allows organizations to extend identity-based access control to IoT, OT & 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
Multiple Authentication Options	Support for multiple authentication methods (802.1X, MAB) on the same port allowing multiple endpoints to authenticate in parallel & periodically re-authentication of the identity of connected users or devices to maintain continuous trust without manual intervention. parallel & periodically re-authentication of the identity of connected users or devices to maintain continuous trust without manual intervention.
Flexible Access Controls	Provides authorizations options from L2-L7 including Dynamic VLANs, ACLs, Group Policy & TrustSec based microsegmentation
Built in authentication fallback mechanisms	Leverages existing fallback mechanisms for wired(RADIUS caching, Guest VLAN) and wireless(extended local auth) networks to provide secure access & business continuity in the event of loss of connectivity to the cloud.
Certificate Authority (CA) integration	Enables robust security through certificate-based, mutual authentication option, protecting against password-based attacks and man-in-the-middle threats by integrating with External Certificate Authority (PKI) infrastructure & providing Certificate Revocation List (CRL) check.





Embed identity into your network

Pure Software As A Service(SaaS) identity-based access embedded into your existing network—eliminating hardware infrastructure, external servers, and complex deployments while delivering enterprise-grade security for lean IT teams.

- Pure SaaS delivery with zero on-prem infrastructure.
- Native integration with Entra ID.
- Cloud-native scalability, availability, and resiliency.

Segment and Protect Everything that Connects

Identity-driven segmentation protects users, endpoints and things across all supported infrastructure—enforced natively at every point, eliminating bottlenecks and delivering adaptive zero-trust protection at scale.

- Dynamic identity-based segmentation using TrustSec policies.
- Context-aware access control adapts to user behavior, posture and location.
- Identity-based segmentation enforced natively across all supported devices.

Extend Zero Trust from Campus to Cloud

Meraki dashboard unifies an identity-based framework and visibility to extend zero trust from campus to cloud, delivering consistent identity-based security and continuous verification across all environments.

- Common identity framework shared between Cisco Access Manager Cisco Secure Access, Application Centric Infrastructure (ACI) & Identity Services Engine (ISE)
- Cisco XDR correlates telemetry from all Meraki-managed devices.
- Unified Meraki Dashboard for identity-based access, cloud security, and threat detection.

Supported Network Devices

Cisco Access Manager (CAM) currently requires all network access devices to communicate with the Cisco Meraki Dashboard's secure management tunnel. Any devices (Cisco or non-Cisco) that do not support the Meraki management tunnel are not supported. Devices should be on the latest stable software version.

Model	802.1X	MAB	VLAN	GPACL	TrustSec (AdP)	URL Redir
Wireless						
MR20, MR70	●	●	●	●		●
MR28/30H/33/42/42E/ 52/53/53E/74/84 MR36/36H/44/45/46/ 46E/55/56/57|76/78/86 CW91xx	●	●	●	●	● 802.11ac Wave2+	●
Switching						
MS120, MS125, MS130	●	●	●			
MS130X/R, MS150	●	●	●	MS18	●	
MS210, MS225, MS250, MS350, MS355	●	●	●	●		●
MS390, C9K-M	●	●	●	●	●	●
MX and Z					SGT Transport only	

Access Manager license is based on the number of concurrent, active endpoint sessions and is orderable under the Meraki Co-Term & Subscription & Cisco Unified Licensing models & Meraki Networking Enterprise Agreements.

For more details on licensing for for Access Manager, please refer to <link to licensing guide>