Cisco Access Manager

© 2026 Cisco and/or its affiliates. All rights reserved.

Contents

Overview 3

Key Benefits 3

Embed identity into your network 5

Segment and Protect Everything that Connects 5

Extend Zero Trust from Campus to Cloud 5

Supported Network Devices 6

© 2026 Cisco and/or its affiliates. All rights reserved.

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

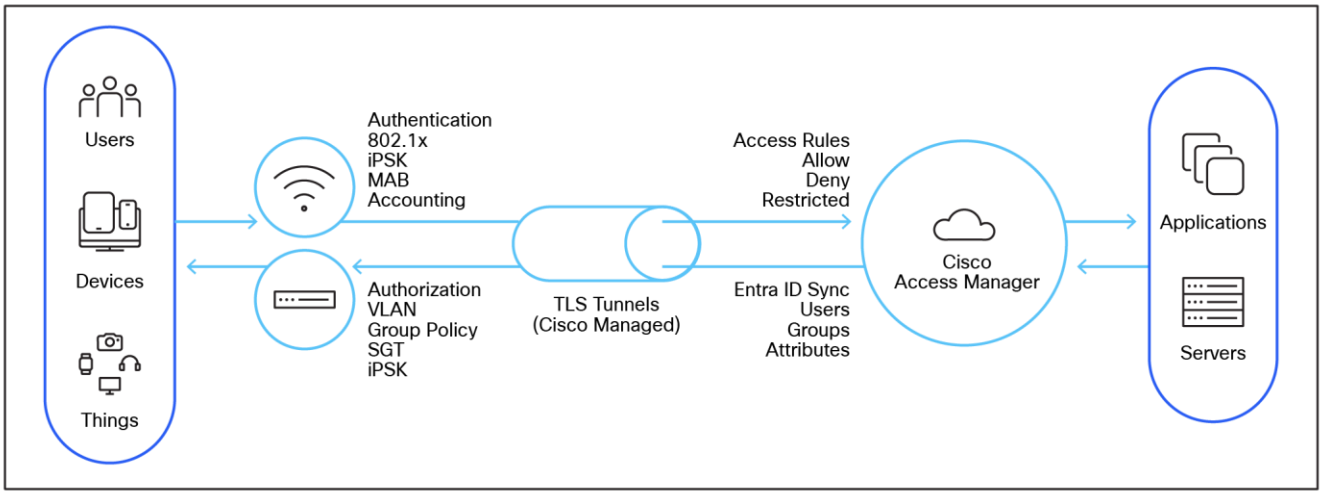
Overview

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).

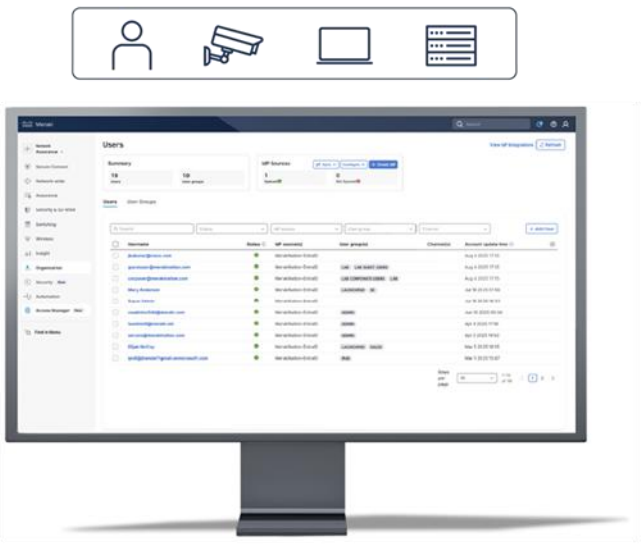
Key Benefits

- **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



© 2026 Cisco and/or its affiliates. All rights reserved.

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 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.
Multiple Authentication Options	Support for multiple authentication methods (802.1X, MAB) on the same port allowing multiple endpoints to authenticate in parallel and periodically re-authentication of the identity of connected users or devices to maintain continuous trust without manual intervention. parallel and 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 and 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 and 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 and providing Certificate Revocation List (CRL) check.



© 2026 Cisco and/or its affiliates. All rights reserved.

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) and 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.

© 2026 Cisco and/or its affiliates. All rights reserved.

Supported Network Devices

Cisco Access Manager 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. For more details on supported devices, please refer to this link.

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

For more details on licensing for Cisco Access Manager, please view our ordering guide.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA C78-5599642-01 05/26

© 2026 Cisco and/or its affiliates. All rights reserved.