Cisco Access Manager

Identity fused into your network

What if you could embed identity-based security into your network without deploying a single appliance, configuring external servers, or spending months on implementation?

Cisco Access Manager makes identity a native attribute of your network—delivering zero-trust access control in minutes without the hardware dependencies, complexity, or operational overhead of traditional solutions. Powered by Cisco Identity Services Engine (ISE), optimized for Meraki, and delivered as Software as a Service (SaaS), Access Manager brings enterprise-grade identity-based security to every user, device and connection on the Meraki network.

Overview

The modern network perimeter no longer exists. Users connect from anywhere, on any device. Your network must recognize who and what is connecting—and grant access based on identity, not just location. Traditional network access control (NAC) systems were built for fixed offices, wired ports, and IT teams with deep infrastructure expertise. They required complex distributed server clusters, policy engines, and weeks—or months—of tuning and deployment. As a result, many organizations delayed or abandoned NAC projects entirely.

Access Manager changes that. It takes the proven security model of Cisco ISE and delivers it as a cloud-native service designed with Meraki simplicity. Now, you can achieve the same level of identity-based control—without the hardware, heavy configuration, or dedicated NAC specialists. In other words: **zero-trust access control, simplified.**

Key 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 quickly and easily.
- **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—ensuring both managed and unmanaged endpoints are protected across your environment.
- **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 directly into your network fabric, providing a fast, practical path to full zero-trust security.
- **Reduce cost and complexity:** Eliminate physical hardware, patch cycles, and specialized NAC teams—reducing operational burden and total cost of ownership while maintaining enterprise-grade control.
- **Manage your entire security architecture from one Meraki Dashboard:** Unify campus access, cloud security, and threat detection, giving IT teams complete visibility and control across the network from a single pane of glass.

Business Value

Cisco Access Manager creates measurable value across your business, from strategy to operations.

For Business Leaders

- Accelerate digital transformation without security slowing innovation
- Reduce total cost of ownership by removing NAC appliances and specialized infrastructure
- Meet compliance requirements with automated enforcement and audit trails

For Security Teams

- Implement a zero-trust architecture with identity-based segmentation
- Stop lateral movement and contain breaches automatically
- Gain unified visibility across users, devices, and access patterns

For IT Teams

- Deploy in minutes—not months—with no specialized training required
- Manage everything directly from the Meraki Dashboard
- Scale effortlessly with SaaS delivery and zero infrastructure to maintain

The Challenge: Operational strain of managing access at scale

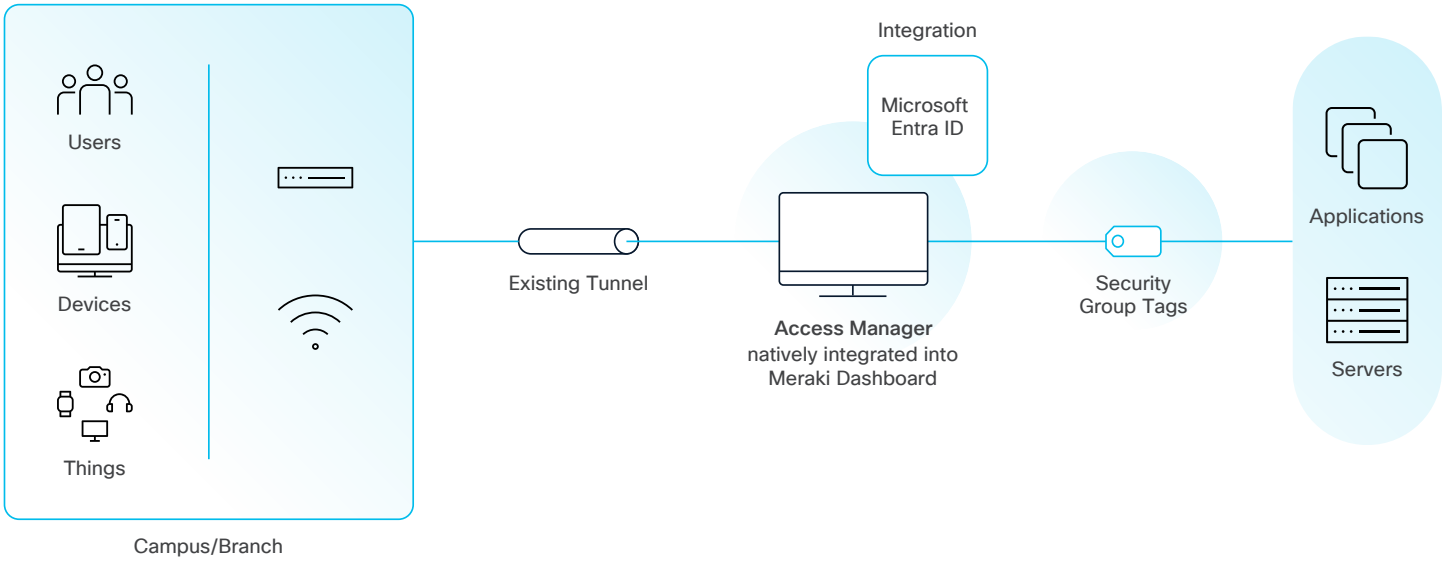
Identity and access control are essential to zero trust. Yet most networks still base trust on *where* a device connects, not *who or what* it is.

Network Access Control (NAC) has existed for years, but adoption remains inconsistent—not because organizations don't value identity-based security, but because many NAC deployments are too complex and infrastructure heavy. This creates three common barriers:

- **Infrastructure Burden:** Historically NAC requires dedicated hardware appliances, external AAA/RADIUS servers, high availability for redundancy, and complex network integrations. This creates capital costs, hardware refresh cycles, and capacity planning challenges—all before the first policy is even enforced. The infrastructure alone overwhelms already resource-constrained IT teams.
- **Lean IT reality:** Deploying and maintaining traditional NAC often require deep networking expertise, lengthy configuration cycles, and dedicated administrators to maintain ongoing operations. As networks grow and user roles evolve, policy management becomes an ongoing project—consuming resources that lean IT teams simply don't have. Most organizations today operate with smaller, more agile teams, spending months deploying and tuning NAC infrastructure doesn't fit that reality
- **Operational Risk:** Rolling out NAC means touching production networks—raising the risk of downtime or user disruption. Fear of breaking connectivity results in many organizations completing the pilot successfully but stop short of full rollout.

The Result? Many organizations settle for "good enough," relying on static IP/VLANs and firewall rules that can't adapt to identity or behavior. "We haven't had a major breach yet" becomes the justification for avoiding the NAC burden. Security loses priority battles against user productivity. The castle-and-moat mentality persists because changing it requires more resources, expertise, and risk than IT teams can absorb. This leaves an open path for attackers who breach the perimeter through phishing or compromised devices. Once inside, lateral movement becomes easy, and detection comes too late.

Cisco Access Manager changes all of this—delivering identity-driven access control without the infrastructure, expertise, or risk that has held back NAC implementation for decades.



How It Works: Identity that travels with every connection

Cisco Access Manager reimagines identity-based access control by delivering it entirely as SaaS—eliminating infrastructure overhead, deployment complexity, and operational burden. Enterprise-grade zero-trust security can be enabled in minutes using your existing Meraki network. It integrates seamlessly with your Meraki environment and uses your existing identity sources, such as Microsoft Entra ID (formerly Azure AD), to enforce access policy across wired and wireless. It's simple, scalable, and entirely cloud managed.

Multi-Tenant Cloud Architecture

Access Manager runs as a multi-tenant SaaS service designed for global scale and continuous availability. Authentication traffic is securely carried over TLS-encrypted tunnels between the Meraki Dashboard and your network devices—no firewall changes, open ports, or new VPNs required.

Activation is seamless: Meraki customers can enable Access Manager directly in the dashboard, configure policies using a familiar interface, and have rules automatically applied across all Meraki switches and access points—whether managing 10 devices or 10,000. The platform scales to support up to 500,000 endpoints and 150,000 users per organization. Zero-touch provisioning ensures new devices automatically receive policies as soon as they connect.

Unified Identity for Every User, Corporate Device, and Thing

Cisco Access Manager secures every connection—corporate laptops, BYOD, or IoT endpoints. Every session is authenticated, authorized, and tagged automatically, with policies dynamically applied based on Microsoft Entra ID attributes, access method, network attributes, and user or client group membership.

Access Manager integrates natively with Microsoft Entra ID via Microsoft Graph API. Users, groups, and attributes sync automatically every six hours, keeping access policies aligned with your directory. Policies can leverage familiar constructs like department, role, or group membership instead of IP addresses or VLANs.

Policies update automatically as users change roles, switch departments, or leave the organization. Access Manager supports up to 100,000 Entra ID groups per tenant, enabling fine-grained, identity-based control for all users and devices.

Policy Engine with Rich Context

All access decisions flow through a unified policy engine that evaluates up to 50 attributes—including certificate fields, device type, network context, and Entra ID metadata. Policies are processed top-down, supporting production, guest, and exception rules.

Supported Authentication methods:

- EAP-TLS / EAP-TTLS: Certificates or Username/ Password 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 support

Key Authentication Features:

- Hybrid Authentication: Supports multiple authentication methods (802.1X, MAB) on the same port, allowing different devices to authenticate in parallel.
- Multi-Authentication: Supports multiple endpoints per port with independent authentication.
- Automatic Reauthentication: Periodically re-authenticates the identity of connected users or devices to maintain continuous trust without manual intervention.

All authentication methods automatically map to Security Group Tags (SGTs), enabling consistent, identity-driven access across your network. SGTs define the “who” and “what” of each session—determining which network segments, applications, and resources each user or device can access. Because SGTs operate at the identity level, policies are consistent across VLANs, sites, and connection types, eliminating policy enforcement through complex subnet design or ACL sprawl.

Supported Authorization actions:

- Allow or deny access
- Allow restricted access and override default with one or more of the following:
  - Apply SGTs for adaptive segmentation
  - Enable iPSK or voice domain access
  - Assign VLAN
  - Apply group policy

The Result, Identity Without Infrastructure.
Cisco Access Manager delivers the power of zero-trust access control without adding operational weight. Access Manager provides unified visibility across every connection. You can see who and what is on your network, where they’re connecting from, and how they’re accessing resources—all from your Meraki Dashboard.

By removing infrastructure dependencies and deployment complexity, Access Manager allows IT and security teams to identify unauthorized devices and quickly respond to security incidents.

Use Cases

Access Manager brings zero-trust access control to a wide range of environments, including: Campus and Branch networks, Retail, Hospitality, Education, Healthcare, Small to Medium Businesses.

Zero-Trust Policy Across Wired and Wireless Networks

Challenge: Traditional NAC systems often rely on location or IP-based segmentation, limiting flexibility, and creating security gaps.

Solution: Access Manager enforces identity-based segmentation across wired and wireless networks using SGTs, VLANs, and Group Policies.

Benefit: Provides consistent, zero-trust access control for all users, devices, and connections, eliminating complex ACLs and manual rule sets.

Authentication & Authorization:

- Certificate-Based (EAP-TLS): Corporate workstations authenticate using digital certificates with authorization based on certificate validation and Entra ID group membership
- Credential-Based (EAP-TTLS): User devices authenticate with username/password with authorization based on Entra ID group membership

Role-Based Access Enforcement

Challenge: Users frequently change roles, departments, or projects, making static access controls cumbersome and error prone.

Solution: Access Manager integrates with Entra ID to dynamically update policies based on role, group membership, or department.

Benefit: Ensures users always have the right level of access while reducing IT effort and risk of misconfiguration.

Authentication & Authorization:

- Certificate-Based (EAP-TLS) or Credential-Based (EAP-TTLS): All user devices authenticate using either certificates or credentials with authorization dynamically updated based on Entra ID group membership changes

BYOD and Guest Access Management

Challenge: Organizations struggle to secure personal devices and guest connections without disrupting corporate network security.

Solution: Access Manager dynamically segments BYOD devices using iPSK or EAP-TTLS, while guest devices are managed via a Meraki dashboard splash page, ensuring restricted access and isolation from sensitive resources.

Benefit: Simplifies onboarding for personal devices and visitors while maintaining zero-trust security.

Authentication & Authorization:

- BYOD - Credential-Based (EAP-TTLS): Personal devices authenticate using employee credentials with authorization based on employee identity and restricted policies
- Guest Access - Splash Page: Guest devices receive time-limited, isolated access through Meraki dashboard (not integrated with Access Manager)

IoT Device Segmentation and Security

Challenge: IoT devices often bypass traditional security controls, introducing vulnerabilities and network risk.

Solution: Devices authenticate via MAB, and can be dynamically segmented using VLANs, group policies, and SGTs, both for themselves and for critical infrastructure.

Benefit: Enables secure, scalable IoT deployments without manual network configuration or risk of lateral movement.

Authentication & Authorization:

- Identity PSK (iPSK): Wireless IoT devices (scanners, sensors) authenticate using unique pre-shared keys with authorization based on device classification
- MAC Authentication Bypass (MAB): Wired/wireless IoT devices (cameras, printers, medical devices) authenticate via MAC address with authorization based on endpoint grouping

Cisco Capital: Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

The Cisco Advantage

- **Powered by Trusted Technology:** Based on Cisco ISE, the industry-leading identity and segmentation framework relied on by the world's largest enterprises.
- **Seamless Integration and SaaS Delivery:** Natively embedded into Meraki Dashboard, Access Manager delivers identity-based security across your existing Meraki infrastructure in minutes.
- **Unified Security from Campus to Cloud:** Meraki Dashboard combines Access Manager for campus access, Cisco Secure Access for cloud security, and Cisco XDR to correlate telemetry across all Meraki-managed devices for real-time threat detection and automated response.
- **Proven Expertise and Ecosystem:** Backed by thousands of global deployments, Cisco offers the industry's broadest security ecosystem to enable practical, scalable zero-trust.

Start Your Zero-Trust Journey Today

Still relying on VLANs and static ACLs to define trust in your network? It's time for a change.

Cisco Access Manager lets you extend zero-trust principles across your environment—securely, simply, and at scale. Delivered as a fully managed SaaS solution, it eliminates the need for servers, complex integrations, and specialized training.

Deploy in minutes, gain visibility into every connection, and enforce identity-based segmentation across users, devices and things—all through your Meraki Dashboard.

No appliances. No complexity. No compromise - Transform your security posture without transforming your infrastructure.

Learn more

P1804090425 10/25