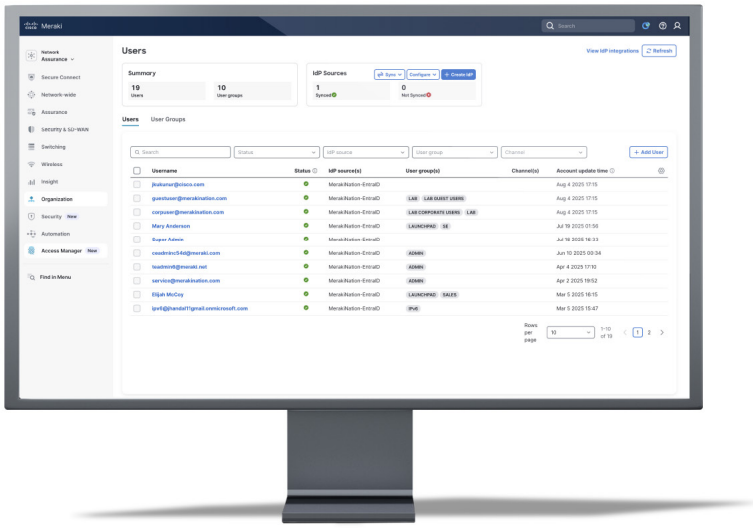
Cisco Access Manager



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

Identity Fused into Your Network

Trust Based on Who, Not Where

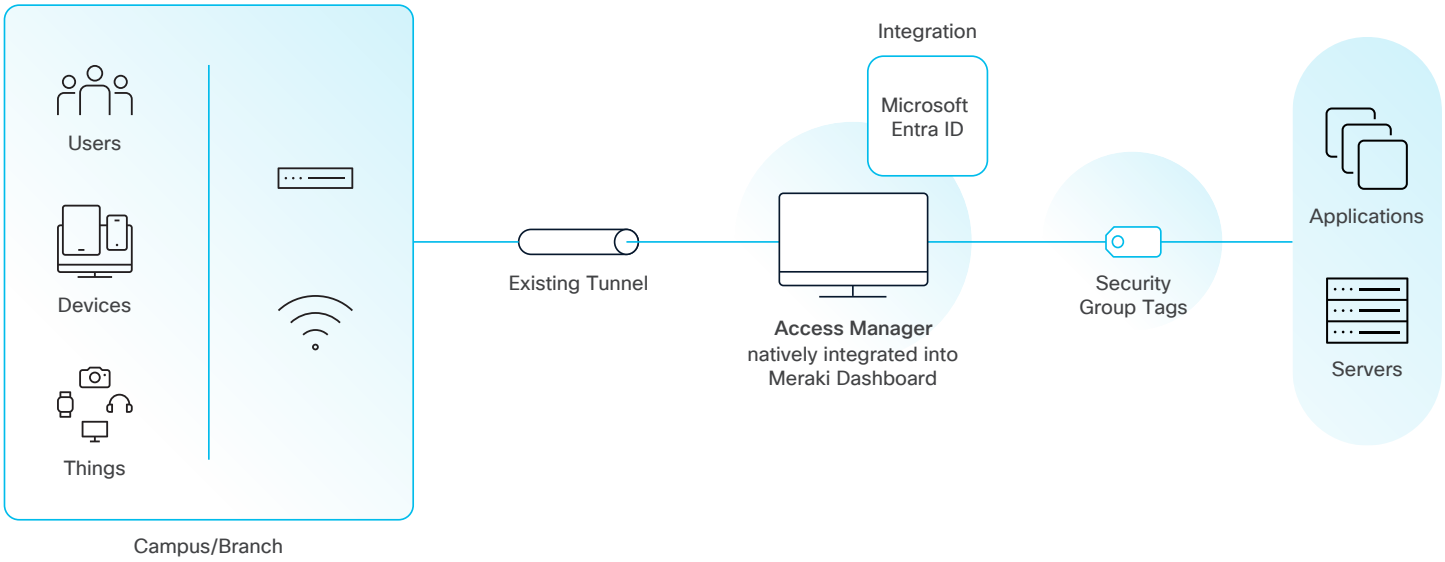
Most networks still anchor trust to where a device connects — wired or wireless. They don't consider who is using it, which device it is, or what it can access. A compromised device can still be treated as safe simply because it's on the "trusted" network. Traditional solutions are no longer relevant for a world of roaming users, IoT growth, and apps that live outside the perimeter.

Identity Built Into the Network

Cisco Access Manager makes identity native to your network, not a bolt-on. Users and devices are verified once, and that identity follows them everywhere in your infrastructure, enforced automatically at every relevant point.

Zero Trust Without the Overhead

Delivered as pure SaaS in the Meraki Dashboard, Access Manager enables identity-based access in minutes using existing infrastructure. No hardware, no complex rollouts, no maintenance burden — just enterprise-grade zero-trust security for every user and device.



Deploy Identity-based Zero Trust Security Without the Infrastructure Burden

Powered by Cisco Identity Services Engine (ISE) and optimized for Meraki, Access Manager enables you to:

- **Embed identity into your network:** Pure 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
- **Segment everything that connects:** Identity-driven segmentation protects users, devices, and things across all supported infrastructure—enforced natively at every point, eliminating bottlenecks and delivering adaptive zero-trust protection at scale
- **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

While competitors require you to choose between simplicity or capability, Access Manager delivers both: security powered by ISE with the ease-of-use of Meraki. Your existing Meraki customers can deploy instantly without network changes, infrastructure additions, or training. The same straightforward setup you rely on for switches and access points now extends to identity-ensuring consistent visibility, protection, and performance across every branch.

Start Embedding Identity into Your Network Today

Is your network still anchoring trust to connection points instead of identities? Transform your security posture with Cisco Access Manager—delivering zero-trust protection without complexity. For additional information, visit <.....>

P0217080105 11/25