



Cisco Access Manager for Secure Hospitality Operations

96%

Of hoteliers are investing in
contactless tools and
IoT endpoints

79%

of hoteliers report a positive
business impact from AI.

65%

Of travelers want hotel technology
to be more advanced than
technology in their homes.

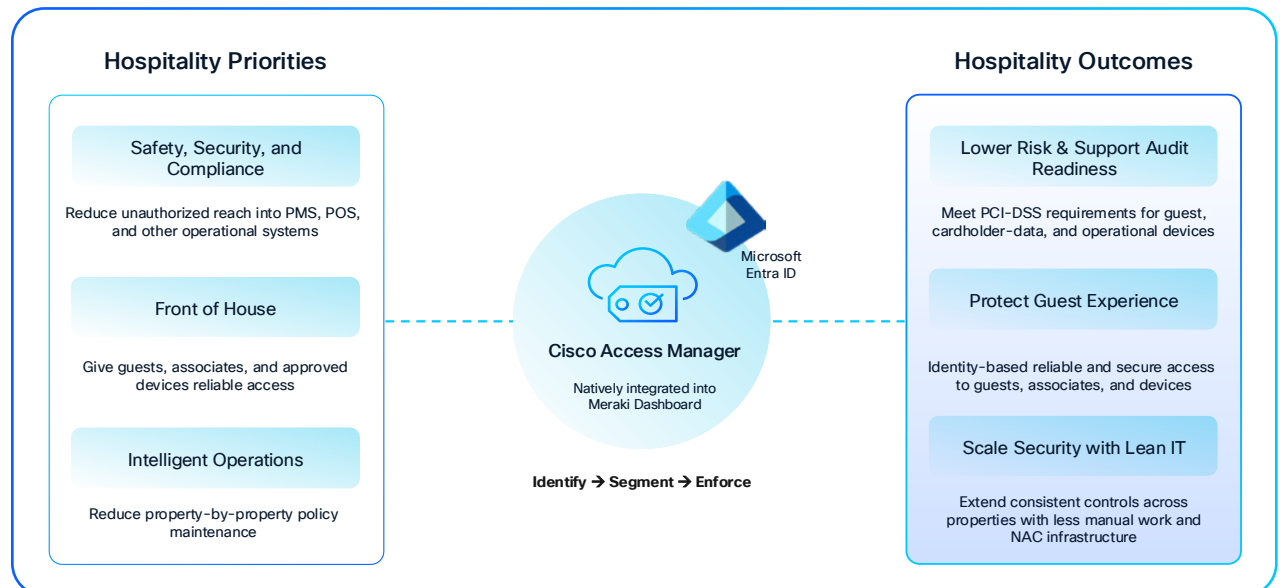
Key Benefits

1. **Protect guest service and revenue-critical operations.** Control network access to PMS, POS/payment, reservations, guest data, and building systems based on user and device context.
2. **Apply consistent policy across your property portfolio.** Extend identity-based access across supported Meraki networks while reducing property-by-property VLAN and ACL changes.
3. **Keep workforce access aligned.** Use context from Microsoft Entra ID to apply the right network access as seasonal associates join, change roles or properties, and leave.
4. **Reduce risk from connected property devices.** Apply appropriate access to shared endpoints, smart-room controllers, cameras, sensors, facilities systems, and other IoT.
5. **Reduce NAC complexity and overhead.** Deliver identity-based access as SaaS in the Meraki Dashboard without separate NAC appliances, external RADIUS servers, or dedicated policy infrastructure.

Protect every property without slowing service

Every check-in, payment, room-service request, and connected guest-room experience depends on property systems remaining available and secure. Protecting those systems becomes more difficult as seasonal associates join, vendors service equipment, staff move between properties, and smart-room and facilities devices come online. Property-specific network rules can drift over time, creating inconsistent policies and broader-than-intended access to PMS, POS/payment, reservation, guest data, and building systems.

Cisco Access Manager addresses this challenge by making identity native to supported Meraki wired and wireless networks. Delivered as SaaS in the Meraki Dashboard and powered by Cisco Identity Services Engine, it uses identity, role, device, and network context—including Microsoft Entra ID roles and groups—to determine what each connection can reach. Hospitality IT and security teams can apply consistent policy across properties, reduce lateral movement, support PCI-DSS requirements, and keep access aligned with workforce and device changes—without slowing guest service.



Make identity part of every connection

Access Manager helps you:

- Translate workforce roles into network access. Use Microsoft Entra ID roles and groups to update access as associates join, change roles or properties, and leave.
- Support diverse devices. Authenticate corporate, shared, and operational devices with EAP-TLS, EAP-TTLS, identity PSK, and MAC Authentication Bypass.
- Segment by purpose and risk. Use VLANs, group policies, and Security Group Tags where supported to limit network access to PMS, POS/payment, guest networks, and building systems.
- Scale consistent policy. Reduce property-by-property VLAN and ACL administration.
- Gain unified visibility. See who and what connects across supported infrastructure from the Meraki Dashboard.

Unlike infrastructure-heavy NAC deployments, Access Manager is a cloud-native service optimized for Meraki. It removes the need to deploy and maintain separate NAC appliances, external RADIUS servers, and a dedicated policy-management environment.

Strengthen access across your property portfolio

See how Cisco Access Manager can help protect guest service and property operations with consistent, identity-based access across supported Meraki networks. Explore the product, request a demo, or start a trial at <https://www.cisco.com/site/us/en/products/security/access-manager/index.html>.

