

Cisco Cloud Networking Innovations

Kevin van Hengel
Solutions Engineer Enterprise Networking



June 23, 2026

Topics

- **Platform**
 - **Innovations**
 - **AI Assistant**
 - **Agentic Workflows**
 - **AI Canvas**
 - **Cloud Control**
- **MX/Secure Routers**
- **Cloud Wireless**
- **Switching**
- **MV & MT**
- **Access Manager**

Platform

Simple, Unified Management Platform

Platform

Management

Assurance

API

AgenticOps

Hardware



Smart
Switches



Secure
Routers



Scalable
Wireless



Industrial
IoT

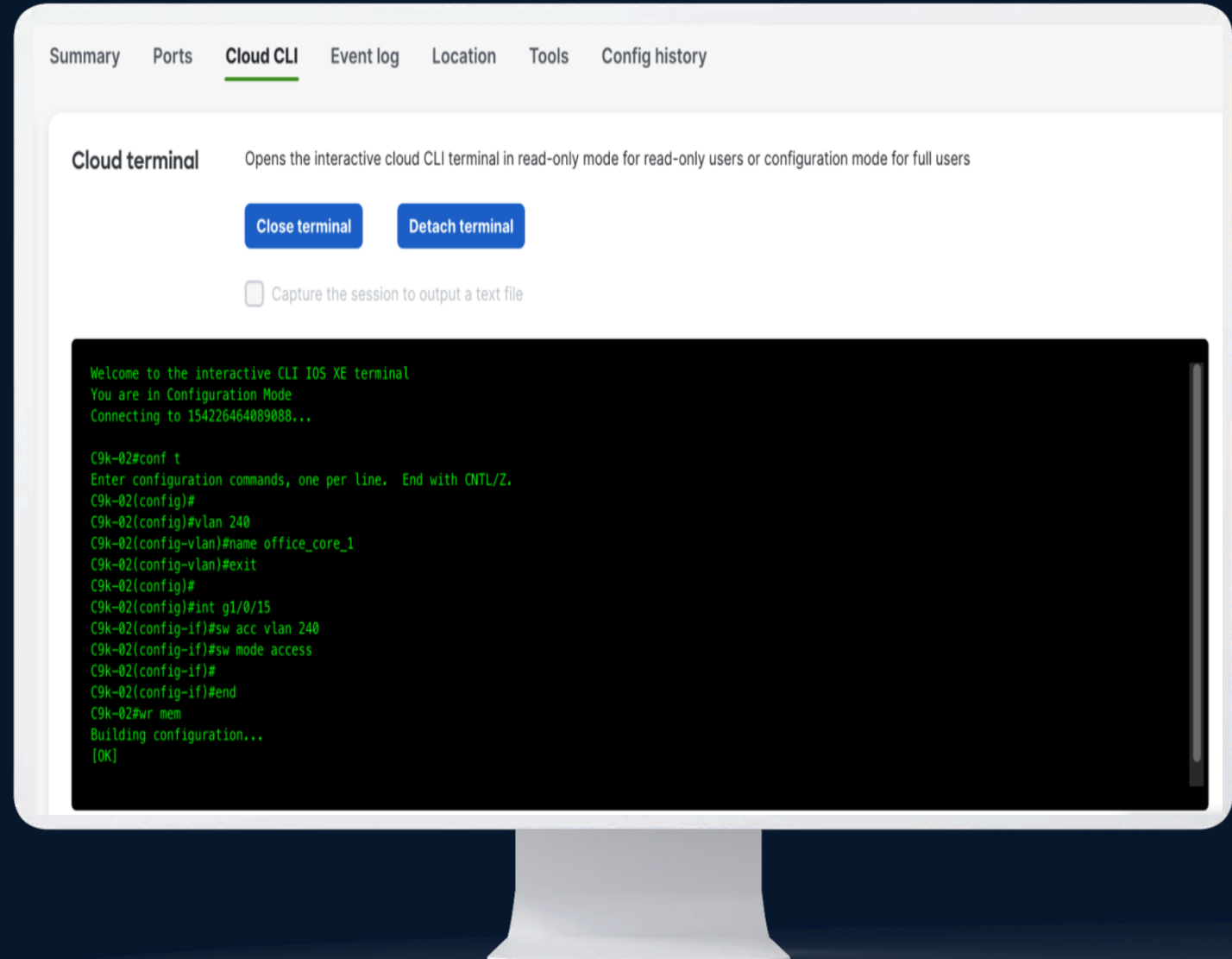
Platform Innovations

You asked for CLI?

Troubleshoot and fix problems quickly

Reduce administration context switching

Access CLI securely from anywhere you can access Dashboard

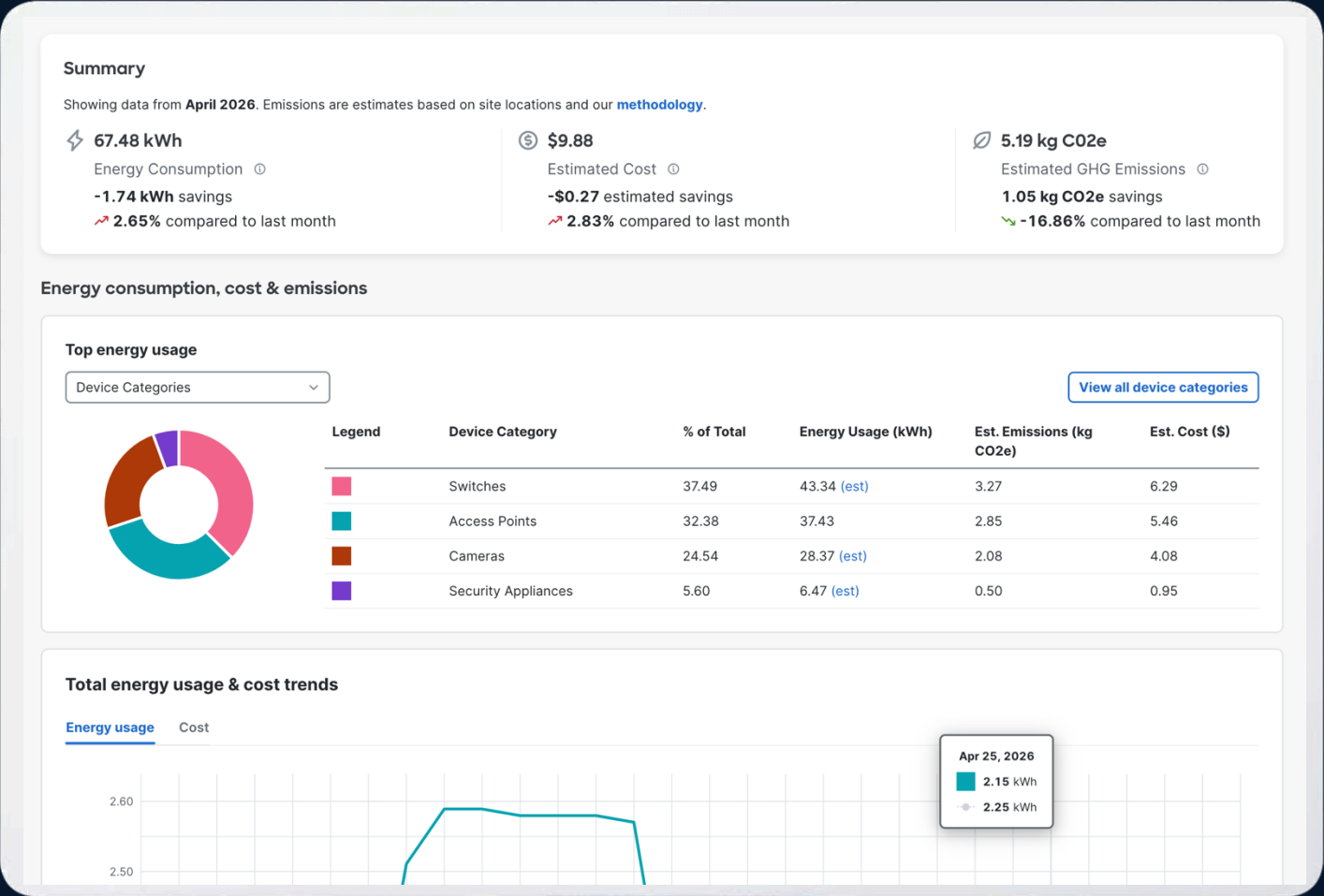


Energy Management?

Overview Summary

Breakdown by device category

Trends and cost estimates



Lifecycle Planning

Alerts

End-of-Sale Dates

End-of-Support Dates

Inventory

View deployed and available devices in your organization, or claim new devices. After selecting devices, you can add to a new or existing network.

×

Networks at Risk: Networks with Hardware and Licensing Alerts

Collapse to hide the details

✖

45 devices

are past the end of support date.

⚠

31 devices

will reach their end of support within the next year.

i

244 devices

have published end of sale dates.

Q Search inventory

Deployment status

2790 devices

Download

+ Claim devices

☐	Cloud ID	Network	Model	Claimed on (UTC)	Order number	End of sale	End of support	
☐	Q3EJ-LD6J-KRNN	San Francisco Decommissioned	MS390-48UX2	Jul 9 2020 15:18	4C4375723	Feb 12 2025	Apr 3 2032	
☐	Q3EJ-KYZU-2D3J	San Francisco Decommissioned	MS390-48UX2	Jul 9 2020 15:18	4C4375723	Feb 12 2025	Apr 3 2032	
☐	Q3EJ-9EMN-FSD8	San Francisco Decommissioned	MS390-48UX2	Jul 9 2020 15:18	4C4375723	Feb 12 2025	Apr 3 2032	
☐	Q3EJ-94UK-N6D4	—	MS390-48UX2	Jul 9 2020 15:18	4C4375723	Feb 12 2025	Apr 3 2032	
☐	Q3EJ-8TZU-ZYG2	San Francisco Decommissioned	MS390-48UX2	Jul 9 2020 15:18	4C4375723	Feb 12 2025	Apr 3 2032	
☐	Q3EJ-8JTL-XPXK	San Francisco Decommissioned	MS390-48UX2	Jul 9 2020 15:18	4C4375723	Feb 12 2025	Apr 3 2032	

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


Cisco Confidential

RBAC Custom Roles

Custom read / write access
for combined networks

Supports Security & SD-WAN,
Switching & Wireless

Custom roles can be integrated with
SAML single-sign-on for scalability and
just-in-time user provisioning

← Administrators

Create custom role

Define permissions for custom access

✓ Basic information

2 Permissions

3 Summary

Set your permissions

Assign roles to organization, networks or tags.

Resource	Description	No access	Read only	Read & write
Security & SD-WAN	Access to monitoring and configuration settings for all security & SD-WAN appliances deployed in this organization	☒	☐	☐
Switching	Access to monitoring and configuration settings for all switches deployed in this organizations	☐	☐	☒
Wireless	Access to monitoring and configuration settings for all access points deployed in this organizations	☒	☐	☐

Cancel

All changes saved

Back

Review role summary

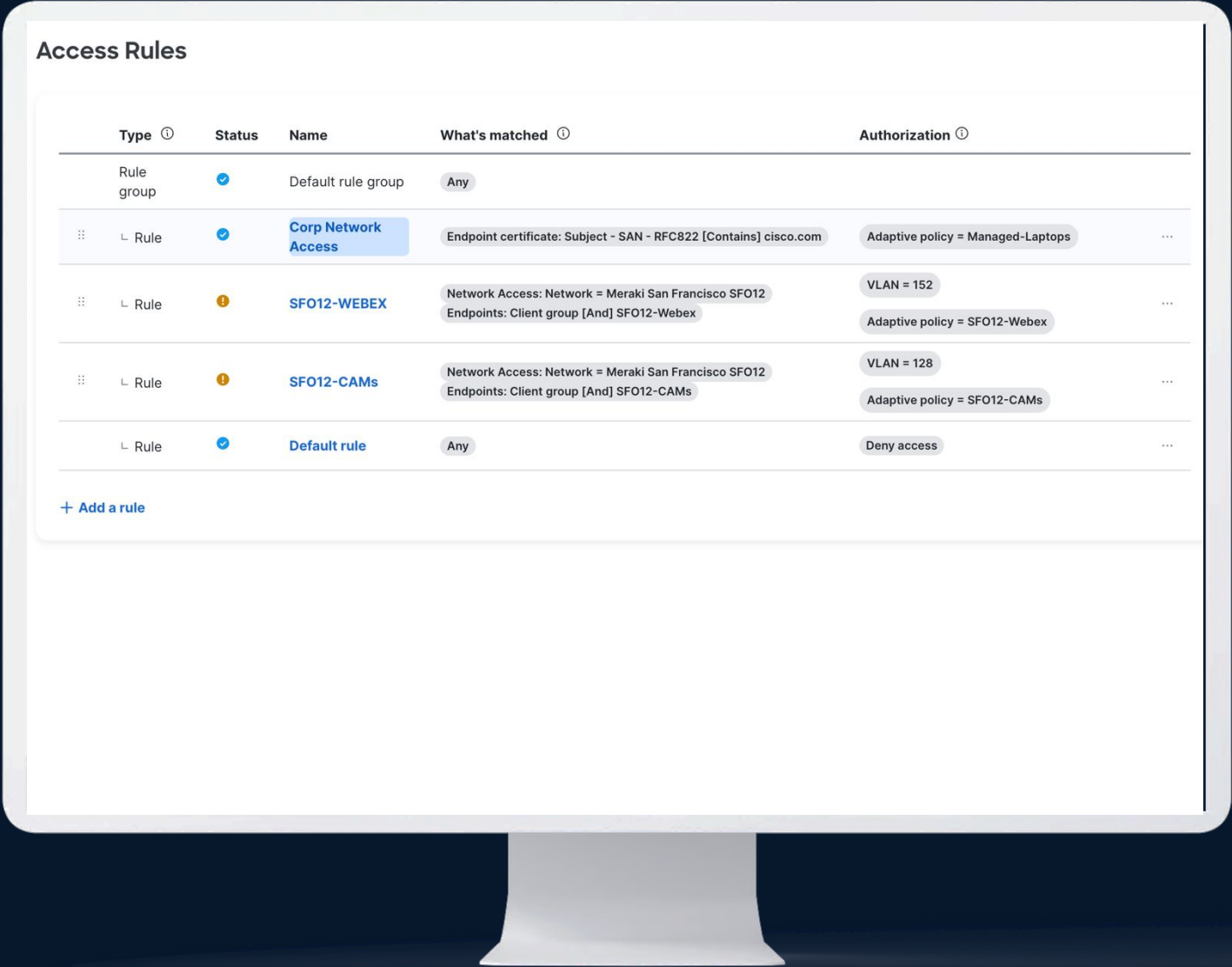
Give Feedback

Access Manager

Cloud-native Network Access Control (NAC)

Secure 802.1x (certificate or username/password auth) and non-802.1x clients with MAC Authentication Bypass

Native integration with adaptive policy for end-to-end SGT segmentation



Experience Metrics (XM)

Meraki: Early Access soon

Essentials

Real-time User Experience Monitoring

Continuously track and analyze user experience in real-time.

Correlation Analysis

Link experience degradation to service health, infrastructure status, and client-specific anomalies.

Key Experience Metrics (XMs)

Monitor essential metrics such as Time to Connect, Successful Connects, Channel Availability, and Coverage.



Infrastructure Health

Meraki: Alpha in June

Essentials

Correlate User Impact

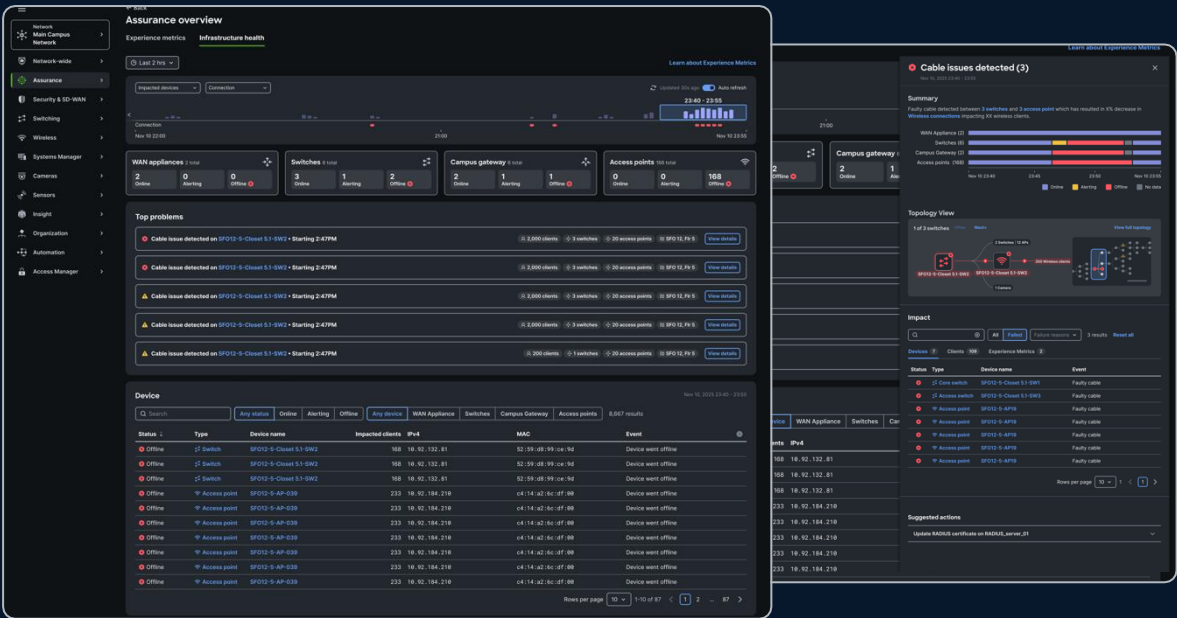
Link reported issues with network components to understand user impact.

Identify Degradation

Analyze performance across wireless, wired, and routing protocols to detect degradation.

Determine Root Cause

Assess if infrastructure health is the ultimate source of the problem.



Today

UX in progress
Wireless, Switch PMs
capturing key KPIs to include

April

In development

June (Alpha)

Integration with XM workflow
Standalone infrastructure health
page focused on device (physical)
health

Introducing AI Packet Analyzer

Meraki: Early Access Available
Catalyst Center: 3.3.1*

Advantage

Automatically seizes the moments of client failure and uploads PCAP files to the AI cloud

Quickly analyzes PCAPs with AI summary

Isolates fault with reasoning view or visually with packet flow view

Actionable recommendation provided to resolve issue

The screenshot displays the Meraki AI Packet Analyzer interface. The top navigation bar includes the Meraki logo and a search bar. The left sidebar shows network management options: Network (Welcome2Helz), Network-wide, Assurance, Security & SD-WAN, Switching, Wireless, Cameras, Organization, and Automation. The main content area is divided into three sections: **Intelligent Capture** (with tabs for New capture, Stored captures, Scheduled captures, and Proactive), **Summary** (AI-generated, Complete PCAP analysis), and **Reasoning** (AI-generated, Complete PCAP analysis). The **Summary** section provides a detailed analysis of a client connection issue, mentioning an invalid PMKID and signal strength improvements. The **Reasoning** section explains the frames involved (21-35: Action Frames, 28-33: ARP, 36-37: DNS) and suggests actions to resolve the issue, such as checking for fast roaming misconfiguration or stale key cache entries. The **Packet Capture** section shows a table of captured packets with columns for No., Time, Source, Destination, and Transmitted. The interface also includes a 'Find in Menu' search bar and a 'Done' button in the bottom right corner.

AI Summary

Reasoning

Packet Capture

Remediation suggestion

Synthetic Testing for Meraki

Meraki: Alpha in May

Essentials /
Advantage (tbd)

Detect Anomalies Early

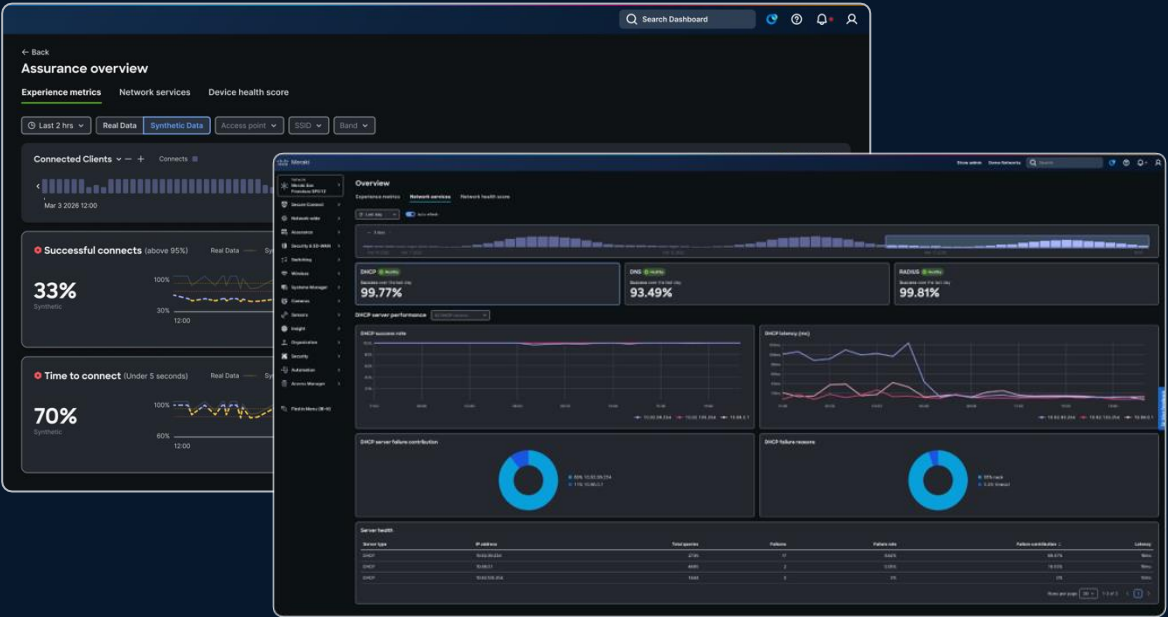
Identify issues through simulated user journeys and network conditions before real users are impacted.

Validate Passive Insights

Corroborate findings from passive monitoring with active testing to confirm the scope and nature of potential problems.

Determine Blast Radius

Quantify the extent of an issue's impact across different user segments or services.



Today

May (Alpha)

July (Beta)

TBD (GA)

UX in progress
Data integration in progress

Integration with Network Services
Support for DNS, DHCP tests

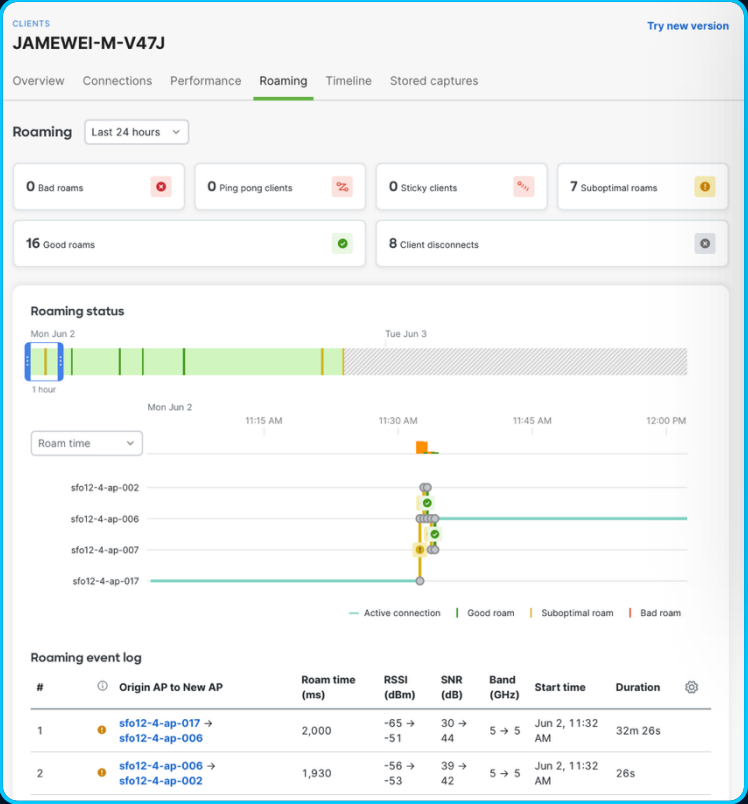
Support for RADIUS tests

Support for over the air tests

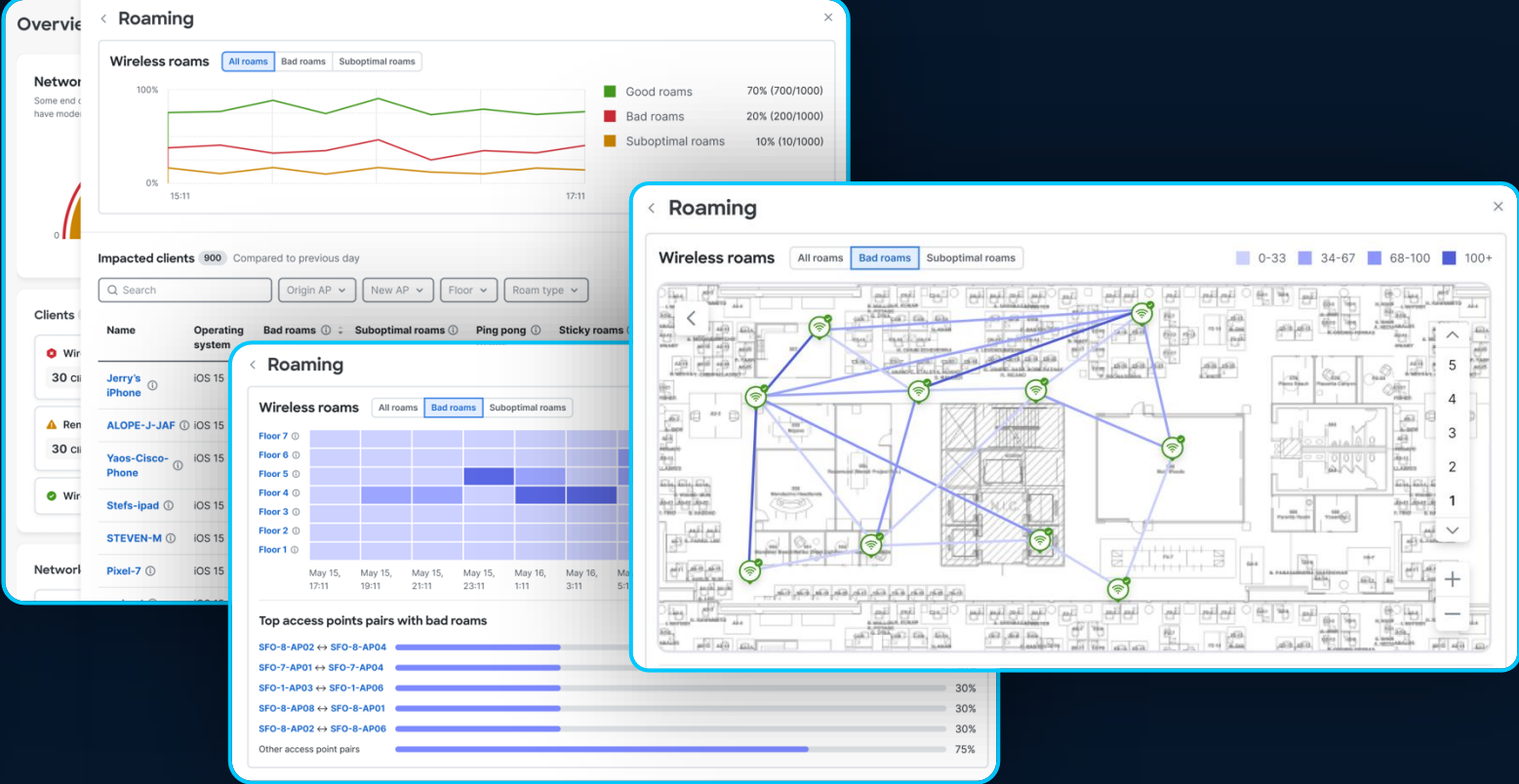
Roaming Analytics

Meraki: available

Essentials



Per-Client Roaming Timeline



Network-wide Roaming Health

Introducing AI Configuration Recommendations

Meraki: Early Access Available

Advantage



AI network optimization

- Assesses readiness - network and client
- Predicts before-and-after performance improvements
- Suggests better configuration recommendations for performance and security improvements



Types of recommendations

Available

- WPA3/6-GHz upgrade
- 802.11r enablement
- Flexible Radio Assignment

Coming Soon

- Coverage hole mitigation
- Transmit power range optimization
- 5-GHz band and channel list optimization

< i Enable 802.11r

i Active

Reduce roaming delay by upto **69%** on eligible SSID(s)
KR-091-PUS01

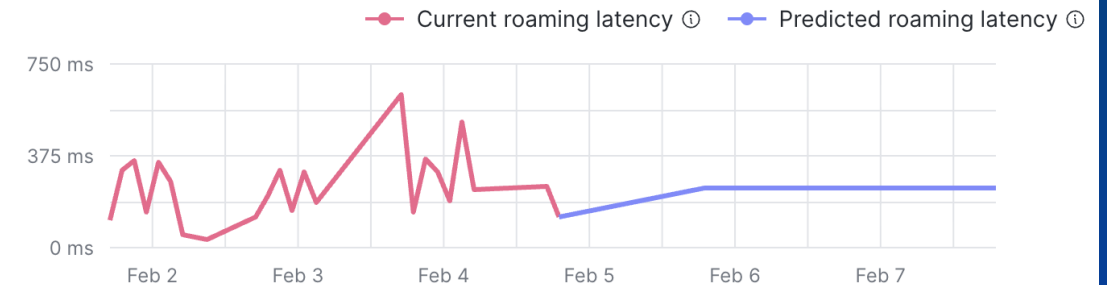
Suggested actions [Details](#)

Predicted roaming latency after changes

To view individual SSIDs and data visualizations, select an SSID below.

All SSIDs

i **Prediction: 67% roaming performance improvement** on 802.11r enabled network



AI Assistant for Networking

AI Assistant Capabilities

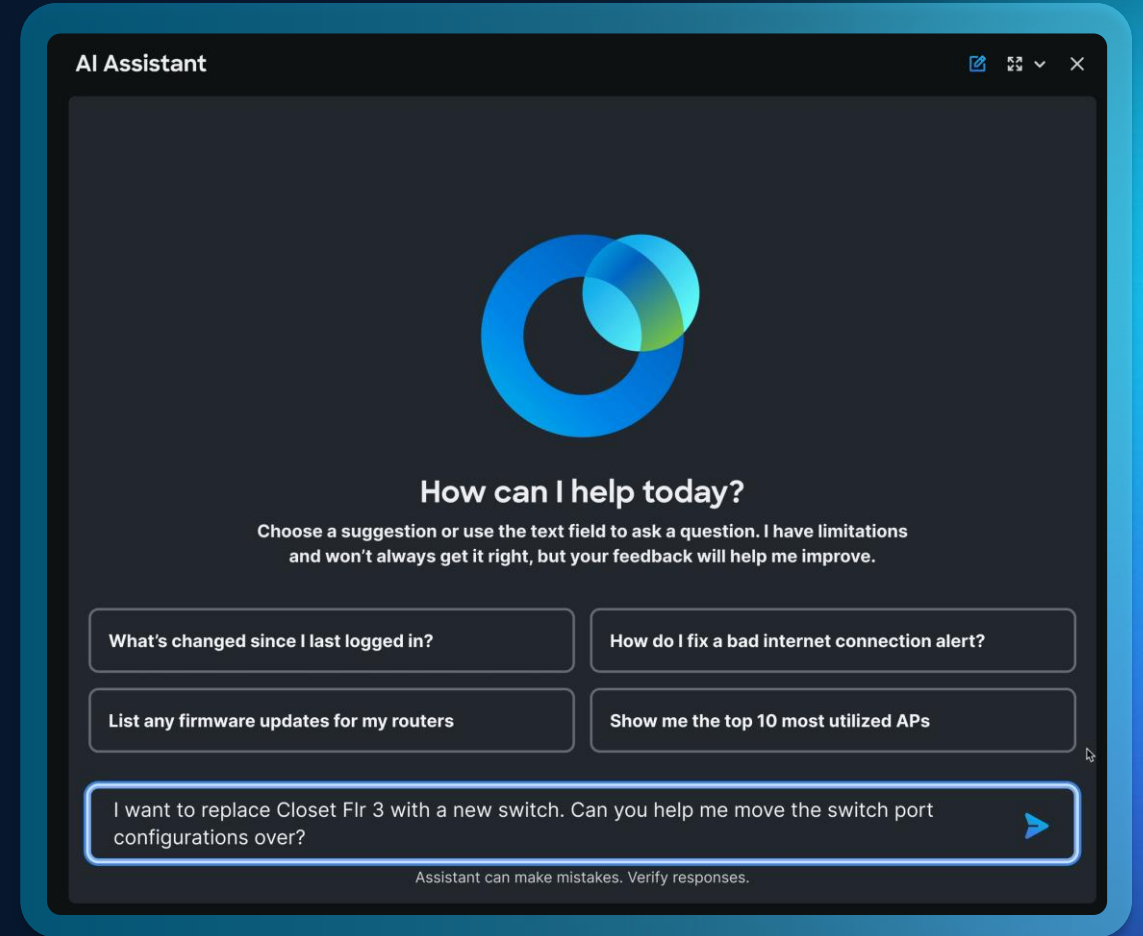
Quick recap of current capabilities

Seamless monitoring, troubleshooting, and Configuration changes across Cisco Networking Products

- | Ask, explore, and act in natural language
- | Use cases for monitoring, troubleshooting, configurations, and Support Case submission
- | Common architecture for Cloud and On-Prem

Meraki GA

Catalyst Center GA



Default Mode Use Cases

AI assistant usage is broad, beyond just troubleshooting

Client and Device Insights (27%)

- “Provide a full list of all connected clients”
- ”List clients currently connected to 2.4Ghz”
- “Show me switches that rebooted today”

Policies and Configuration (23%)

- “List the access policies for the network”
- ”How do I configure root bridge?”
- “I want to create a network using workflow”

Troubleshooting (22%)

- “Why is my wifi slow?”
- ”Troubleshoot AP "X”
- “Troubleshoot client Local Server”

Network Overview (22%)

- “Show me networks with issues”
- ”Show my WAN port usage for network”
- “Whats the VPN status for my network?”

Deep Reasoning Use Cases (sample list)

Deep Reasoning is positioned to deliver a broad set of use cases



Network Audit

Proactive

- Security Audit



Wireless Optimization

Proactive

- Wireless / Channel Planning



Capacity Planning

Proactive

- Capacity planning (WAN, PoE, DHCP)



Security & Changes

Investigative

- Compliance to standards (NIST, PCI)



Alerts & Events

Reactive

- Critical Alerts



Troubleshooting & RCA

Reactive

- App down (Wireless, Switching, WAN)

- Multi-domain triage in a single session
- Networking runbooks (Cisco specific knowledge)
- API driven – suggestions and conclusions backed by network data
- Transparent reasoning steps for explainability
- Remediation path (via Agentic workflows)

Agentic Workflows

AVAILABLE

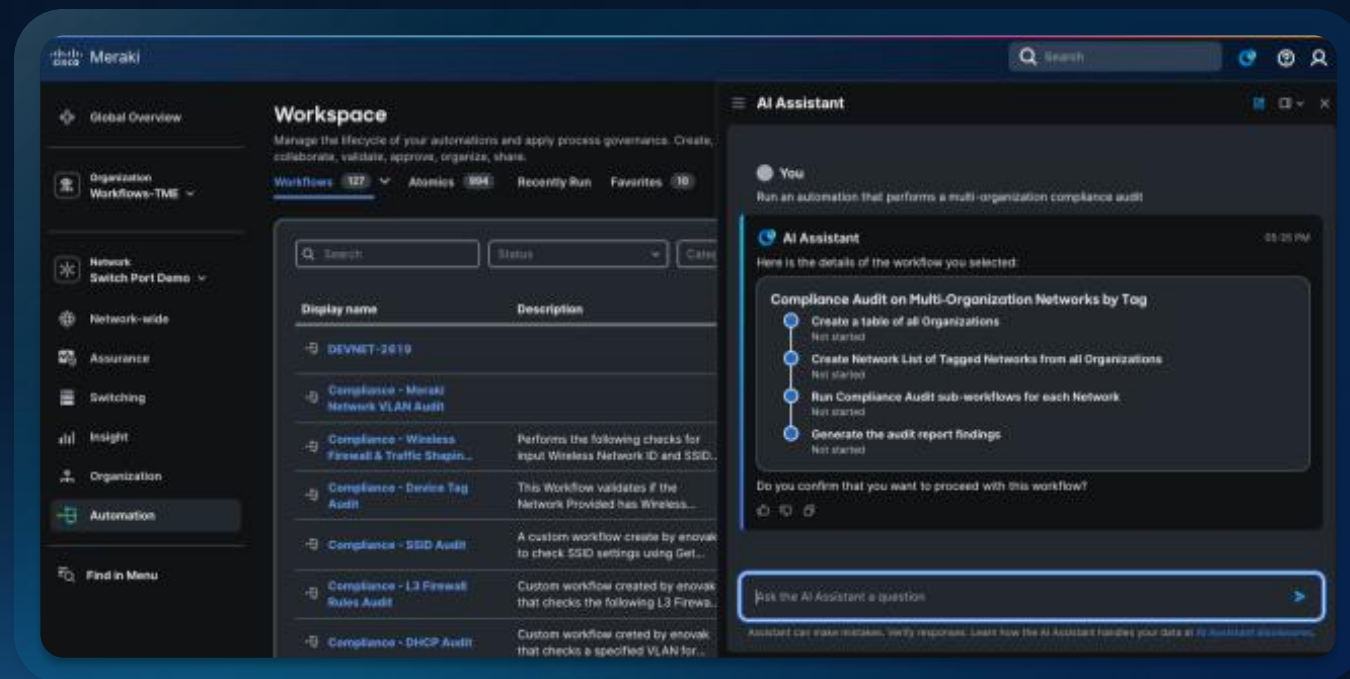
Agentic Workflows

Agentic automation across cloud and on-prem deployments

AI-powered automation natively in the Meraki dashboard

Leverage built-in AI Assistant integration for agentic operations

Automate workflows across Meraki, Catalyst Center, Catalyst SD-WAN Manager, ISE, Nexus, and more



Site turn-up & change execution

Fleet visibility, risk & readiness

Natural Language Workflow Generation

You

Generate a Workflow that moves ports from a Meraki Switch into a secure VLAN called, "Quarantine".

User MUST provide the following:

- Meraki Switch Serial Number containing the switch ports
- The user will provide a string of ports in this format: 1,2,4,7-8

Output Variables

- Return an output variable in Markdown with a Table Summary of only the matching networks found.
- The Table Columns should be PortID, Name, Original VLAN, New VLAN

Constraints

- This VLAN should already exist. If it doesn't, end the workflow and indicate
- In order to understand which ports,
- Expand the Ports from ranges into individual values and store them in a Table.
- Loop over the table and Update Device Switch Port using each PortID from the Table and assign to the VLAN ID of "Quarantine".

AI Assistant

01:29 PM

You have requested to generate a workflow plan. It can take several minutes to complete. Do you want to proceed?

You

yes

AI Assistant

01:29 PM

Organizing input

Intent

Distinct Inputs

Required Output

Constraints

Natural Language Workflow Generation

Iterative development:

- Add Step(s)
- Change Step(s)
- Remove Step(s)

Workflow Plan

Step-by-Step Plan: Move Switch Ports to Quarantine VLAN

This plan outlines the steps to move specified ports on a Meraki switch to a 'Quarantine' VLAN.

Step 1: Expand Port Ranges

- **Action:** Expand the user-provided port string (e.g., "1,2,4,7-8") into a list of individual port IDs.
- **Method:** Engine primitive (JSON parsing/String manipulation)
- **Expected Result:** A list of individual port IDs.

Step 2: Get Device Information

- **Action:** Retrieve device details to find the Network ID.
- **Method:** Workflow: Meraki - Get Device
- **Expected Result:** The ID of the network the switch belongs to.

Step 3: Check for 'Quarantine' VLAN

- **Action:** List all VLANs in the network and check if one is named 'Quarantine'.
- **Method:** Workflow: Meraki - Get Network Appliance VLANs
- **Expected Result:** A list of VLANs to identify the 'Quarantine' VLAN ID.

Step 4: Validate VLAN Existence

- **Action:** Check if the 'Quarantine' VLAN was found.
- **Method:** Engine primitive (Condition)
- **Expected Result:** Proceed if VLAN exists, otherwise end the workflow with an error message.

Step 5: Process Each Port

- **Action:** Iterate through the list of ports and update each one.
- **Method:** Engine primitive (Loop)
- **Expected Result:** All specified ports are processed.

Step 5a: Get Current Port Configuration

- **Action:** Retrieve the current name and VLAN of the port.
- **Method:** Workflow: Meraki - Get Device Switch Port
- **Expected Result:** Current configuration details for the summary report.

Step 5b: Update Port to Quarantine VLAN

- **Action:** Assign the port to the 'Quarantine' VLAN.
- **Method:** Workflow: Meraki - Update Device Switch Port
- **Expected Result:** Port updated to the secure VLAN.

Step 6: Generate Summary Report

- **Action:** Create a Markdown table summarizing the changes.
- **Method:** Engine primitive (Formatting)
- **Expected Result:** A table showing Port ID, Name, Original VLAN, and New VLAN.

Plan Summary:

- Total Steps: 6
- Risk Level: Medium (Configuration change on switch ports)

Would you like me to generate a workflow JSON from this plan? If you would like to refine this plan please supply me with instructions on how you would like to change it.

Workflows Role Based Access Control (RBAC)

Features

Security & SD-WAN

Core Security

Firewall

Controls network traffic and enforces security policies through firewall rules.

Threat protection

Detects and mitigates security threats through configurable protection mechanisms.

Content filtering

Restricts or allows web content using URL and category-based policies.

Other features

Monitoring and visibility, access integrations and control, VPN, routing and traffic management.

Wireless

Switching

Workflows

Organization only

Save

Cancel

Selected permissions

--None--

--None--

Deny

Read-Only

Write

Deny

Read-Only

Write

Deny

Read-Only

Write

--None--

--None--

Execute

--None--

Deny

Read-only

Write

Execute

AI Canvas

A man and a woman are working at a desk in a dimly lit office. The man, wearing glasses and headphones, is pointing at one of several computer monitors. The woman, also wearing glasses, is looking at the same monitor. The desk is cluttered with multiple monitors, keyboards, and a desk lamp. The background shows other office equipment and a window with a view of the outside.

The Familiar *Pain Points*

Too many consoles | Too many alerts | Not enough context
Automation needs babysitting | Troubleshooting starts with “*Where do I look?*”

AI Canvas

Where work gets done

Ask anything

Natural language queries across your entire Cisco portfolio and beyond.

Let agents do the work

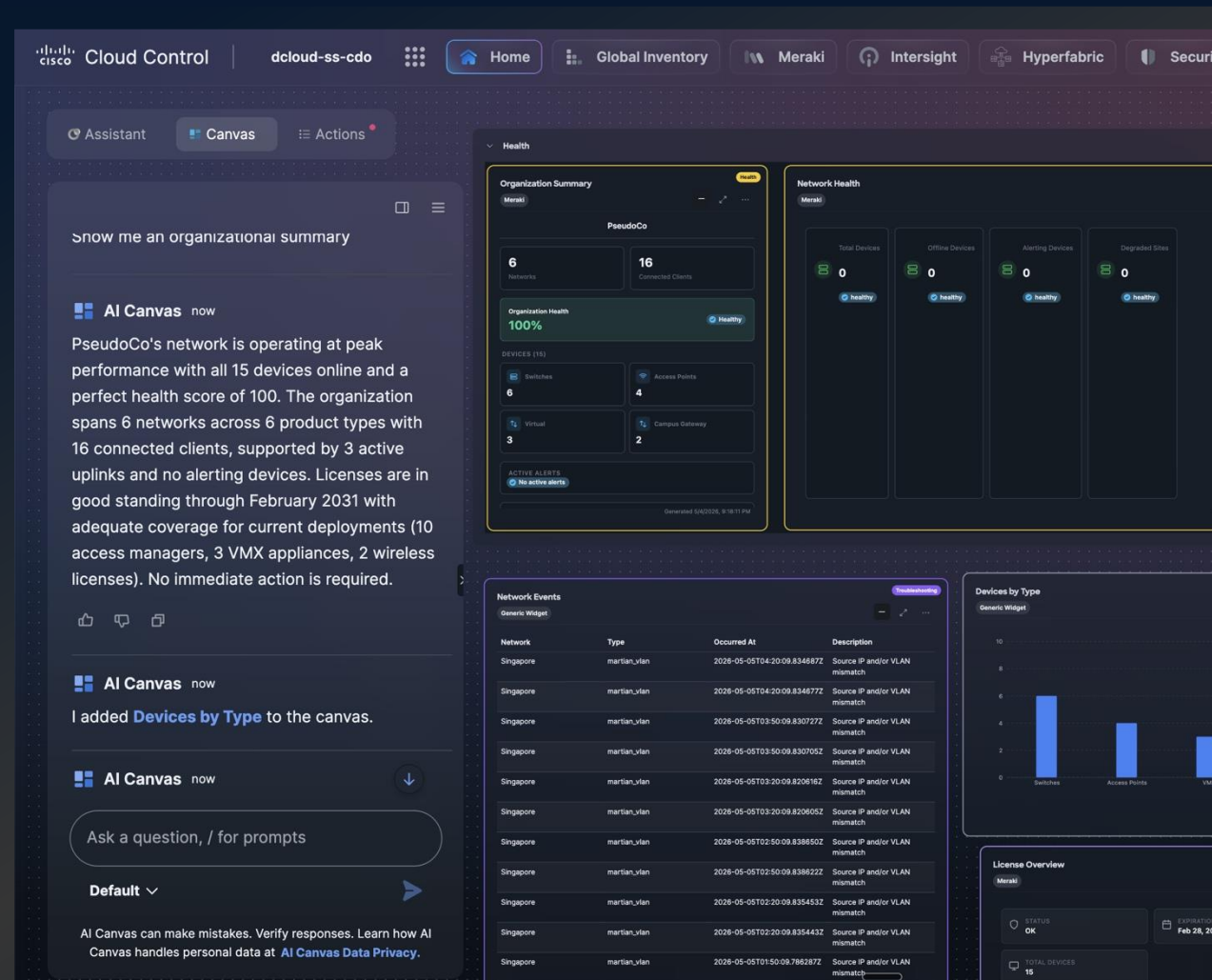
Agents plan, pull data, execute, and resolve end-to-end.

Collaborate live

One shared session. Every teammate sees the same view.

Never lose context

Every handoff, every shift change, every escalation – context stays intact.



Inside AI Canvas

A workspace purpose-built for the operator

Conversational interface

- Ask questions in natural language
- Watch agents reason live

Bring your context

- # to reference your upload docs
- + to attach an image for multi-modal reasoning

Agentic Modes

- Default for fast answers
- Reasoning for deep investigations

Widgets

- Visualize topologies, charts, summaries, reports
- Drill into supported widgets to investigate further
- Export widgets as PDF

Multiplayer

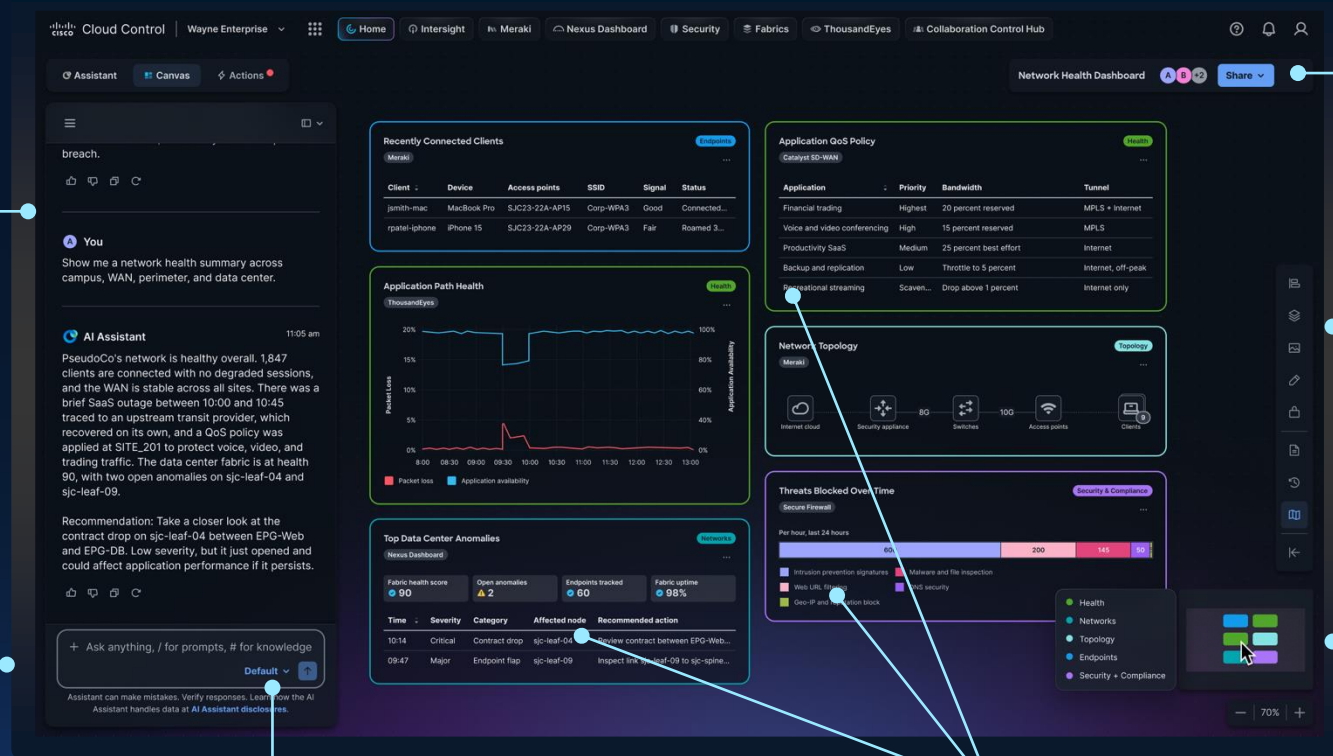
- Share the board via link
- Everyone sees the same view

Usability

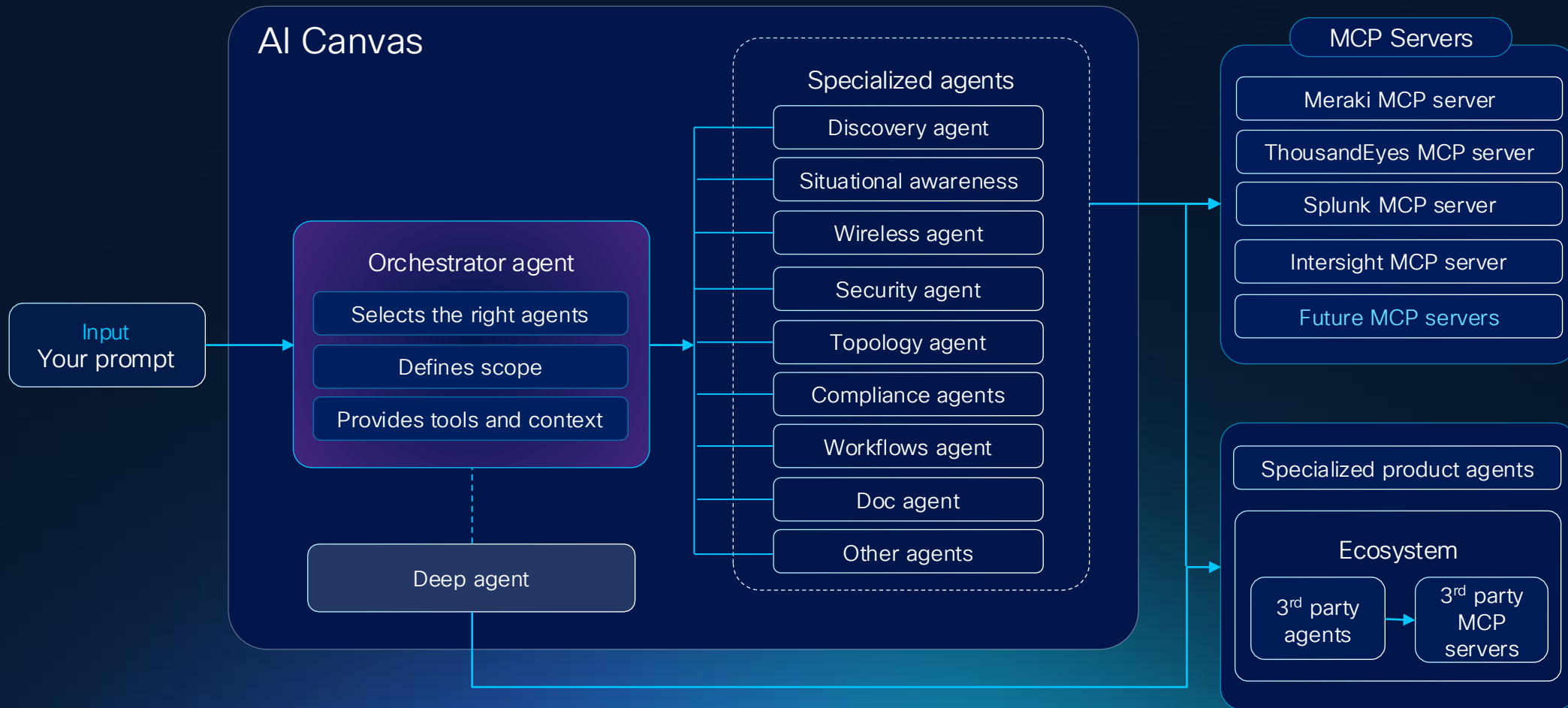
- Annotate, generate reports, activity timelines, group widgets, and more

Board Organization

- Widgets color coded by category
- Mini-map for ease of navigation

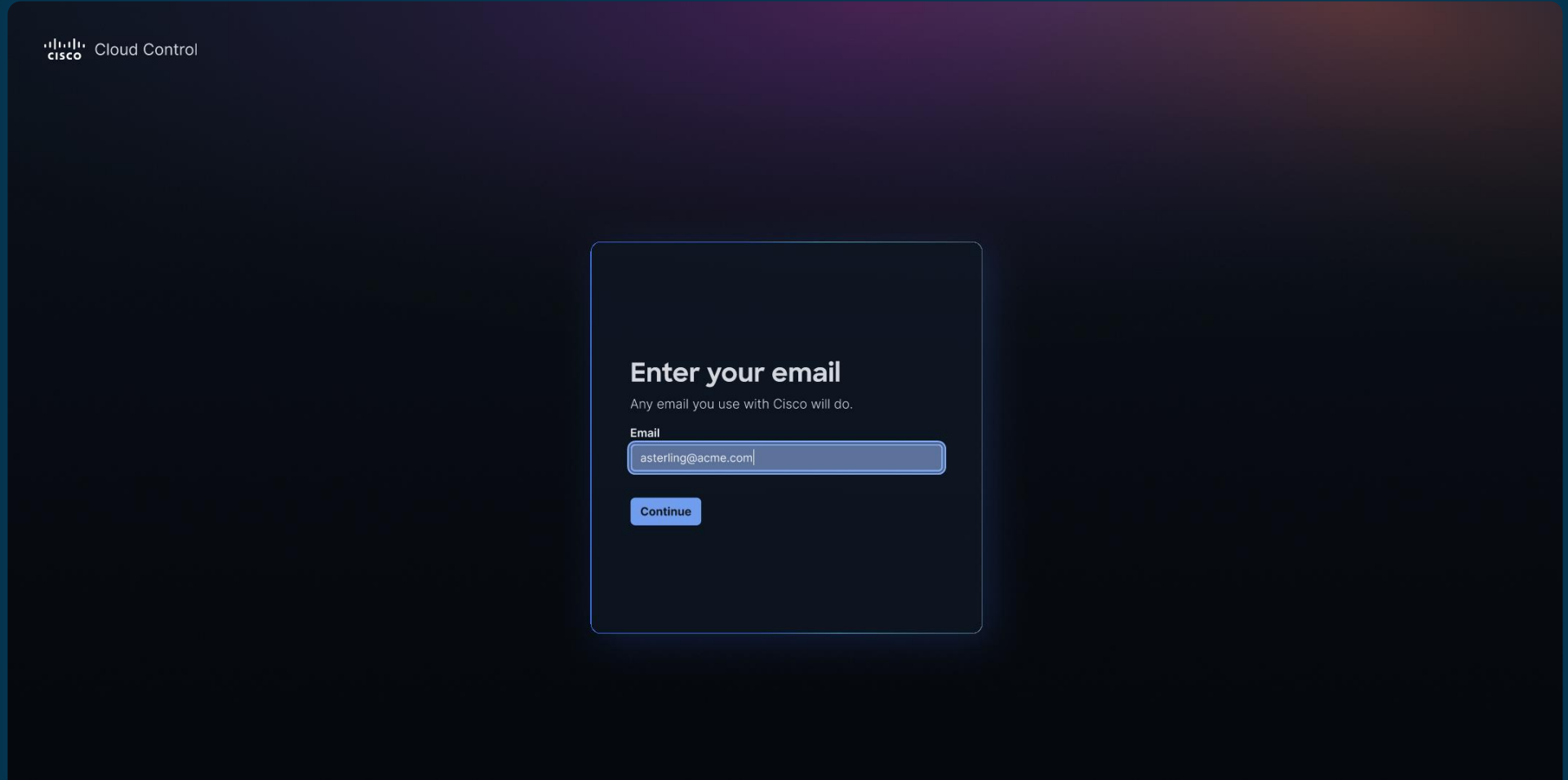


Architecture | AI Canvas orchestration



Cisco Cloud Control

One sign on, **one time.**



The screenshot shows a dark-themed web interface for Cisco Cloud Control. In the top-left corner, the Cisco logo is followed by the text "Cloud Control". The main content area is a dark rectangle with a subtle gradient. Centered within this area is a white-bordered box containing the sign-on form. The form has the heading "Enter your email" in bold, followed by the instruction "Any email you use with Cisco will do." Below this is a label "Email" above a text input field. The input field contains the email address "asterling@acme.com". At the bottom of the form is a blue button labeled "Continue".

Cloud Control

Enter your email

Any email you use with Cisco will do.

Email

Continue

Meet Cisco Cloud Control

The unified interface for AgenticOps



Cisco Cloud Control

The power of one

One login

Sign in once. See everything.

One inventory and topology

Every asset. See how it all connects, in real time.

One view for alerts

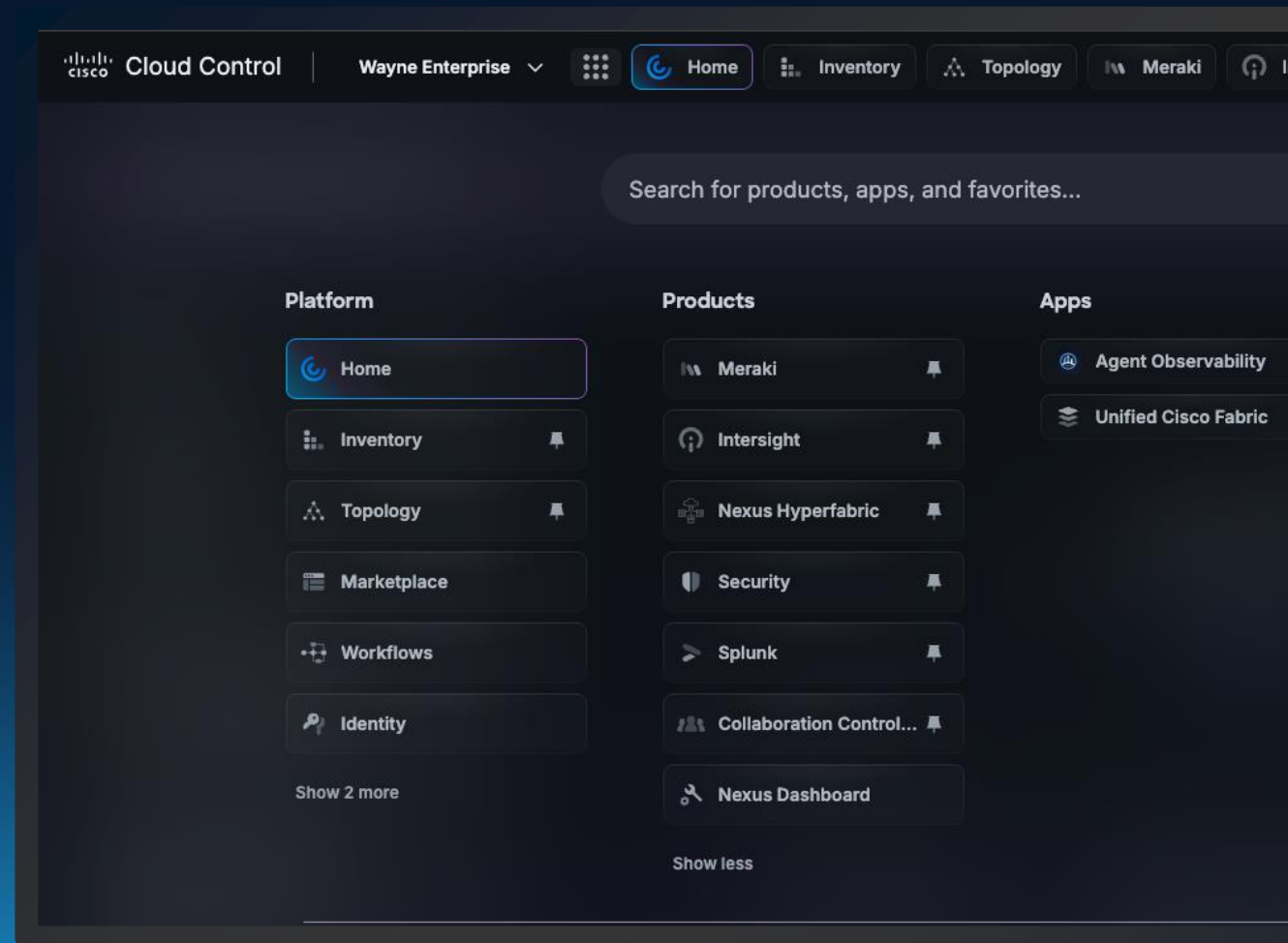
Actions correlates alerts across every product.

One assistant

Quick answers and tasks with AI Assistant.

One agentic workspace

Investigate, execute and resolve with AI Canvas.



Alerts and notifications

Correlated issues, ownership and action tracking

Troubleshoot in AI Canvas

Bring alert context into a workspace. Begin investigating.

Lifecycle states

The same across every controller – New, Read, Active, Snoozed, Dismissed, Resolved

Filter & sort
By alert severity and assignee.

Correlated by what matters

IP, site, MAC, time, device serial, and CVE/PSIRT ID.

Ask follow-ups

Ask questions, for clarifications or explanations of the alert.

The screenshot displays the Cisco Cloud Control interface. The top navigation bar includes 'Cloud Control', 'Wayne Enterprise', and various tool icons like Home, Inventory, Topology, Meraki, and Intersight. The main content area is titled '[MOCK] Critical wireless onboarding failures in Catalyst infrastructure'. It features a 'Critical Alert' status, a timestamp 'Today, 9:22 PM', and an 'Unassigned' assignee. Below this, there's a section for 'Related alerts' with a table listing products, titles, descriptions, and event times. The table has columns: Product, Title, Description, and Event time. The first row shows 'Catalyst Center' with the title 'Multiple wireless onboarding failures' and a description 'Affected: London Catalyst wireless infrastructure'. To the right of the main alert, there's a 'Notifications' panel showing a list of alerts with their severity levels (High, Critical, Low) and timestamps. A 'Give feedback' button is visible on the right side of the notifications panel. At the bottom of the main alert area, there's a 'Ask anything' input field with a submit button.

Product	Title	Description	Event time
Catalyst Center	Multiple wireless onboarding failures	Affected: London Catalyst wireless infrastructure	Today, 9:22 PM

The platform

The foundation everything is built on.

Cisco Cloud Control

Integrated products

Meraki

Catalyst Center

Intersight

Nexus Dashboard

Nexus Hyperfabric

Security Cloud
Control

ThousandEyes

Splunk

Catalyst SD-WAN

Collaboration
Control Hub

IQ

AI workspace

AI Canvas

Collaborative agentic workspace

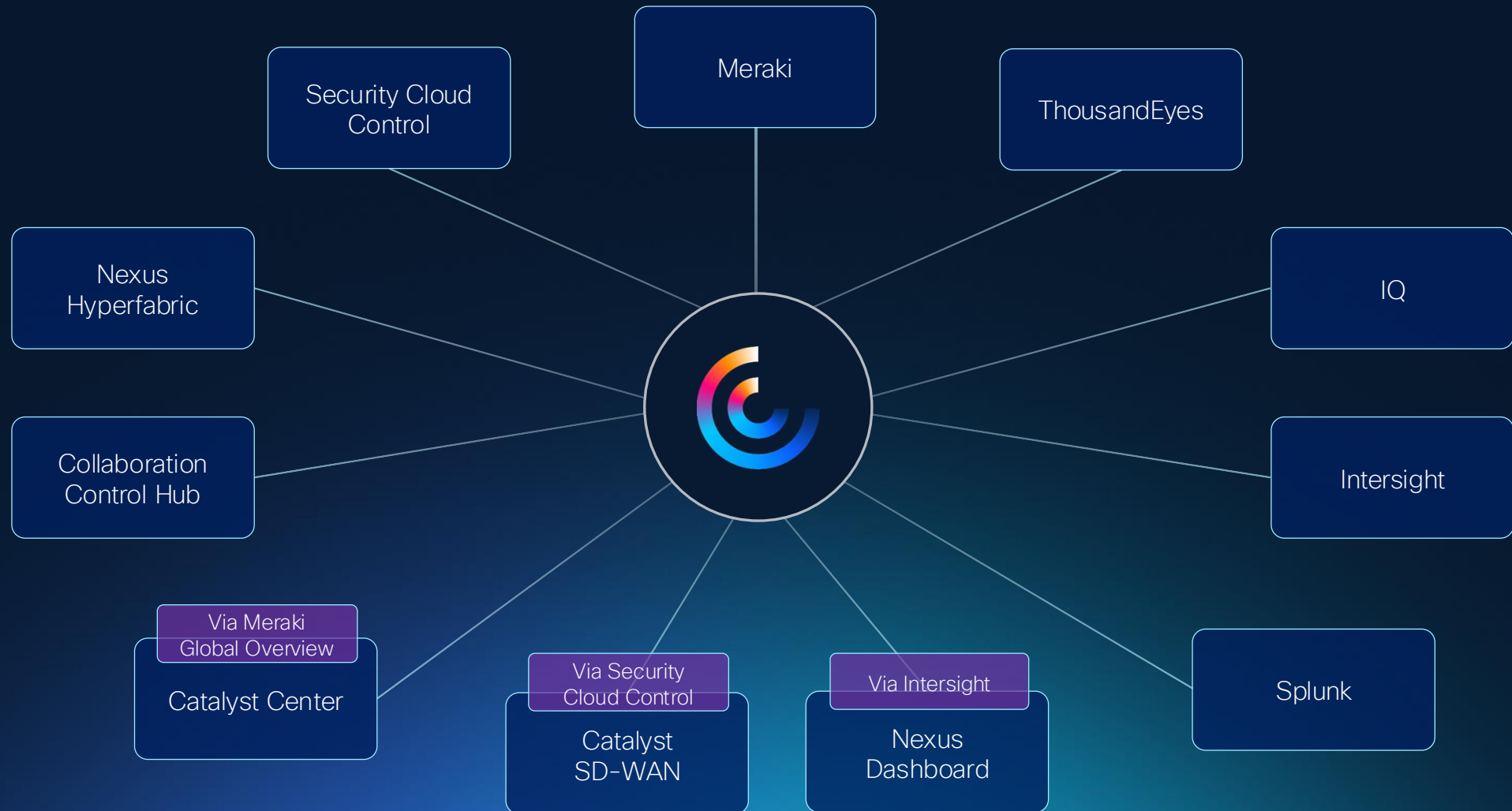
AI Assistant

Conversational entry point

Platform services

- Identity
- Inventory
- Topology
- Alerts
- Licensing

Architecture | How Cisco products connect



One destination. Every domain.

Cisco built the platform
no one else could



MX

Transition to simplified Secure WAN portfolio

Catalyst 8000
ISR 1K/4K
ASR 1K



IOS XE with Routing
and SD-WAN

NEW

Cisco 8000 Series
Secure Router



Taking the best into a
converged portfolio
Continued investment in
IOS-XE and MX OS

Meraki MX



MX OS and
Meraki Dashboard

Secure your network at every size and location

AVAILABLE	AVAILABLE	AVAILABLE	AVAILABLE	AVAILABLE	JUNE 2026
					
Cisco 8100 Series Secure Routers	Cisco 8200 Series Secure Routers	Cisco 8300 Series Secure Routers	Cisco 8400 Series Secure Routers	Cisco 8500 Series Secure Routers	Cisco 8600 Series Secure Routers
Small Branch	Medium Branch	Large Branch	Campus	Data Center	Data Center
IOS XE					
AVAILABLE	AVAILABLE	AVAILABLE	AVAILABLE	AVAILABLE	JUNE 2026
		MX			
AVAILABLE	OCT 2026	JUNE 2026	AVAILABLE	-	-

Cisco 8300 and 8200 Series Secure Routers (MX OS)

Expanding Cisco 8000 Series Secure Routers (MX-OS)

Small Branch
C8111-G2-MX &
C8121-G2-MX
(Ethernet Models)



Threat Protection:
Up to 1Gbps

Small Branch
C8111-G2-MX &
C8121-G2-MX
(Cellular / Wi-Fi Models)



Threat Protection:
Up to 1Gbps

Medium Branch
C8235-G2-MX



Threat Protection:
Up to 2.4 Gbps

Large Branch
C8355-G2-MX



Threat Protection:
Up to 4 Gbps

Campus & Aggregation
C8455-G2-MX



Threat Protection:
Up to 8 Gbps

Available

Orderable Now
(Q4-FY26)

Orderable Soon
(Q2 FY2027)

Launch at Cisco
Live US '26

Available

C8235 Secure Router with MX OS

Faster performance, Improved Scale and PQC Capable



8200 Secure Routers (MX OS)

Supported with Co-Term and Subscription License

Up to **2.4 Gbps** of Threat Protection & 750K Flows**2x UPoE+** with 120W PoE power by default**4 x WAN**** + 6 x LAN ports with UPoE**MX** experience enhanced with VRF, multi-WAN, Improved BGP*

- * Summarization, attributes, communities
- ** 2 x WAN + 2 x LAN/ WAN

C8355 Secure Router with MX OS

Faster performance, Improved Scale and PQC Capable



8300 Secure Routers (MX OS)

Supported with Co-Term and Subscription License

Up to **4Gbps** of Threat Protection & 1-Million Flows

Dual Redundant AC Power Supply with UPoE+

4 x WAN** + 6 x LAN ports with UPoE

MX experience enhanced with VRF, multi-WAN, Improved BGP*

- * Summarization, attributes, communities
- ** 2 x WAN + 2 x LAN/ WAN

C8455 Secure Router with MX OS

Faster performance, Improved Scale and PQC Capable



8400 Secure Routers (MX OS)

Supported with Co-Term and Subscription License

Up to **8Gbps** of Threat Protection & 1.5-Million Flows

Dual (Internal) Redundant AC Power Supply

4 x WAN** + 6 x LAN ports with UPoE

MX experience enhanced with VRF, multi-WAN, Improved BGP*

- * Summarization, attributes, communities
- ** 2 x WAN + 2 x LAN/ WAN

Secure WAN Portfolio Transition

Branch

Small



8100 Secure Router



ISR1000



MX67/68/75

Medium



8200 Secure Router



Catalyst 8200



MX85/95/105

Large



8300 Secure Router



Catalyst 8300



MX250/450

Campus / Datacenter



8400 Secure Router



Catalyst 8500L



Net-New MX
Scale



8500 Secure Router



Catalyst 8500

Cloud



Catalyst 8000V



Cellular



CG522



MG41/E
MG52/E

Cisco Secure WAN Software Innovations & Roadmap - MX

Mar. 2026
26.1

Aug. 2026
26.2

Routing & SD-WAN

- VRFs (multi-release) – Org-wide enablement, VRF-aware AutoVPN, Serviceability
- BGP (multi-release) – independent BGP, outbound communities, explicit outbound advertisements, inbound filtering.
- VPN Exclusions – NBAR-based & Source-based
- NAT Enhancements – overlay NAT, many to many, port forwarding, IPsec NAT

- VRF: Static Routes and eBGP (LAN)
- VRF: Traffic Shaping, Internet Traffic, VPN Traffic, Primary Uplink/Failover/Load balancing (SD-WAN)
- Hub priority selection
- Route table update
- Routed mode IPv6 peer support
- Prefer eBGP routes over AutoVPN

Routing Core & Infra

- N-uplinks – WAN 3-4 support

- High Availability – WAN uplink sharing
- BGP Route Table Enhancement

Cloud

- vMX for Private Cloud (S/M/L) – VMware & KVM support
- vMX for Colocation – Megaport support

Security & SASE

- TrustSec: Security Group Tags (SGT) (multi-release) – Group Policy assignment and VPN transport
- Client VPN – IKEv2 support

- Unified Firewall Rules
- SSL Inspection
- Custom Snort Rules

Dashboard Managed Secure Routers IOS-XE

Ease of Cloud-scale
operations with
enterprise-grade
performance

Unified dashboard for Full Stack Platform Management

The image shows a laptop screen displaying the Cisco Meraki dashboard for an SFO99 Cisco Secure Router. The interface is clean and modern, with a dark blue header bar at the top containing the Cisco and Meraki logos. The main content area is white and features a sidebar on the left with various navigation options. The central part of the screen displays the router's configuration and status, including a 'Summary' tab and a 'Cloud CLI' button. A dropdown menu is open under the 'Security & WAN' section, listing various services and their status. The bottom section shows the WAN configuration with two active connections.

Navigation Sidebar:

- Network SFO99
- Network-wide
- Security & WAN**
 - Switch
 - Wireless
 - Systems Manager
 - Camera
 - Sensors
 - Insight
 - Organization-wide

Router Information:

- SFO99 - Cisco Secure Router**
- Status: Online
- Configuration source: Cloud
- Cloud CLI

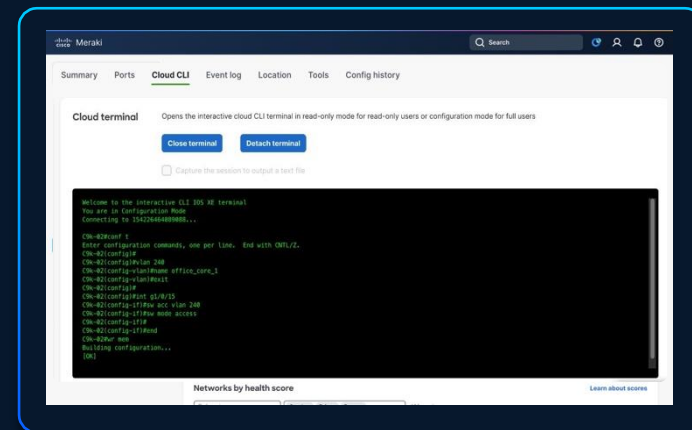
Security & WAN Services:

Service	Status
Monitor	Configure
Appliance status	Addressing & VLANs
Security center	DHCP
VPN status	Firewall
Client VPN status	Site-to-site VPN
	Client VPN
	SD-WAN & traffic shaping
	Threat protection
	Content filtering

WAN Configuration:

WAN	IP Address	Status
WAN 1	124.55.808.233	Active
WAN 2	84.23.422.411	Active

Cloud CLI



Supported Platforms

Cisco Silicon leapfrogs with **2x security performance** and **sustainability**

Powering the **next generation Secure WAN** with NGFW, higher performance interfaces, LEO & 5G with eSIM

Post Quantum Cryptography ready with up to **5x higher throughput**

Built-in assurance with Traffic Insights from **ThousandEyes**

Small / Medium Branch



8235-G2

Large Branch



8355-G2

Campus / Headend



8455-G2

Operational Modes Covering All Deployment Models

Cloud Management

Cloud mode

Full Dashboard-delivered management

- ✓ Support for 8235, 8355, 8455 in beta
- ✓ API-driven configuration
- ✓ Full Show CLI tools supported
- ✓ Complete cloud management experience



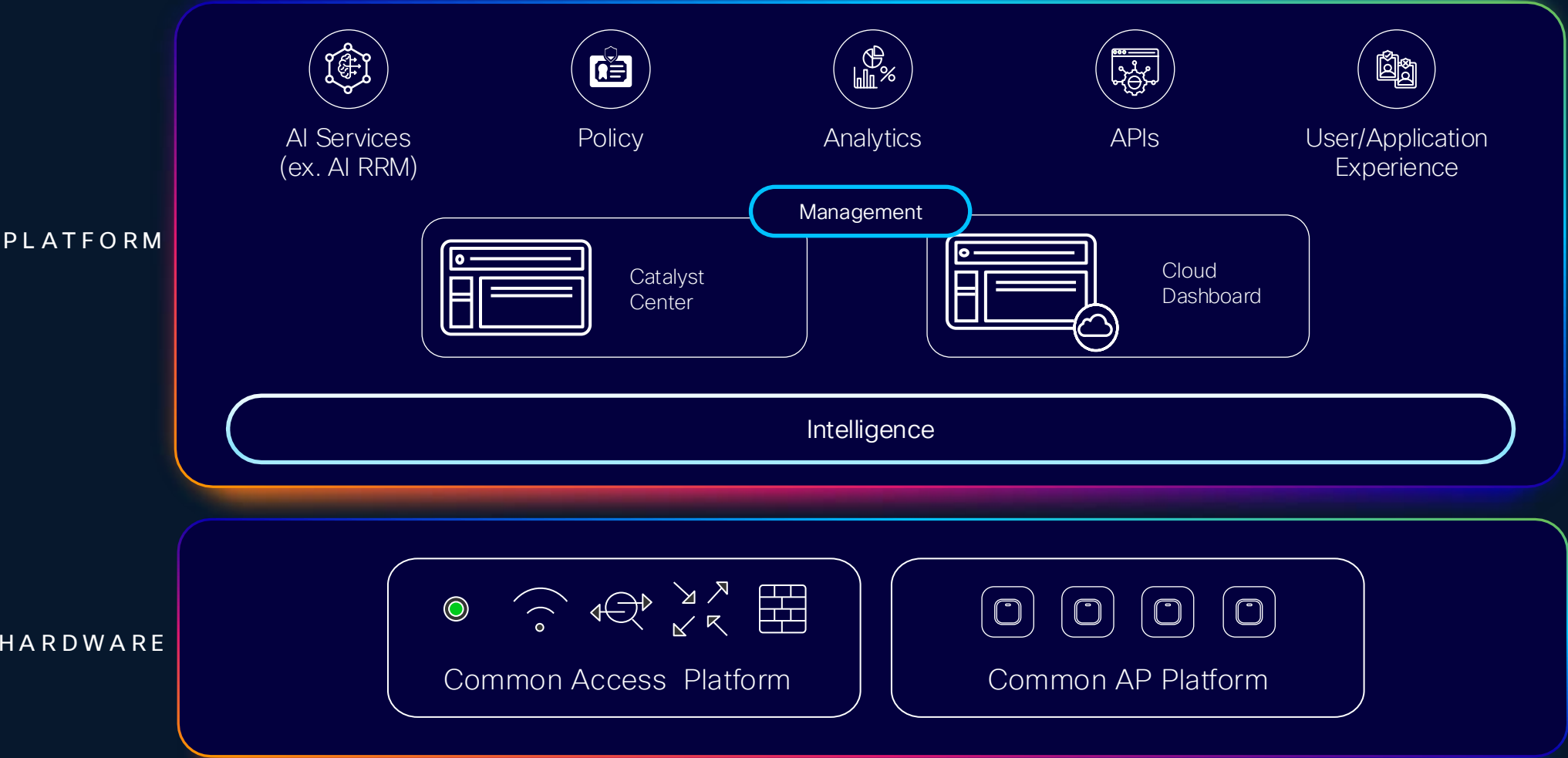
Hybrid mode

Configuration remains local to device

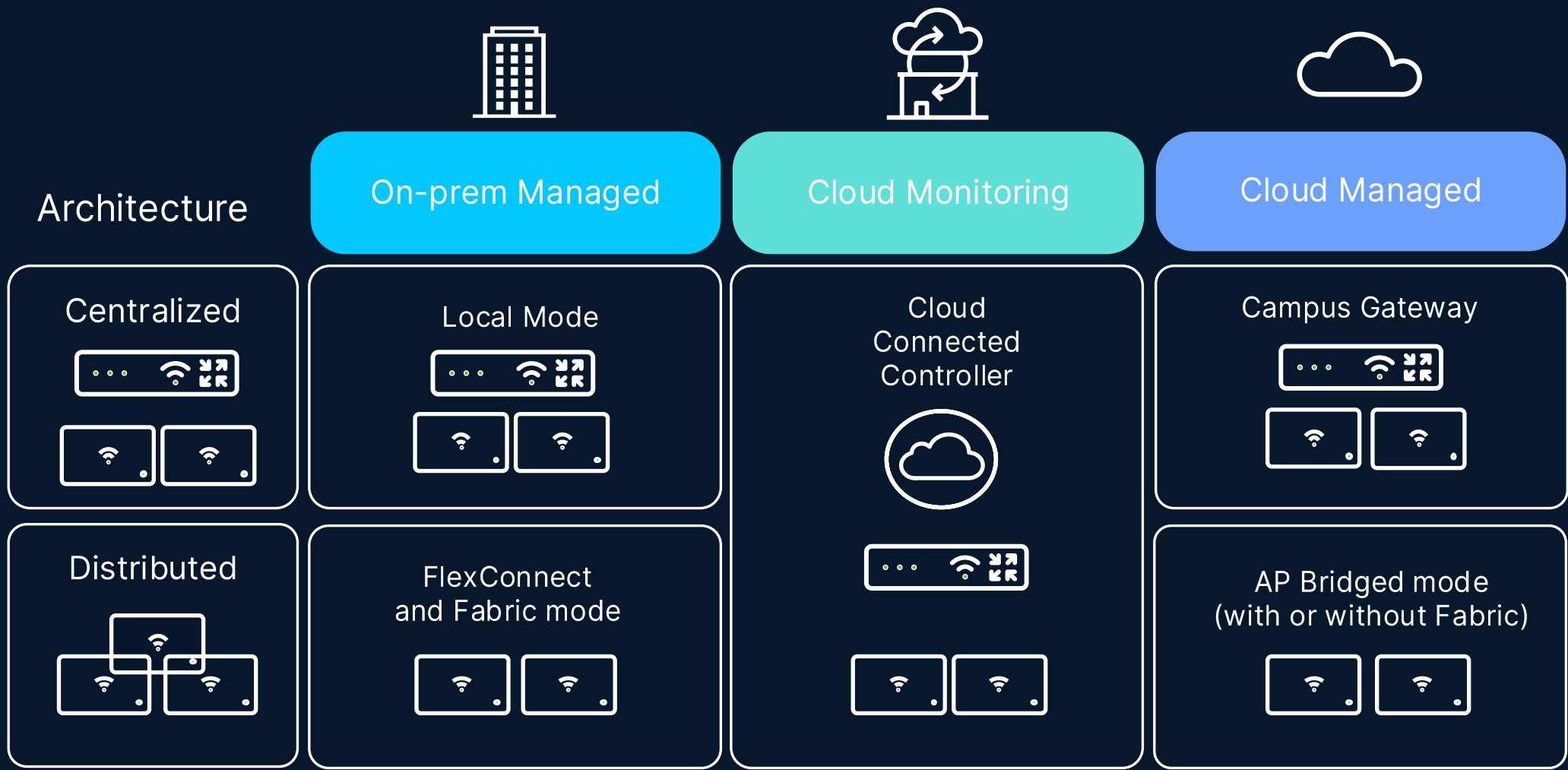
- ✓ Support for all fixed Catalyst products
- ✓ Non-destructive onboarding (preserve configs)
- ✓ Read/Write CLI in Dashboard
- ✓ Full CLI Support via Dashboard
- ✓ Chose to manage via CLI or via UI features – not both

Cloud Wireless

Unified Access Platform

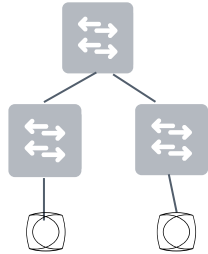


Cisco Wireless Network Architecture Flexibility



Network Architecture: What to choose?

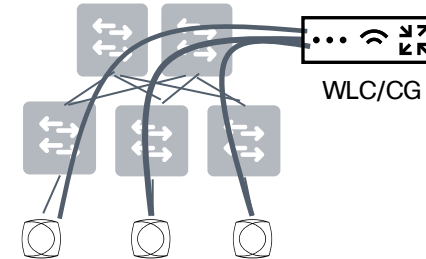
Distributed Data plane



<300 APs*

Use bridging
(Meraki or Flex local switching)

Centralized Data Plane



>300 and up to 6K APs

Add a WLC/CG for L3 roaming,
scale and simplified operations

(*) Meraki: Not a hard limit, just a recommendation. Clients < 8k

(*) Catalyst Flex Local switching: 300 APs (site tag) and 3k clients for max scale in a fast-roaming domain

(*) Switching: 10k clients recommended based on MAC/ARP tables scales and STP limitations due to spanning a VLAN

Cloud Monitoring for Wireless

On-premise functionality in the cloud | Access your wireless network anywhere, no on-prem NMS overhead

**Unified view of Cisco
Wireless Infrastructure**

**Device Health and
Troubleshooting**

**Network Client and
Traffic Information**

**Cloud-Based
Access Anywhere**



Licensing
DNA Essentials
DNA Advantage

Wireless Models
WLC - 98xx, CW98xx
APs - 28xx, 38xx, 48xx, 156x
C91xx, CW91xx

Controller Scale
2,000 Access Points
20,000 Clients

Coexistence with Cat Center
Not supported today

Cloud Monitoring for Wireless Roadmap

Available Now in Meraki Dashboard for Cisco Wireless Controllers !!!

Organization Level

- Overview
- Summary
- Summary Report
- Alerts
- Change log
- Wireless LAN Controllers
- Cloud Monitoring Info
- Create Network
- Inventory

Network Level

- Clients
- Maps & Floor Plans
- Topology
- Add Devices
- Wireless Overview
- Access Points List
- Access Points Connections
- Access Points Map
- Wireless LAN Controllers

Detail Level

- Client Detail
 - Overview
 - Connections
 - Performance
 - Roaming
 - Timeline
- Controller Detail
 - Summary
 - Ports
 - Redundancy
 - APs
 - Tools (show CLI)
- AP Detail
 - Summary
 - Location
 - Connections



- Wi-Fi 7 APs Support
- CW9800M, CW9800H1/H2 Support
- AP Live Tools Support
- Cloud CLI for WLCs
- 9800-CL
- Packet Capture
- Cloud Mon in Canada, India

Coming Soon to Meraki Dashboard for Wireless Controllers and joined Access Points

- Cloud Mon in China
- Software Image Upgrade
- FedRAMP Moderate Support
- Newer Wi-Fi 7 APs
- CW9800L Support
- Experience Metrics (XMs)
- Simplified Log Collection
- Config History / Versioning

Wi-Fi 7 Portfolio

A model for every use case

Coffee shops



CW9171I

Lower density deployments, compact form factor

AVAILABLE

Residence halls, retail



CW9172I/H

Moderate-density deployments, wall plate

AVAILABLE

Classrooms, carpeted spaces



CW9174I/E

Moderate to high-density deployments

AVAILABLE

Lecture halls, libraries



CW9176I/D1

High-performance, omni & directional antenna options, URWB

AVAILABLE

Outdoor



CW9177I/D/E

High-end outdoor, 3 variants for optimal coverage, URWB

NEW

Campus with Location



CW9178

Ultra-high performance, high-density deployments, URWB

AVAILABLE

Stadiums, large venues



CW9179F

High-density, large venues, configurable beam patterns

AVAILABLE

Introducing the CW9177 Series

Tri-band 4x4, 12ss
2/5/6 or 2/5/5

Compatible with both Catalyst
and Meraki mounts where
possible

AFC support for 6 GHz
outdoor in US, CA at Launch



Cisco URWB and Mesh
on Wi-Fi 7 HW

SFP+ port for fiber to the AP

Unified Licensing & Global
Use AP – both WLC and
Meraki

Orderable by 12th of June
Shipping in September

CW9177 Specs

IOS-XE 26.2.1 and 26.1.x



CW9177I

Omni directional antenna
For Horizontal mounting



CW9177D

Directional antenna
(72x72 – 7 dBi)



CW9177E

External antenna
8x N-type connector

Key specs

12 spatial streams
4x4 on 2GHz, 4x4 on 5 GHz, 4x4 on 6 GHz
-or-
4x4 on 2GHz, and dual 4x4 on 5 GHz
Accelerometer (I,D,E*)
CleanAir Pro

BLE/IoT and dedicated scan radio

10 Gbps copper and SFP+ port

DC Power input

Global Use AP

IP67

Operating Temp: -40°C to 65°C w/o solar

That looks a lot like the CW9179F ?!



Expanding our Antenna Portfolio



NEW!

CW-ANT-T-D4-N

Directional antenna

Designed for 9177E

88 x 40 patch, 8 dBi gain*

Supports 2/5/6 and 2/5/5

Accelerometer



NEW!

CW-ANT-T-O3-N

Omnidirectional antenna

Designed for 9177E

360 coverage, 5 dBi gain*

Supports 2/5/6 and 2/5/5

Campus Gateway: Device Conversion

Phase 1: Available June 8th

Who?

Customers who have already started Cloud migrations with CG and want to re-use their existing CW9800 HW

Why?

Provide investment protection of the CW9800 Platform and continue to reduce friction to migrate to cloud

How?

Phase 1 - Call Cisco TAC or Meraki Support and ask for conversion

Phase 2 - Automation

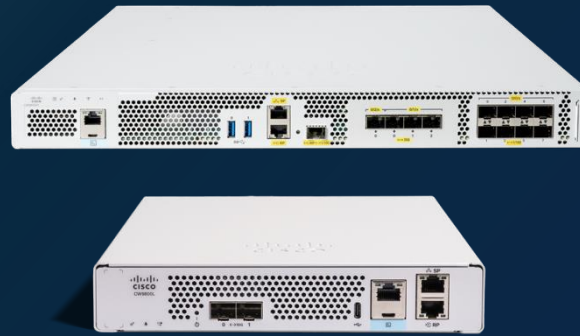
When?

Phase 1 planned availability June 08th

Phase 2 planned availability 1H CY2027

Phase 1

One way conversion



CW9800H1 & CW9800L

Phase 2 planning

Forward & Backwards Conversion

Dashboard Orchestrated



CW9800H1, CW9800L

CW9800H2 , CW9800M

WLC IOS-XE Version: 17.15.5
Dashboard: r31.2.6 network

Cloud Managed features 33.1

3-Radio Support on CW9179F

Overview:

- The Cisco Wireless 9179F supports software-configurable radio operating modes to provide flexibility and support several deployment scenarios
- At launch CW9179F supported only the 4-radio mode (2.4/5L/5H/6) which required 2 channels (low and high) in 5GHz

Use-case:

- **Why would I want 3 radios and not 4?** When in 4-radio mode, the 5GHz radios are band-locked (5GH, 5GL) and thus channel planning becomes more constrained in regions with fewer 5GHz channels. Having 3-radio mode makes the "decision" easier, as every AP/radio can use "any" 5GHz channel.
- For example **warehouses** where hand scanners **don't support DFS channels**

Meraki

General 2.4 GHz 5 GHz 6 GHz

Flex radio selection

Access point model	Band preference	Radios
MR57	5 GHz	2.4 GHz and Dual 5 GHz
CW9166I	5 GHz	2.4 GHz and Dual 5 GHz
CW9166D1	5 GHz	2.4 GHz and Dual 5 GHz
CW9178I	3 Radios	2.4 GHz, 5 GHz and 6 GHz
CW9176I	2.4 GHz	2.4 GHz, 5 GHz and 6 GHz
CW9176D1	2.4 GHz	2.4 GHz, 5 GHz and 6 GHz
CW9172I	3 Radios	2.4 GHz, 5 GHz and 6 GHz
CW9179F	3 Radios	2.4 GHz, 5 GHz and 6 GHz
CW9174E	4 Radios	2.4 GHz, 5 GHz and 6 GHz
CW9174I	3 Radios	2.4 GHz, 5 GHz and 6 GHz
CW9171I	5 GHz	2.4 GHz and 5 GHz

3-Radio Support on CW9179F

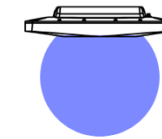
Considerations:

- When operating in Tri-Radio mode, only **Boresight** antenna beamwidth will be supported providing a narrower beamwidth.

Benefits:

- The 5 GHz radio is not band-locked, allowing the use any available 5 GHz channel.
- Simplifies channel planning by providing full access to the 5 GHz spectrum, which reduces co-channel interference.
- Improves legacy device support, especially in industrial environments where older clients may not support DFS channels, by allowing easier assignment of non-DFS channels across the entire 5 GHz band

3-radio mode only supported with Boresight



Boresight (Default)

2.4 GHz: 70×70 beamwidth
5 low/5 high/6 GHz: 35×35 beamwidth

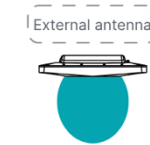
■ 2.4 GHz + 5 GHz low + 5 GHz high + 6 GHz



Wide

2.4 GHz: 70×70 beamwidth
5 low/5 high GHz: 35×35 beamwidth (+/- 15° offset)
6 GHz: 70×35 beamwidth

■ 5 GHz low ■ 5 GHz high ■ 2.4 GHz + 6 GHz



Front-and-back

2.4 GHz: External antenna
5 low GHz: External antenna
5 high/6 GHz: 35×35 beamwidth forward

■ 5 GHz high + 6 GHz

AAA Seamless Accounting

Why is it needed?

Overview:

- Previously, APs sent AAA accounting start/stop messages for every client roam, generating a high volume of messages.
- With MR 33.1, the new AAA Seamless Accounting feature ensures only one pair of start/stop messages is sent for the entire duration of a client's connection, significantly reducing AAA server load.

Default Behavior:

- Seamless Accounting is now the default for all cloud-managed APs running MR 33.1 or later, regardless of SSID tunnel configurations to Cisco Campus Gateway (CG).
- Users can configure to send **periodic and/or interim accounting messages** as well

Campus Gateway Deployment:

- When Cisco CG is deployed, all accounting messages are proxied through the CG to the AAA server.

Benefits:

- Reduces pressure on AAA servers in large-scale wireless deployments
- Maintains accurate session tracking and reporting
- Simplifies accounting message handling across roaming events

AAA Seamless Accounting

Configuration

1. Navigate **Wireless > Configure > Access Control** and select the SSID which should be configured.

2. Within the the **RADIUS accounting servers** set the value for **Periodic accounting interval**.

Note: Entering a value of 0 will disable periodic accounting. For non-zero values, one message update will be sent per interval.

RADIUS 1 RADIUS server, 1 accounting server

RADIUS accounting servers

#	Host IP or FQDN	Acct port	Secret	Actions
1	10.10.105.35	1813		...

[Add server](#) 3 max.

Periodic accounting interval ⓘ minutes

☒ Enable event-based interim accounting ⓘ

Accounting start delay seconds

☐ RADIUS Accounting Device Profiling support ⓘ

AAA Seamless Accounting Accounting Updates

Configuration

Configuration:

Administrators can optionally configure event-based interim accounting updates and trigger updates for client state change events (e.g., roams)

Set the toggle for **Enable event-based interim accounting**.

Enhanced Session Tracking:

Session-ID and Multi Session-ID are preserved for the entire client session.

All counters from the client's fast-roaming path are included in the accounting messages

RADIUS 1 RADIUS server, 1 accounting server

RADIUS accounting servers

#	Host IP or FQDN	Acct port	Secret	Actions
1	10.10.105.35	1813		...

[Add server](#) 3 max.

Periodic accounting interval 1 minutes

☒ **Enable event-based interim accounting**

Accounting start delay 0 seconds

☐ RADIUS Accounting Device Profiling support

Cloud Switching

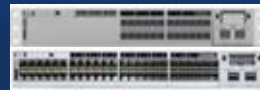
Unlocking Cloud Management for the Full C9000

17.15

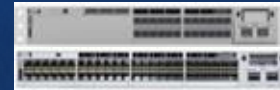
Recommended



C9300L
(Cloud + Device)



C9300*
(Cloud + Device)



C9300X
(Cloud + Device)



C9200L
(Cloud + Device)

**Includes specific C9300 models. See documentation for more details.*

↓ All platforms supported on 17.15 are also supported on 17.18.1+

17.18.3 GA available now!

17.18

Generally Available



C9500
(Cloud + Device)



C9200/CX
(Cloud + Device)



C9350
(Cloud + Device)



C9300LM
(Cloud + Device)



C9610
(Device Mode)

Includes all 17.15 platforms; adds C9200 - C9200CX - Remaining C9300 models - C9350 Smart Switches - C9500

26.1

Beta



9400/9600
(Device Mode)



IE3500
(Cloud Mode)



C9200CX-8PT-2G
(Cloud Mode)

26.2

Beta



C9550 series
(Cloud + Device)



C9350 Ph.2
(Cloud Mode)

Cloud Management for Cisco Catalyst C9400 and C9606

IOS XE 26.1.2

Device Configuration Mode

Leverage the cloud dashboard while maintaining local and flexible control

Expanded platform support

Increased platform support to include modular switches for complete campus cloud management

Operational simplicity

Easily manage Cisco Catalyst modular switches with centralized visibility from the Meraki dashboard, anytime and anywhere



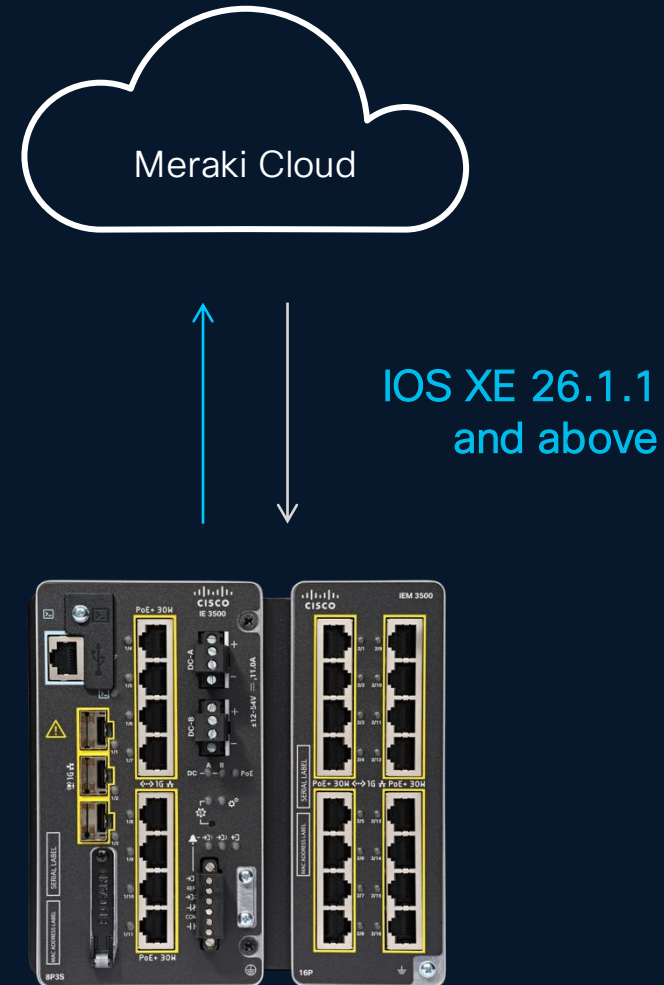
*Modular Cloud Config – Coming Soon

What's supported for cloud managed IE3500?

- Unified cloud management across enterprise and rugged enterprise networks
- Simplified onboarding process* with guided workflows
- Intuitive user interface to build configurations at scale
- Micro-segmentation with Adaptive Policy
- Automated 'show' CLI commands for advanced troubleshooting
- Features match C9200L in Cloud Configuration mode (IOS XE 17.18.1)

Note: Rugged Enterprise use cases only; OT protocols are not supported currently

Migration leverages *service cloud-mgmt connect*



Streamlined Onboarding

Available Now

It starts with a streamlined onboarding process

Users can quickly onboard new devices to the network, choose the configuration source, and begin cloud management without any additional applications.

Add devices to network



Select network

2

Configure IOS-XE
devices

3

Summary

Device management and configuration source

C9500

Device

C9500H refers to C9500-48Y4C, C9500-24Y4C, C9500-32C, C9500-32QC

C9200/C9300/C9500H ⓘ devices



Cloud configuration ⓘ

Configuration is sourced from the Meraki Dashboard.



Device configuration ⓘ

Configuration remains local to the device.

Device configuration credentials

Please provide the [level 15 configuration access credentials](#) ⓘ so the Meraki dashboard can make necessary configuration changes to these devices.

Username

Password

Streamlined Onboarding

```
WW_CORE_9300(config)# service meraki connect

Switch 1 has been successfully registered
Meraki MAC: AABBCDDDEEFF
Cloud ID: QXXX-XXXX-YYYY

*May 7 00:16:03.519: %MERAKI-5-SWITCH_REGISTER_SUCCESS: Switch 1 has been successfully registered.
*May 7 00:16:03.519: %MERAKI-5-MAC_ADDR: Meraki MAC: AABBCDDDEEFF
*May 7 00:16:03.519: %MERAKI-5-CLOUD_ID: Cloud ID: QXXX-XXXX-YYYY

Device Registration Status:
-----
Switch          Serial
Num   PID      Number      Cloud ID      Mac Address    Migration
-----
1     C9300-24UX  XYYYQQCCXXC  QXXX-XXXX-YYYY  aabb.ccdd.eeff  Registered  C9K-C [Monitoring]
```

Cloud Management app-free onboarding

- Automated Registration and Nextunnel creation (service meraki connect)
- Simply claim the Cloud ID and add to a network

```
Service meraki connect: enable

Meraki Tunnel Config
-----
Fetch State:
Fetch Fail:
Last Fetch(UTC):
Next Fetch(UTC):
Config Server:
Primary:          usw.nt.meraki.com
Secondary:        use.nt.meraki.com
Client IPv6 Addr: FD0A:9B09:1F7:1:9A18:88FF:FE00:CC00
Network Name:     .Corrin - switch

Meraki Tunnel State
-----
Primary:          Up
Secondary:        Up
Primary Last Change(UTC): 2024-05-29 23:34:02
Secondary Last Change(UTC): 2024-05-29 23:34:02
Client Last Restart(UTC): 2024-05-29 23:33:56

Meraki Tunnel Interface
-----
Status:          Enable
Rx Packets:      795767
Tx Packets:      600246
Rx Errors:       0
Tx Errors:       0
Rx Drop Packets: 0
Tx Drop Packets: 0

Meraki Device Registration
-----
url:             https://catalyst.meraki.com/nodes/register
```

Connection state
(show meraki connect)

Maintain operational flexibility with cloud management

Configuration Source: Cloud



UNLOCK FULL CLOUD SIMPLICITY

Configurations are performed in the cloud and managed using the dashboard UI

Configuration Source: Device



RETAIN ADVANCED CONTROL

Configurations are managed via traditional methods and performed local to the device

FLEXIBLE OPTIONS FOR MANAGING YOUR DEVICES FROM THE CLOUD

Configuration Source: Cloud

The full cloud experience with management and configurations performed in the cloud

- Cloud CLI Support for read-only 'show' commands for advanced troubleshooting
- Leverage the intuitive user interface to build configurations that are performed directly from the Meraki cloud at scale.

The screenshot shows the 'Add devices to network' configuration page in the Meraki interface. At the top, a progress bar indicates three steps: 1. Select network (completed with a checkmark), 2. Configure IOS-XE devices (current step, highlighted with a blue circle), and 3. Summary. Below the progress bar, the section 'Device management and configuration source' is titled. Under the sub-header 'C9200/C9300 devices', there are two radio button options. The first option, 'Cloud configuration', is selected and highlighted with a blue border; its description is 'Configuration is sourced from the Meraki Dashboard.' The second option, 'Device configuration', is marked as 'Beta' and has the description 'Configuration remains local to the device.' At the bottom left is a 'Cancel' button, and at the bottom right are 'Back' and 'Next' buttons.

[Full List of Supported Models Here](#)

Configuration Source: Device

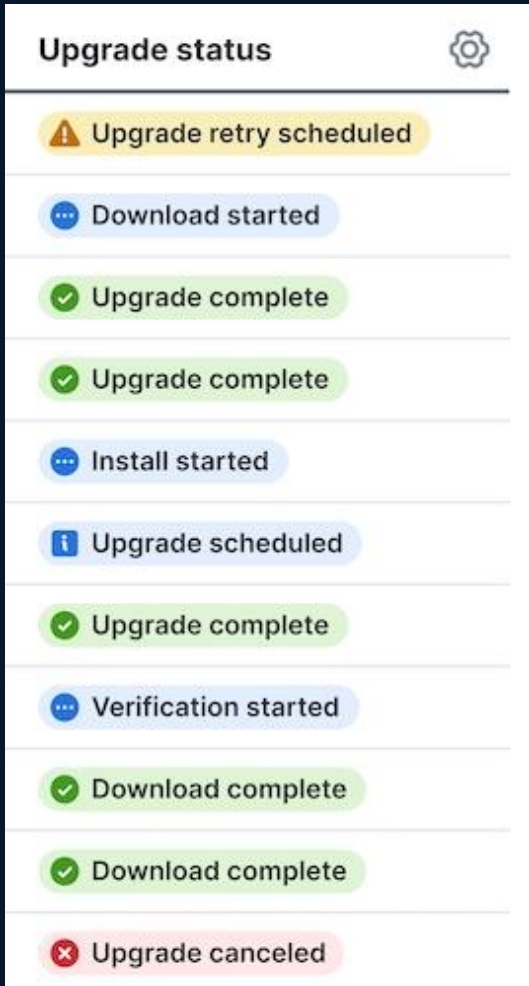
Cloud scale visibility with localized configurations and the full IOS XE feature set

- Non-destructive onboarding preserves configurations, which are managed and performed local to the device via traditional methods.
- Cloud CLI support for show and config commands in dashboard
- Configuration back up in the cloud.

The screenshot shows a web interface titled "Add devices to network". At the top, there is a progress bar with three steps: 1. Select network (marked with a checkmark), 2. Configure IOS-XE devices (marked with a blue circle and the current step number), and 3. Summary. Below the progress bar, the section "Device management and configuration source" is displayed. Under the sub-header "C9200/C9300 devices", there are two radio button options. The first is "Cloud configuration" with the description "Configuration is sourced from the Meraki Dashboard." The second is "Device configuration" with a "Beta" label and the description "Configuration remains local to the device." The "Device configuration" option is selected and highlighted with a blue border. At the bottom of the form, there are three buttons: "Cancel", "Back", and "Next".

[Full List of Supported Models Here](#)

Firmware Upgrade Status for IOS XE

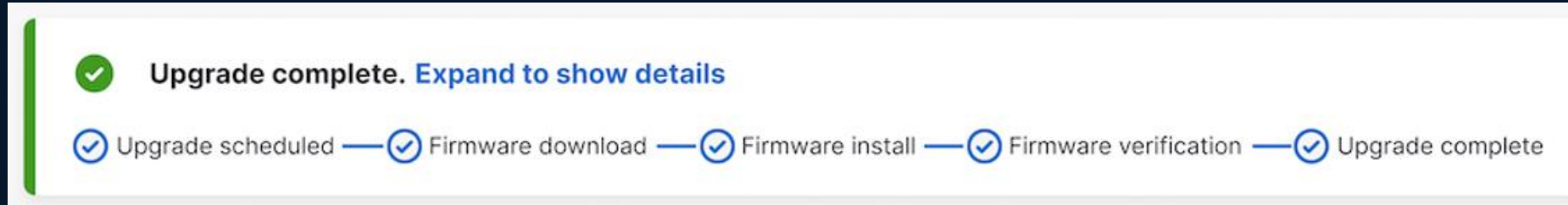


Monitor each stage of firmware upgrades for all switches in a single view:

- Download
- Installation
- Verification

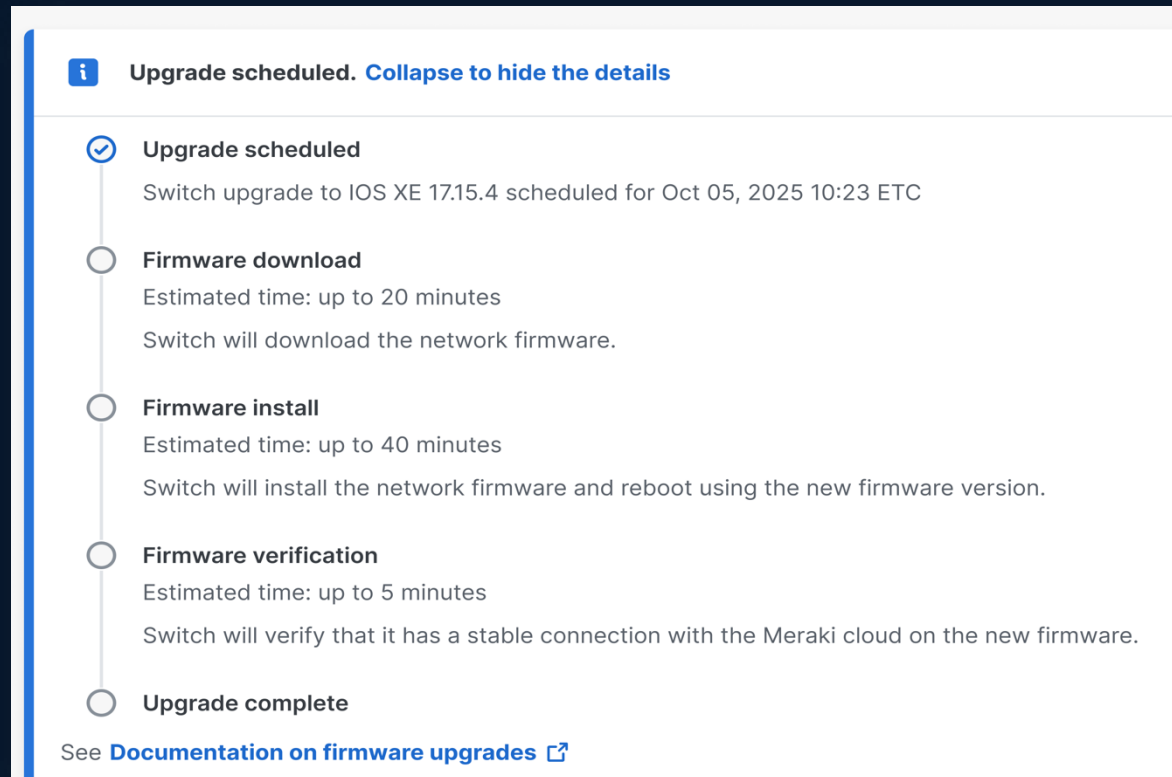
Supports CS or IOS XE to IOS XE upgrades

Firmware Upgrade Status for IOS XE



Drill down into each switch to view progression through each stage, with guidance on expected times, and success and failure states.

Supports CS to IOS XE and all IOS XE upgrades.



Cloud Management with IOS XE 17.18

Advanced Management

Routed Ports, BGP, VRF, Local VLAN DB Config, Sticky MAC allow list, and Cloud EVPN Fabric

High Availability

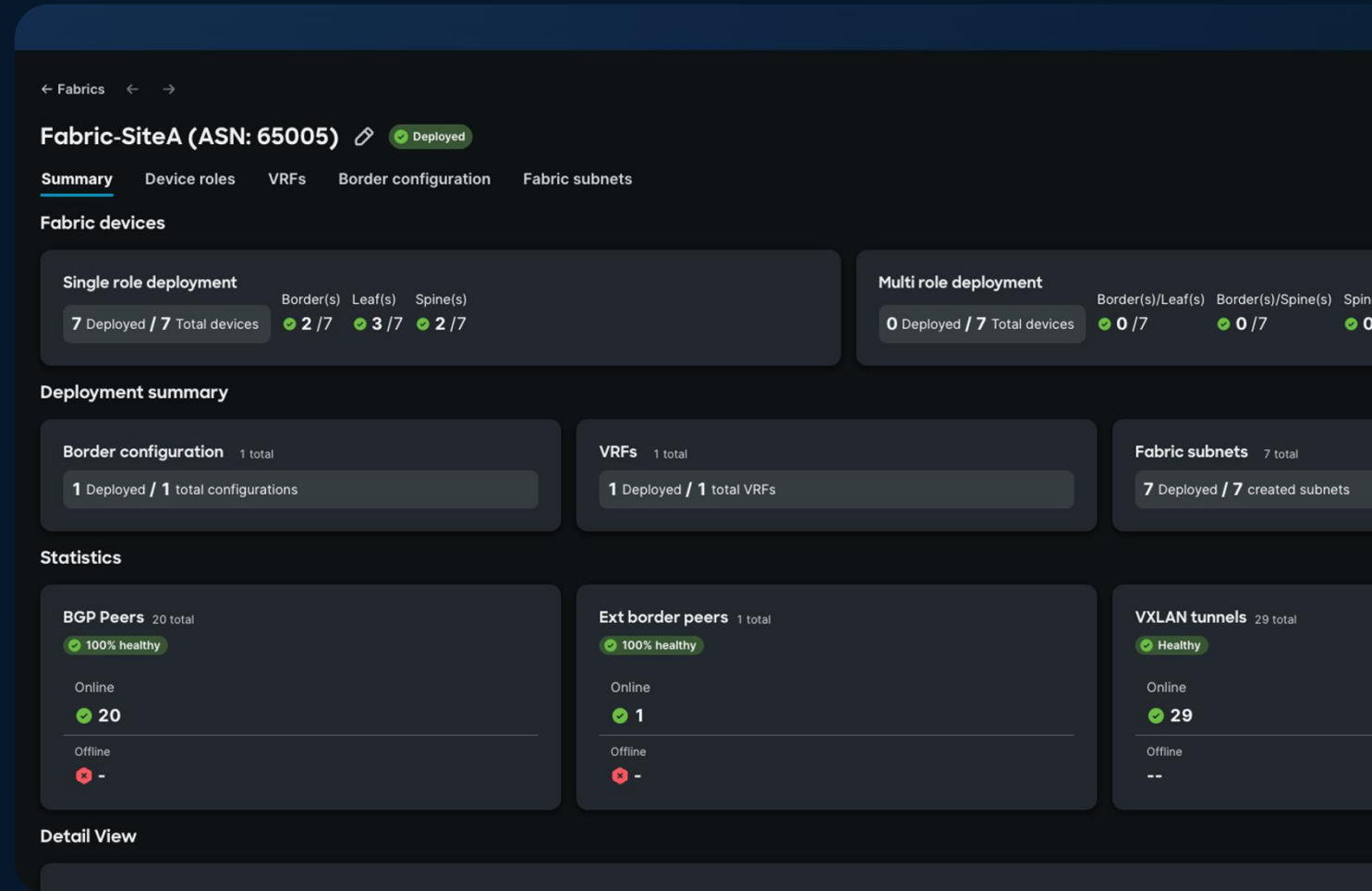
StackWise Virtual, ISSU, RPVST+, UAC enhancement, and Warm Spare (VRRP)

Cloud Value

SmartPorts, Intelligent Capture, Device Uptime, Device Health, Digital Optical Monitoring,

Additional Platform Support

All C9200/CX/L, C9300/L/X/LM, C9500 high performance, C9350



26.1.1



Stability & Reliability Improvements

100+ bug fixes and enhancements



Expanded Device Support

Introduction of Industrial Ethernet switching with the IE3500 line



Feature Parity

C9350 Feature Parity with the rest of the C9K portfolio in Dashboard

NOW IN BETA

Sneak peek: Cloud CLI Profiles

Access to XE capabilities that are not exposed via Meraki Dashboard

Configuration Profiles

Define and apply common configurations across networks in your organization.

SSID profiles

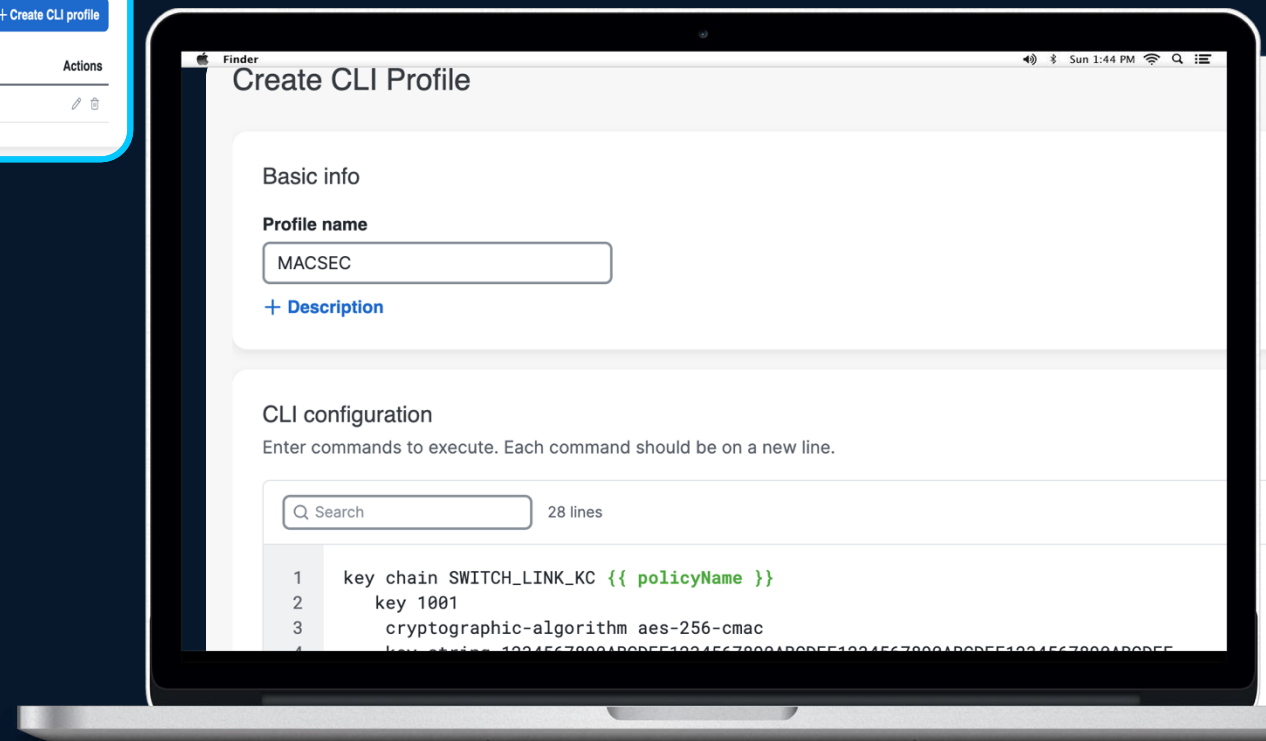
CLI profiles

Create reusable settings that can be easily applied to Catalyst IOS XE switches using tags. [Documentation](#)

1 result
+ Create CLI profile

Profile name	Variables	Device tag	Applied to	Devices	Status	Actions
MACSEC	2	Core Switches	1 network	132 switches	Provisioned	

- Full IOS XE CLIs in Dashboard
- Jinja2 variable supported in Profile
- Assigned to switches at scale via Device Tags
- Single Profile per device



CLI Profiles

Demo

- Network SFO-100 >
- Network-wide >
- Assurance >
- Security & SD-WAN >
- Switching >
- Wireless >
- Systems Manager >
- Cameras >
- Sensors >
- Insight >
- Organization >

Configuration Profiles

Define and apply common configurations across networks in your organization.

- SSID profiles
- CLI profiles



Create reusable settings that can be easily applied to Catalyst IOS XE switches using tags.

Documentation

+ Create CLI profile

Config Analyzer

Internal Preview:
Target Q4FY26

Reduce time spent answering "can I move to cloud-config"?

Quickly determine cloud readiness and configs that need further review

Upload config files or analyze connected device-mode switches

Download or copy configurations for further review

How to sign up:

[Config Analyzer Sign Up](#)

Meraki

Admin ▾ Demo Networks 🔍 Search

Network BGLMonitorC9550 >

Network-wide >

Assurance >

Switching >

Sensors >

Organization >

Automation >

Admin >

Find in Menu (⌘+K)

Device Inventory **Switch Config Analyzer**

☒ Upload
Upload a .cfg or .txt file (max 2MB)

☐ Paste
Paste configuration from a device

☐ From Device
Select a device to analyze

Click or drag file to this area to upload

customer 9300.txt

Analyze

Details

Supported configurations 58 ▾

Needs Review 34 ▲

These commands may not be fully supported for switches in cloud configuration. Many features may be configurable in cloud configuration in a similar or modified manner. Review this section carefully to determine whether any commands may no longer be required or alternate configurations are possible.

Download Copy

```
7 et-analytics
8 inactive-timeout <TIMEOUT>
9 ip flow-export destination <IPv4_ADDR> 2055
10 flow exporter <FLOW_EXPORTER>
11 description <DESCRIPTION>
12 destination <IPv4_ADDR>
13 option application-table timeout <TIMEOUT>
14 option interface-table
15 source Vlan<N>
16 template data timeout <TIMEOUT>
17 transport udp <PORT>
18 flow monitor <FLOW_MONITOR>
19 cache timeout active <SECONDS>
20 exporter <FLOW_EXPORTER>
21 record <FLOW_RECORD>
22 flow record <FLOW_RECORD>
23 collect counter bytes long
```

English

MV & MT

Introducing!



A win-win partnership
that delivers more for our customers

Scale and simplicity with Cisco's unified, cloud-managed software combined with Axis' breadth of hardware delivers a seamless end-to-end solution for joint customers

Available Today – Public Preview – Essential License

Unified Cloud Platform Focus

<http://dashboard.meraki.com/integrations/axis>

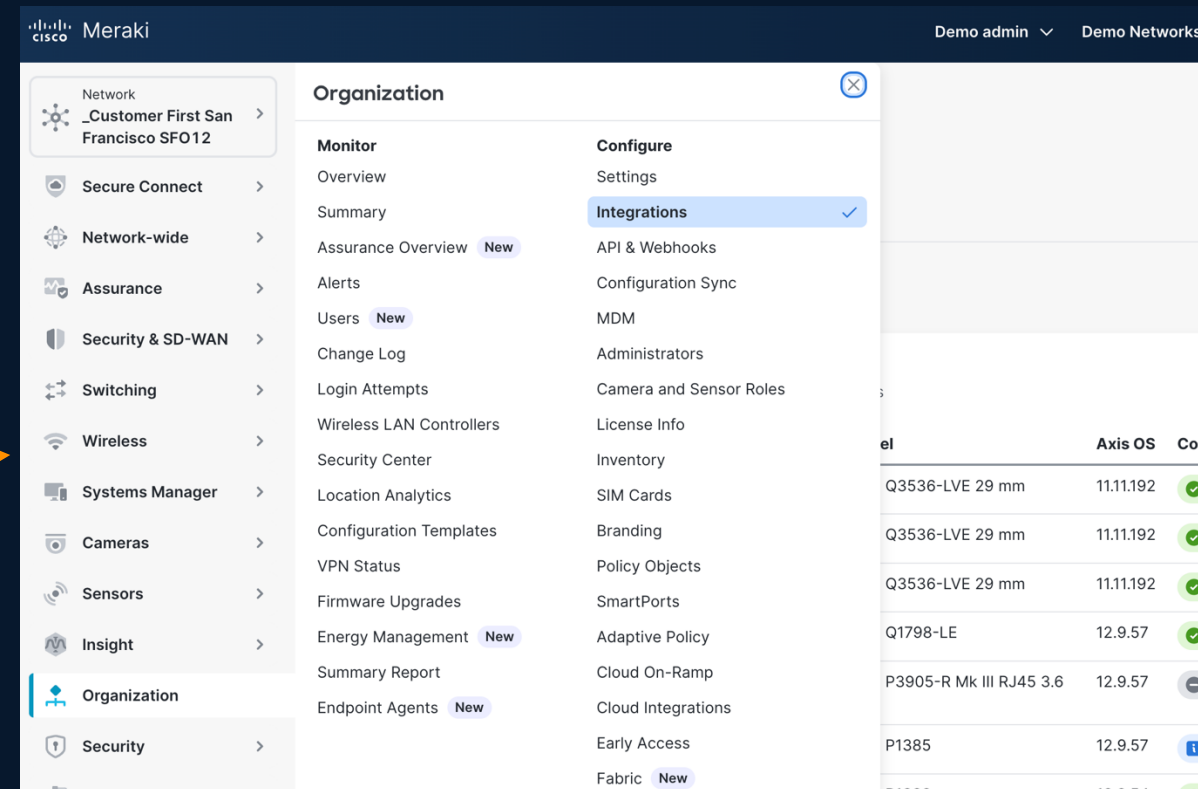
Manage **Axis cameras** inside your
Cisco unified cloud management platform

Benefits

- Add cloud management with a simple software update
- Easier to deploy and adopt
- End-to-End visibility and assurance
- Single pane of glass IT and OT management
- Automatic updates with best-in-class security



AXIS[®]
COMMUNICATIONS



License Offerings

Coming soon

Feature	Essentials Tier	Advantage Tier
Live Video Streaming	✓	✓
Device Health Monitoring	✓	✓
Fleet Management	✓	✓
Managed Firmware Updates	✓	✓
Configuration Management	Basic (Zoom, Aperture, Focus)	✓
Local SD Card Recording	✗	✓
Cloud Video Storage	✗	✓ (30 days)
Video Export	✗	✓
Video Analytics	✗	✓
Cloud-Based Historical Playback	✗	✓

- Essential license requires no change to your existing solution while adding a layer of visibility and management on top, accessible via Dashboard.
- Advantage license allows you to fully cloud manage your Axis devices via the dashboard eliminating the need to support multiple VMS's or on-prem NVR

IMPORTANT ANNOUNCEMENT

Cisco Meraki MT Sensors: End-of-Sale

Executive summary for Channel Partners on Cisco's Sensor Market Exit



Market Exit

All Meraki MT Sensor models are scheduled for an official **End-of-Sale on May 12, 2026**.



Runway Timeline

Customers have a **six-month window** from the announcement date to evaluate replacement sensors and secure final Meraki MT purchases.



Partner Action

Proactive outreach required. Contact active accounts, address transition questions, and reference the official **Meraki MT End-of-Sale FAQ**.



May 12, 2026
EOS ANNOUNCED



Nov 10, 2026
LAST BUY DATE



Nov 30, 2031
END OF SUPPORT

Cisco Access Manager

Introducing Cisco Access Manager

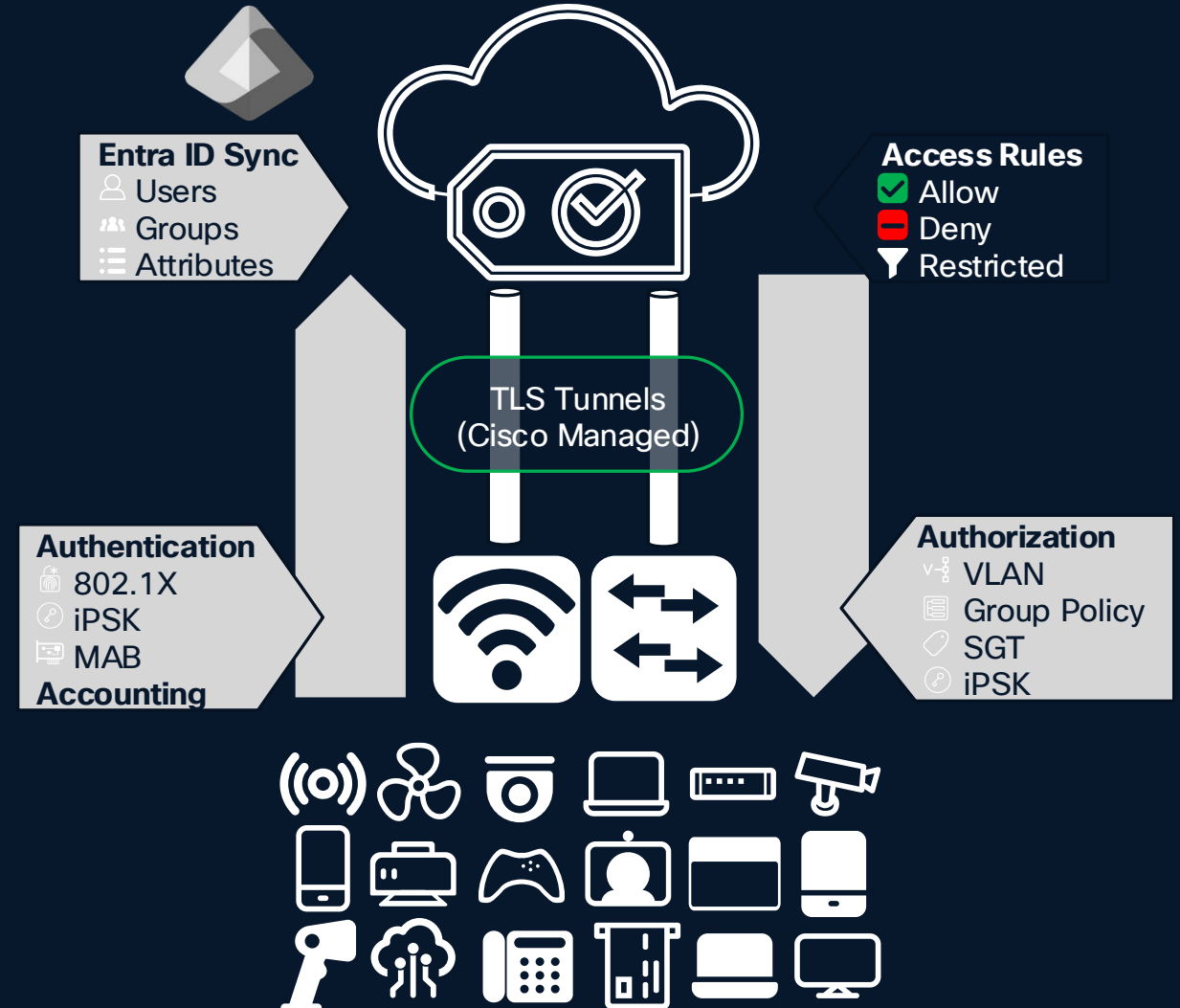
Cloud-delivered access control services to enforce identity and context-based access to the users and devices for Meraki managed infrastructure

Multi-tenant SaaS (Software as a Service)
for High Availability and Scale globally

Secure RADIUS transport over encrypted
TLS tunnels to the Meraki Dashboard

Simplified and rapid Zero-Trust adoption
using identity-based micro-segmentation

Flexible Authentication Options for wired
and wireless users, computers, and I/OT



Cisco Access Manager Architecture

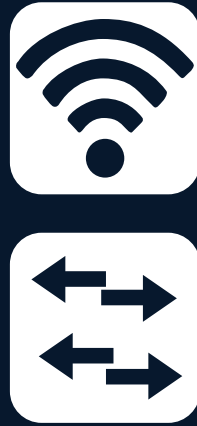
Endpoints



Users, Computers, Things

-  EAP-TLS
-  EAP-TTLS+PAP
-  iPSK (Identity PSK)
-  Guest
-  MAB (MAC Auth)

Network Devices



Meraki Managed *only*

MR + CW91xx: 30.7+
MS: 17+; Cloud Config
Catalyst: 17.18.1+
MX / Z: *Unsupported*

Access Manager



Cisco Meraki Dashboard

Auto Scaling Service
HA Multi-Tenant Service
MAB Clients & Groups
Simple Access Rules

Identity Providers



Microsoft Entra ID *only*

Certificate User identity
Username + Password
User Group Lookup only

Identity-based Zero Trust Access with Access Manager

Users, Computers, and Things

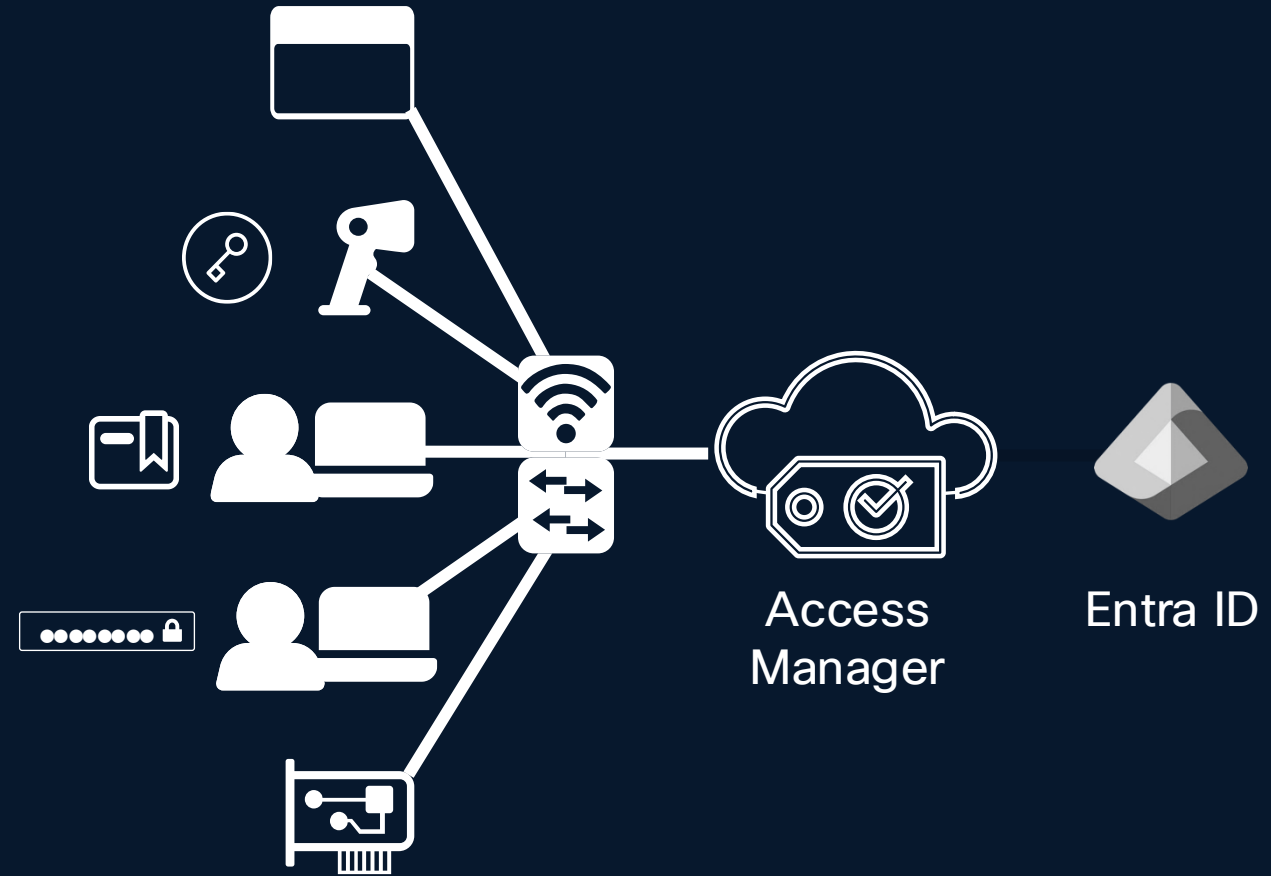
Wireless Guests (AUP optional)
Acceptable Usage Policy

iPSK (Identity PSK) for Wireless IOT

EAP-TLS Auth (Entra ID optional)

EAP-TTLS Auth with Entra ID Lookup

MAC Auth Bypass (MAB) for IOT



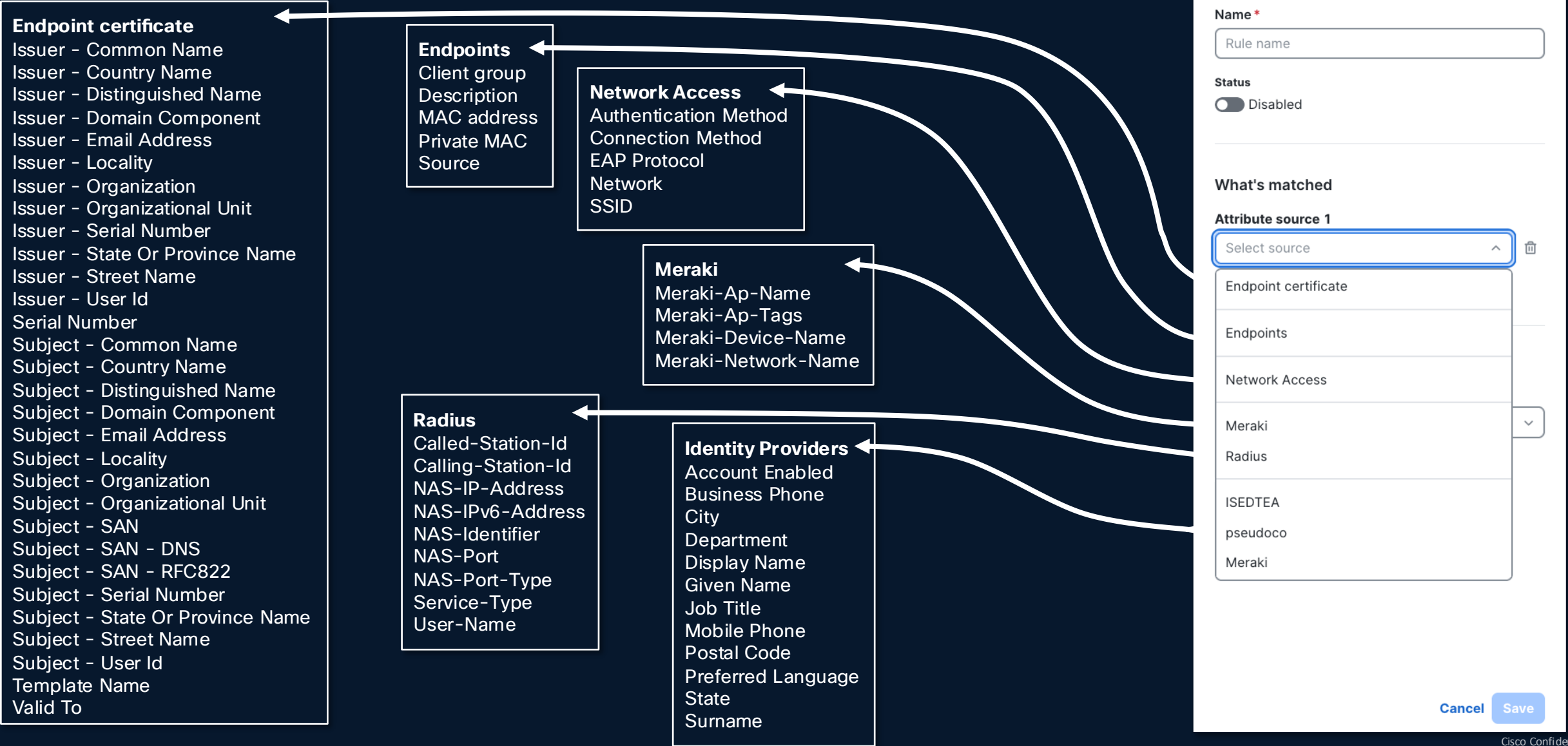
Access Rules

↑ Maximum 50 Rules

Access Manager > Policies > Access Rules

Type	Status	Name	Why	What's Matched	When	Where	Authorization	How Much
⋮ Rule Group	✓	Default Rule Group		Any				
⋮ ↳ Rule	✓	Blocked		Endpoints: Client group = Blocked			Deny Access	Edit
⋮ ↳ Rule	✓	Workstations		Certificate:Issuer = My Org Certificate:Subject-DN [Contains] workstation			Adaptive Policy = Workstation ...	
⋮ ↳ Rule	✓	Admins		Certificate: Issuer = My Org EntraID:Group = Admins Who			Ac ...	
⋮ ↳ Rule	✓	Employees		EntraID:Group = Employees			Ac ...	
⋮ ↳ Rule	✓	Guests		Network Access: SSID = Guest Authentication Method = MAB			Ac ...	
⋮ ↳ Rule	✓	Scanners		Network Access: SSID = IOT Endpoints: Client group = Scanners			Ac ...	
⋮ ↳ Rule	✓	Phones		Endpoints: Client group = Phones What			Ac ...	
⋮ ↳ Rule	✓	Cameras		Endpoints: Client group = Cameras			Adaptive Policy = Cameras ...	
⋮ ↳ Disabled	⊖	Exceptions		Endpoints: Client group = Exceptions			Allow Access ...	
⋮ ↳ Rule	✓	Default Rule		Any		Secure default	Deny Access ...	
+ Add a Rule								

Access Rules: Attribute Sources & Attributes



Endpoint Profiling

- Automates real-time device identification and classification using DHCP, CDP and LLDP data
- Enable dynamic granular access control to streamline operations, reduce manual effort and accelerate troubleshooting

Global Overview

Organization
AccessManager

Network
Demo

Network-wide

Assurance

Teleworker gateway

Switching

Wireless

Cameras

Insight

Organization

Automation

Access Manager

Find in Menu (⌘+K)

Meraki

Search

?

?

?

Clients

Client groups

Search MAC address

Filters

17 matching results

☐	Type ^① Beta	Manufacturer ^① Beta	Model ^① Beta	OS ^① Beta	Status	MAC address	Description	Client groups ^①
☐	Mobile	Google	Pixel 9a	Android 16	⊖	0a:70:c0:8a:8f:64	-	-
☐	Wi-Fi Extender	Cisco	Meraki MR46		⊖	2c:3f:0b:56:e3:6c	MR46-HW	1
☐	Access Point	Cisco	Catalyst CW9166I		⊖	68:49:92:37:61:a0	CW9166I-MR V01	1
☐	Mobile	Apple		iOS	⊖	7a:1b:af:64:ab:a4	-	-
☐	Raspberry	Raspberry Pi	Raspberry Pi		⊖	88:a2:9e:06:f3:7b	Raspberry Pi 5	1
☐	Mobile	Apple		iOS	✓	9a:e7:b8:61:f7:56	-	-
☐	IP Camera	Amcrest			⊖	9c:8e:cd:28:84:2f	Amcrest IP8M-2496EW-28MM	1
☐	IP Camera	Amcrest			⊖	9c:8e:cd:2d:2c:17	Amcrest IP8M-2496EW-V2	1
☐	IP Camera	Amcrest			⊖	9c:8e:cd:37:da:13	Amcrest IP8M-2696EW-AI	1
☐	IP Camera	Cisco	Meraki MV12W		⊖	ac:17:c8:0c:17:a0	-	-

Select columns

Check to add, drag columns to reorder.

☒ Status

☒ MAC address

☒ Description

☒ Type ^①

☒ Manufacturer ^①

☒ Model ^①

☒ OS ^①

☒ Client groups ^①

☒ Last login network

☒ SSID

☒ Last seen (UTC)

By default unchecked

Create Access Rules using Profiling Classifications

Access Rules

	Type	Status	Name	What's Matched
::	Rule Group	✓	Default Rule Group	Any
::	└ Rule	✓	Blocked	Endpoints: Client group = Blocked
::	└ Rule	✓	Workstations	Certificate:Issuer = My Org Certificate:Subject-DN [Contains] workstation
::	└ Rule	✓	Employees	Certificate: Issuer = My Org EntraID:Group = Employees
::	└ Rule	✓	Guests	Network Access: SSID = Guest Authentication Method = MAB
::	└ Rule	✓	Scanners	Network Access: SSID = IOT Endpoints:Client group = Scanners
::	└ Rule	✓	Phones	Authentication Method = MAB, Endpoints:Type = VoIP Device
::	└ Rule	✓	Cameras	Authentication Method = MAB, Endpoints:Type = IP Cameras
::	└ Rule	⊖	Exceptions	Authentication Method = MAB, Endpoints:Client group = Exceptions
::	└ Rule	✓	Default Rule	Any
+ Add a Rule				

Rule

Name *

Phones

Status

Enabled

What's matched

Attribute source 1

Endpoints

Group or Attribute

Type

1

Terminal

Thermostat

Touch Panel

Toy

UPS

USB

VPN

Virtual Machine

VoIP Device

Voice Assistant

Water Sensor

Wearable

Weather Station

Web Server

Daily Active Sessions and Session Log

Active sessions

1 All networks

Last 10 days

Summary

8
Highest daily sessions

4
95th percentile daily sessions

3
90th percentile daily sessions

Daily concurrent sessions

Date	Daily concurrent sessions
Oct 30	8
Oct 31	4
Nov 1	0
Nov 2	2
Nov 3	2
Nov 4	0
Nov 5	3

Session log

1 All networks

Last 30 minutes

Q Search

Filters

9 matching results

Time (UTC)	Status ①	Details	Username	Endpoint MAC address	Authenti Protocol
Nov 11 22:37:31	Success	ESP32s	b43a458a1d9c	b4:3a:45:8a:1d:9c	MAB
Nov 11 22:36:03	Failed	Session failed due to a time...		70:d8:23:4d:d6:ef	EAP
Nov 11 22:35:26	Failed	Session failed due to a time...		70:d8:23:4d:d6:ef	EAP
Nov 11 22:34:42	Failed	Session failed due to a time...		70:d8:23:4d:d6:ef	EAP
Nov 11 22:29:10	Rejected	The matched rule has an AC...	92db17cb31aa	92:db:17:cb:31:aa	MAB

Network Access Details

Network

Network name

Lab

Connection Method

Wireless

SSID

AM-iPSK

Port

1

Network Device name

lab-cw9166-3Z93

Network Device MAC address

68:49:92:37:61:a0

Network Device IP address

192.168.128.9

Incoming Radius AVP

Called-Station-Id

6e:49:92:37:61:a0

Called-Station-SSID

AM-iPSK

Calling-Station-Id

b4:3a:45:8a:1d:9c

Cloud-NAC-Connection-Method

Wireless

Cloud-NAC-Locale-Name

Lab

Cloud-NAC-NAS-Identifier

68:49:92:37:61:a0

Cloud-NAC-Network-Name

Lab - wireless

Thank you



