

Cisco Cloud Networking

...aneb Enterprise Networking spravovaný z cloud dashboardu

Stanislav Kraus

stakraus@cisco.com



Another massive technology disruption

Internet

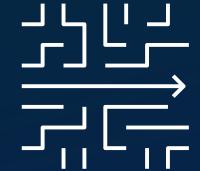
Mobility

Cloud

AI

Architecture for the AI-Ready Secure Network

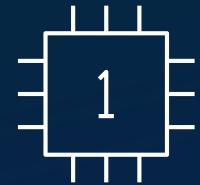
Operational simplicity
powered by AI



Security
fused into the network



Scalable devices
ready for AI



Simplifying operations by Unifying our platforms

Catalyst

Catalyst Center

Catalyst License

Catalyst Hardware

MANAGEMENT

LICENSE

CISCO HARDWARE

Meraki

Meraki Dashboard

Meraki License

Meraki Hardware

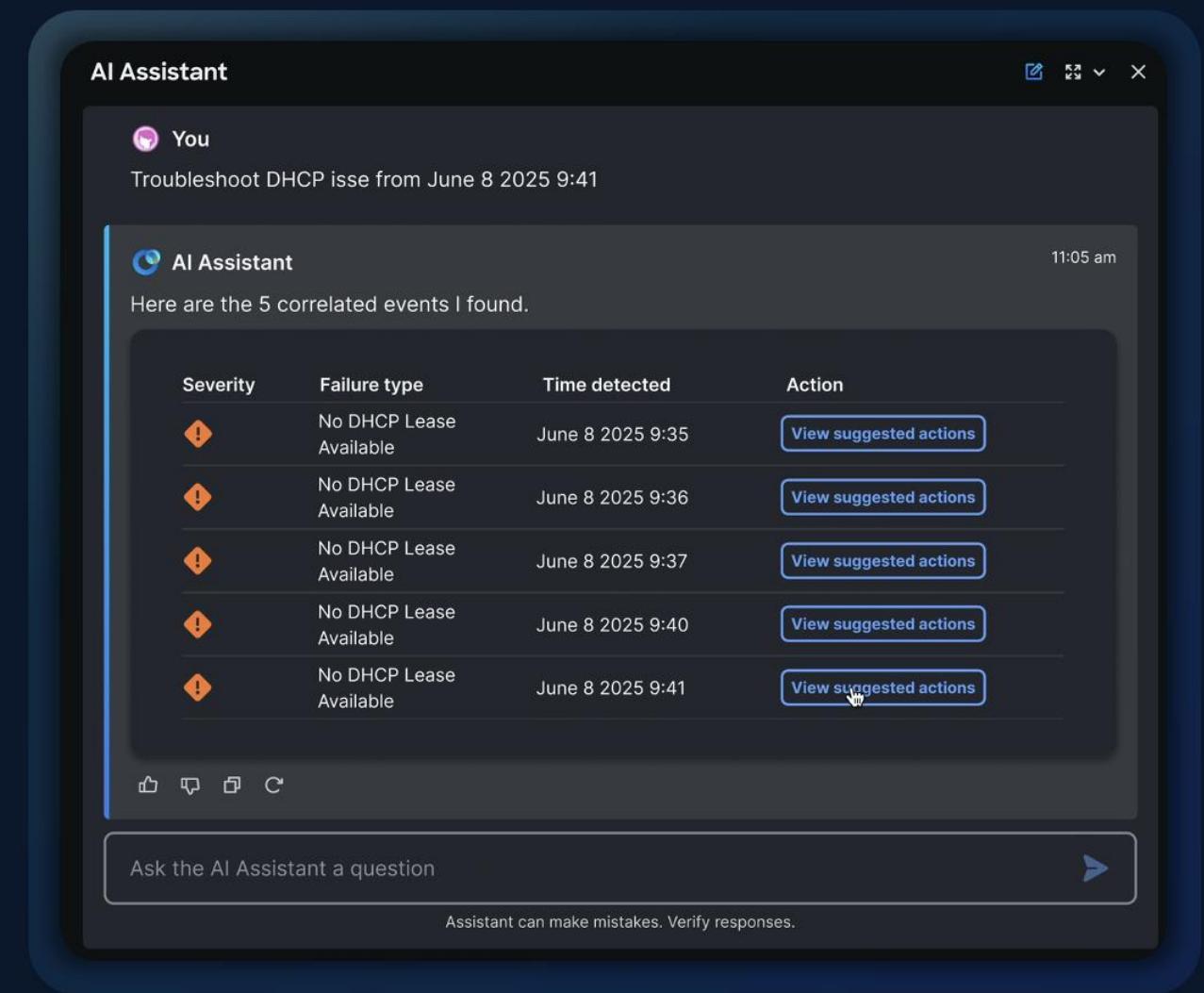
AI Assistant

Rapid troubleshooting and RCA

Finds root cause—not just the alert

Provides full stack visibility

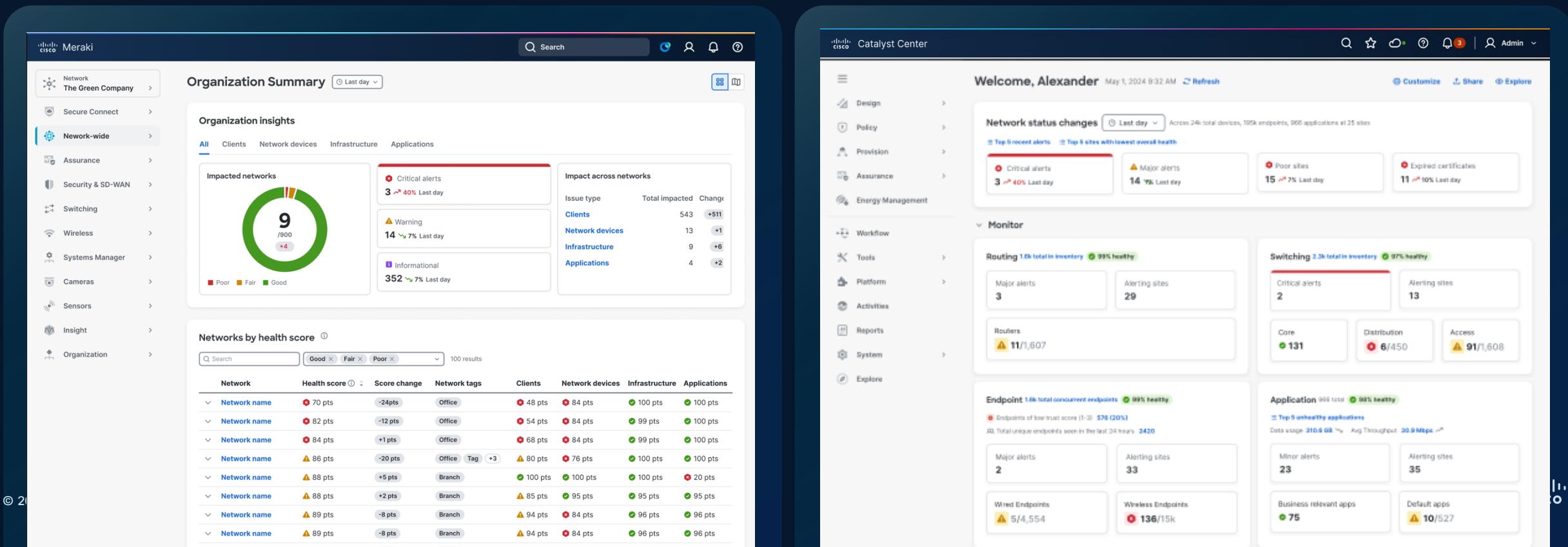
Pinpoints the issue and guides the fix



AVAILABLE NOW

Common experience: Meraki & Catalyst Center

Bringing together the power of **Catalyst** and simplicity of **Meraki**



The image displays two screenshots of the Cisco Catalyst Center interface. The left screenshot shows the 'Organization Summary' page, which includes a 'Network insights' section with a '9/900' status and a 'Impact across networks' table. The right screenshot shows the 'Welcome' page, which includes a 'Network status changes' section and a 'Monitor' section with various network health metrics.

Organization Summary

Organization insights

Impact across networks

Issue type	Total impacted	Change
Clients	543	+511
Network devices	13	+1
Infrastructure	9	+6
Applications	4	+2

Networks by health score

Network	Health score	Score change	Network tags	Clients	Network devices	Infrastructure	Applications
Network name	70 pts	-24pts	Office	48 pts	84 pts	100 pts	100 pts
Network name	82 pts	-12 pts	Office	54 pts	84 pts	99 pts	100 pts
Network name	84 pts	+1 pts	Office	68 pts	84 pts	99 pts	100 pts
Network name	86 pts	-20 pts	Office, Tag	80 pts	76 pts	100 pts	100 pts
Network name	88 pts	+5 pts	Branch	100 pts	100 pts	100 pts	20 pts
Network name	88 pts	+2 pts	Branch	85 pts	95 pts	95 pts	95 pts
Network name	89 pts	-8 pts	Branch	94 pts	84 pts	96 pts	96 pts
Network name	89 pts	-8 pts	Branch	94 pts	84 pts	96 pts	96 pts

Welcome, Alexander May 1, 2024 9:32 AM

Network status changes

Monitor

Routing 1.6k total in inventory 99% healthy

Switching 2.3k total in inventory 97% healthy

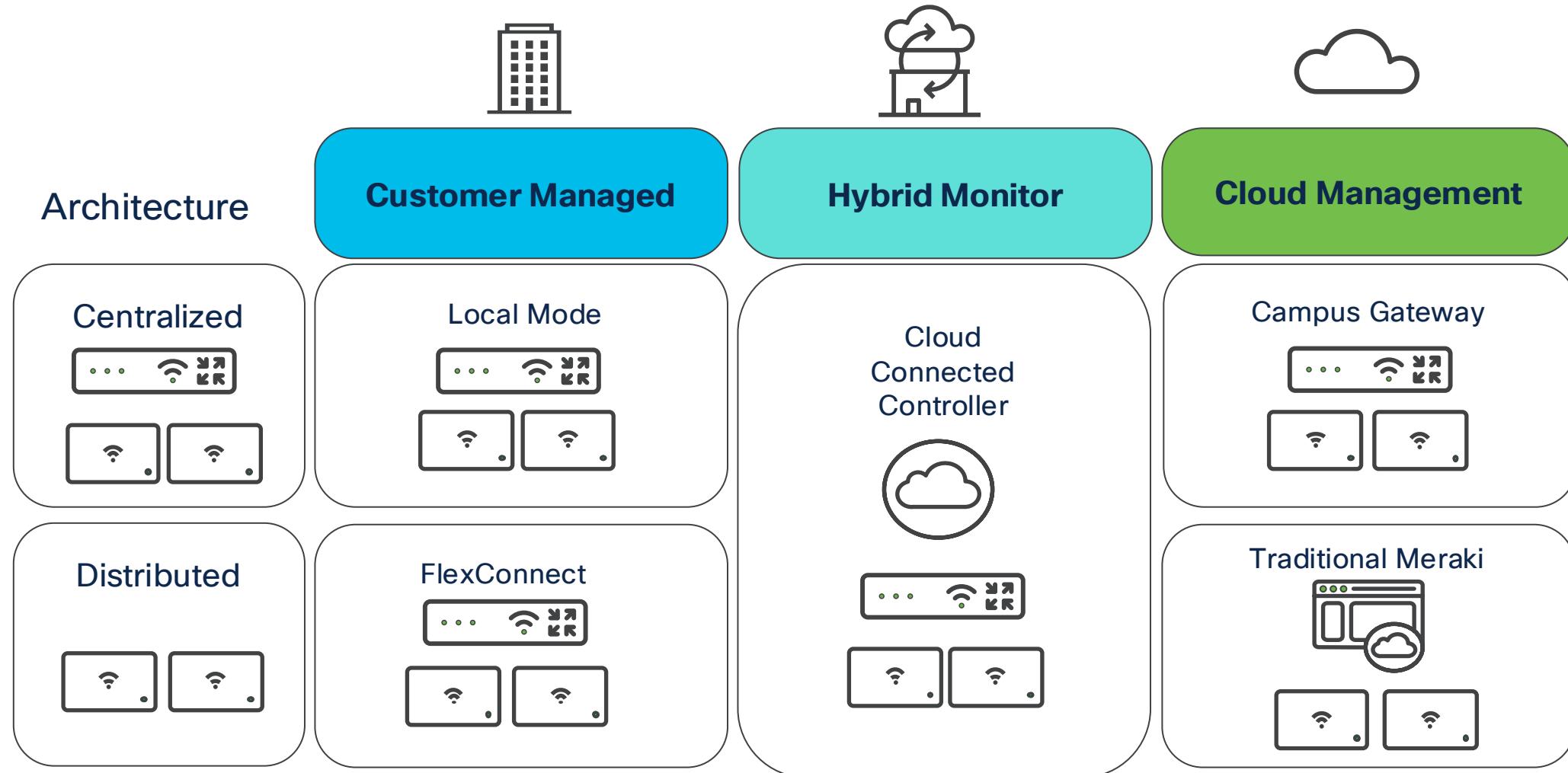
Endpoint 1.6k total concurrent endpoints 99% healthy

Application 988 total 99% healthy

Wireless



Deliver simplified outcomes to all customers

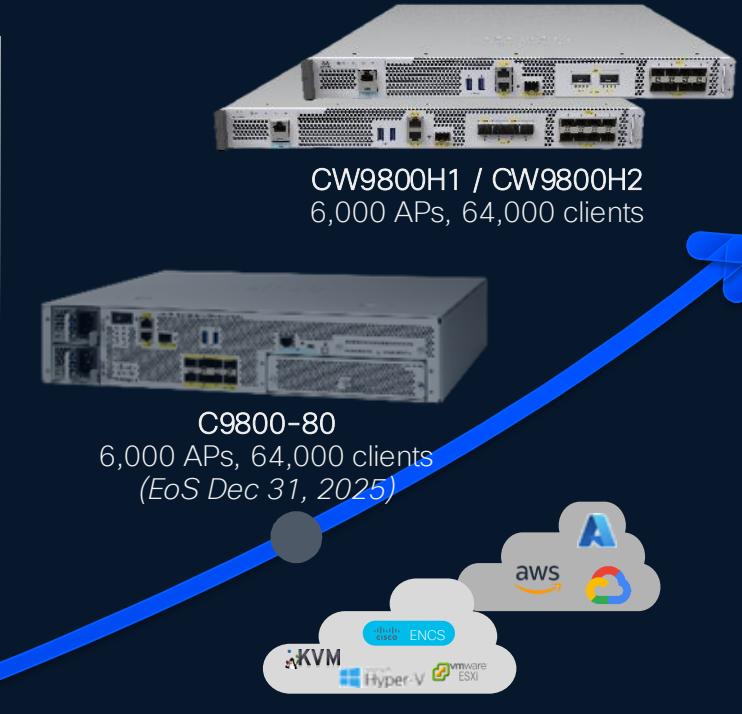
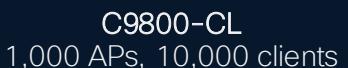
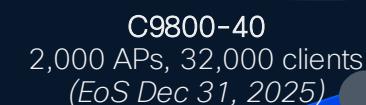


Cloud Monitoring Wireless Controller Portfolio

WLC Requirements

Connecting WLC to Dashboard

Adding WLC & AP to Dashboard



Up to 200 APs

Up to 500 APs

Up to 1000 APs

Up to 3000 APs

Up to 6000 APs

Distributed branch and small campus

Medium campus

Large campus

Scales up to
5,000 APs
and 50,000 clients

Easy migration for
existing LAN
controller
architectures

No need to
re-cable, change
VLANs, or disrupt
operations

Introducing The New Campus Gateway



Cisco Campus Gateway

Cloud Managed/Monitored Wi-Fi 7 Access Points



CW9172H

6 Spatial Streams

Dorm Rooms, Hospitality



CW9174E

8/10 Spatial Streams

External antennas

NEW!



CW9176D1

12 Spatial Streams

Integrated Directional

UWB



CW9179F

16 Spatial Streams

LPV/Stadium



CW9171I

4 Spatial Streams

Omnidirectional

NEW!



CW9172I

6 Spatial Streams

Omnidirectional



CW9174I

8/10 Spatial Streams

Omnidirectional

NEW!



CW9176I

12 Spatial Streams

Omnidirectional

UWB



CW9178I

16 Spatial Streams

Omnidirectional

UWB

Wi-Fi 7 | Global Use AP | Unified License | AI Optimized

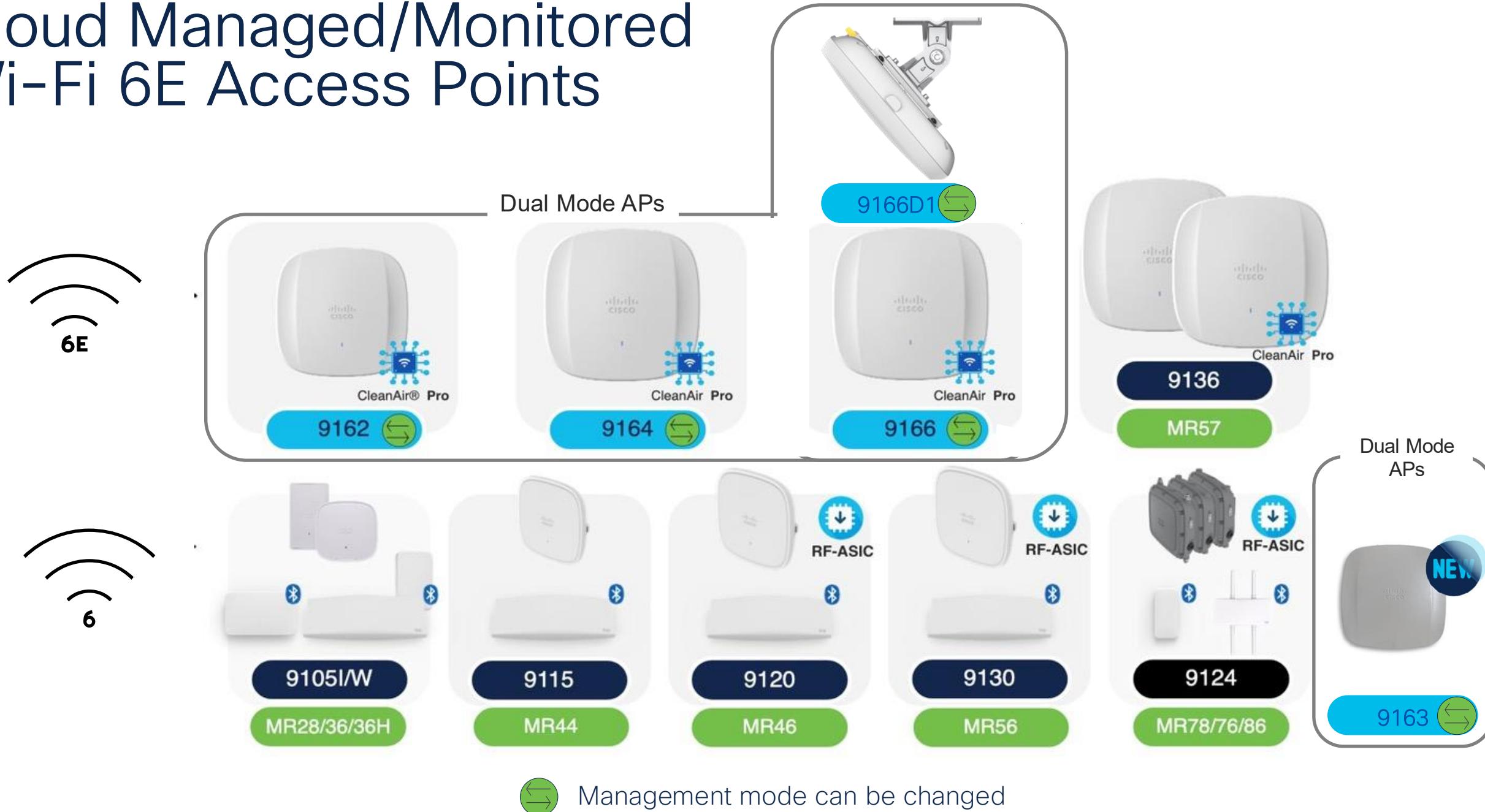
GUAP - Global Use AP Deployment Guide

- Link: [global-use-ap-dg.html](#)



The screenshot shows the Cisco Wireless Global Use Access Points Deployment Guide page. The page title is "Cisco Wireless Global Use Access Points Deployment Guide". The left sidebar contains a "Table of Contents" with sections like "Cisco Wireless Global Use AP ...", "Map of a Global Use AP's Jour...", "Cloud ID", "Day 0 Workflow: Technical Det...", "Country Code and Regulatory ...", "Factory Reset", and "Important Links". The main content area features a section titled "Cisco Wireless Global Use AP Overview" with a sub-section "Global Use AP, Unified Product, Single SKU". It shows a diagram with three components: "Cisco Catalyst Management Mode C9800 & Catalyst Center Stack" (represented by a server icon), "Meraki Management Mode MR Dashboard Stack" (represented by a smartphone and laptop icon), and a central "Global Use AP" (represented by a white AP icon with a gear inside). Arrows indicate a "Join WLC or Meraki stack on Day 0, based on Intent" and a "Management Mode Change from Day 1 to N". Below the diagram, the text "The Global Use AP simplifies the Cisco Wireless AP portfolio, by" is followed by two numbered points: 1. Decoupling the AP PID/SKU from which geography (regulatory domain) they can be used. 2. Decoupling AP PID/SKU from the boot mode; that is, WLC or Meraki based. The page also includes a "Bias-Free Language" link, a "Contact Cisco" dropdown, and download/print buttons.

Cloud Managed/Monitored Wi-Fi 6E Access Points

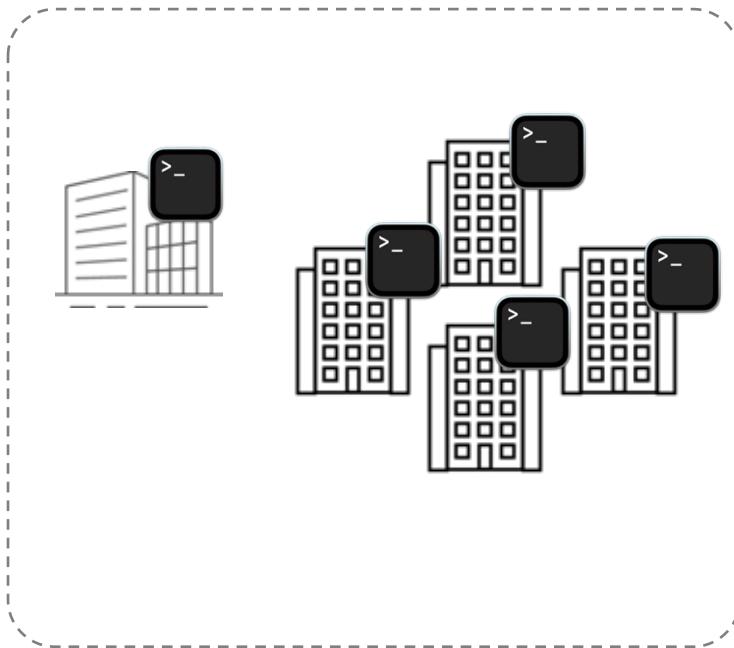


Switching

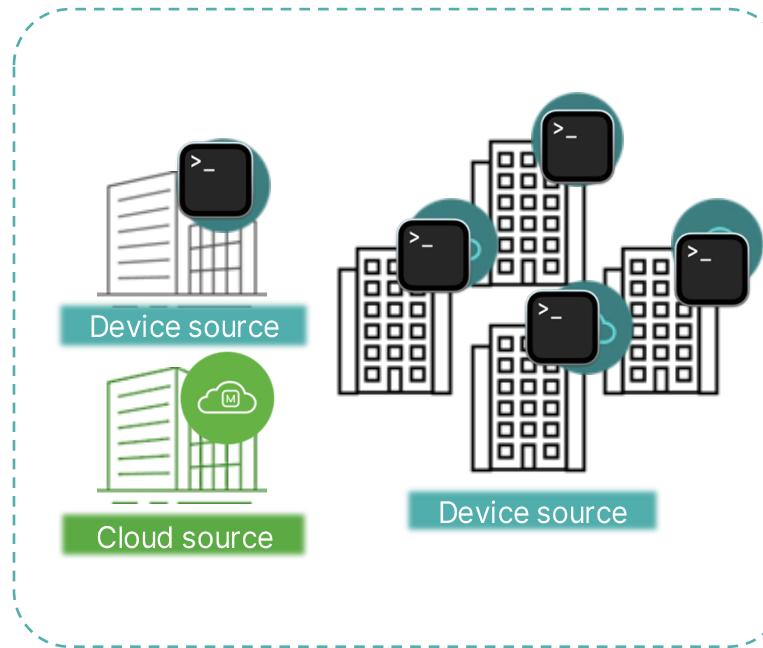


Cloud platform adoption option

Today



No Platform CLI managed



Simplified Hybrid Network Operations

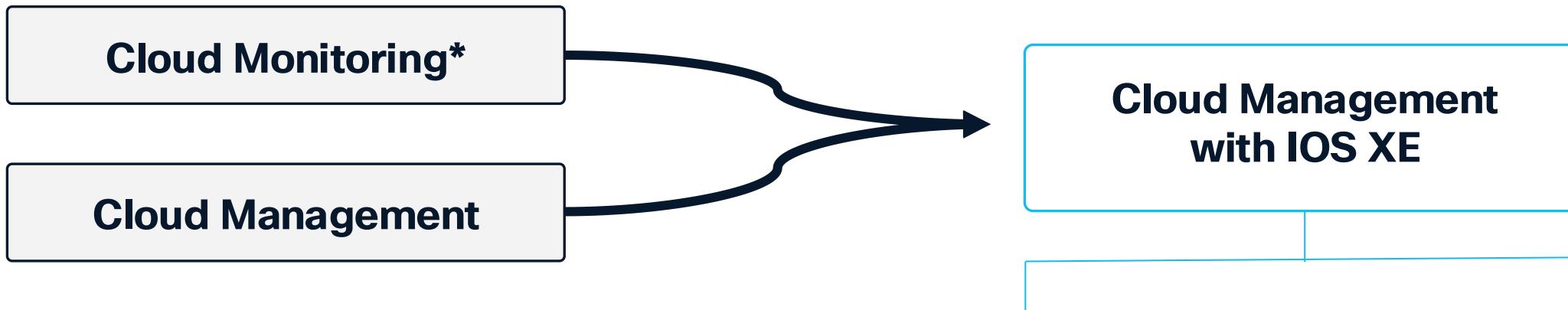


Cloud Managed

Cloud Management Evolution

Before XE 17.15 (CS Firmware)

Currently - After XE 17.15 (IOS XE)



Device Configuration Mode

- *Evolution of cloud monitoring*
- *Retain **full access** to IOS XE feature set*
- *Configure devices locally*

Cloud Configuration Mode

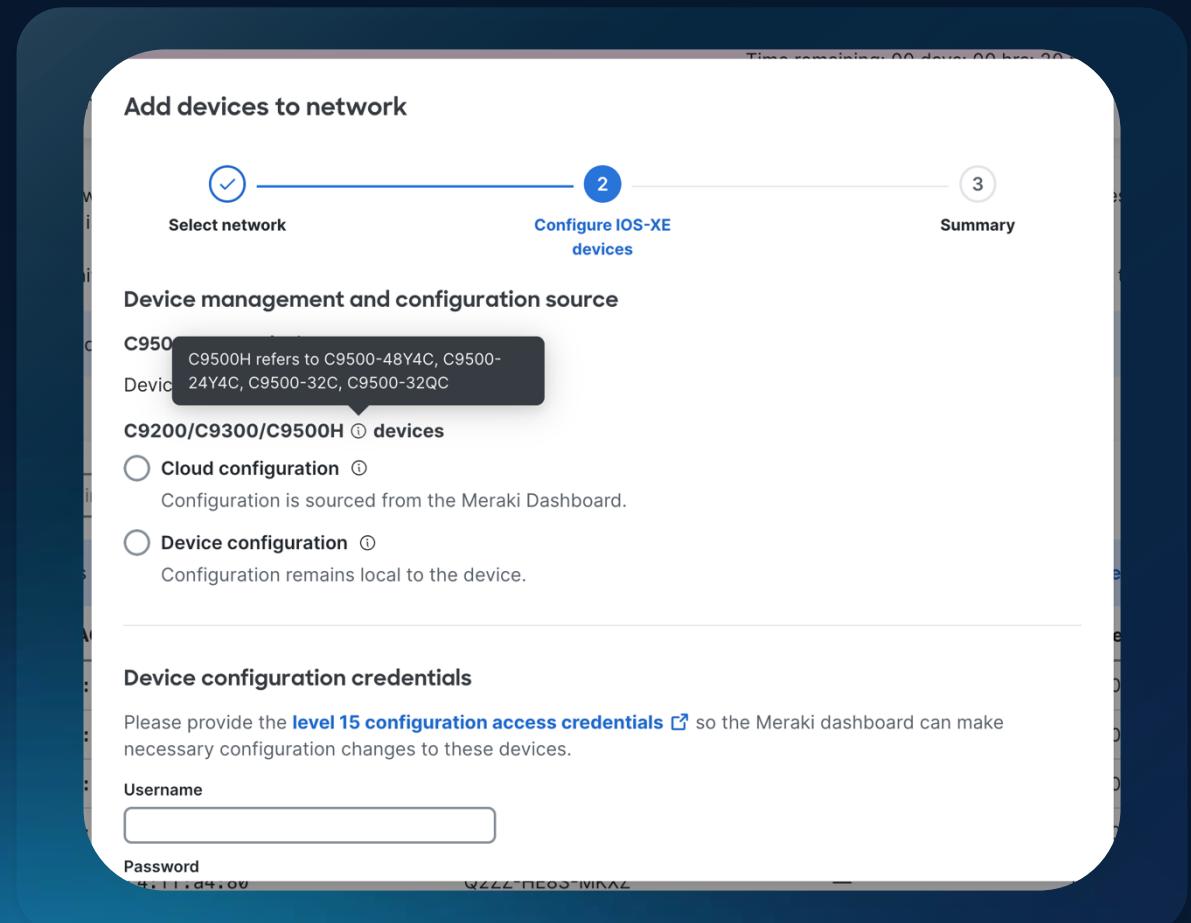
- *Evolution of cloud management*
- *Embrace **full-cloud simplicity** (MS-like)*
- *Configuration largely driven by UI*

* End-of-Life (March 2026) Announcement & migration

Available Now

It starts with a **streamlined** onboarding process

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



GA: IOS XE 17.15.4

Configuration Source

Device Config



Existing management tools/management operations

Config Source of truth:
IOS XE

IOS XE CLI



*config
backup*



Config Source of truth:
Dashboard



Cloud Config

Config updater



*Adopt cloud-managed networking as you evolve
your IT operations to cloud*

*Full cloud-managed for efficient and scalable
cloud network operations*

Cisco (cloud) switching access portfolio

Resilient campus

Catalyst® 9000 family

- Catalyst product experience with Cisco IOS® XE
- Cloud + CLI support
- Deep switching feature set



Catalyst 9350*



Catalyst 9300X-M



Catalyst 9300/-M



Catalyst 9300L/-M



Catalyst 9200L/-M



MS130



MS150

*Single SKU – Unified Licensing model

MS100 Series

- MS product experience with Meraki® OS
- Cloud only (no CLI)
- Basic switching features

MS130 and MS150

MS130(X)



Simple and secure
for **distributed sites**

2.5GbE

- 30W PoE+
- Up to 740W budget
- MS130X – Adaptive Policy

MS150



Cost-effective options
for Wi-Fi 7 and stacking

5GbE

- 60W PoE++
- Up to 740W budget
- Perp. PoE / Fast PoE
- Stacking 80 Gbps
- Static Routing
- Adaptive Policy

Cloud Only

Cloud-Managed Catalyst Switching

Intuitive and efficient
Scalable operations



Powerful and customizable
Advanced core networks

Same powerful hardware with flexible operations

IOS XE 17.15

IOS XE 17.18

Up next



C9300L



C9300



C9300X



C9200L



C9500



C9200/CX



C9300LM

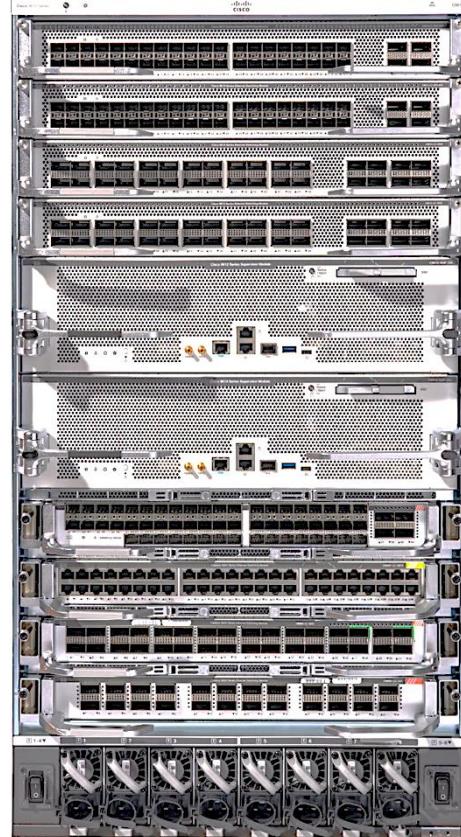


C9350



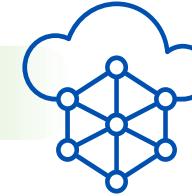
Modular*

Cisco's first cloud managed modular switch - C9610



Supervisor and line cards				
Slot	Model	Role	Serial number	...
1	C9600-LC-48TX	—	FDO2832072A	
2	C9600-LC-48TX	—	FDO28360KH5	
3	C9600X-LC-56Y4C	—	FDO27230H8M	
4	C9600X-LC-56Y4C	—	FDO27230H8M	
5	C9610-SUP-3XL	Active	FDO282	
6	C9610-SUP-3XL	Standby	FDO282	
7	C9610-LC-32CD	—	FDO284	

Cloud Management



Meraki Cloud

Configuration Source: Cloud

Full Cloud Management Experience



Configuration Source: On-Device

Configuration remains local to the device

17.18.2



Roadmap

Cloud Managed Switch

New features enabled by IOS XE

Advanced Routing

Routed Ports

Loop free Routed Access

VRF Lite

Scalable Macro Segmentation

BGP

Flexible open dynamic routing

High-Availability

Rapid PVST+

Enhanced L2 loop Prevention

StackWise Virtual (SVL)
ISSU

Sub-second downtime firmware
upgrades

C9500

SVL

ISSU

C9200/9300

RPVST+

VRF

Routed Ports

BGP*

*BGP supports on C9200CX, MS390, C9300 and C9500



Introducing VRF deployment from the cloud

Easily create isolated routing domains without additional hardware

Strengthen security with scalable macro-segmentation, limiting lateral movement of threats

Simplify network management by eliminating the need for ACLs on every SVI

The screenshot displays the Cisco Cloud Network Controller interface with three main windows:

- Routing & DHCP**: A table showing network interfaces and their configurations. Key data includes:

Interface	Name	VRF	Subnet	IP
80 VLAN	eighty	BLUE_VRF	10.80.80.0/24	10.80.80.254
80 VLAN	BLUE VLAN 80	BLUE_VRF	10.80.80.0/24	10.80.80.253
Bob / 13	Bobs routed port	BLUE_VRF	10.88.88.0/24	10.88.88.252
Bob / 14	Bobs 2nd routed port	BLUE_VRF	10.89.89.0/24	10.89.89.252
0 Loop	0	BLUE_VRF	10.252.252.252/32	10.252.252.252
20 VLAN	Uplink Vlan 20	Default	10.20.20.0/24	10.20.20.2
- Edit BLUE_VRF**: A configuration dialog for the VRF 'BLUE_VRF'. It includes fields for 'VRF name' (set to 'BLUE_VRF'), 'Description' (set to 'IoT'), 'Route distinguisher' (set to '52:106'), and 'Route target' (empty). Buttons for 'Save changes' and 'Cancel' are at the bottom.
- VRF**: A summary view showing 0 VRFs with associated interfaces and 0 VRFs without associated interfaces. It includes a search bar and a 'Add VRF' button. A table lists existing VRFs: Default (Route distinguisher: —, Route target: —, Networks: —), BLUE_VRF (Route distinguisher: 52:106, Route target: —, Networks: —), GREEN_VRF (Route distinguisher: 52:108, Route target: —, Networks: —), and RED_VRF (Route distinguisher: 52:107, Route target: —, Networks: —).

Introducing Routed Ports from the cloud

Reduce convergence time while simplifying network management

Routed peer to peer links including east/west and north/south traffic

Minimize VLAN ID consumption while joining separate networks

New port icon

The interface shows a 'Routing & DHCP' section with a table of interfaces, a 'Selected Switch / Port' dialog, and a 'New port icon' grid.

Selected Switch / Port: Bob/13

Interface mode: Routed port (selected)

Tags: Transit Network

Port status: Enabled

Link negotiation: Auto negotiate

EEE: Enabled

Port schedule: Unscheduled

PoE: Enabled

Port isolation: Enabled

Cancel **Update**

Port	13	15	17	19	21	23	1	3
13								
14								
15								
16								
17								
18								
19								
20								
21								
22								
23								
24								
2								
4								

Introducing support for StackWise Virtual from the cloud

Simplify configuration management by presenting two physical switches as one logical entity

Lower the risk associated with a looped topology while reducing operational failure points

Maintain HA with support stateful switch failover (SSO) by ensuring minimal downtime during failures or maintenance

Create Stack

Stack name

Q Search

Name
<input checked="" type="checkbox"/> Ash Twin
<input checked="" type="checkbox"/> Ember Twin

Configure your StackWise Virtual pair

To successfully provision Catalyst 9500 switches as a StackWise Virtual pair, select switch ports below to set up SVL and DAD links.

⚠ Please ensure you have physically connected the ports selected below before proceeding

Stack name: Hourglass Twins
Members: [Ash Twin](#), [Ember Twin](#)

SVL links

Select between 2 and 8 ports on each switch to establish the SVL link. Note that any existing switch port config will be overwritten for ports selected here.

Ash Twin	Ember Twin
<input type="button" value="1 x"/> <input type="button" value="2 x"/> <input type="button" value="3 x"/> <input type="button" value="4 x"/> <input type="button" value="5 x"/> <input type="button" value="6 x"/> <input type="button" value="7 x"/> <input type="button" value="8 x"/>	<input type="button" value="1 x"/> <input type="button" value="2 x"/> <input type="button" value="3 x"/> <input type="button" value="4 x"/> <input type="button" value="5 x"/> <input type="button" value="6 x"/> <input type="button" value="7 x"/> <input type="button" value="8 x"/>

DAD link

Select 1 port to establish the DAD link. Note that any existing switch port config will be overwritten for the port selected here.

Ash Twin	Ember Twin
<input type="button" value="3"/>	<input type="button" value="3"/>

I acknowledge that by clicking 'Configure' I have physically connected the ports selected for SVL and DAD links.

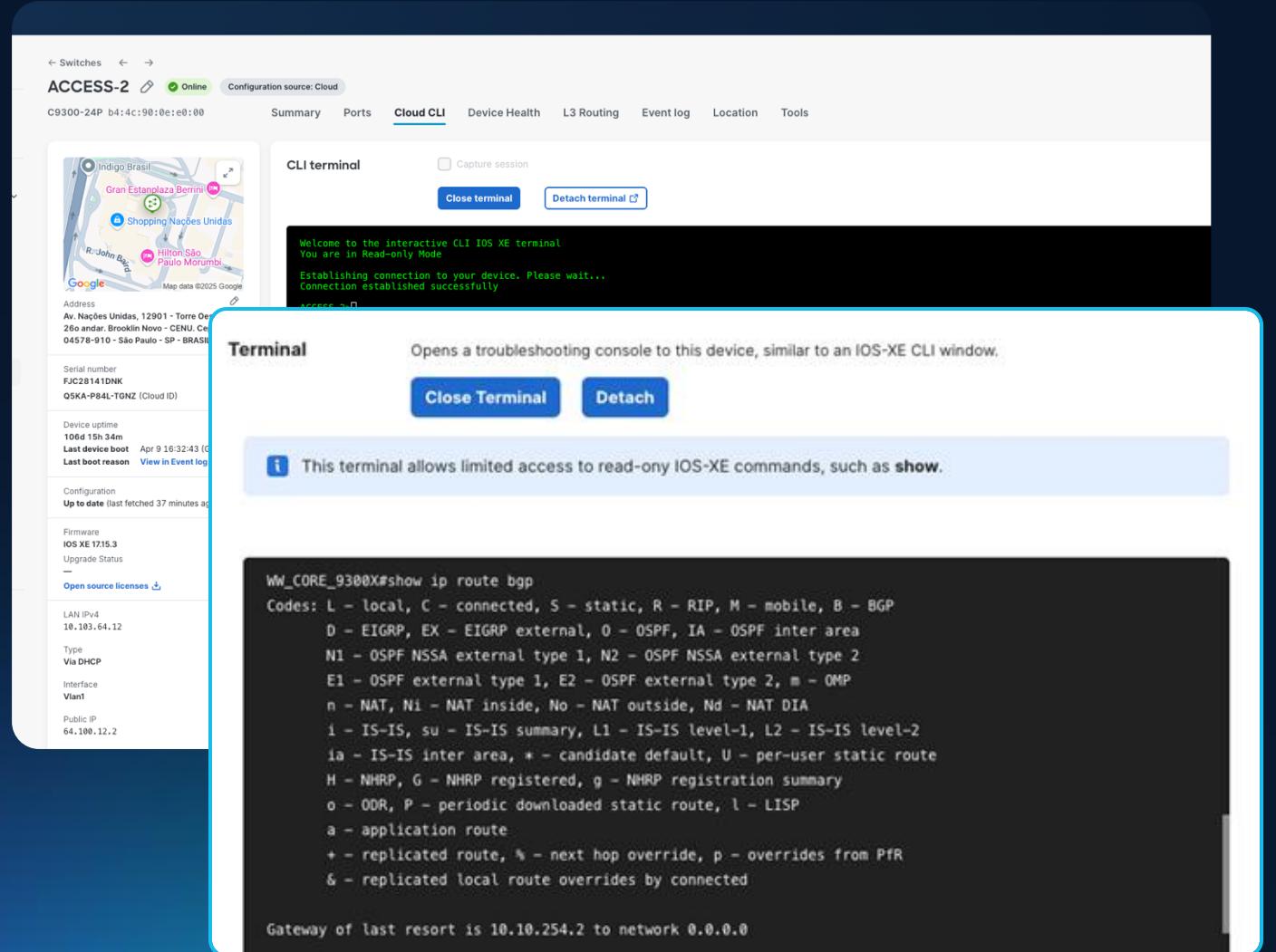
[Cancel](#) [Configure](#)

Introducing a secure Cloud CLI terminal, directly in dashboard

Access an embedded cloud-hosted CLI terminal within the Meraki dashboard without the need for VPN or jump host

Support for common CLI commands to uncover network issues effecting network devices

Leverage existing and familiar skillsets while ensuring your teams maintain access to detailed device data with CLI



Coming Soon: Cloud CLI Config

Expanding Cloud CLI capabilities to introduce select 'config' commands for cloud config mode devices.

Device Configuration

A fully functional CLI terminal in dashboard. Support for full IOS XE feature set.

Cloud Configuration

A safe guarded CLI terminal with support for 'show' commands, plus an expanding set of 'read/write' commands for features not supported by the dashboard UI.

Access Manager

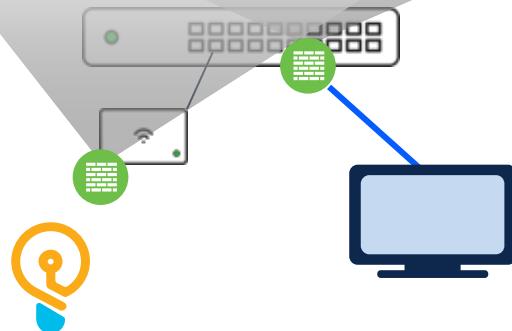
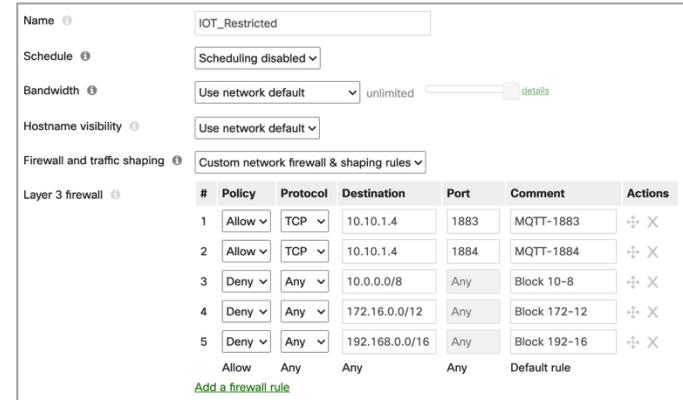


802.1X and RADIUS Support is not new to Meraki

Per-Session VLAN Assignment



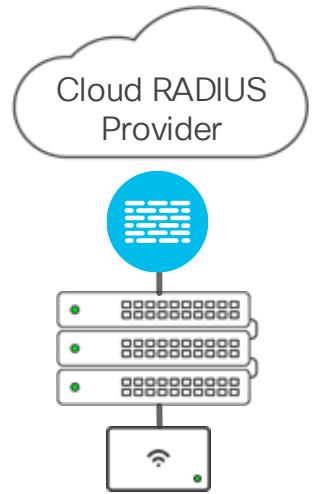
Per-Session Dynamic L3/L4 ACL



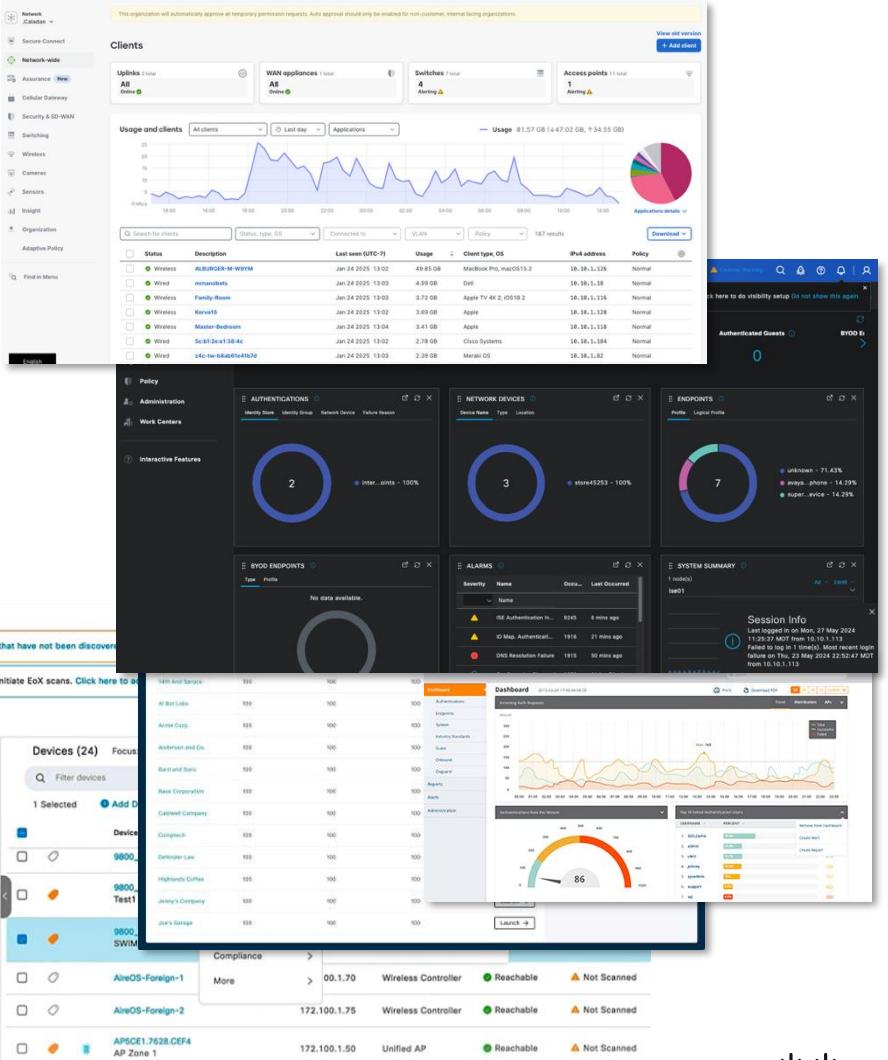
Zero-Trust micro-segmentation



In this case, not everything is simple

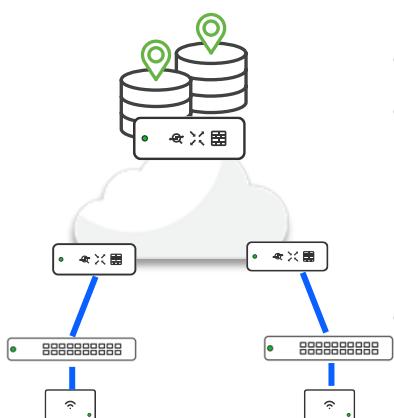


- Complex firewall rulesets
- Complex connectivity security requirements
- Potential in-transit security implications
- Manual input of network and security contexts



Higher OpEx from console pivots

On-premises AAA



- Complex deployment management and Operations
- Connectivity complexity in distributed deployments
 - VPN tunnel management
 - Load-balancers
 - Etc.
- Manual input of network and security contexts

Introducing Cisco Access Manager

Cloud-delivered access control services to enforce identity and context-based access to the users and devices

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/O/T



Cisco Access Manager Current Capabilities

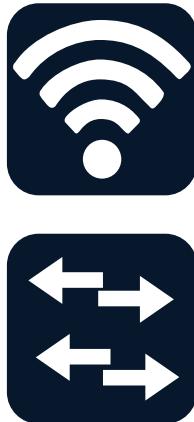
Clients/Endpoints



Users, Computers, Things

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

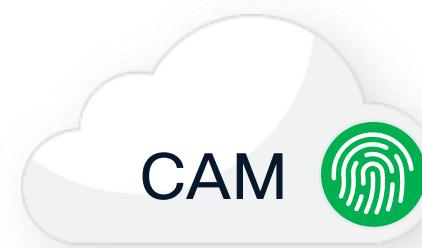
Network Devices



Cloud Managed *ONLY*

MS: 17+
CW91xx: 30.7+
MR: 30.7+
MX / Z: *Unsupported*

Access Manager



Cisco Meraki Dashboard

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

Identity Providers



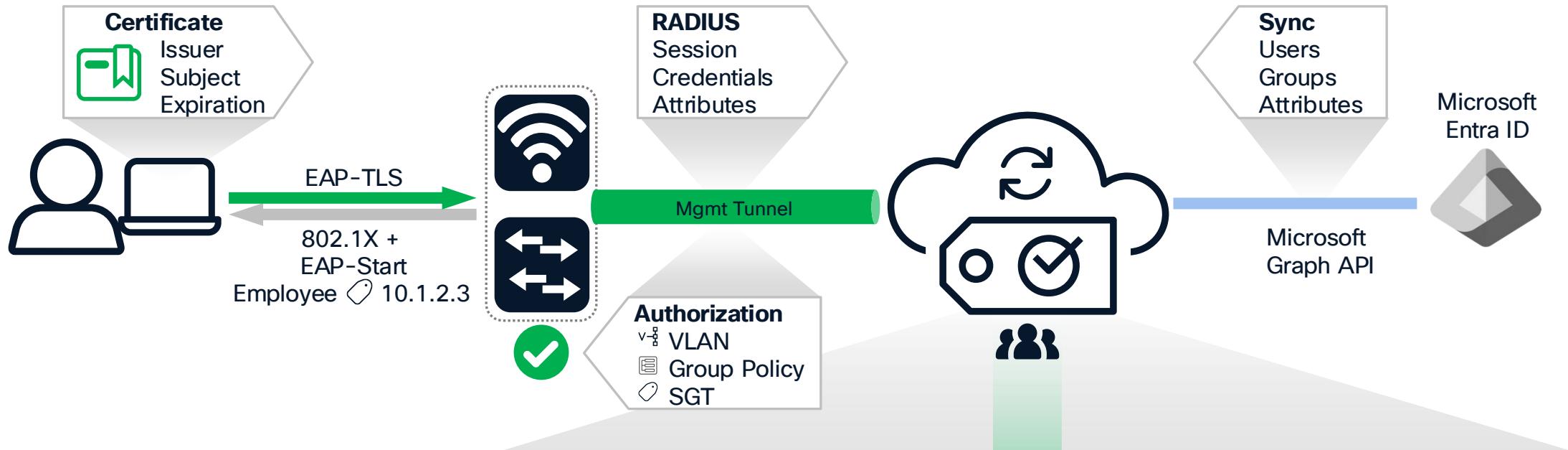
Microsoft Entra ID *ONLY*

Certificate Identities
Username + Password
User Group Lookups

Securing managed endpoints with Entra ID Lookup

EAP-TLS Certificate Based Authentication with Entra ID Lookup

EAP-TLS Client Configuration



Type	Status	Name	What's Matched	Authorization
- Rule	<input checked="" type="checkbox"/>	Workstations	Certificate:Issuer = My Org EntraID:Group = Workstations	Adaptive Policy = Workstation
- Rule	<input checked="" type="checkbox"/>	Employees	Certificate:Issuer = My Org EntraID:Group = Employees	Adaptive Policy = Employee

Routing & SD-WAN



Secure Routers for the AI-powered unified branch

Cisco 8000 Secure Routers

More throughput to support increased traffic to data center

Advanced routing and firewall for secure SD-WAN and SASE

Post-quantum secure



Cisco Secure Router 8455-G2-MX

Network Concentrator

- Handoff of VPN Transport within Data Centre Infrastructure

Next-Gen Edge Router & Firewall

- Routing at scale
- Next Generation Firewall services at the edge

SD-WAN & VPN Transport

- Application awareness
- Routing at scale
- Next Generation Firewall services at the edge

AVAILABLE NOW



8455-G2-MX

Maximum NGFW Throughput	20 Gbps
Flow Table Capacity	2,000,000
Recommended Clients	15,000
Recommended AutoVPN Peers	5,000
Recommended Route Table Capacities	BGP – 50,000 Static / Dashboard – 10,000

Release Naming post MX 19.2

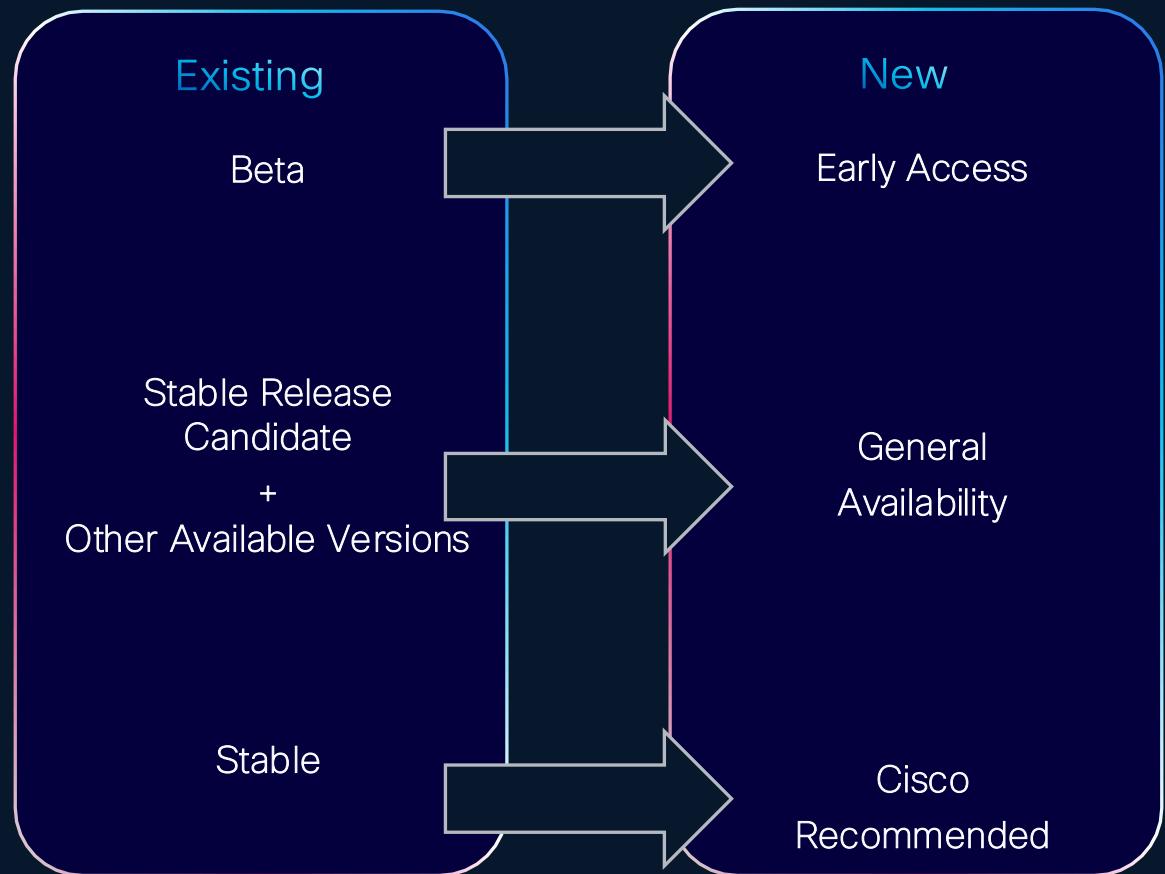
MX Release version change (also applicable to wireless, switching, IoT portfolio)

20.X → 26.X
[year].[feature release]

Industry Initiative to help simplify software versions

Not new in Cisco (Cisco IOS-XR taxonomy since 2024)

Release Phase rename - Dashboard



From November 1st 2025

ThousandEyes Agent



- **Onboard** the TE agent on Meraki Dashboard
- **Activate** on 100+ networks with few clicks
- **Overview** of results from the tests

Set up ThousandEyes

1 Set up ThousandEyes

Authorize ThousandEyes access to Meraki

Log into an existing account [Create a new account](#)

2 Select networks to activate as agents

3 Review selection

Cancel All changes saved

Back Next

Set up ThousandEyes

1 Set up ThousandEyes

ThousandEyes account synced with your Meraki account

2 Select networks to activate as agents

Search by network name Network tags 138 networks

Network tags

Network

Meraki Chicago - Post Office CHG12 Office Chicago Branch

Meraki Chicago - Data Center Office Chicago Branch

Meraki London - Post Office LON12 Office London Branch

Meraki London - Bishopsgate LON16 Office London Branch

Meraki London - Finsbury LON11 Office London Branch

3 Review selection

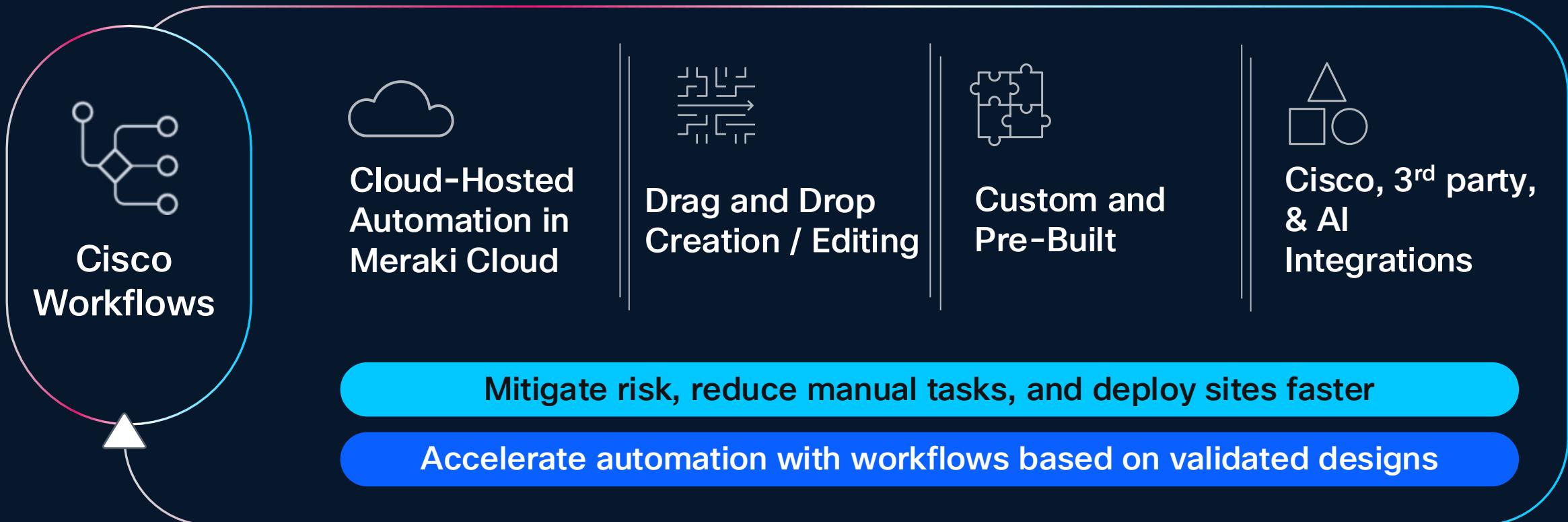
Cancel All changes saved

Back Next

Cisco Workflows



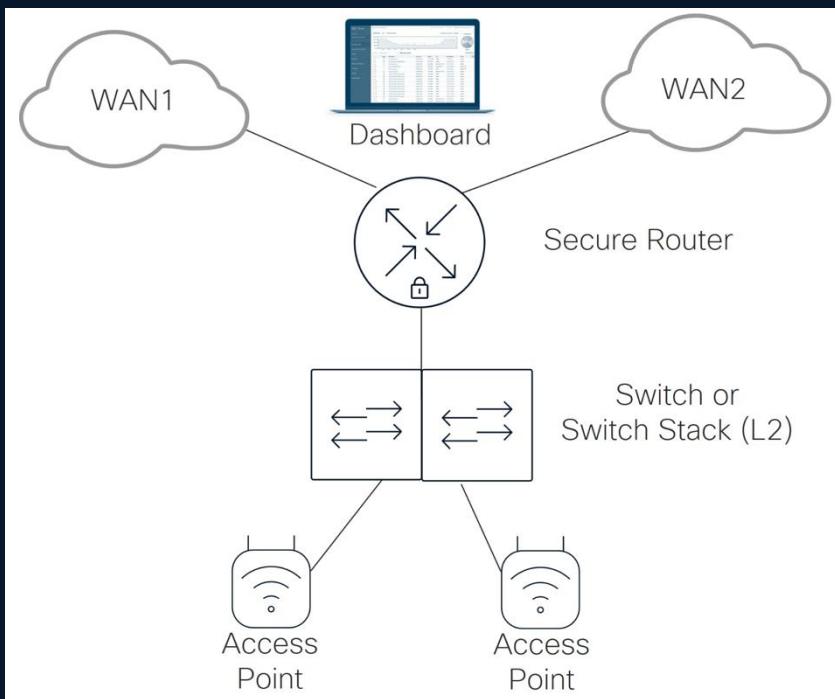
Cisco Workflows in the Meraki Dashboard



Deploy Branches in minutes using Cisco Workflows and AI Assistant

Key Points :

- Pre-built workflow that will help configure an entire branch with MX-MS-MR
- Openly customizable. Can be altered to get creative with customer use cases
- Used for large scale deployments in customer teams where automation skillset is limited



← Explore

Unified Branch

Version 1.0 [Release Notes](#)

★★★★★ Average Rating

Average Rating 5 out of 5 (1 ratings)

Community

This workflow deploys a full-stack Cisco Unified Branch, powered by Cisco Validated Designs (CVDs) and advanced automation. It accelerates... [Read more](#)

Author unifiedbranch-queries@cisco.com

Integration Meraki

Workflow [Unified Branch](#)

Installation Instructions

1. **Install from Exchange**
Install "Unified Branch" workflow from the Exchange.
1. **Create a Meraki Target for the workflow to run against**
Navigate to Targets → Create Target
Target A: Meraki Endpoint
Target Type: Meraki Endpoint. Complete setup using the Meraki Credentials account key type.

1. Input Branch Details

Define your branch details by using the workflow variables. The variables listed below are just some key examples, for more details on the branch variables, please refer to the [Unified Branch documentation](#).

- Unified Branch Network Name: Network name for your unified branch.
Example: Houston Branch Office. Can only contain letters, numbers, spaces, and these characters: @ # _ -

Install Workflow

Choose to 'Install' and configure the workflow along with updating necessary objects such as accounts and variables, or 'Skip Configuration and Install' to install the workflow now and configure or update later in the Workflow Designer.

The following Variables are used with the workflow.

Type	Name	Description
String	Unified Branch Network Name	Network name for your unified branch. Example: Houston Branch Office. Can only contain letters, numbers, spaces, and these characters: @ # _ -
String	Appliance VLAN ID for IoT Traffic	VLAN ID for IoT Traffic Example: 10
String	Appliance Serial Number	Serial number of the MX appliance. Example: XXXX-YYYY-ZZZZ
String	Appliance VLAN ID for Network Device Management	VLAN ID for Network Device Management Example: 10
String	Appliance VLAN ID for Guest Traffic	VLAN ID for Guest Traffic Example: 10
String	Organization ID	The Meraki Organization ID when the network is created.
Boolean	Ignore If Devices are Claimed	When enabled, workflow will skip this step and be marked as successful if devices are already claimed to Network. If workflow execution stops at this step when first device that is already encountered.
String	Switch Serial Number	Example: Q2HP-LPX9-BKM
Secure String	Wireless PSK Password SSID 1	Pre-shared key (PSK) password for the wireless network. Required Authentication Mode is set to WPA2-PSK. The password must meet minimum complexity requirements (typically 8-63 characters), and it is encrypted during transmission.
String	Appliance VLAN ID for Staff and POS Traffic	VLAN ID for Staff and POS Example: 12
String	Appliance VLAN ID for second wireless network. Example: Q2HP-LPX9-BKM	Pre-shared key (PSK) password for the second wireless network. Required Authentication Mode is set to WPA2-PSK. The password must meet minimum complexity requirements (typically 8-63 characters), and it is encrypted during transmission.

CISCO Live ! 2026 Amsterdam 9-13.2.2026



[Registrace](#)

[Broadcast](#)

Cisco TechClub

Lokální edukační on-line webináře každých 14 dní

Cisco TechClub
hlavní portál



Cisco TechClub
registrační stránka



Cisco TechClub
Webex Space



