

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

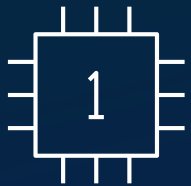
Operational simplicity
powered by AI



Security
fused into the network



Scalable devices
ready for AI



Simplifying operations by Unifying our platforms

Catalyst

Meraki

Catalyst Center

MANAGEMENT

Meraki Dashboard

Catalyst License

LICENSE

Meraki License

Catalyst Hardware

CISCO HARDWARE

Meraki Hardware

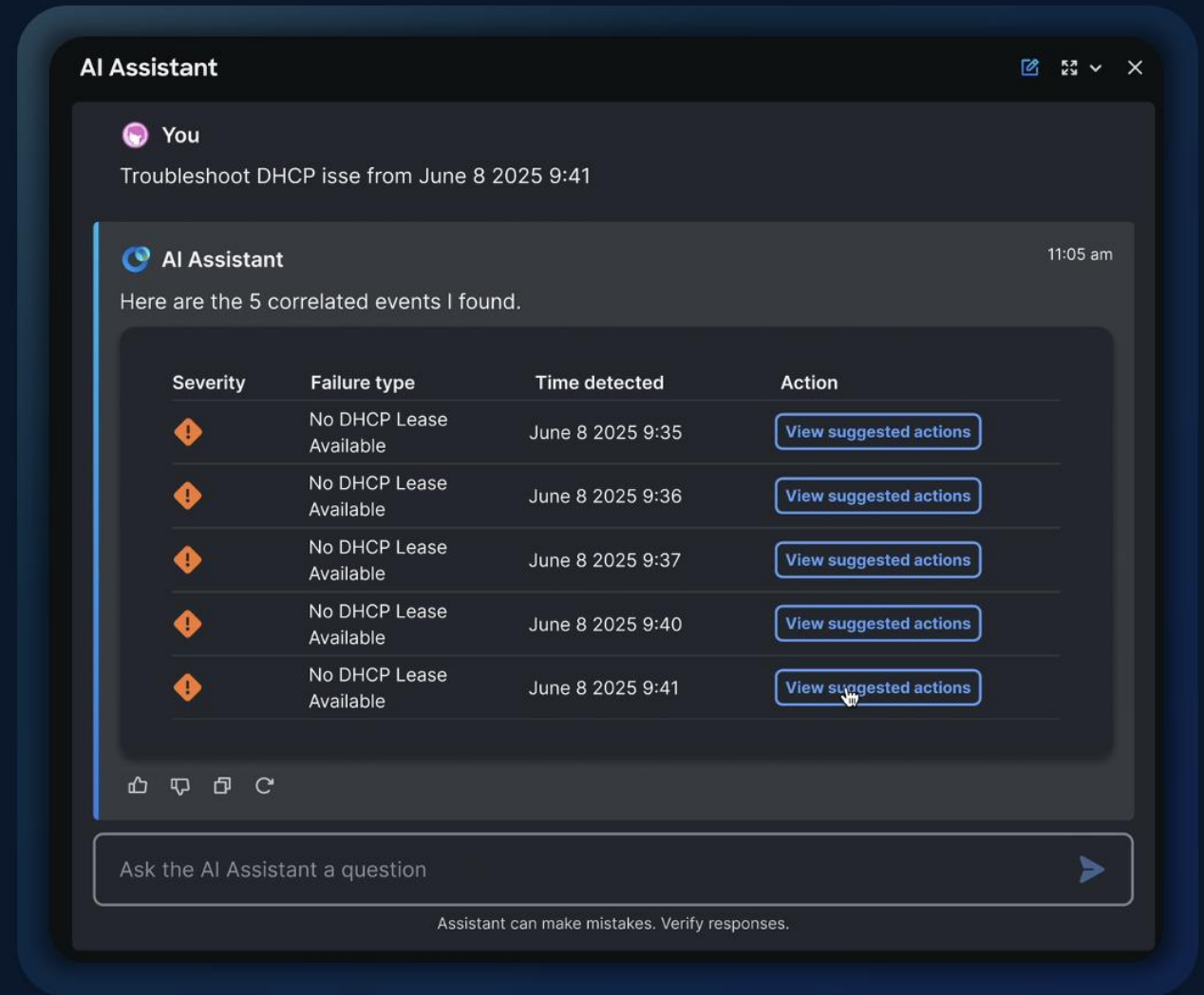
AI Assistant

Rapid troubleshooting and RCA

Finds root cause—not just the alert

Provides full stack visibility

Pinpoints the issue and guides the fix



Common experience: Meraki & Catalyst Center

AVAILABLE NOW

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

Meraki

Search

Network

The Green Company

Secure Connect

Network-wide

Assurance

Security & SD-WAN

Switching

Wireless

Systems Manager

Cameras

Sensors

Insight

Organization

Organization Summary

Last day

Organization insights

All Clients Network devices Infrastructure Applications

Impacted networks

9 / 900

Poor Fair Good

Critical alerts

3 40% Last day

Warning

14 7% Last day

Informational

352 7% Last day

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

Good Fair Poor

100 results

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	-12pts	Office	54 pts	84 pts	99 pts	100 pts
Network name	84 pts	+1pts	Office	68 pts	84 pts	99 pts	100 pts
Network name	86 pts	-20pts	Office Tag +3	80 pts	76 pts	100 pts	100 pts
Network name	88 pts	+5pts	Branch	100 pts	100 pts	100 pts	20 pts
Network name	88 pts	+2pts	Branch	85 pts	95 pts	95 pts	95 pts
Network name	89 pts	-8pts	Branch	94 pts	84 pts	96 pts	96 pts
Network name	89 pts	-8pts	Branch	94 pts	84 pts	96 pts	96 pts

Catalyst Center

Search

Admin

Welcome, Alexander

May 1, 2024 9:32 AM

Refresh

Customize Share Explore

Design

Policy

Provision

Assurance

Energy Management

Workflow

Tools

Platform

Activities

Reports

System

Explore

Network status changes

Last day

Across 24k total devices, 105k endpoints, 966 applications at 25 sites

Critical alerts

3 40% Last day

Major alerts

14 7% Last day

Poor sites

15 7% Last day

Expired certificates

11 10% Last day

Monitor

Routing 1.6k total in inventory 99% healthy

Major alerts 3

Alerting sites 29

Routers 11/1,607

Switching 2.3k total in inventory 99% healthy

Critical alerts 2

Alerting sites 13

Core 131

Distribution 6/450

Access 91/1,608

Endpoint 1.6k total concurrent endpoints 99% healthy

Endpoints of low trust score (1-30) 576 (20%)

All Total unique endpoints seen in the last 24 hours 2420

Major alerts 2

Alerting sites 33

Wired Endpoints 5/4,554

Wireless Endpoints 136/15k

Application 968 total 99% healthy

Top 5 unhealthy applications

Cats usage 210.6 GB % Avg Throughput 30.9 Mbps

Minor alerts 23

Alerting sites 35

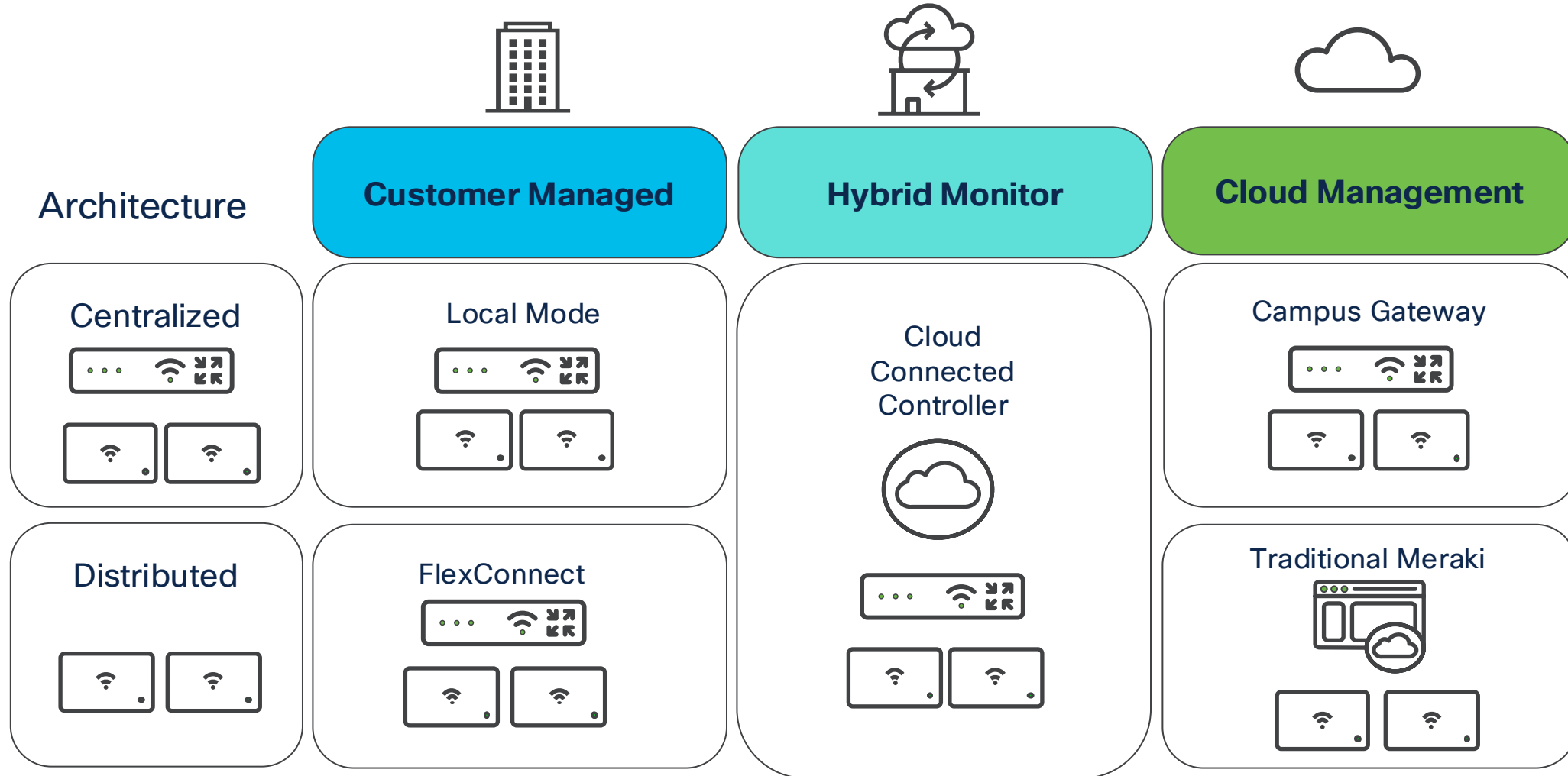
Business relevant apps 75

Default apps 10/527

Wireless

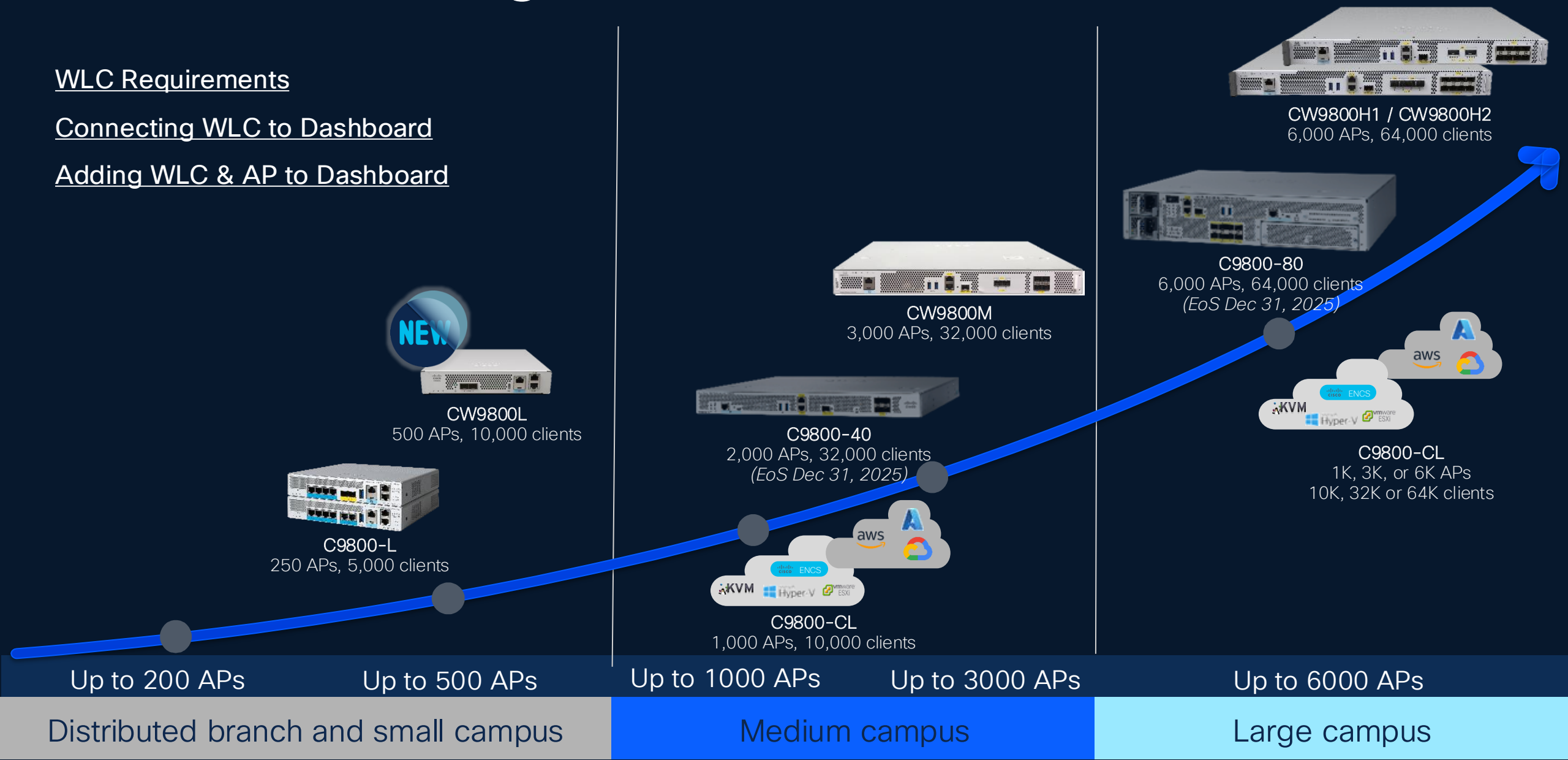


Deliver simplified outcomes to all customers



Cloud Monitoring Wireless Controller Portfolio

- WLC Requirements
- Connecting WLC to Dashboard
- Adding WLC & AP to Dashboard



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



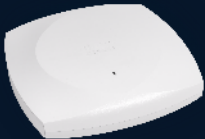
Cisco Campus Gateway

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

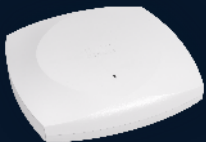
4 Spatial Streams
Omnidirectional

NEW!



CW9172I

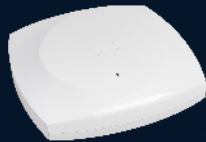
6 Spatial Streams
Omnidirectional



CW9174I

8/10 Spatial Streams
Omnidirectional

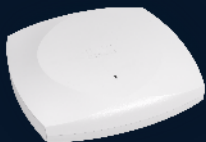
NEW!



CW9176I

12 Spatial Streams
Omnidirectional

UWB



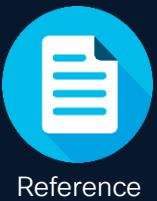
CW9178I

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](https://www.cisco.com/.../global-use-ap-dg.html)

... / Cisco Catalyst 9100 Access Points / Technical References /

Cisco Wireless Global Use Access Points Deployment Guide

Updated: December 11, 2024

Bias-Free Language Contact Cisco

Save Download Print

Cisco Wireless Global Use AP Overview

The Cisco Wireless CW917x Series Access Point is a Unified Hardware with a single product ID, that can be deployed with a Cisco Catalyst 9800 Wireless LAN Controller or Meraki Cloud based deployments. The CW917x Series Access Points can be deployed anywhere in the world just with the single product ID (PID or SKU) and avoids the need to buy a region or country specific access point hardware based on regulatory domain.

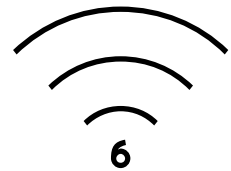
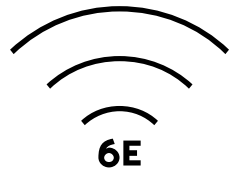
Figure 1. Global Use AP – Management Mode

The Global Use AP simplifies the Cisco Wireless AP portfolio, by

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.

Examples of PID/SKU (in the past):

Cloud Managed/Monitored Wi-Fi 6E Access Points



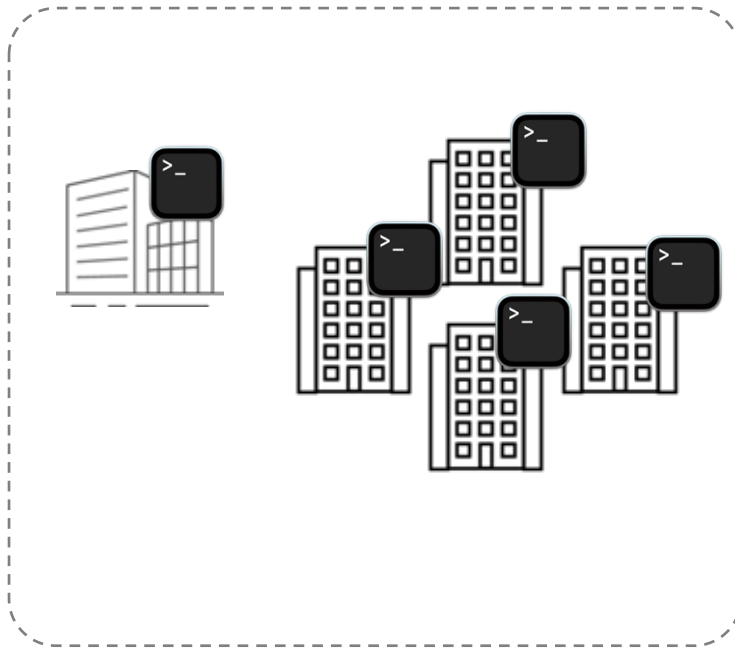
Switching



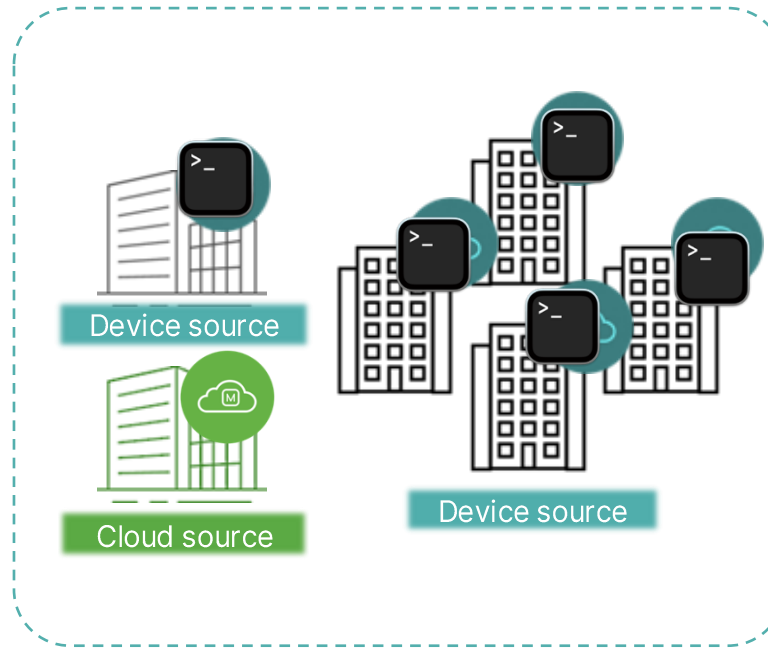
Cloud platform adoption option

Today

Tomorrow



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.

Add devices to network



Select network

2

Configure IOS-XE
devices

3

Summary

Device management and configuration source

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

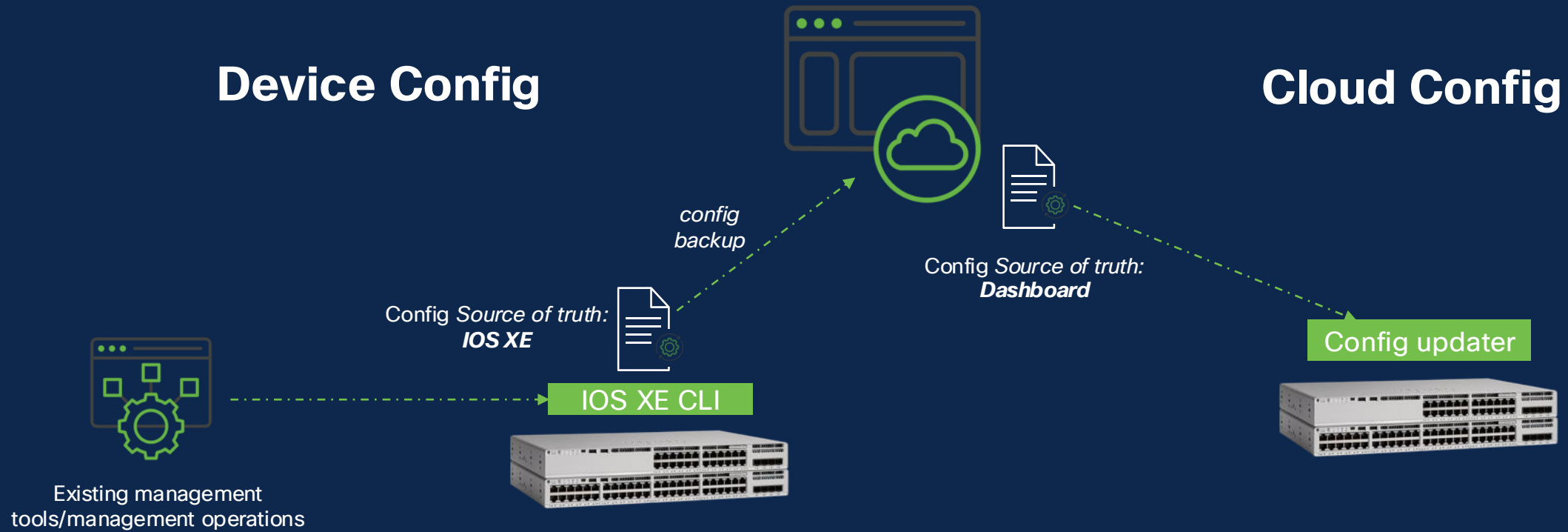
Please provide the [level 15 configuration access credentials](#) ⓘ so the Meraki dashboard can make necessary configuration changes to these devices.

Username

Password

GA: IOS XE 17.15.4

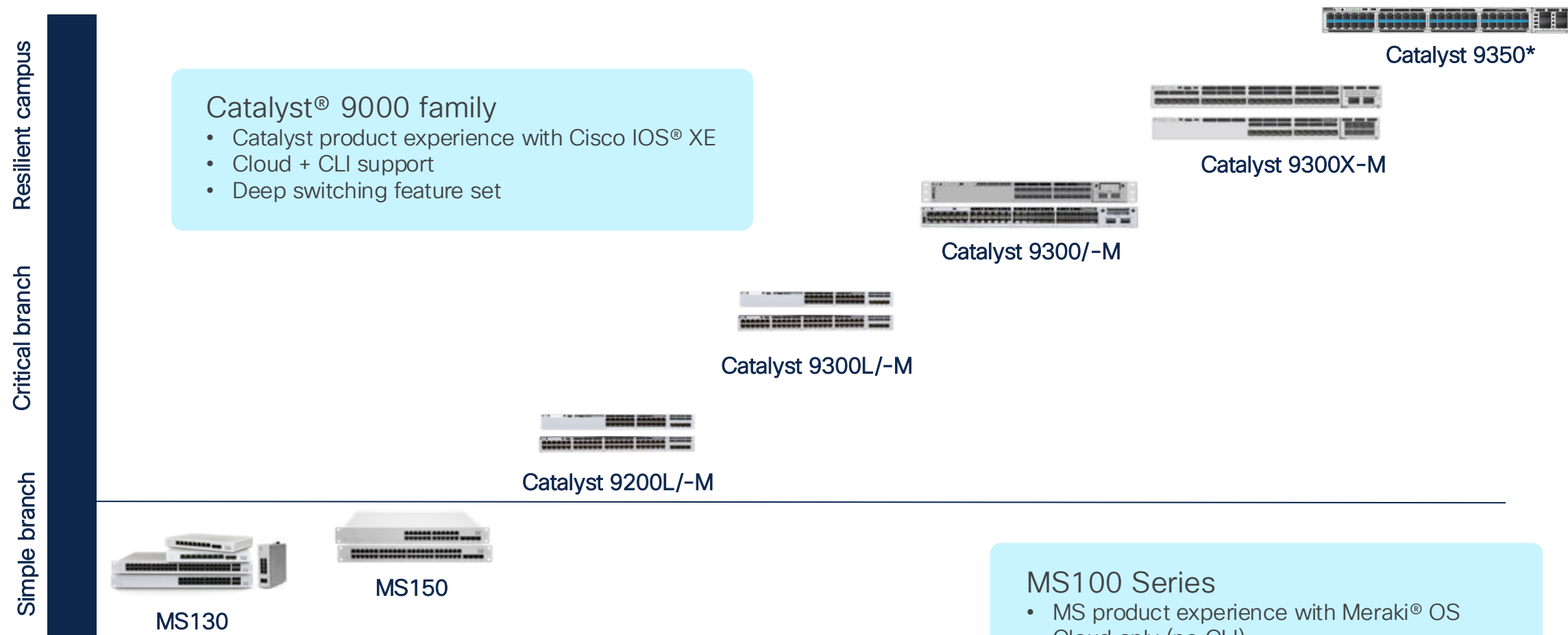
Configuration Source



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



*Single SKU – Unified Licensing model

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



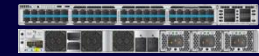
C9500



C9200/CX



C9300LM

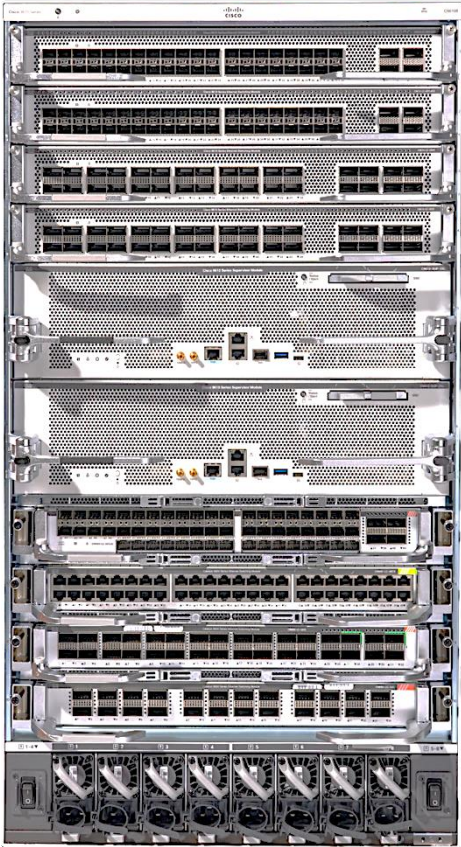


C9350



Modular*

Cisco's first cloud managed modular switch – C9610




Supervisor and line cards

Slot	Model	Role	Serial number
1	C9600-LC-48TX	---	FD0283207ZA
2	C9600-LC-48TX	---	FD028360KH5
3	C9600X-LC-56YL4C	---	FD027230H8M
4	C9600X-LC-56YL4C	---	FD027230H8M
5	C9610-SUP-3XL	Active	FD0282
6	C9610-SUP-3XL	Standby	FD0282
7	C9610-LC-32CD	---	FD0284

Cloud Management



Meraki Cloud



Configuration Source: On-Device

Configuration remains local to the device



Configuration Source: Cloud

Full Cloud Management Experience

17.18.2



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

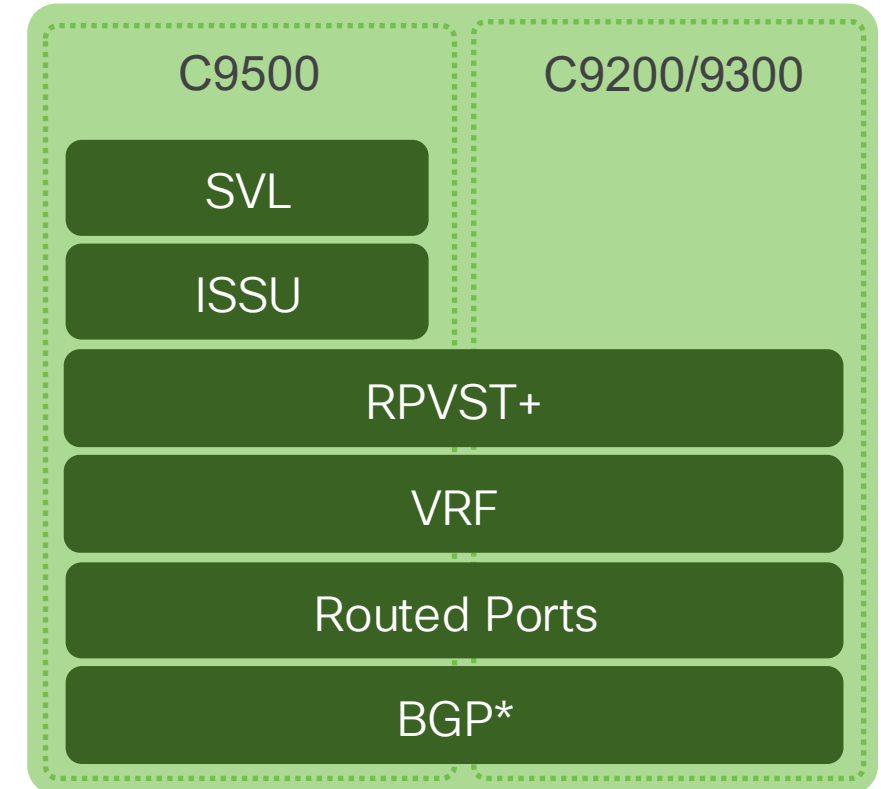
High-Availability

Rapid PVST+

Enhanced L2 loop Prevention

StackWise Virtual (SVL)
ISSU

Sub-second downtime firmware
upgrades



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 image displays the Cisco Cloud Managed Network (CMN) interface, specifically the 'Routing & DHCP' section. A modal window titled 'Edit BLUE_VRF' is open, showing configuration details for a VRF named 'BLUE_VRF'. The modal includes fields for 'VRF name', 'Description' (IoT), 'Route distinguisher' (52:106), and 'Route target'. Below the modal, a table lists the interfaces associated with the VRF. The table has columns for 'Switch or switch stack', 'Interface', 'Name', 'VRF', 'Subnet', and 'IP'. The interfaces listed are 'Doug' (80 VLAN, eighty, BLUE_VRF, 10.80.80.0/24, 10.80.80.254), 'Rocky_and_Bullwinkle' (80 VLAN, BLUE VLAN 80, BLUE_VRF, 10.80.80.0/24, 10.80.80.253), 'Bob' (Bob / 13, Bobs routed port, BLUE_VRF, 10.88.88.0/24, 10.88.88.252), 'Bob' (Bob / 14, Bobs 2nd routed port, BLUE_VRF, 10.89.89.0/24, 10.89.89.252), 'Doug' (0 Loop, 0, BLUE_VRF, 10.252.252.252/32, 10.252.252.252), and 'Doug' (20 VLAN, Uplink Vlan 20, Default, 10.20.20.0/24, 10.20.20.2). Below the table, a 'VRF' section shows a list of VRFs with associated interfaces and a '+ Add VRF' button. The VRFs listed are 'Default', 'BLUE_VRF', 'GREEN_VRF', and 'RED_VRF', each with a description, route distinguisher, route target, and networks.

Switch or switch stack	Interface	Name	VRF	Subnet	IP
<input type="checkbox"/> Doug	80 VLAN	eighty	BLUE_VRF	10.80.80.0/24	10.80.80.254
<input type="checkbox"/> Rocky_and_Bullwinkle	80 VLAN	BLUE VLAN 80	BLUE_VRF	10.80.80.0/24	10.80.80.253
<input type="checkbox"/> Bob	Bob / 13	Bobs routed port	BLUE_VRF	10.88.88.0/24	10.88.88.252
<input type="checkbox"/> Bob	Bob / 14	Bobs 2nd routed port	BLUE_VRF	10.89.89.0/24	10.89.89.252
<input type="checkbox"/> Doug	0 Loop	0	BLUE_VRF	10.252.252.252/32	10.252.252.252
<input type="checkbox"/> Doug	20 VLAN	Uplink Vlan 20	Default	10.20.20.0/24	10.20.20.2

Name	Description	Route distinguisher	Route target	Networks
<input type="checkbox"/> Default	—	—	—	—
<input type="checkbox"/> BLUE_VRF	IoT	52:106	—	—
<input type="checkbox"/> GREEN_VRF	PCI	52:108	—	—
<input type="checkbox"/> RED_VRF	Evil Printers and Fax Machines	52:107	—	—

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

Routing & DHCP

SWITCH OR SWITCH STACK: IP ADDRESS
Select... Select...

Interfaces
Search... 9 Interfaces

Switch	VLAN	Name	Subnet	IP Address	MTU	Link Negotiation	EEE	Port Schedule	PoE	Port Isolation
CAMPUS01-CORE	10	Corp-Data	172.16.10.0/24	172.16.10.254	False	False	Server	Enabled		
CAMPUS01-CORE										
CAMPUS01-CORE										
CAMPUS01-CORE										
CAMPUS01-CORE										
CAMPUS01-CORE										
CAMPUS01-CORE										
CAMPUS01-CORE										
CAMPUS01-CORE										

Static routes
Search... 1 Static route

Multicast routing

Update 1 Ports

Selected Switch / Port 1 ^
Bob/13

Interface mode
☐ Switch port ☒ Routed port

☒ Navigate to configure routed port

Name
Transit Network

Tags
▼

Port status
☒ Enabled

Link negotiation
Auto negotiate ▼

EEE ⓘ
☐ Enabled

Port schedule
Unscheduled ▼

PoE
☒ Enabled

Port isolation
☐ Enabled

Cancel Update

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
Hourglass Twins

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

1 × 2 ×

⇒

Ember Twin

1 × 2 ×

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

3

⇒

Ember Twin

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

The screenshot displays the Meraki dashboard interface for a device named 'ACCESS-2'. The top navigation bar includes tabs for 'Switches', 'Summary', 'Ports', 'Cloud CLI' (which is active), 'Device Health', 'L3 Routing', 'Event log', 'Location', and 'Tools'. Below the navigation bar, there's a map showing the device's location in São Paulo, Brazil, with a Google map overlay. To the right of the map, a 'CLI terminal' section is visible, featuring a 'Capture session' checkbox, a 'Close terminal' button, and a 'Detach terminal' button. The terminal window itself shows a welcome message: 'Welcome to the interactive CLI IOS-XE terminal. You are in Read-only Mode. Establishing connection to your device. Please wait... Connection established successfully.' Below the terminal window, there's a 'Terminal' section with a description: 'Opens a troubleshooting console to this device, similar to an IOS-XE CLI window.' It includes 'Close Terminal' and 'Detach' buttons. A blue information box states: 'This terminal allows limited access to read-only IOS-XE commands, such as show.' The terminal output shows the command 'WM_CORE_9300X#show ip route bgp' and its output, which lists various routing codes and their meanings: 'Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP, D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2, E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP, n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA, i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area, * - candidate default, U - per-user static route, H - NHRP, G - NHRP registered, g - NHRP registration summary, o - ODR, P - periodic downloaded static route, l - LISP, a - application route, + - replicated route, % - next hop override, p - overrides from PFR, & - replicated local route overrides by connected. Gateway of last resort is 10.10.254.2 to network 0.0.0.0'.

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.

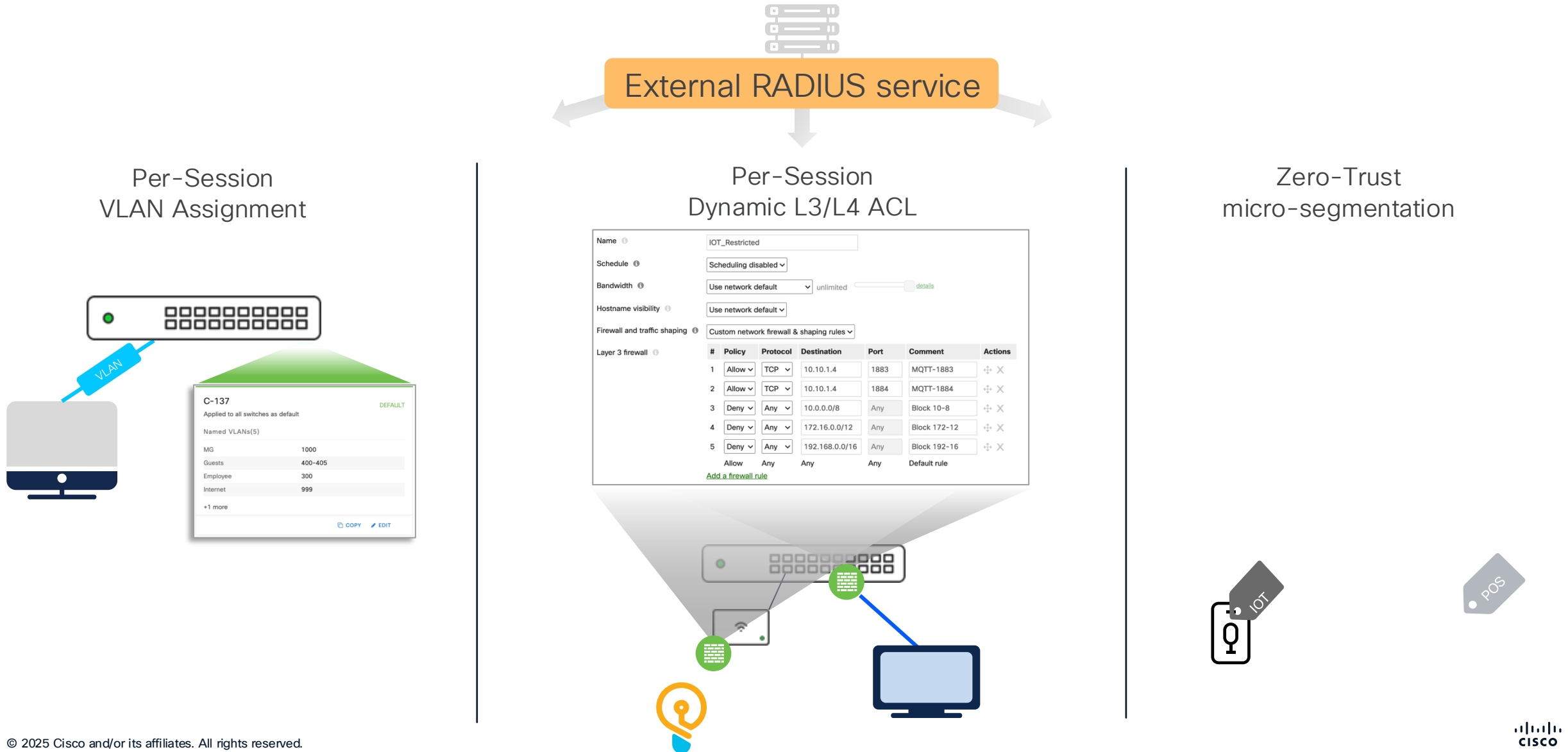
Cloud Configuration

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.

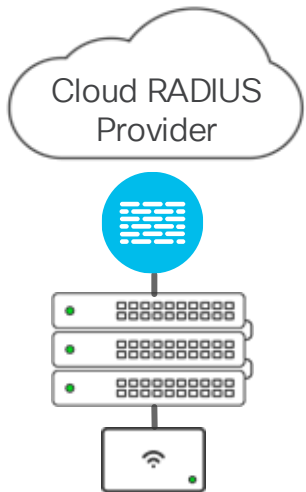
Access Manager



802.1X and RADIUS Support is not new to Meraki



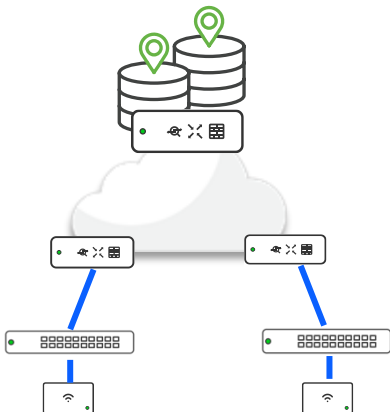
In this case, not everything is simple



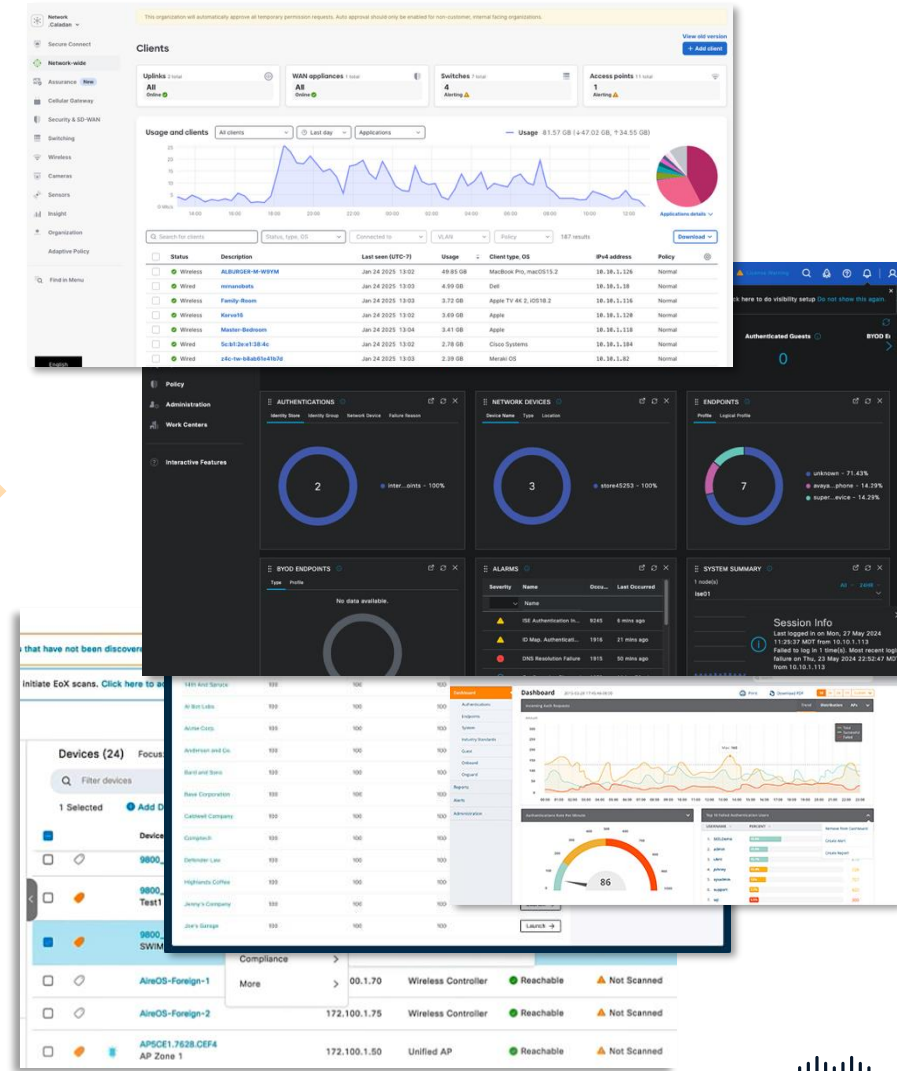
- Complex firewall rulesets
- Complex connectivity security requirements
- Potential in-transit security implications
- Manual input of network and security contexts

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

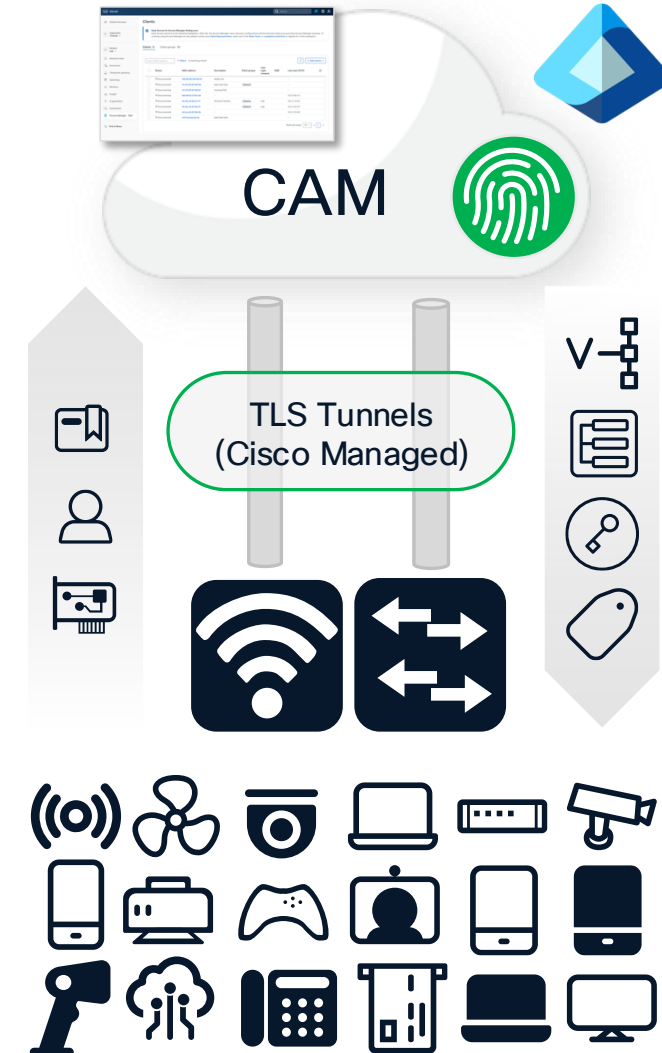
Cloud-delivered access control services to enforce identity and context-based access to the users and devices

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/OT







Cisco Access Manager Current Capabilities

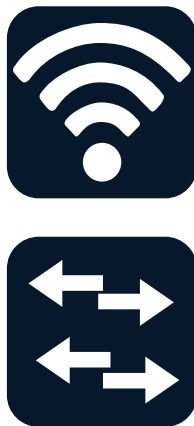
Clients/Endpoints



Users, Computers, Things

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

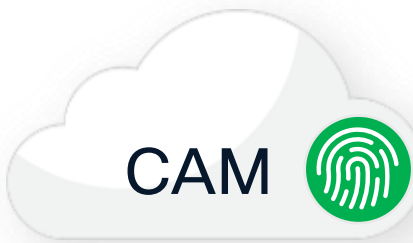
Network Devices



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



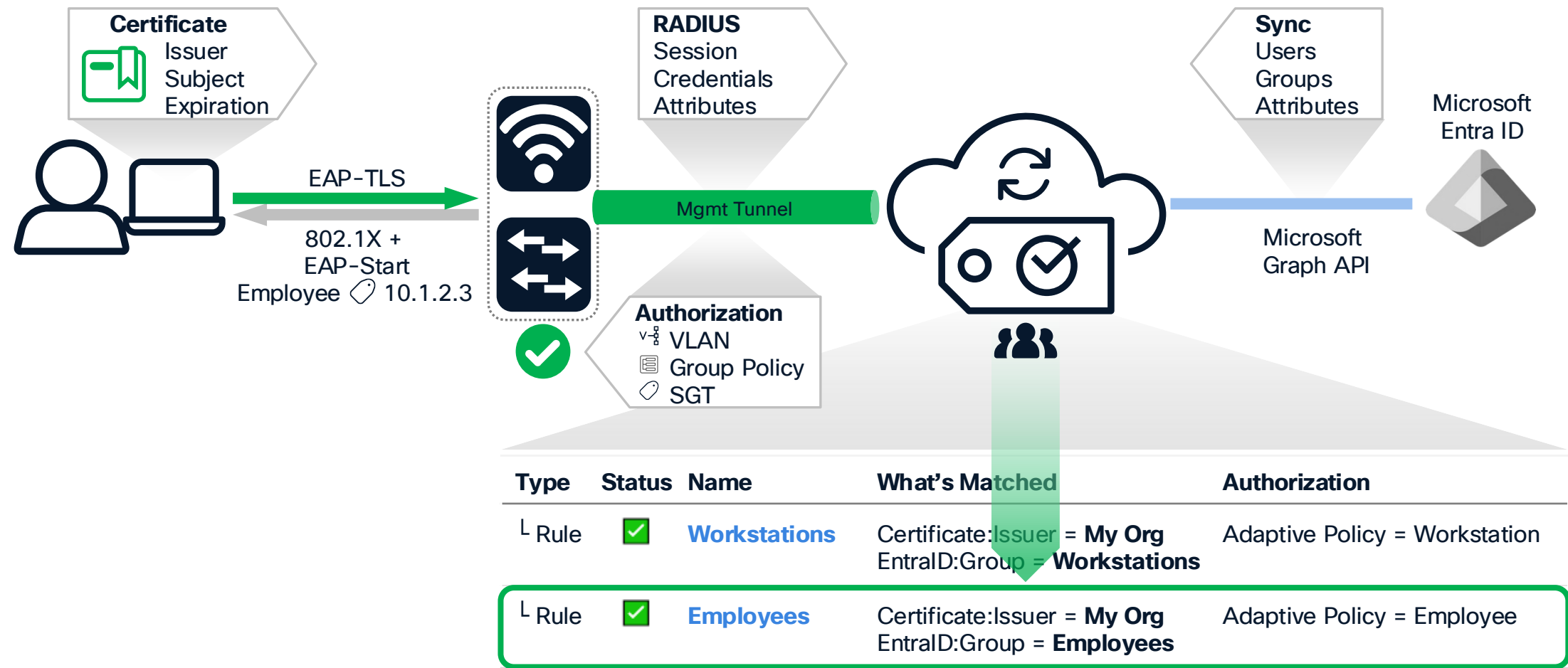
Microsoft Entra ID *ONLY*

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



Routing & SD-WAN



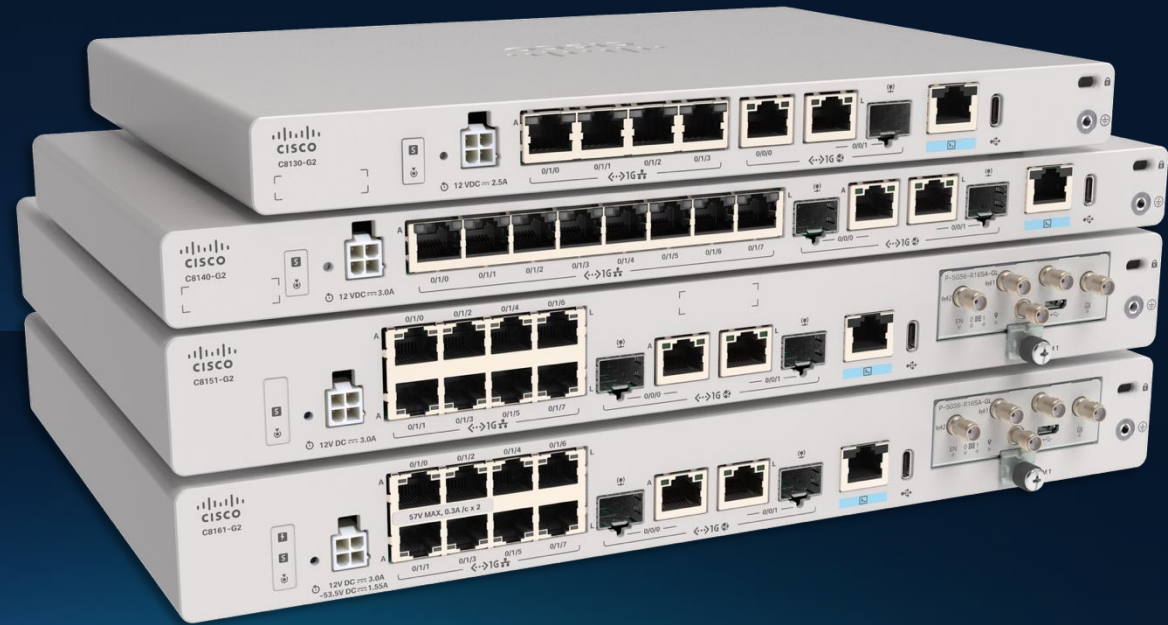
Secure Routers for the AI-powered unified branch

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

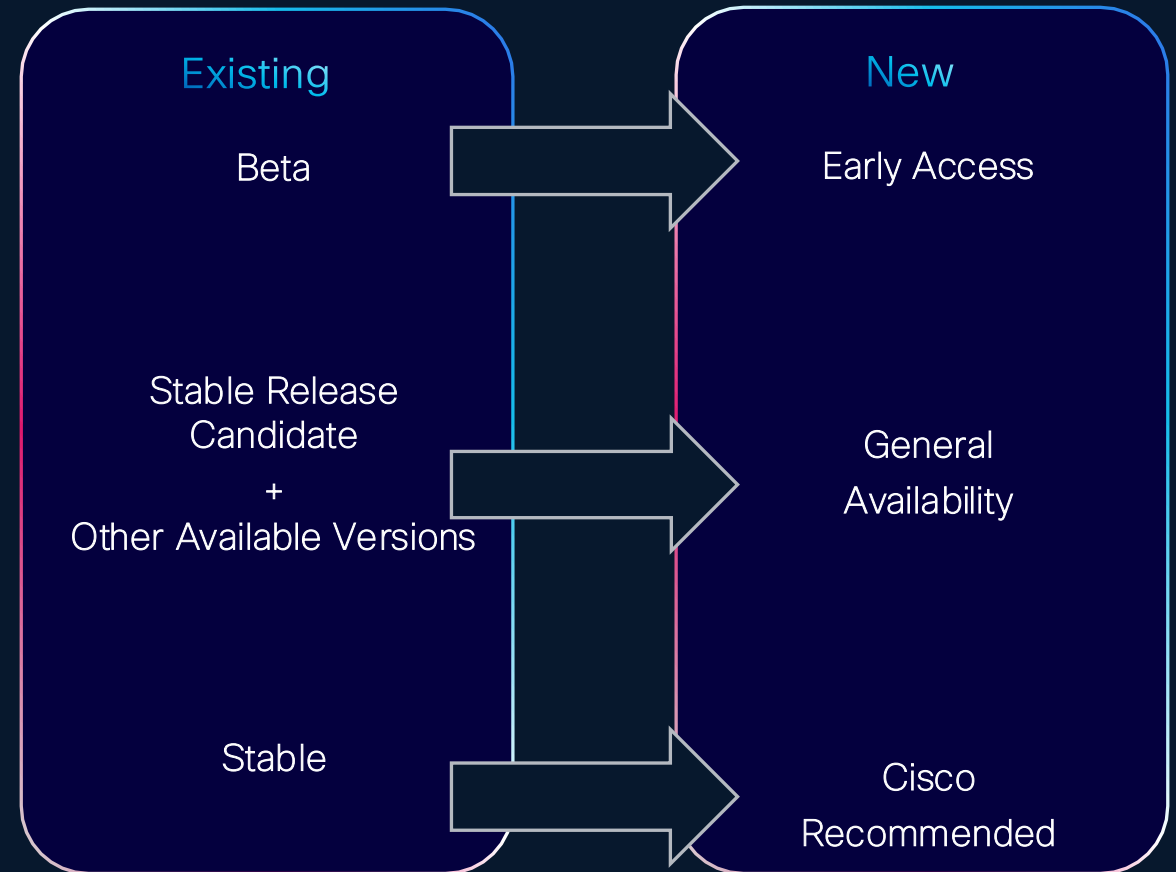
MX Release version change (also applicable to wireless, switching, IoT portfolio)

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

The image displays two screenshots of the Meraki dashboard's 'Set up ThousandEyes' interface. The top screenshot shows the initial setup steps: 1. Set up ThousandEyes (with a button to 'Log into an existing account' or 'Create a new account'), 2. Select networks to activate as agents, and 3. Review selection. The bottom screenshot shows the 'Select networks to activate as agents' step in more detail. It features a search bar, a 'Network tags' dropdown, and a list of 138 networks. The list includes columns for 'Network' (with checkboxes) and 'Network tags' (with buttons for 'Office', 'Chicago', and 'Branch'). The networks listed are Meraki Chicago - Post Office CHG12, Meraki Chicago - Data Center, Meraki London - Post Office LON12, Meraki London - Bishopsgate LON16, and Meraki London - Finsbury LON11. The bottom screenshot also shows the 'Review selection' step and a 'Cancel' button.

Network: Nook-HQ-SF

← Outage overview

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](#)

Environment: Network

← Outage overview

Set up ThousandEyes

✓ Set up ThousandEyes
ThousandEyes account synced with your Meraki account

- 2 Select networks to activate as agents
 - Search by network name [1](#) Network tags 138 networks

Network	Network tags
<input checked="" type="checkbox"/> Meraki Chicago - Post Office CHG12	Office Chicago Branch
<input checked="" type="checkbox"/> Meraki Chicago - Data Center	Office Chicago Branch
<input checked="" type="checkbox"/> Meraki London - Post Office LON12	Office London Branch
<input checked="" type="checkbox"/> Meraki London - Bishopsgate LON16	Office London Branch
<input checked="" type="checkbox"/> Meraki London - Finsbury LON11	Office London Branch
- 3 Review selection

[Cancel](#) All changes saved [Back](#) [Next](#)

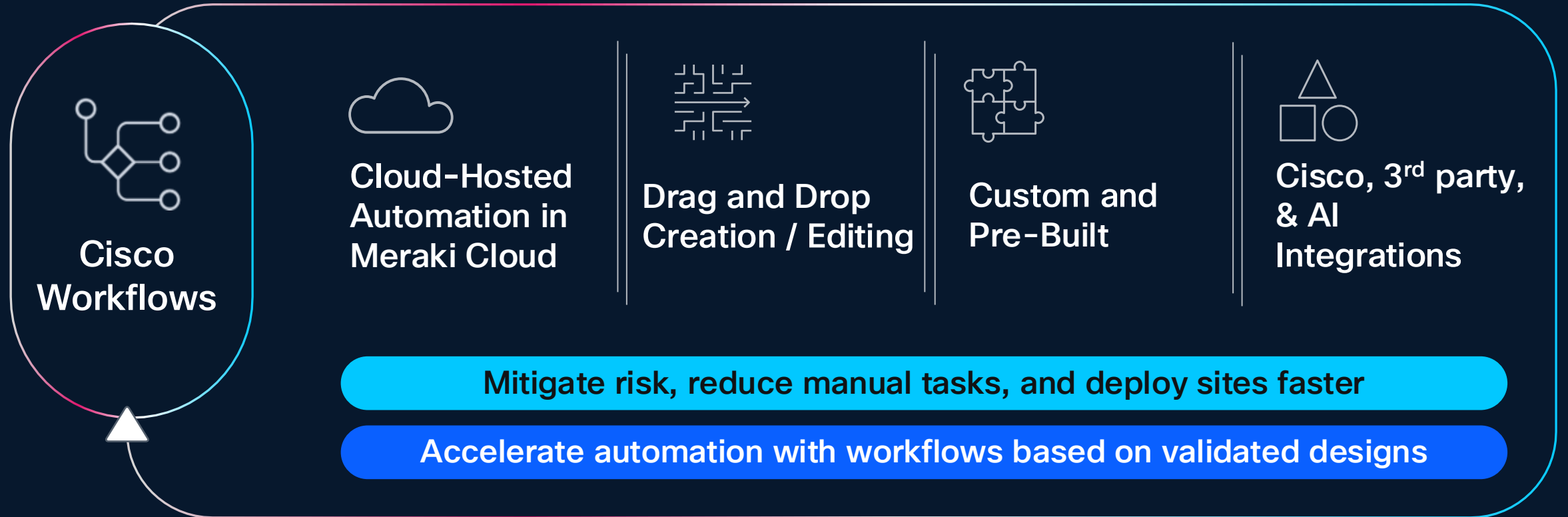
Last login
about 2 hours ago from your current IP address

© 2022 Cisco Systems, Inc.
[Privacy](#) [Terms](#)

Cisco Workflows



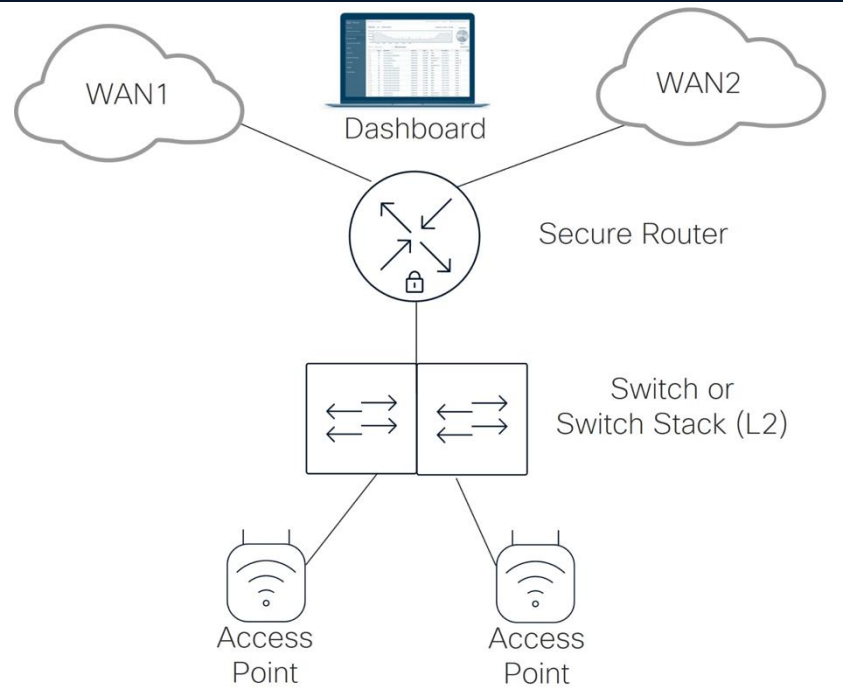
Cisco Workflows in the Meraki Dashboard




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 Traffic Example: 10
String	Appliance VLAN ID for Guest Traffic	VLAN ID for Guest Traffic Example: 10
String	Organization ID	The Meraki Organization ID for the network is creation.
Boolean	Ignore If Devices are Claimed	When enabled, workflow will skip step and be marked as successful if devices are already claimed to Network. Workflow execution stops when first device that is already claimed is encountered.
String	Switch Serial Number	Example; Q2HP-LPX9-BKM
Secure String	Wireless PSK Password SSID 1	Pre-shared key (PSK) password for wireless network. Required for WPA3-Enterprise. Authentication Mode is set to WPA3-Enterprise. Password must meet minimum complexity requirements (typically 8-63 characters). Password is encrypted during transmission.
String	Appliance VLAN ID for Staff and POS Traffic	VLAN ID for Staff and POS Traffic Example: 12
Secure String	Wireless PSK Password SSID 2	Pre-shared key (PSK) password for second wireless network. Required for WPA3-Enterprise. Authentication Mode is set to WPA3-Enterprise. Password must meet minimum complexity requirements (typically 8-63 characters). Password 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



