# Cisco Campus Gateway

## Campus Gateway overview

**Q: What is Cisco® Campus Gateway?**

A: Cisco® Campus Gateway is a cloud-native platform managed directly by the Cisco Meraki™ dashboard. It provides client traffic aggregation and acts as a client authentication proxy and mobility manager for large campus solutions without altering the existing wired network infrastructure.

**Q: What is the Product ID for Campus Gateway?**

A: CW9800H1-MCG

**Q: Is Campus Gateway the next generation of Cisco wireless LAN controller?**

A: No, Campus Gateway is a completely different architecture and solution, designed for cloud-managed environments and integrated with the Meraki dashboard.

**Q: How is Campus Gateway different from a wireless LAN controller?**

A: Unlike a wireless LAN controller, which is part of the on-premises, customer-managed Cisco Catalyst™ wireless stack, Campus Gateway is integrated into the cloud-managed Meraki stack, offering distinct services and architectural differences.

**Q: Will Campus Gateway replace Cisco wireless LAN controllers?**

A: No, Campus Gateway and Cisco wireless LAN controllers serve different purposes and architectures. Cisco wireless LAN controllers are for on-premises deployments, while Campus Gateway is for cloud-managed deployments.

**Q: Can I convert my existing wireless LAN controllers to become Campus Gateways?**

A: The CW9800 hardware is capable of operating in cloud and on-prem mode. However, the ability to migrate between modes is not available at this time. There is no ETA. Please have your Cisco representative reach out to the wireless product management team if you have questions regarding migration.

The Cisco Catalyst 9800 wireless LAN controllers series hardware (C9800-80, C9800-40, etc.) is not capable of operating in cloud management mode and is not eligible for migration.

## Features and functionality

**Q: What challenges does Campus Gateway solve?**

A: Campus Gateway allows for larger-scale deployments by tunneling traffic centrally, eliminating the need for large Layer 2 VLANs and maintaining cloud-managed benefits without altering wired network designs.

**Q: How is Campus Gateway different from the wireless concentrator on MX?**

A: The Campus Gateway architecture is designed for large-scale wireless deployments with different scalability, tunneling technologies, and functions like a centralized client database, which are not present in MX.

**Q: What functions run on Campus Gateway?**

A: Campus Gateway manages data plane aggregation, mDNS gateway, RADIUS proxy, and centralized mobility database functions, among others. Other real-time functions remain on cloud-mode access points.

## Compatibility and technical specifications

**Q: Which access points are compatible with Campus Gateway?**

A: Campus Gateway supports native cloud-managed access points capable of running the R31.2 release, including the Wi-Fi 6, Wi-Fi 6E, and Wi-Fi 7 models below:

- Wi-Fi 6: Meraki MR44, MR36, MR36H,[1] MR46E, MR56, MR76, MR78, and MR86.

- Wi-Fi 6E: Meraki MR57 and Catalyst 9162, 9163, 9164, and 9166 Series.

- Wi-Fi 7: Cisco Wireless 9178, 9176, and 9172 Series, and any other Wi-Fi 7 models.

**Q: Do access points and Campus Gateway need to be part of the same Meraki network?**

A: Yes, at the First Customer Shipment (FCS), this is required. This limitation will be removed in future updates.

**Q: Can legacy access points operate in the same network as Campus Gateway?**

A: Yes, legacy access points can coexist, but a Campus Gateway-tunneled SSID will not be broadcasted on unsupported access points.

**Q: Are the access points managed by Campus Gateway?**

A: No, access points continue to be managed directly by the Meraki dashboard, with each access point connecting to Campus Gateway to exchange control plane information and tunnel client traffic.

**Q: Does Campus Gateway use the Control and Provisioning of Wireless Access Points (CAPWAP) protocol to communicate with access points?**

A: No, Campus Gateway uses the QUIC protocol for control traffic and Virtual Extensible LAN (VXLAN) for data traffic, which differs from CAPWAP communication.

**Q: How does Campus Gateway alter the scale guidelines of 1,000 nodes per Meraki Dashboard network?**

A: The Meraki Network scale has been increased for both combined and standalone Networks to 5,000 nodes, Please find the new guidelines [here]. This is the result of multiple optimizations done at the Cloud Platform architecture level, like the adoption of Elastic Shards where we use Kubernetes technology to scale up and scale out, or the adoption of

Outpost where critical services have been extracted from the customer shards and run centrally to allow dedicated scale. Examples of Services on Outpost: NexTunnel, HA-Splash, Licensing API, Meraki API OAuth Server, etc.

At the organization level, the limit has been increased to 35,000 devices per organization. At the Meraki Network level, each device type limit has been increased, and so has the combined network limit.

**Q: Will Meraki dashboard scale guidance change with the use of Campus Gateway?**

A: Yes, the guidelines will be updated to support up to 5,000 access points, facilitated by advancements in the Meraki cloud architecture and optimizations.

**Q: Is a higher Maximum Transmission Unit (MTU) required because of the Virtual Extensible LAN (VXLAN) encapsulation between the access point and Campus Gateway between the access point and Campus Gateway?**

A: No, it is not required because the access point performs dynamic path MTU discovery on both the QUIC and VXLAN tunnels.

[1] At release, there will be no support for tunneling from wired ports on the MR36H.

**Q: Do we have a list of recommended Cisco switches which best support the memory required for Campus Gateway data and traffic?**

A: Yes, as you aggregate traffic, there is an important design consideration, which is to choose a switch that can scale in terms of MAC address and ARP entries, and this is based on the capacity you expect. These are some switches that we recommended to match the scale for Campus Gateway:

- Cisco Catalyst 9600
- Cisco Catalyst 9500
- Cisco Catalyst 9500X
- Cisco Nexus 7000/7700
- Cisco Nexus 9500
- Cisco Nexus 9300
- Cisco Nexus 9200

**Q: Can the Campus Gateway act as a gateway/proxy for management traffic to the cloud?**

A: No. All cloud-managed devices will maintain their own individual connections to the Meraki Dashboard. Campus Gateway will not act as a gateway/proxy for this.

**Q: When the access points and both Campus Gateways lose internet connectivity will they keep forwarding traffic?**

A: The behavior will be consistent with other Meraki devices today when they lose connectivity; clients will stay connected, and traffic will continue to flow. You will not be able to manage the device, so you cannot change the configuration and will not have visibility.

**Q: Can you still manage cloud managed access points with Campus Gateway if internet is down?**

A: Management of devices will remain the same with or without Campus Gateway, because management is reserved for the dashboard. Campus Gateway acts as an aggregator and has some real-time control plane functionality but Campus Gateway does not manage or control access points like in a traditional WLAN controller architecture.

**Q: What happens if the Campus Gateway cluster goes down, or an access point loses connectivity to both Campus Gateways in the cluster?**

A: All affected access points will bring down both the QUIC and VXLAN clusters and stop broadcasting any tunneled SSID. If the access point has some configured SSID for local bridging, those will remain funcitonal.

After the first customer shipment, backup Campus Gateways will be supported.

## Licensing and availability

**Q: What are the licensing requirements for Campus Gateway?**

A: No device license is required for Campus Gateway. An Enterprise or Advanced License is necessary for all connected access points, with support for co-term, Meraki subscription, and unified licensing (Cisco Networking subscription). Enterprise Agreements are also supported.

**Q: Will Campus Gateway support access points with mixed-tier licensing? Or do all access points need to be the same tier?**

A: It is not recommended to mix license tiers because features and services depend on that, and the customer would risk being non-compliant. However, the same licensing tier is not going to be enforced at the first customer shipment on Campus Gateway.

For any further inquiries or updates, please contact your Cisco representative.