



Using Cloud Monitoring as a Solution for Network Monitoring

- [Cloud monitoring, on page 1](#)

Cloud monitoring

Cloud Monitoring is a network management service that:

- simplifies onboarding without requiring an external onboarding agent
- improves tunnel connectivity by using native Meraki Nextunnel
- aligns operational data models with the Cisco Meraki Dashboard for seamless device authentication and operations

Cloud Monitoring allows network administrators to monitor Cisco Catalyst 9800 Wireless Controllers by using the Cisco Meraki Dashboard.

Feature history for Cloud Monitoring

This table lists release information for the feature described in this section.

This feature is available in all releases after its introduction unless noted otherwise.

Table 1: Feature history

| Release | Feature | Feature information |
|---|------------------|--|
| Cisco IOS XE 17.15.1, 17.12.4, and 17.9.5 | Cloud Monitoring | Cloud Monitoring is a cloud-native solution that connects devices to the cloud for network monitoring. |

Examples of Cloud monitoring

- Automated onboarding requires no external onboarding agent for device registration.
- Native Meraki Nextunnel technology enhances tunnel connectivity.

When to use cloud monitoring

Cloud Monitoring allows you to monitor your devices from the Cisco Meraki Dashboard without additional on-premises resources.

To monitor your network, you must log in to a specific device or deploy on-premises solutions.

To deploy an on-premises solution, you must set up additional servers and pay ongoing maintenance costs. Supporting on-premises solutions requires significant resources. Offloading these operations to the cloud reduces overhead.

Use Cloud Monitoring to monitor your devices from the Cisco Meraki Dashboard without additional resources.

Cloud monitoring features

This topic explains the features of cloud monitoring, including simplified onboarding, improved tunnel connectivity, operational data alignment, and seamless authentication with the Cisco Meraki dashboard.

- Simplified onboarding without any external onboarding agent.
- Improved tunnel connectivity with native Meraki Nextunnel.
- Aligning pull-based operational data with the current Cisco Meraki dashboard models.
- Seamless authentication from Cisco Meraki dashboard to the device using the cloud console.

Prerequisites for cloud monitoring

- To enable cloud monitoring for controllers, the controllers must be connected to, registered, and provisioned by the Cisco Meraki dashboard.
- To add a wireless controller to a network, the username and password must have **privilege 15 access** and **enable password** (optional) in the dashboard.
- The wireless controller must have 4 unused consecutive VTY slots.



Note The VTY lines must be provisioned and secured for only the dashboard to access the controller on these lines.

Enable cloud monitoring (GUI)

Enable cloud monitoring through the GUI so that you can monitor Meraki devices centrally and have visibility into their registration and connection status.

Procedure

-
- Step 1** Choose **Configuration > Services > Cloud Services > Meraki** .
- Step 2** Use the slider to enable **Meraki Connect** .

Step 3 Click **Apply** to automatically refresh and view the registration or Nextunnel connection status.

Note

Click **Refresh** to update the changes.

Cloud monitoring is activated for Meraki devices, and you can view their registration or Nextunnel connection status from the interface.

Enable cloud monitoring (CLI)

Enable cloud monitoring features so that your device can integrate with cloud-based management tools.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enable cloud monitoring.

Example:

```
Device(config)# service meraki connect
```

Cloud monitoring is enabled on your device, allowing it to connect to the cloud management service.

Onboard the controller using Cisco Meraki dashboard

To monitor wireless devices, claim an eligible wireless controller into your Dashboard inventory.

For more information, see the [Catalyst Wireless Onboarding Guide](#).

Verify cloud monitoring

To verify the Cloud ID (Meraki Serial Number) fetched as part of the registration and status of the operation, use this command:

```
Device# show meraki connect
Service meraki connect: enable

Meraki Tunnel Config
-----
Fetch State:                Config fetch succeeded
Fetch Fail:
Last Fetch(UTC):            2024-07-11 15:13:07
Next Fetch(UTC):            2024-07-11 16:39:21
Config Server:              cs594-2037.meraki.com
Primary:                    apa.nt.meraki.com
```

```

Secondary:                aps.nt.meraki.com
Client IPv6 Addr:         2001:DB8::1
Network Name:             WLC - wireless controller

```

```

Meraki Tunnel State
-----

```

```

Primary:                   Up
Secondary:                 Up
Primary Last Change(UTC): 2024-07-09 19:02:09
Secondary Last Change(UTC): 2024-07-09 19:02:09
Client Last Restart(UTC): 2024-07-05 19:56:58

```

```

Meraki Tunnel Interface
-----

```

```

Status:                    Enable
Rx Packets:                26595318
Tx Packets:                32514152
Rx Errors:                 0
Tx Errors:                 0
Rx Drop Packets:          0
Tx Drop Packets:          0

```

```

Meraki Device Registration
-----

```

```

url:                       https://catalyst.meraki.com/nodes/register
Device Number:             1
Serial Number:             FCL264000NN
Cloud ID:                  Q2ZZ-3HC4-5R5A
Mac Address:               00:00:5E:00:53:AF
Status:                    Registered
Timestamp(UTC):            2024-06-03 11:54:28
Device Number:             2
Serial Number:             FCL263900RW
Cloud ID:                  Q2ZZ-GC8U-Y24D
Mac Address:               00:00:5E:00:53:B0
Status:                    Registered
Timestamp(UTC):            2024-06-03 11:23:55

```

To verify the access point registration status, use this command:

```

Device# show ap meraki monitoring summary

```

```

Meraki Monitoring          : Enabled
Number of Supported APs   : 3

```

| Number | AP Name Cloud ID | AP Model Status | Radio MAC | MAC Address | AP Serial |
|--------|---------------------|--------------------|-------------------|-------------------|--------------|
| | APM-9164-1 | CW9164I-ROW | 00:00:5E:00:53:A1 | 00:00:5E:00:53:A2 | FGL2704LXZ5 |
| | Q5AN-2RAT-SZUE | Registered | | | |
| | APM-9120-1 | C9120AXI-D | 00:00:5E:00:53:A3 | 00:00:5E:00:53:A4 | FGL2532LNR7 |
| | Q2ZZ-FL9D-HL8Z | Registered | | | |
| | APM-9136-1 | C9136I-ROW | 00:00:5E:00:53:A5 | 00:00:5E:00:53:A6 | FGL2717MEFUJ |
| | Q2ZZ-VX3L-66MT | Registered | | | |

Troubleshoot cloud monitoring

This topic provides troubleshooting steps for cloud monitoring, focusing on device and access point registration issues with the Cisco Meraki Dashboard.

| Scenario | Reason | Action |
|--|---|---|
| Your device cannot register with the Cisco Meraki Dashboard. | You see this error message: No required SSL certificate was sent | Check that the required certificate is installed on the device. Note Ensure that your device has the hardware SUDI certificates. |
| Your device cannot register with the Cisco Meraki Dashboard. | You see this error message: Error message: ip http client source-interface not configured. | Configure the http client source interface by using the ip http client source-interface <interface name> command. |
| If the controller fails to register with the Cisco Meraki Dashboard, it retries nine times. | | Disable and then enable service meraki connect to reinitiate the registration. |
| If the access point fails to register with the Cisco Meraki Dashboard, it retries five times. | The show ap meraki monitoring summary command displays this status: AP Registration Has Failed Five Times. Please Reboot the AP. | Reload the access point to reinitiate the registration. |

