Using Cloud Monitoring as a Solution for Network Monitoring

Feature History for Cloud Monitoring

This table provides release and related information about the feature explained in this section.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 1: Feature History for Cloud Monitoring

Release	Feature	Feature Information
Cisco IOS XE 17.15.1, 17.12.4, and 17.9.5	Cloud Monitoring	The Cloud Monitoring feature is a cloud native solution to which devices are connected for network monitoring.

What is Cloud Monitoring

Cloud monitoring provides the ability to monitor Cisco Catalyst 9800 Wireless Controllers from a centralized dashboard on Cloud. Here, the centralized dashboard on Cloud refers to the Cisco Meraki dashboard.

When to use Cloud Monitoring

To monitor network, you will need to either log into a specific device or deploy on-premise solutions.

To deploy on-premise solution, you will need to deploy additional servers with additional cost associated in maintaining the servers. It is not feasible to have resources to support on-premise solutions and offload such operations to the cloud.

To accomplish this, you can use Cloud Monitoring wherein the device can be monitored from the Cisco Meraki dashboard without the need for additional resources.

Features of Cloud Monitoring

The Cloud Monitoring offers the following services:

- Simplified onboarding without any external onboarding agent.
- Improved tunnel connectivity with native Meraki Nextunnel.

Note The Cisco Meraki dashboard uses Nextunnel as the communication channel with the controller.

- 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.

Different Methods to Enable Cloud Monitoring

Enabling Cloud Monitoring (GUI)

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.

Enabling Cloud Monitoring (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode
Step 2	**service meraki connect** **Example:** `Device(config)# service meraki connect`	Enables cloud monitoring.

Onboarding 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.

Verifying Cloud Monitoring

To verify the Cloud ID (Cisco Meraki Serial Number) fetched as part of the registration and status of the operation, use the following 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:           FD0A:9B09:1F7:1:8E1E:80FF:FE68:B100
  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
  PID:                        C9800-L-F-K9
  Serial Number:              FCL264000NN
  Cloud ID:                   Q2ZZ-3HC4-5R5A
  Mac Address:                8C:1E:80:68:B1:00
  Status:                     Registered
  Timestamp(UTC):             2024-06-03 11:54:28
  Device Number:              2
  PID:                        C9800-L-F-K9
  Serial Number:              FCL263900RW
  Cloud ID:                   Q2ZZ-GC8U-Y24D
  Mac Address:                8C:1E:80:68:BD:00
  Status:                     Registered
  Timestamp(UTC):             2024-06-03 11:23:55
```

To verify the AP registration status, use the following command:

```
Device# show ap meraki monitoring summary

Meraki Monitoring          : Enabled
Number of Supported APs    : 3

AP Name          AP Model        Radio MAC      MAC Address  AP Serial Number  Cloud ID
      Status
------------------------------------------------------------------------------------------
APM-9164-1      CW9164I-ROW   10a8.29cf.e740 6849.9259.09d0 FGL2704LXZ5     Q5AN-2RAT-SZUE
   Registered
APM-9120-1      C9120AXI-D    1cd1.e0db.28a0 1cd1.e0d2.a4f0 FGL2532LNR7     Q2ZZ-FL9D-HL8Z
   Registered
APM-9136-1      C9136I-ROW    6cd6.e35c.17a0 4891.d5ef.8118 FGL2717MEFJ     Q2ZZ-VX3L-66MT
   Registered
```

Troubleshooting Cloud Monitoring

Table 2: Troubleshooting Cloud Monitoring

Scenario	Reason	Action
Device is not able to register to the Cisco Meraki Dashboard.	You get to view the following error message: **No required SSL certificate was sent**	You must check the required certificate in the device. **Note** The device must have the hardware SUDI certificates.
Device is not able to register to the Cisco Meraki Dashboard.	You get to view the following error message: **Error message: ip http client source-interface not configured.**	You must configure the **http client source interface** using the **ip http client source-interface <interface name>** command.
When the controller registration with the Cisco Meraki Dashboard fails, the controller retries 9 times.		You need to disable and enable **service meraki connect** to reinitiate the registration.
When the access point registration with the Cisco Meraki Dashboard fails, the AP retries 5 times.	The **show ap meraki monitoring summary** command displays the status as follows: **AP Registration Has Failed 5 Times. Please Reboot The AP!**	You need to reload the access point to reinitiate the registration.