Managed Cisco Meraki Technology Service Description

Overview

This document provides information relating to the management and monitoring of Cisco Meraki devices under the standard MCN offering. The monitoring, configuration, limitations, and available standard service requests are outlined hereunder. The scope of the Managed Cisco Meraki Service is as follows:

- Meraki Wired & Wireless LAN including
  - MR Series Wireless Access Points (AP's)
  - MS Series switches
- Meraki Security & Routing devices including
  - MX Series Security & Routing devices
- Meraki Sensors
  - Bluetooth beacons and indoor sensors
- Meraki Insights analytics platform

Client Responsibilities and Prerequisites

There are no technology specific pre-requisites required, however, a description of the standard pre-requisites for the offering are documented in the MCN Statement of Work.

Technology Specific Operations

Configuration Management

The Cisco Meraki solution is a full SaaS offering therefore device configuration backups are inherent to the solution and are executed automatically with the built-in toolsets to the Cisco Meraki Cloud. All Meraki configuration backups are stored in the Cisco Meraki Cloud itself as part of Management Orchestration.

Firmware Maintenance

Firmware maintenance for the Cisco Meraki solution is an automated process and is included within the Meraki Cloud solution. Firmware schedules and frequencies are determined and managed by the Cisco Meraki vendor. For further details in this regard refer to the vendor’s relevant documentation.

MX Security Appliance Specific Monitors

Cisco Meraki MX appliances provide cloud managed security and routing functionality.

The following technology specific monitors are configured by default:

Monitor	Description	Alerts	Performance Info	Resolution	Poll interval (sec)
Disk (if any)	Disk usage in %	✓	Graphs of the parameter measured over time	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	300
Interfaces	Status of device interfaces (virtual or physical), Connection status, client count, sent / received packets and bytes, errors, throughput	✓	N/A	Engineering Teams will solve the issue	180

Monitor	Description	Alerts	Performance Info	Resolution	Poll interval (sec)
Sessions	Check the number of current/active sessions in the device	✓	Graphs of the parameter measured over time	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	180
Device Status and Operational State	Operational status of the device	✓	N/A	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	180
HA Status (if any)	Check the status of High Availability	✓	N/A	Engineering Teams will solve the issue	60
Device Load	Device load / utilisation	✓	Comprises of a combination of the CPU Utilisation and interface utilisation.	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	300

Security Appliance Configuration Management

Refer to Configuration Management under the Technology Specific Operations section herein.

Security Appliance Firmware Maintenance

Refer to Firmware Maintenance under the Technology Specific Operations section herein.

Security Appliance Supported Configurations

- Meraki MX physical or vMX virtual appliances
- Single devices
- HA security appliance configurations meaning two compatible physical or virtual security appliances in an active / passive configuration, both connected at the same time or stacked devices.

Security Appliance Limitations

- The managed Cisco Meraki service does not include procurement of internet or WAN circuits, or Meraki software or hardware / virtual devices.
- Not all metrics listed in the Common Network Management Service Description, such as memory utilisation, CPU utilisation, power supply unit status, fan status are available from a management and monitoring perspective. This is a limitation imposed by the vendor and not because of any restrictions enforced by NTT Data. The vendor documentation should be consulted for further information.

Security Appliance Standard Service Requests

A list of standard service requests available for this technology can be found in the MCN Request Catalogue.

MX Requests not Included with the Service

IDS / IPS

The correct operation of IDS and other advanced security features is heavily dependent on the application(s) being protected, which means that the features and policies applying the intelligence on the security policy must be the Client's relevant contacts. The scope of the managed IDS and advanced security features will be limited to applying changes based on what the Client requests. NTT expects the Client will identify the changes to perform based on the SIEM (or other relevant tools used by the Client.). The reasons why applications are blocked, generating false positives, or not blocked when they should be, must be identified by the Client. Ongoing management of Advanced Security devices is excluded from the review of the log. This is an activity to be undertaken by the Client’s support teams.

While NTT will make all attempts to reduce the number of false positives, it will not be responsible for authentic users being denied access to the Client application.

SIEM Services
A SIEM independent log management system or SOC threat analysis team is not included in the Meraki MX Management Service. i.e. the detection of vulnerabilities, threats and similar security activities are limited to the features included in the devices under management. Furthermore, NTT will not include any additional tooling for these purposes unless specifically contracted in the MCN Statement of Work

Security Appliance Transition Tasks

No technology specific transition tasks are required. A description of the standard transition tasks included for the service offering is documented in the MCN Statement of Work.

Optional Tasks
The following tasks may be provided at additional charge, unless specified in the Statement of Work:

- Security policy definition: this is a consultancy task which must be contracted in addition to the Service.
- Analysis of the Clients applications, consultancy, audits, and advisory services are not included in the setup fee.
- SIEM and SOC services

Note:

Any tasks not explicitly described under the Technology Transition Tasks are implicitly excluded from transition.

Cisco Meraki SD-WAN

MX Security Appliance Specific Monitors

The Cisco Meraki MX family of appliances provide the capability to natively support Meraki’s SD-WAN feature. SD-WAN provides for the optimisation and securing of enterprise networks by dynamically adjusting to changing WAN conditions. Some key features and benefits thereof are:

- Dynamic Path Selection
- Simplified Management
- Enhanced Security (if enabled)
- Cost Efficiency
- Scalability

The following technology specific monitors are configured by default:

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
SD-WAN VPN tunnel status	Provides VPN tunnel status for the networks in the organisation.	✓	N/A	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	300
SD-WAN VPN tunnel bandwidth	Monitor the bandwidth of a VPN tunnel interface.	✗	Provides bandwidth usage details (upload/download) across the tunnels.	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	300

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
SD-WAN link packet loss, latency	Monitor packet loss and latency over a link in specified period.	✓	Provides Packet Loss metrics measured as a percentage and Latency measured as milliseconds.	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	300

SD-WAN Configuration Management

Refer to Configuration Management under the Technology Specific Operations section herein.

SD-WAN Firmware Maintenance

Refer to Firmware Maintenance under the Technology Specific Operations section herein.

SD-WAN Appliance Supported Configurations

Meraki SD-WAN is configured on MX Security Appliances. In addition to the configurations supported under Security Appliances, the following SD-WAN specific configurations are supported:

- Routed (NAT) mode
- VPN concentrator mode (Passthrough)
- One-armed concentrator mode
- Hub and spoke topology
- Full tunnel mode
- Split tunnel mode

SD-WAN Limitations

- Refer to the Security Appliance Limitations section herein for details

SD-WAN Standard Service Requests

A list of standard service requests available for this technology can be found in the MCN Request Catalogue.

SD-WAN Transition Tasks

No technology specific transition tasks are required. A description of the standard transition tasks included for the service offering is documented in the MCN Statement of Work.

Note:
Any tasks not explicitly described under the Technology Transition Tasks are implicitly excluded from transition.

Meraki Insight

Cisco Meraki Insights provides visibility and clarity with traffic analytics over both overlay network traffic flows and underlay circuits, allowing for more detailed reporting and faster incident resolution. Some of the features of Meraki Insight includes:

- Web Application Health
- WAN Health
- Root Cause Analysis

NTT recommends this functionality is added for all clients particularly in environments where the SD-WAN feature has been enabled. Where Meraki Insights is not available, some more advanced reporting functionality will not be available. Features and capabilities of Meraki Insight are dependent on the licensing purchased. More information in this regard is available in the vendor documentation.

Cisco Meraki MS Switches

Cisco Meraki MS switches provide wired switching functionality in Cisco Meraki networks.

Meraki Switch Specific Monitors

The additional monitors which can be configured for switch management are:

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
Uplink Port Status	Check port status	✓	N/A	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	60
Uplink Port Usage	Check uplink port bandwidth usage	✓	Graphs of the parameter measured over time	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	600

Meraki Switch Configuration Management

Refer to Configuration Management under the Technology Specific Operations section herein.

Meraki Switch Firmware Maintenance

Refer to Firmware Maintenance under the Technology Specific Operations section herein.

Meraki Switch Supported Configurations

The following switch configurations are supported:

- Single switch: A standalone switch or a set of standalone switches (managed independently from each other)
- Set of switches in high availability configuration: Two or more switches of compatible models in an HA configuration
- Stacked switches: physical stacking and connection of multiple compatible switch models providing redundancy and allowing the stacked switches to be monitored and managed as a single unit.

Meraki Switch Limitations

- Not all metrics listed in the Common Network Management Service Description, such as memory utilisation, CPU utilisation, power supply unit status, fan status and so forth are available from a management and monitoring perspective. This is a limitation imposed by the vendor and not because of any restrictions enforced by NTT Data. The vendor documentation should be consulted for further information.

Meraki Switch Standard Service Requests

A list of standard service requests available for this technology can be found in the MCN Request Catalogue.

Meraki Switch Transition Tasks

No technology specific transition tasks are required. A description of the standard transition tasks included for the service offering is documented in the MCN Statement of Work.

Note:
Any tasks not explicitly described under the Technology Transition Tasks are implicitly excluded from transition.

Cisco Meraki MR Wireless Controllers and Access Points

Cisco Meraki MR Wireless infrastructure provides the cloud-based control plane, as well as wireless Access Points (AP's) that form part of a Cisco Meraki network.

Meraki Wireless Controller and Access Point Specific Monitors

The following technology specific monitors are configured by default:

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
Availability	Device is available	✓	N/A	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	180
Uplink Port Usage	Check port's bandwidth usage	✗	Graphs of the parameter measured over time	N/A	180
Port Errors	Existence of a problem or error in a port	✓	N/A	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	180

Meraki Wireless Access Point Configuration Management

Refer to Configuration Management under the Technology Specific Operations section herein.

Meraki Wireless Access Point Firmware Maintenance

Refer to Firmware Maintenance under the Technology Specific Operations section herein.

Meraki Wireless Access Point Supported Configurations

- Location analytics is excluded from the offering

Meraki Wireless Access Point Limitations

- Not all metrics listed in the Common Network Management Service Description, such as memory utilisation, CPU utilisation, power supply unit status, fan status are available from a management and monitoring perspective. This is a limitation imposed by the vendor and not because of any restrictions enforced by NTT Data. The vendor documentation should be consulted for further information.
- Cisco Meraki Access Points will only be managed from the Meraki Cloud platform.

Meraki Wireless Access Point Standard Service Requests

A list of standard service requests available for this technology can be found in the MCN Request Catalogue.

Meraki Wireless Access Point Transition Tasks

No technology specific transition tasks are required. A description of the standard transition tasks included for the service offering is documented in the MCN Statement of Work.

Note:
Any tasks not explicitly described under the Technology Transition Tasks are implicitly excluded from transition.

Meraki MG Cellular Gateways and Z3 Teleworker Gateways

Cisco Meraki MG Cellular Gateways provide a simple way to extend a Meraki network to a location without fixed line connectivity while the Meraki Z3 Teleworker Gateways provide a light touch way to extend the Client's network to remote workers in a secure fashion.

Meraki MG Cellular and Teleworker Gateways Specific Monitors

The following technology specific monitors are configured by default:

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
Device / Appliance Availability	Device is available	✗	N/A	Due to the nature of these devices, the uplink connectivity used, and the specific uses, NTT does not alert for device availability	180
Uplink Port Usage	Check port's bandwidth usage	✗	N/A	N/A	180

Meraki MG Cellular and Teleworker Gateways Configuration Management

Refer to Configuration Management under the Technology Specific Operations section herein.

Meraki MG Cellular and Teleworker Gateways Firmware Maintenance

Refer to Firmware Maintenance under the Technology Specific Operations section herein.

Meraki MG Cellular and Teleworker Gateways Supported Configurations

- Cisco Meraki MG Cellular Gateways configured as stand-alone devices
- Cisco Meraki Teleworker Gateways configured as stand-alone devices configured with one physical network and an optional 4G failover network.

Meraki MG Cellular and Teleworker Gateways Limitations

- Not all metrics listed in the Common Network Management Service Description, such as memory utilisation, CPU utilisation, power supply unit status, fan status are available from a management and monitoring perspective. This is a limitation imposed by the vendor and not because of any restrictions enforced by NTT Data. The vendor documentation should be consulted for further information.

Meraki MG Cellular and Teleworker Gateways Standard Service Requests

A list of standard service requests available for this technology can be found in the MCN Request Catalogue.

Meraki MG Cellular and Teleworker Gateways Transition Tasks

No technology specific transition tasks are required. A description of the standard transition tasks included for the service offering is documented in the MCN Statement of Work.

Note:
Any tasks not explicitly described under the Technology Transition Tasks are implicitly excluded from transition.

Meraki MV Cameras

Cisco MV Camera's provide remotely manageable smart camera functionality.

Meraki MV Camera Specific Monitors

The following technology specific monitors are configured by default:

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
MV Camera Availability	Device is available	✓	N/A	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	180
Uplink Port Usage	Check port's bandwidth usage	✗	N/A	N/A	180

Meraki MV Camera Configuration Management

Refer to Configuration Management under the Technology Specific Operations section herein.

Meraki MV Camera Firmware Maintenance

Refer to Firmware Maintenance under the Technology Specific Operations section herein.

Meraki MV Camera Supported Configurations

- Single camera deployment
- Multi camera deployment
- Hybrid camera deployment (wired and wireless)

Meraki MV Camera Limitations

- Not all metrics listed in the Common Network Management Service Description, such as memory utilisation, CPU utilisation, power supply unit status, fan status are available from a management and monitoring perspective. This is a limitation imposed by the vendor and not because of any restrictions enforced by NTT Data. The vendor documentation should be consulted for further information.
- Monitoring of any actual camera feeds are excluded from the offering.
- Integration with any third-party systems and applications is excluded from the offering.

Meraki MV Camera Standard Service Requests

A list of standard service requests available for this technology can be found in the MCN Request Catalogue.

Meraki MV Camera Transition Tasks

No technology specific transition tasks are required. A description of the standard transition tasks included for the service offering is documented in the MCN Statement of Work.

Note:

Any tasks not explicitly described under the Technology Transition Tasks are implicitly excluded from transition.