

Managed Cisco Meraki Technical Service Description

Overview of Service

All Cisco Meraki devices which are managed as part of the Service will be supported in accordance with the NTT processes described in the *MCN Statement of Work*. Technology specific tasks associated with the Cisco Meraki technology stack are described in this section. 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

- The Client must be in possession of an active hardware service contract with the vendor of the device(s) under management
- The Client must grant authority to NTT Engineers to contact the hardware vendor directly
- Any management of licenses, if required
- Administrative access to the Cisco Meraki cloud based portal is required to manage the described devices.

Service Design

The complete service is defined by the combination of the following items:

- **Managed Campus Network Service Operations**- service delivery operations that are common to all Managed Campus Network Services. See *MCN Statement of Work*, latest version.
- **Common Operations**- service delivery operations that are common to all services within the category of Network Management. See *MCN Common Network Management Service Description*
- **Service-Specific Operations**- service delivery operations that are specific to this Service. These operations are additive to the *MCN Statement of Work* and Common Operations.

Setup and Deployment

Tasks associated with new environment installation and configuration

As part of the Service, the following tasks are included in the setup fee for all Cisco Meraki devices:

- Inventory of the device
- Creation of templates for the different Cisco Meraki device types
- Setup of initial access - configuration of network interfaces
- Deployment of initial configuration data to devices using zero touch provisioning (ZTP) where available
- Application of firmware upgrades to the latest recommended level
- Creation of administrative and supervisor users required for management by NTT and the Client
- Configuration of syslog parameters (if an external syslog or SIEM service exists)
- Configuration of high availability (if 2 devices exist at specific locations)
- [Configuration of Virtual Networks \(where applicable\)](#)
- Monitoring setup
- Configuration backup setup
- Configuration management setup and implementation of security standards
- Device documentation

Tasks excluded from new environment installation and configuration

- Rack mounting or physical installation of the device(s)
- Physical setup (cabling of Ethernet and power chords) and labelling of the device(s), or
- Configuration of other connected device(s) not managed by NTT

These tasks can be completed by the relevant NTT country or regional team as required.

Tasks associated with taking over an existing installation

As part of the Service, the following tasks are included in the setup fee:

- Inventory of the device
- Review of the existing Cisco Meraki templates
- Review of the configuration of network interfaces
- Review of the control plane deployment, including high availability and redundancy configuration (for on-premise deployments)
- [Review of firmware upgrades and their installation if agreed with the Client as detailed in section *Platform Maintenance of the Base Service Description*](#)
- [Change of the credentials required by the administrative and supervisor users required for management by NTT and the Client](#)
- Review and change the configuration of syslog or SIEM parameters (if a syslog or SIEM exists)

- Review and documentation of the device configuration
- Deliver recommendations after the initial review by NTT network engineers
- *In highly available environments*: Review and documentation of the Service high availability, clustering or stack configuration
- Configuration of Virtual Networks (where applicable)
- Creation and review of monitoring
- Implementation of security standards
- Documentation of the device

Tasks excluded from taking of an existing installation, and require further services

- Physical activities at the premises where the device is installed
- Audit and review of the physical premises where the device is installed
- Review of the configuration or actions of other connected devices not under management
- Analysis and redesign of the network topology is an activity that can be conducted as a chargeable engagement, if not included as part of the Statement of Work, or
- Remediation Activities to be conducted after the audit may be chargeable, if not included as part of the Statement of Work.

Configurations Not Supported

The managed Cisco Meraki service does not include procurement of internet or WAN circuits, or Meraki software or hardware / virtual devices. These services are available from NTT under a separate Statement of Work.

Ongoing Cisco Meraki Device Management

Cisco Meraki Cloud Management Portal

All Cisco Meraki physical and virtual devices are managed via the Meraki Cloud platform, which acts as a centralized control plane. The Cisco Meraki Cloud platform controls all endpoints, providing centralized functions like automated template provisioning and updates, de-commissioning, single screen administration, web-scale reporting, and monitoring and alerting.

Alerts can be configured for a variety of failure conditions. These alerts will be sent to NTT's ticketing system.

From a monitoring and management perspective, not all elements of Meraki devices can be managed and monitored. This is a limitation imposed on the solution by the vendor and not as a result of any restrictions enforced by NTT. Elements such as CPU and memory utilisation are not available for monitoring, managing or reporting.

NTT will manage the Meraki Cloud Portal for the devices included in the solution as explained in this section, including the following activities:

- Management of *Configuration Templates*
- *Configuration of reports to be sent to the Client*
- *Configuration of monitoring information as per Client needs and Meraki capabilities*

Periodic Maintenance Tasks

As part of the Service, the following periodic maintenance tasks are included for Managed Campus Network devices unless explicitly described to the contrary in the Technology Service Description:

Task	Frequency	Description
Firmware review	Continuous process	Notify the Client of outstanding critical firmware upgrades which address vulnerabilities that may affect the Service, such as security exploits or bugs. If the Client chooses to proceed with the upgrade, follow the process defined for firmware patching in <i>the MCN Statement of Work</i> . Upgrade of firmware is not considered the same as patching, but as an installation of a new operating system version for the device.
Configuration Management	On Request	Review of the correct execution of the associated configuration, operational and local node backup; in case of an error with the execution of a backup configuration, operational or local node backup, resolution will follow the process for Incident Management.

Firmware Review

Keeping up-to-date on firmware allows administrators to utilize the latest features and ensures that the latest security enhancements are running on their hardware.

Because Meraki is Cloud-based, many aspects of operation are controlled by the vendor and result in specific limitations and or restrictions.

Firmware upgrades for Meraki devices have some limitations such as firmware upgrades being forced within a specific period of time once it has been made available.

These upgrades can be for beta versions of the firmware (only advised under guidance of the vendor) or stable versions. Upgrades can be scheduled to take place outside of critical business hours from the Dashboard. Failure to schedule upgrades may result in upgrades occurring during normal business hours.

Firmware upgrades can be manually manipulated in the Meraki Dashboard under *General Settings*.

The options defined here include:

- Schedule an upgrade for a specific date and time (by device type)
- Perform an immediate upgrade (by device type)
- Ignore the upgrade (by device type)

It should be noted that the options will only apply to those devices for which an upgrade is available.

Upgrades of Meraki Access Points have two policies that could be applied to the upgrade strategy:

- Minimize total upgrade time
- Minimize client downtime

The former option performs the upgrade simultaneously on as many APs as possible while the latter attempts avoid upgrading adjacent APs simultaneously to ensure that most of the wireless clients stay connected during the upgrade.

The firmware upgrade strategy must be agreed with NTT during the setup of the Meraki environment.

NTT will communicate with the Client to proceed with firmware updates:

- For all the networks in scope
- For a series of networks of the total scope
- For all the devices of a certain type
- For all devices in a certain version, or
- For an individual device

The firmware upgrade will not be executed unless:

- It was previously agreed as part of the Patching Design sessions with the Client (as an example, all the critical security patches must be applied within 24 hours of a firmware release), or
- It was approved by the Client specifically

The firmware upgrade will be executed at an agreed time by NTT engineers. The firmware upgrade process can happen out of business hours if required.

Configuration Management - Backup and Restore

An integral part of the Service is the management of the backup policy and execution of configuration restoration requests. The specifics of Meraki Cloud Management Portal does not allow execution of the standard and typical backup and restore processes. As this is a cloud-based Service, the configuration is stored in the Cloud provided by Meraki. Backup during configuration changes is an automated process in Meraki and NTT is not responsible for taking configuration backup. All the changes to the configuration can be checked using the configuration audit menu from within the Meraki portal. The Change Log allows checking of all the changes executed in a Meraki deployment. This is helpful for basic troubleshooting and manual changes on individual Client requests.

The following tasks are included as part of Network Device Management:

Task	Description
Configuration Backup Policy implementation	When the Service is initially delivered, a Configuration backup policy will be implemented. This policy copies all the configuration data of the managed device so that should a full reinstall of the device be required, all the configuration files can be restored if needed.
Restore of System Configuration	Restore of system configuration from the backup policy.

For details of backup and restore, consult MCN Managed Configuration Backup Service Description.

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. NTT recommends this functionality is added for all clients. Where Meraki Insights is not available, some more advanced reporting functionality will not be available.

Cisco Meraki MX Security and Routing Appliances

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

Supported Configurations


- Meraki MX physical or virtual appliances
- Single devices
- HA security appliance configurations - 2 compatible physical or virtual security appliances in an active / passive configuration, both connected at the same time

Supported Technologies

For a listing of supported Routing and Security Appliance models and their respective sizing, consult the MCN Supported Technology documentation.

Security Appliance Specific Monitors

The following monitors are configured by default:

Monitor	Description	Alerts	Performance Info	Resolution	Poll interval (sec)
Disk (if any)	Disk usage in %		Graphs of the parameter	Engineering Teams will diagnose and try to solve	300

Monitor	Description	Alerts	Performance Info	Resolution	Poll interval (sec)
			measured over time	the issue, and escalate to the Client if needed	
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
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 & 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

Required from the Client for Managed Meraki Security Services

As a general approach, the following will happen when a IDS/IPS device starts its managed service:

- The installation process will configure all the policies as desired by the Client
- This will generate a huge number of false positives, so on the first days of the Service the security policy should be loosened
- Additional rules are added little by little to strengthen the security policy
- This will eliminate false positives and provide a more secure environment for the Client's applications; and
- Once stabilised, no more changes would be required until new versions of the Client's applications are released and deployed. At that moment, the process can start again.

Because of the above expected results, it is important that the starting point of the firewall policy operation counts with the relevant Client contacts to adapt the firewall policy to the Client's applications. This activity is not something the engineers managing the devices will do. In the case of issues once the policy has been activated, the only expected outcome from the engineers will be complete deactivation of the policy or (if possible) changing the policy from "Block" to "Alert", "Log" or whatever non-blocking option is available. 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.

Tasks Included in the standard transition

As part of the Service, the following tasks are included in the setup fee to validate NTT's ability to manage the devices

- Registration of the device to the Cisco Meraki portal
- Create, delete, modification of security zones and associated interface configurations etc.
- Create, delete, modifications of layer3 physical interfaces
- Create, delete, modification of layer3/4 port-based access list without security profiles.
- Create, delete, modification of "one to one" / "many to one" Source static & Source dynamic NAT policies.
- Create, delete, modification of basic S2S IPsec with pre-shared key & Static routes.
- Create, delete, modification of basic Remote access VPN configuration with local accounts.
- Create, delete, modification of Default & Static routes.
- Initial licenses and contracted subscriptions configuration
- Configuration of error pages and error page groups
- Setting up VPNs between MX FW (Meraki Auto VPN)
- Configuration of log relaying and other log management mechanisms if contracted
- Routing configuration in the Meraki Portal
- Dual uplink port configuration
- LTE failover configuration
- Configuration of Intelligent Path Control policies
- Configuration of Branch Routing (route redistribution) policies

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
- Hardware, Software and/or support around it

Service Requests

As part of the Service, the fulfilment of the tasks listed in the table below are included.

Meraki MX Security Appliance Service Requests

Task	Description	Included
Creation and management of Security Zones	Create, delete, modification of security zones and associated interface configurations etc.	✓
Creation and management of VPNs	Creation, change and deletion of VPNs configured in the device, including the users in the VPNs; this does not include connection to the external peer to configure the remote end point, or the installation of any customer on any end user computer	✓
Management of access rules	Creation, change and deletion of access rules configured in the device that allow and deny traffic to/from the servers in the DMZs and other internal networks without security profiles.	✓
Creation and management of NATs	Create, delete, modification of "one to one" / "many to one" Source static & Source dynamic NAT policies.	✓
Routing management	Management of the routing elements available in the firewall applicable to static and default routes.	✓
Management of failover	Only in HA or clustering configurations: management of failover policy to allow the service to continue working if a device error occurs	✓
Management of disk space	Evaluation and study of actions for freeing and optimising disk space (if disk is present in the device)	✓
Bandwidth Management and connectivity features	Basic creation, addition or deletion of Bandwidth Management, Quality of Service or shaping rules. Additionally, changes to the most specific routing features, including changes and reconfiguration of: <ul style="list-style-type: none"> Intelligent Path Control administration Branch Routing (route redistribution) administration Traffic shaping management Dual uplink port management LTE failover management 	✓
Management of SSL certificates and settings	Addition, removal and modification of SSL certificates associated to the device and services	✓
Relaying of network generic services	Configuration of NTP, DHCP and DNS settings for these to be resolved by external services.	✓
Creation and management of Geo-based security	Configuration and management of: <ul style="list-style-type: none"> Reputation Geo-IP and Botnet filter Other Geo-related policies 	✓
Forward logs to an external SIEM service	Changes in the settings to forward logs to an external SIEM and SOC solution, destination, port, and/or information being sent	✓
Forward logs to a managed log management service	Changes in the settings to forward logs to an associated (and managed) log management system.	✓

MX Requests Not Included with the Service

IDS / IPS

IDS and other advanced security features' correct operation is heavily dependent on the application(s) being protected, which means that the ones 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 whatever the log management tool the Client uses). On the SIEM, the reason why applications are blocked generating false positives, or not blocked when these

should, would be identified by the Client. As part of the ongoing management of an Advanced Security device, it is not included in the review of all the logs for an unidentified error or false positive. This is an activity for the Client to perform. 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 analyst team is not included as part of the Meraki MX Management Service. This means that the detection of vulnerabilities, threats and similar security activities are limited to the features included in the devices under management and that NTT will not include additional tooling. As such, the following is not part of the Service unless additionally contracted:

- Log Management Service
- Log Correlation Service
- Threat Correlation, Collaborative Intelligence, Monitoring and Analysis of Logs with SOC analysts to detect and/or investigate alerts

Cisco Meraki MS Switches

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

Supported Configurations

- 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

Supported Technologies

For a listing of supported Switching models and their respective sizing, consult the [MCN Supported Technology](#) documentation.

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

Specific Tasks Associated with Installation of a Switch

As part of the Service, the following tasks are included in the setup fee to validate NTT's ability to manage the devices:

- Creation of VLANs
- Creation and configuration of spanning tree
- *In stack environments* : service clustering

Service Requests

As part of the Service, the fulfilment of the tasks listed in the table below are included.

Meraki MS Switch Service Requests

Task	Description	Included
Creation and management of VLANs	Creation, change and deletion of VLANs configured in the device and its nodes	✓
Management of spanning tree	Management of the spanning tree protocol to handle link redundancy	✓
Management of port channel / ether channel	Creation, change and removal of port channel interfaces	✓

All of the above tasks will be performed according to the Change Management process defined in the *MCN Statement of Work*.

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.

Supported Configurations

- Cisco Meraki Cloud (Wireless Controller)

- Cisco Meraki APs will only be managed from the Meraki Cloud platform.

Supported Technologies

For a listing of supported Switching models and their respective sizing, consult the MCN Supported Technology documentation.

Wireless Controller Specific Monitors

The additional monitors which can be configured for Wireless Controller management are:

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

Specific Tasks Associated with Installation

As part of the Service, the following tasks are included in the setup fee to validate NTT's ability to manage the devices:

- Creation of SSID's, VLANs and WLANs
- Creation and configuration of new wireless networks
- Creation and configuration of security policies
- Addition of APs to networks
- Connection to external user directory or database
- *In HA environments* : Service clustering

Specific Tasks Excluded from Installation

- End User support, or
- Management of the AP's if these AP's are not in-scope

Cisco Meraki MG Cellular Gateways, Z3 Teleworker Gateways and MV Cameras

- Cisco Meraki MG Cellular Gateways provide a simple way to extend a Meraki network to a location without fixed line connectivity.
- Cisco Meraki Z3 Teleworker Gateways provide a light touch way to extend the Client's network to remote workers in a secure fashion.
- Cisco MV Camera's provide remotely manageable smart camera functionality.

Supported Configurations

- Cisco Meraki MG Cellular Gateways configured as stand alone devices
- Cisco Meraki Z3 Teleworker Gateways configured as stand alone devices, and configured with 1 physical network and an optional 4G failover network
- Cisco Meraki MV Camera's configured as stand alone devices

Supported Technologies

For a listing of supported Switching models and their respective sizing, consult the MCN Supported Technology documentation.

Cellular and Teleworker Gateway and MV Camera Specific Monitors

The additional monitors which can be configured for Cellular and Teleworker gateway management are:

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
MG and Z3 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
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

Specific Tasks Associated with Installation

As part of the Service, the following tasks are included in the setup fee to validate NTT's ability to manage the devices:

- Adding the device to the Meraki Cloud console

Specific Tasks Excluded from Installation

- End-user support
- Any physical installation activity, unless specific in the Statement of Work