Product specifications:
Cloud Managed Network – Cisco Meraki

1.1 Service overview

Cloud Managed Network – Meraki (“the Service”) provides monitoring, alerting, reporting and management of a customer’s Wide Area Network and on-premises network equipment using Meraki cloud-based network management. Customers are provided an actively managed service for a range of Spark supplied Cisco Meraki devices. The service can be provided at one or multiple customer sites with multiple network connections able to be supported at the same site.

1.2 Pre-requisites

For the service to be provided devices must be able to connect to the Cisco Meraki cloud-based network management system, through a network connection that can access the internet. A fixed network connection is not provided as part of the service and must be purchased separately. Fixed network connections that are supported include Fixed Line Broadband and Managed Internet Services that can be provided by Spark. Wireless Internet Access is as part of the Cloud Managed Network – Meraki service as an add-on.

1.3 Standard features

The standard features of the service are:

- Spark will supply and provide support for a range of devices including SD-WAN devices, LAN switches, security cameras* and Wi-Fi access points. The devices will remain the property of Spark during the term.
- 4G capable SD-WAN devices allow for Wireless Internet Access or Wireless Failover. Data comes included in the cost of the device where Wireless Failover is selected. Wireless Internet Access can be selected as the primary internet access where 4G coverage is sufficient. Wireless Internet Access has a monthly fee in addition to the cost of the 4G capable device and data is uncapped with a fair use policy**
- 24/7 network management, with problem alerting
- Cloud controlled and deployed network and security policies
- Software-Defined WAN (SD-WAN) – VPN creation between multiple sites
- Standard SLA covering Monday–Friday 7am–7pm with next business day hardware replacement
- Automatic firmware updates for devices
- Dashboard – an online portal showing in real time: Device location and status
- Network topology
- Application usage
- Bandwidth utilisation
- Security – Stateful firewall, IPsec encryption
- Application control
    - Application blocking
    - Application bandwidth restriction
    - User blocking
    - Device blocking
- Pre-configuration of devices – SD-WAN devices will automatically download their network and security configurations and policies from the cloud management system and self-configure when first plugged into a supported network connection.

* Spark will enable you to manage and troubleshoot your security camera network through phone-based support. Installation and repair of security cameras is excluded and must be carried out by a licensed security technician.

** For Wireless Failover, a Spark SIM card will be put into the device and it will failover to mobile connectivity if fixed line connectivity fails. Once fixed line connectivity is restored, the service will failback to the fixed line connection. You need to take reasonable steps to restore the fixed line connectivity and you must use Wireless Failover consistently with the way you use your fixed line connectivity. Should the device need to operate in a failover state for an extended period of time, then Spark may substitute an alternate connectivity solution.

For Wireless Internet Access, a Spark SIM card will be put into the device and it will provide internet access via the mobile network using the failover mode of the device. Wireless Internet Access is a data-only add-on – it does not support voice calling.

For both Wireless Internet Access and Wireless Failover, the SIM cannot be used in a device other than the Cloud Managed Network router. The device and SIM cannot be used in a different location other than the installed location and you cannot move the device to another location without Spark's permission. The site must have sufficient Spark LTE coverage.

1.4 Service options

For an additional cost, customers can select the following service options for the service:

1.4.1 Advanced Security

Advanced Security can be chosen as an option for the SD-WAN device. This provides:

- Advanced Malware Protection
- Intrusion Prevention
- Content Filtering
- Web Search Filtering

Note that Advanced Security must be applied to all SD-WAN devices in your network and cannot be applied on a device by device basis.

1.4.2 Service target add-on

For an additional cost, you can choose to have the agreed service hours extended beyond the standard service hours and have a shorter hardware swap-out time than that specified in section 1.10.1.

Service attribute	Attribute definition	Service target
Agreed service hours	The hours during which, if a customer call indicates a fault, Spark will commence restoration work.	24/7
Hardware swap-out	Device replacement in the event of a hardware failure while under warranty	Within 6 hours for available locations.

Note:

1. The 24x7 SLA add-on is available for sites within 40km travel distance of Spark Service Centre locations in Whangarei, Auckland, Hamilton, Mt Maunganui/Tauranga, Rotorua, New Plymouth, Napier, Palmerston North, Wellington, Nelson, Greymouth, Christchurch, Queenstown, Timaru, Dunedin and Invercargill.
2. The 24/7 SLA add on must be applied to all devices of a common type at a site.

3. 24/7 SLA add on is not available for Wi-Fi access points or security cameras.

1.5 Devices

A range of device types and models are available with the service. These include SD-WAN devices with or without 4G LTE, LAN switches, Wi-Fi access points and security cameras.
The range and type of devices will change over time as the Service evolves and as current devices are superseded by newer models. A full list of the currently available devices can be supplied upon request.

Spark will retain ownership of the hardware, excluding external antennae, supplied as part of the service and of the software licenses required for all devices provided as part of the service. Use of the devices and software is governed by the end user agreement. View Cisco Meraki End Customer Agreement

Using this service means that you are collecting data regarding the devices that connect to your network and how your network is being used. Through the service, you are transferring the data to Spark and/or Cisco Meraki for processing and storage (including in the cloud). This may include personal information relating to your network users (e.g. traffic information, geolocation information, location analytics, information regarding content transmitted). It is your responsibility to provide notice to and obtain any necessary consents from, your network users regarding the collection, processing, and storage of such data.

1.6 Service implementation

You can choose to self-install devices provided as part of the service or alternatively request a managed install from Spark. If a customer chooses self-install, Spark will ship devices directly to the customer site or on request to the customer's nominated third-party installer. Spark will provide phone support during business hours for any issues that arise regarding self-installation. For managed install a Spark or Spark contracted field service technician will install devices at the customer's site.

1.7 Service boundaries

Spark will ensure the correct functioning of the devices provided as part of the service within the service boundary. These are as follows:

- SD-WAN device – the WAN ethernet port/s facing the external network connection/s and the LAN ethernet ports facing the internal customer network
- LAN switches – the LAN ethernet ports facing the internal customer network and LAN switch uplink port/s
- Wi-Fi access points – the Wi-Fi access point LAN port
- Security cameras – the security camera LAN port

The following fall outside of the service boundary:

- Network connections – Network connections are not part of the service. If the network connection is provided by Spark, a call to the helpdesk may be passed through to the appropriate team to deal with any network connection issues. Any network connection issues related to other network connectivity providers cannot be dealt with by the helpdesk and must be passed to the appropriate connectivity provider for resolution.
- Configuration and support of other customer network components including mail servers, web servers, web sites and any routers, switches and Wi-Fi access points that are not provided as part of the service.
- Internal building cabling.

1.8 Service management

1.8.1 Dashboard

Spark will make available an online portal ("the Dashboard") for you to view the status and performance of your network and devices. From the Dashboard you will be able to see a range of information including:

- Device status
- Network utilisation
- Applications usage
- User devices connected to the network
- Network and security configuration settings

The Dashboard is accessible from a web browser and is available 24/7. Logins will be provided to customer-nominated employees or third-party IT provider. Unless otherwise agreed, access to the Dashboard will be read-only. Use of the Dashboard is governed by the Cisco terms of use. View Cisco Meraki Website Terms of Use

1.8.2 Helpdesk

Helpdesk support will be available for the Service according to the Service Targets in Section 1.10 and will:

- Resolve any faults reported with the service
- Action any Move Add or Change requests
- Provide phone support for issues related to self-install of devices

1.8.3 Automatic firmware upgrades

Automatic firmware upgrades for devices will be periodically deployed. Customers will receive an email notifying them of the upgrade and can reschedule their update through the Dashboard if the automatic upgrade is occurring at a time not suitable to the customer.

It is important that firmware updates are deployed in a timely manner for the best operation of your network. If you choose to defer updates there is a greater risk of security or network incidents arising as a result of your network being on an out of date version of the firmware.

1.9 Responsibilities

1.9.1 Customer responsibilities

You are responsible for:

- Providing Spark with all necessary information to ensure the Services can be set up correctly.
- Assisting Spark with implementation, fault resolution and MACs.
- Providing a suitable physical environment for devices provided as part of the Service and if necessary, obtaining consent from applicable third parties in order for Spark to complete installation.
- Conducting post installation testing to confirm that your network and applications are running as expected.
- Notifying Spark as soon as possible of any faults or network issues with the service.

- Your network and security policies. These belong to you and you retain the responsibility for the end-to-end security and firewall policies in place for your organisation. Spark can assist with the definition and development of these.
- Providing security within your network, including:
  - Keeping usernames and passwords to the cloud management portal secure
  - Physical security, including physical access to the premises and access to computer systems
  - Security for trusted servers, applications, desktop computing devices, notebooks and other mobile or remote computing devices
- Ensuring only authorised personnel can request moves, adds or changes to the service.
- Providing network connectivity to its sites and complying with the 4G Failover requirements in section 1.4.1.
- Comply with the Cisco Meraki Software License Terms and Cisco Meraki Website Terms of Use, including ensuring appropriate user consents are in place.

1.9.2 Our responsibilities

Spark will be responsible for:

- Ordering and supplying devices to your sites
- Installation of devices (other than security cameras which must be installed by a licensed security technician) at your sites when managed installation has been requested
- Setting up the network and security policies and configuration in the cloud management system as specified by you

Actioning any Move Add and Change requests to your network and security policies and device configurations using the cloud management system.

1.9.3 Exclusions

The Service specifically excludes:

- Network connections, as per Section 1.7
- Management of any other network devices not provided as part of the service
- Onsite support, other than that required to replace hardware
- Managed Security Services such as a Security Operations Centre, Vulnerability Management and Security Event monitoring
- Anything that falls outside of the services boundaries defined in Section 1.7

1.10 Service targets

The following definitions apply to this section 1.10:

- **Business days:** Monday to Friday, excluding national public holidays and the provincial anniversary day applicable to the affected customer site
- **Business hours:** 9:00am to 5:00pm on Business Days, New Zealand time

Service attribute	Attribute definition	Service target
Availability	The cloud management system is available for customer use and functioning in accordance with this Product Specification during agreed service hours.	Available 24/7/365 except during planned outages.
Agreed service hours	The hours during which, if a customer call indicates a fault, Spark will commence restoration work.	7am–7pm Monday–Friday business days or longer where the service target uplift has been selected.
Call reception	The hours during which incoming telephone calls from customers to the helpdesk are accepted and logged, and call answering times.	Calls accepted 24/7 days and answered within 20 seconds 85% of the time.
Monitoring hours	The hours during which monitoring systems are operational.	24/7
Response time	The elapsed time during agreed service hours between call reception and Spark commencing restoration work.	Within 4 hours and 80% within 2 hours.
Remote service restoration	The elapsed time during agreed service hours between call reception and the customer being notified that service is restored to the defined levels.	Within 4 hours and 80% within 2 hours.
Hardware swap-out[1]	Device replacement in the event of a hardware failure whilst under warranty.	Next business day, provided replacement request is received prior to 3pm on business days or shorter where the service target uplift has been selected.
Planned outage notification	Prior notice of planned maintenance that could cause a service outage.	5 business days. Planned outages are normally scheduled after midnight.

[1] For privacy reasons, we don’t hold third party broadband provider username and password details. In the event of a hardware swap-out, you will need to re-supply these details for the above service target to be met.

1.10.2 Provisioning and change targets

Service attribute	Attribute definition	Service target
Provisioning service hours	The hours during which Moves, Adds and Changes will be actioned, or self-installation assistance provided	Business hours, during business days

Provisioning / change acceptance	The elapsed time between a customer logging a Move, Add or Change request and the confirmed acceptance of that request	Receipt acknowledged within 2 business hours
Change completion	The elapsed time between the confirmed acceptance of a MAC request and the completion of that request	For changes that can be completed remotely within 1 business day, otherwise as agreed
Provisioning completion	The elapsed time between the confirmed acceptance of a device order request and completion of that request	Within 15 business days