



# Connected Society Cloud Managed Network Service

## G-Cloud 15 Service Definition Document

Crown  
Commercial  
Service  
Supplier



## Contents

|                                          |   |
|------------------------------------------|---|
| Cloud Managed Network Service .....      | 3 |
| Simplicity .....                         | 3 |
| Manageability .....                      | 3 |
| Security.....                            | 3 |
| Management Interface .....               | 4 |
| Organisation Summary .....               | 4 |
| Clients and Applications.....            | 4 |
| Site Activity .....                      | 5 |
| Security Activity .....                  | 5 |
| Support and Service Management .....     | 6 |
| Managed Service Desk .....               | 6 |
| Ticket notifications and updates .....   | 6 |
| Incident Management.....                 | 6 |
| Monitoring.....                          | 6 |
| Escalation Procedures.....               | 6 |
| Major Incident Management .....          | 7 |
| Hardware and Software Lifecycle .....    | 7 |
| Maintenance updates .....                | 7 |
| Reporting and analytics.....             | 8 |
| Change requests.....                     | 8 |
| Co-management .....                      | 8 |
| Staff training .....                     | 8 |
| Documentation .....                      | 8 |
| Account Management .....                 | 8 |
| Regular Service Management Meetings..... | 8 |

## Cloud Managed Network Service

Key benefits of our Cloud Managed Network Service include the following:

### Simplicity

- ✓ Managed service wrap of the solution based upon a simple flexible per user per month basis.
- ✓ A complete end to end solution, including Internet Circuits, 5G Sim Cards, SD-WAN Multi-Functional Security Gateways, Secure Access Service Edge, Network Switching, WiFi and IoT Devices.
- ✓ A responsive Service Desk and Support Service, including Remote Monitoring and Onsite Support where specified.

### Manageability

- ✓ A single pane of glass to manage all aspects of the solution through the Meraki Dashboard and Cisco Secure suite of products.
- ✓ Unlimited simple changes such as firewall policies, VLAN's and SSID's.
- ✓ Ability for internal buyer resource to co-manage the solution by having access to make necessary small adds, moves, and changes (i.e. – firewall policy changes).
- ✓ Notifications of any maintenance updates that will affect the managed service solution with minimum 14 days' notice.
- ✓ Email Notifications to advise of tickets, resolutions, breaches and security reports.
- ✓ Proactive monitoring of underlay circuits with automated alerts and tickets.
- ✓ Reporting and analytics for performance, trend analysis, and troubleshooting.

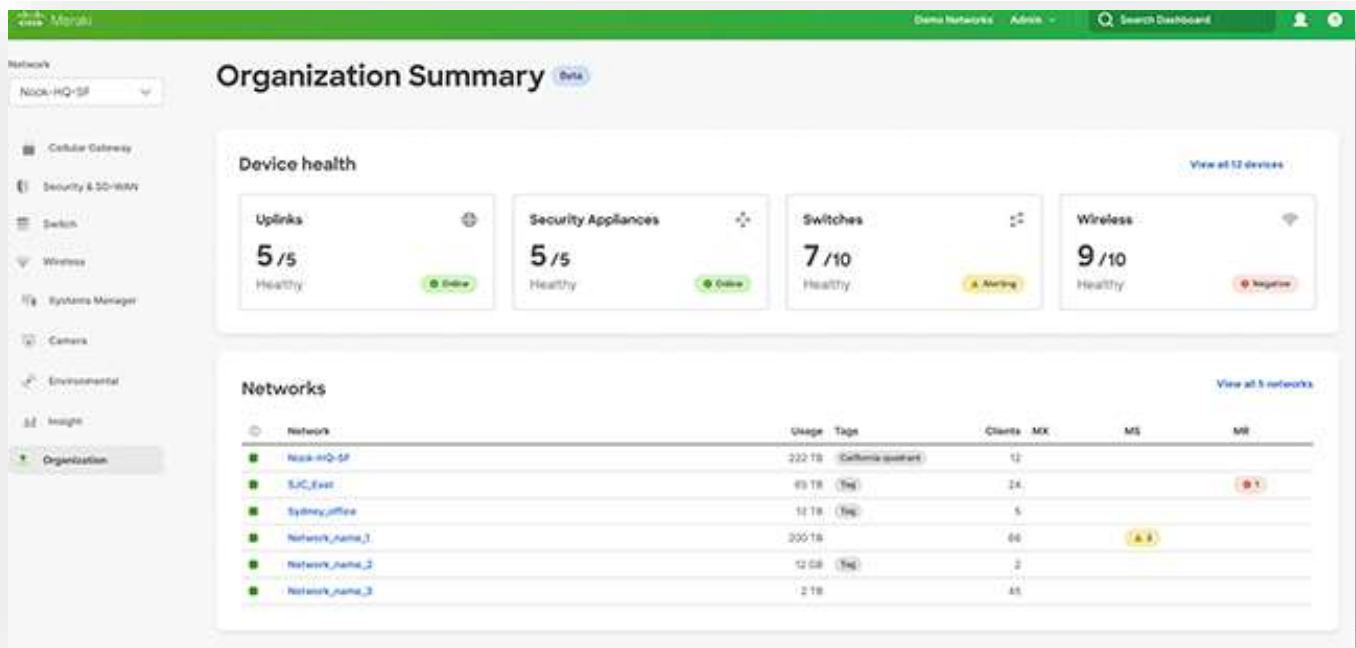
### Security

- ✓ Devices are kept up to date with the latest firmware and Security patches as part of the managed service aligning to an N-1 industry standard methodology.
- ✓ Software and hardware patched to the latest vendor security patches and software version throughout the lifecycle of the contract.
- ✓ The ability to administer, rollout and manage security policies across the entire estate using the Meraki dashboard to maintain a consistent security posture.

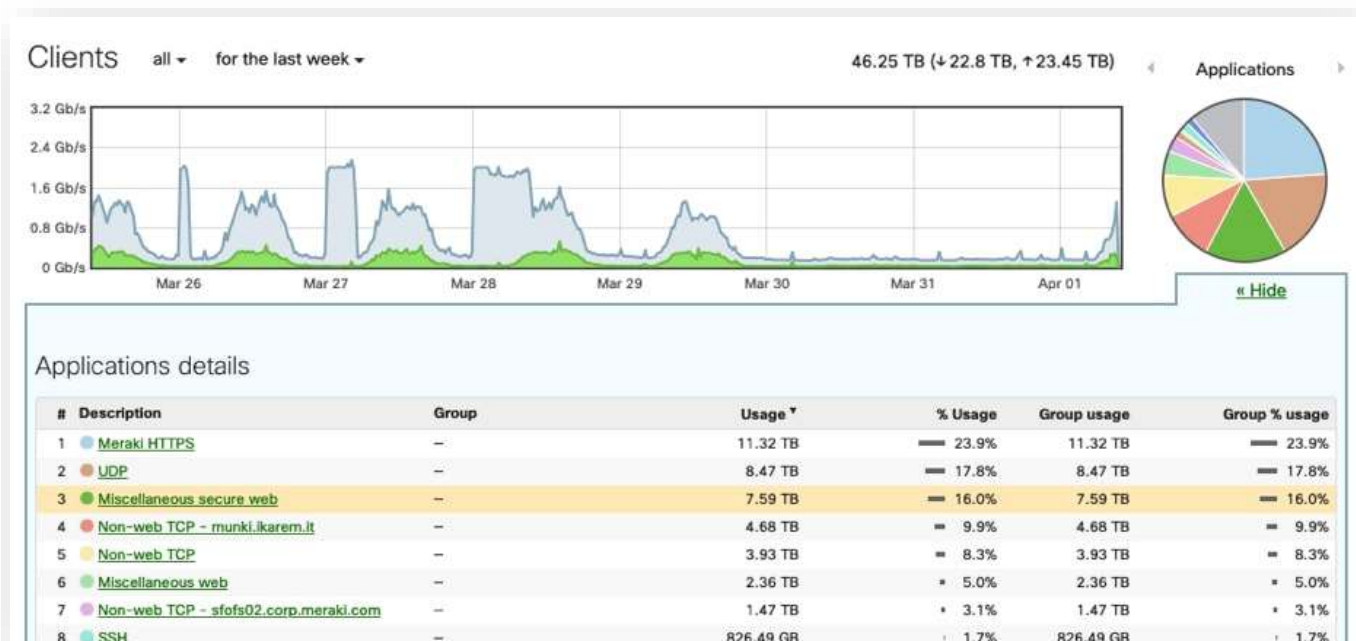
## Management Interface

All aspects of the Cloud Managed Network Service are managed through a single pane of glass – the Meraki Dashboard with integrated Cisco Secure. Example views from the Meraki Dashboard is shown below:

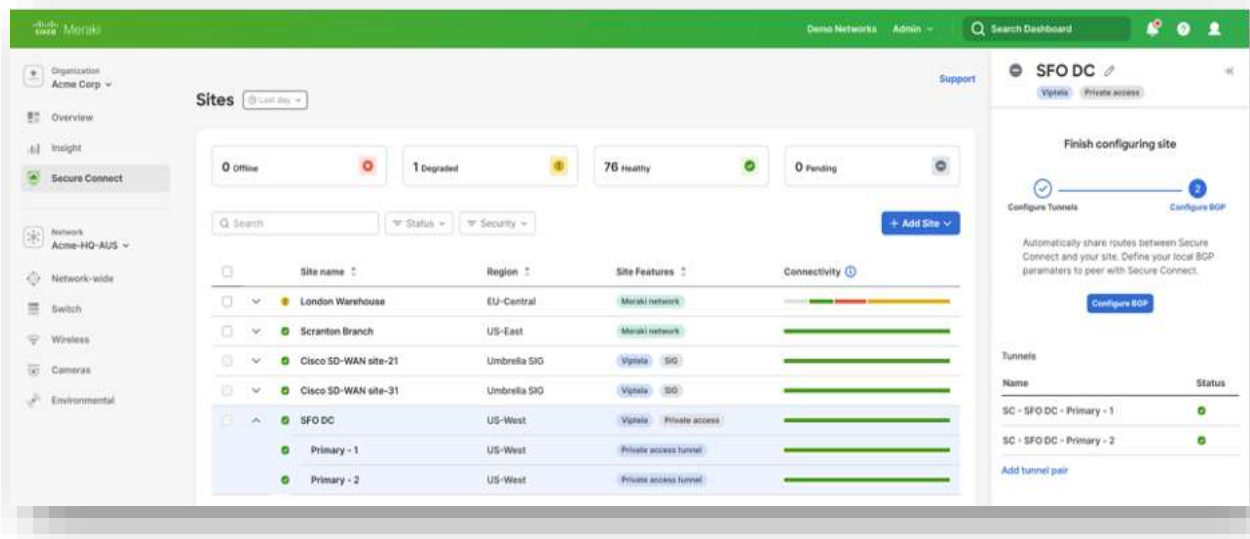
### Organisation Summary



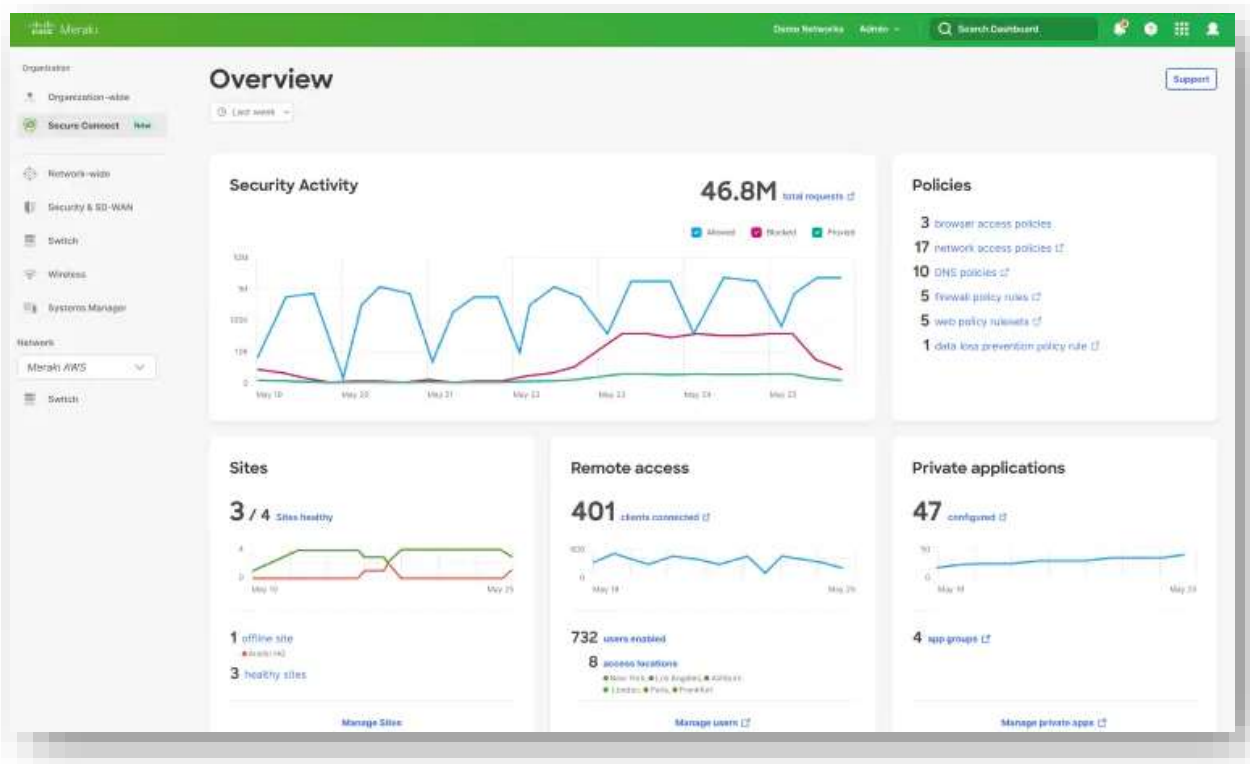
### Clients and Applications



## Site Activity



## Security Activity



## Support and Service Management

### Managed Service Desk

We will provide a dedicated, single point of contact responsible for the ongoing managed support. Tickets are raised by authorised buyer staff through the Service Desk and then all subsequent communication and updates will be managed by the desk which is accessed via phone or email.

### Ticket notifications and updates

As part of the Managed Service Desk, any new tickets and alerts will be notified to nominated contacts to advise users and analysts of new calls, resolutions, breaches change notifications and reports. This will include both buyer generated tickets or those raised by automated monitoring facilities.

### Incident Management

dbfb will investigate, manage, and support any faults or issues on the managed SD-WAN infrastructure from the technical service desk. Once identified and logged, the service desk will provide you with remote assistance to rectify the issue or advise and implement remediation actions to reduce the likelihood of the issue recurring. Where on site hands are required, these will be provided by dbfb on site engineers. Additionally, dbfb will manage the provision and support of transmission circuits. Where an issue is not immediately identifiable as a hardware issue, our service desk team will work to reduce the impact and resolve.

### Monitoring

We will proactively monitor underlay circuits in addition to the monitoring of the Cisco SD-WAN service, including routers, interfaces and underlay circuit connections. We will maintain a baseline of the throughput and/or capacity of the managed environment and establish KPIs related to the capacity that will be monitored.

We can create and maintain customised alerts to provide automated notifications based on the KPIs as well as potentially specific events that you wish to report on. Where we identify an ongoing or recurring issue, a problem record will be raised and senior engineers will be engaged to resolve the problem.

### Escalation Procedures

As detailed in the Incident Management Process Flow diagram, tickets will generally be initially handled by first line level engineers. Where technical escalation is required, we have access to 2<sup>nd</sup> line, 3<sup>rd</sup> line, support consultants and support architects.

Where needed the Managed Services team would contact the vendor and fully co-ordinate investigations until a resolution is found. The escalation contacts will be notified internally based on the triggers identified below:

- ✓ Level 1: Duty Manager: Contacted when 50% of any P1 or P2 is reached, or when any ticket's SLA has breached.
- ✓ Level 2: Contacted when 75% of any P1 is reached, or when any ticket's SLA has breached.
- ✓ Level 3: Contacted when 90% of any P1 is reached, or when any P2 ticket's SLA has breached.

## Major Incident Management

We have a robust Major Incident Management (MIM) process in place. The process aligns with the ITIL framework and can be summarised in four main areas:

- ✓ Identification – The incident will be identified and triaged. If required, a major incident will be declared and all key stakeholders will be informed.
- ✓ Containment – A Major Incident Manager will be appointed. Conference bridge calls will be set up with key technical resources. Stakeholders will be updated at regular intervals.
- ✓ Resolution – A resolution will be identified. An emergency change will be raised to implement the fix. All stakeholders will be updated by the MIM.
- ✓ Maintenance – A Root Cause Analysis (RCA) will be performed. The RCA will be shared with the buyer. If required, actions will be implemented to prevent reoccurrence of the issue.

## Hardware and Software Lifecycle

As part of the Managed Service we will perform quarterly reviews of the hardware and firmware running on supported devices within the buyers network. These reviews would be presented as part of a regular monthly service review meeting.

## Maintenance updates

Notification of any planned maintenance activity will be provided via email to the designated maintenance contact, with a minimum of 14 days notification.

## Reporting and analytics

We will collate a range of reporting and analytical information as part of monthly service reviews for performance monitoring, analytics, trend analysis and troubleshooting. This will include collating data from both the Cisco SD-WAN platform and other sources of information including the performance, utilisation and availability of circuits and any mobile data sim cards. In addition to providing regular reports, we will build intuitive dashboards within platforms such as PowerBI, for your team to access, in order to undertake regular assessment of the performance of the services and support future planning.

## Change requests

The Cloud Managed Network Service includes unlimited requests. Any change requests will be handled through the service desk using ITIL-defined processes for change review and approval, in accordance with your requirements.

## Co-management

Included in the service will be the ability for buyer authorised staff to co-manage the solution by having access to make necessary small adds, moves, and changes (i.e. – firewall policy changes).

## Staff training

Where specified the Cloud Managed Network Service will include training via access to Cisco learning credits, to enable buyer staff to be trained on the solution and become Cisco accredited.

## Documentation

Full documentation, change control processes, knowledgebases and reference guides will be provided and kept updated as part of the ongoing managed service.

## Account Management

You will be provided with an assigned Account Manager and Service Manager throughout the contract who will be available for your team to contact and who will attend monthly service reviews.

## Regular Service Management Meetings

In addition to informal Account and Service Management, we will hold Monthly Service Management meetings, either online via Microsoft Teams, or on site at the buyers or dbfb offices. It is expected that such meetings may need to be more regular, for example weekly or bi-weekly during the early stages of the contract.