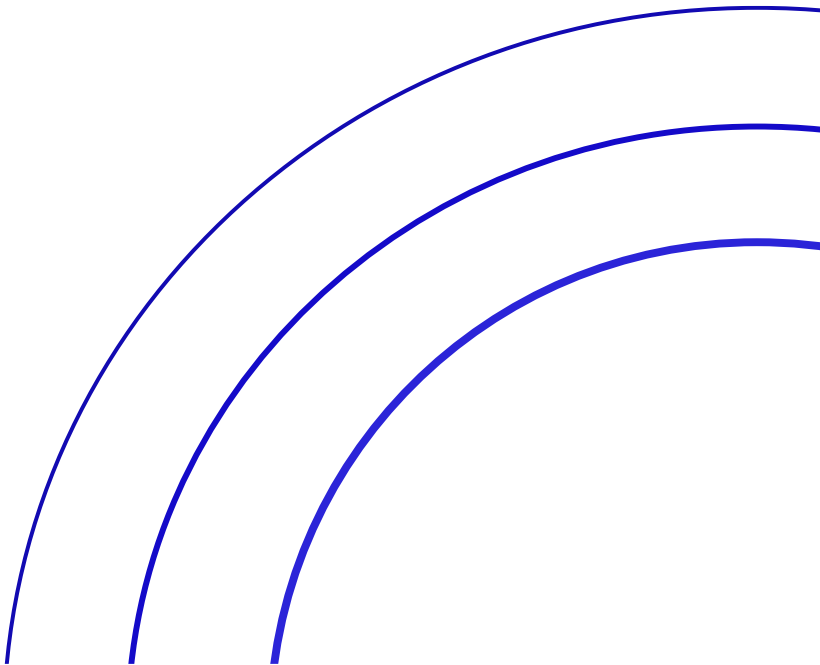
Managed Network Device
Service Description



1. Document Control

TITLE:	**Managed Network Device Service Description**	**DOCUMENT REF NO:**	QMS REC154
DESCRIPTION:	This document defines the services provided by Calligo's Managed Network Device service.		
OWNER/ AUTHORITY:	VP Cloud Operations	**VERSION NO:**	1.3
DOCUMENT CROSS REFERENCE:	N/A	**VERSION DATE:**	25/09/2023
DISTRIBUTION METHOD	Email and Website	**DOCUMENT CLASSIFICATION**	Internal

DOCUMENT OWNER & APPROVAL
The VP, Cloud Operations, is the owner of this document and is responsible for ensuring that this service description is reviewed in line with the review requirements of Calligo's Information Security Management System, Project Management Frameworks as well as the guidance and requirements of the CSSF.
Approved by the Chief Operating Officer, Calligo ("Entity") on 25 September 2023

CHANGE HISTORY RECORD				
VERSION	**DESCRIPTION OF CHANGE**	**AUTHOR**	**APPROVAL**	**DATE OF ISSUE**
1.0	Initial Issue	Director, Operations Management	VP Cloud Operations	23/01/23
1.1	Updated formatting	Director, Operations Management	VP Cloud Operations	01/02/23
1.2	Updated supporting documentation links	Director, Operations Management	VP Cloud Operations	20/02/23
1.3	Added in Managed UPS	Director, Operations Management	VP Cloud Operations	25/09/23

Contents

2. Service Overview

This document defines the services provided by Calligo's Managed Network Device service. The Managed Network Device service is one of a suite of services within the Calligo Operating Model.

3. Service Inclusions

3.1. CO-ITSM-PFWL (as required)

This service leverages client specific requirements for on premises firewall and or router support.

3.2. CO-ITSM-PSW (as required)

This service leverages client specific requirements for on premises switch support.

3.3. CO-ITSM-WAP (as required)

This service leverages client specific requirements for wireless access points.

3.4. CO-ITSM-UPS (as required)

This service leverages client specific requirements for Managed Uninterruptable Power Supply (UPS) and support for on-premises physical devices.

3.5. CO-ITSM-SD

This service leverages an ITSM platform and trained Level 1 Service Desk Analysts to cover activities that provide a client facing Service Desk.

4. Service Provisions

4.1. CO-ITSM-PFWL (as required)

4.1.1. Inclusions

CO-ITSM-PFWL	
Scope Item	**Description**
Firewall Policies	Management of traffic policies including zone traversal allow/deny rules, SNAT rules, proxying and inspection of common protocols (e.g., HTTP, FTP, SMTP)
Security Services	Management of Unified Threat Management services (e.g., DDoS prevention, IDS/IPS, geolocation and source IP control, APT Blocker, DLP. Application control, botnet detection, URL reputation checks)
WAN configuration	Internet connection, multi-WAN link monitor and failover, SD-WAN
VPN (Virtual Private Network) Connectivity	Site-to-site and client access VPN configuration using secure protocols
IP Network services	DHCP, DNS, VLAN (Virtual Local Area Network), routing, and NTP service configuration for internal LAN (Local Area Network) networks

CO-ITSM-PFWL	
Scope Item	**Description**
Network performance optimization	QoS (Quality of Service) policies, bandwidth management, link aggregation
Firmware Updates	Installation of latest firewall OS and firmware updates
Troubleshooting	Investigation and remediation of abnormal or unwanted firewall behaviour
Logging	Firewall and traffic event logging

4.1.2. Exclusions

CO-ITSM-PFWL	
Exclusion Item	**Description**
Out of support appliance	Any appliance that has passed its end-of-life date or manufacturer support contract has expired
Integration of firewall(s) covered by the Service with Third Party solutions used by the Client.	Integrating the firewall with a product or service not directly supported by the manufacturer
Client internet connectivity	Availability and operability of ISP infrastructure (modem, routers, fibre/coax, etc.) located beyond the firewall interface (demarcation point).
Internet performance	ISP service issues e.g., latency, jitter, low/insufficient bandwidth
Intra-network performance	Connectivity among devices in the same subnet
VPN connectivity to an uncovered device/appliance	Connectivity and configuration of a remote VPN endpoint not covered by the service
Local network of client attempting to use VPN	Some remote networks may have strict policies that block client VPN connectivity

4.2. CO-ITSM-PSW (as required)

4.2.1. Inclusions

CO-ITSM-PSW	
Scope Item	**Description**
IP Network services	DHCP, DNS, VLAN (Virtual Local Area Network), L3 routing, spanning tree, POE, Trunks and NTP service configuration for internal LAN (Local Area Network) networks
Network performance optimization	QoS (Quality of Service) policies, ACL, IGMP and link aggregation
Firmware Updates	Installation of latest switch OS and firmware updates
Troubleshooting	Investigation and remediation of abnormal or unwanted switch behaviour
Logging	Switch logging

4.2.2. Exclusions

CO-ITSM-PSW	
Exclusion Item	**Description**
Out of support switch(es)	Any switch that has passed its end-of-life date or manufacturer support contract has expired

Integration of switch(es) covered by the Service with Third Party solutions used by the Client.	Integrating the switch with a product or service not directly supported by the manufacturer
Unmanaged Switch(es)	Any unmanaged switches
LAN cable drops	Local cabling issues between switch and endpoint
Unauthorized changes	Configuration changes made by 3rd parties, without consultation

4.3. CO-ITSM-WAP (as required)

4.3.1. Inclusions

CO-ITSM-WAP	
Scope Item	**Description**
Wireless Access Point (WAP) services	SSID profile configuration, POE Injector, Radio/Channel configuration, Radius integration, bandwidth profiles
Wireless performance optimization	QoS (Quality of Service) policies, Multicast
Firmware Updates	Installation of latest Access Point OS and firmware updates
Troubleshooting	Investigation and remediation of abnormal or unwanted Access Point behaviour
Logging	Access Point logging (when supported by controller/SNMP)

4.3.2. Exclusions

CO-ITSM-WAP	
Exclusion Item	**Description**
Out of support Access Points	Any Access Point that has passed its end-of-life date or manufacturer support contract has expired
Integration of switch(es) covered by the Service with Third Party solutions used by the Client.	Integrating the Access Point with a product or service not directly supported by the manufacturer
Unmanaged Access Points	Any unmanaged Access Points (e.g., retail WAPs, Mesh)
End user mobile/tablet	Wifi troubleshooting and remediation of end user devices (unless widespread issue)
LAN cable drops	Local cabling issues between switch and Access Point
3rd party troubleshooting	Troubleshooting end user devices with manufacturer/Telecommunications provider
Unauthorized changes	Configuration changes made by 3rd parties, without consultation

4.4. CO-ITSM-WAP (as required)

4.4.1. Inclusions

CO-ITSM-WAP	
Scope Item	**Description**

Wireless Access Point (WAP) services	SSID profile configuration, POE Injector, Radio/Channel configuration, Radius integration, bandwidth profiles
Wireless performance optimization	QoS (Quality of Service) policies, Multicast
Firmware Updates	Installation of latest Access Point OS and firmware updates
Troubleshooting	Investigation and remediation of abnormal or unwanted Access Point behaviour
Logging	Access Point logging (when supported by controller/SNMP)

4.4.2. Exclusions

CO-ITSM-WAP	
Exclusion Item	**Description**
Out of support Access Points	Any Access Point that has passed its end-of-life date or manufacturer support contract has expired
Integration of switch(es) covered by the Service with Third Party solutions used by the Client.	Integrating the Access Point with a product or service not directly supported by the manufacturer
Unmanaged Access Points	Any unmanaged Access Points (e.g., retail WAPs, Mesh)
End user mobile/tablet	Wifi troubleshooting and remediation of end user devices (unless widespread issue)
LAN cable drops	Local cabling issues between switch and Access Point
3rd party troubleshooting	Troubleshooting end user devices with manufacturer/Telecommunications provider
Unauthorized changes	Configuration changes made by 3rd parties, without consultation

4.5. CO-ITSM-UPS (as required)

4.5.1. Inclusions

CO-ITSM-UPS	
Scope Item	**Description**
Configuration review	Reporting on sizing, scale, and suitability: • Load Capacity – 80% VA or less for green status • Runtime – Meets minimum requirements for asset safe shutdown times. (To be assessed based on workload) Advisory on suitability, scalability, and redundancy. • Discussion on future workloads and load balancing. Discussion on results of Reporting (above)
Monitoring	Monitored UPS device in Datto / email. Alerts configured within limitations of manufacturer's control software.
Preventative maintenance	Battery check: • Load • Battery Lifecycle • Available status reports by device Agreed scheduled maintenance, review of management software: Discussion on version upgrades, benefits, and impact.
Testing	Remote testing of UPS functionality.
Associated devices	Configuration and scheduled maintenance and monitoring of associated devices – e.g., additional network cards, automatic transfer switches, PDUs.

Software / Firmware Updates	Installation of current device management software and firmware updates.
Troubleshooting	Investigation and remediation of abnormal or unwanted behaviour.
Logging	Event logging.

4.5.2. Exclusions

CO-ITSM-UPS	
Exclusion Item	**Description**
Out of support appliance	Any appliance that has passed its end-of-life date or manufacturer support contract has expired.
Appliances deemed unsafe	Where the device is hard-wired but has not been installed by a Registered Electrical Contractor (REC) and certified as such. Where the device or associated peripherals does not have a current PAT test (EU/UK). Where the device or electrical environment shows signs of physical damage. Where environment containing UPS does not have adequate ventilation or cooling or does not have adequate fire suppression in place.
Client infrastructure changes	Where the client has made undocumented changes resulting in damage to or overloading of the appliance.
Rejected maintenance requests	Where updates defined as critical by Calligo have not been sanctioned by the client.
Electrical	Where a Registered Electrical Contractor (REC) cannot be provided on-site to ensure safe access, for aspects of preventative maintenance or to make repairs which Calligo staff would not be qualified to carry out.

4.6. CO-ITSM-SD

4.6.1. Inclusions

CO-ITSM-SD	
Scope Item	**Description**
Access to the Calligo ITSM platform	24/7 access to the Calligo ITSM platform that provides capabilities for clients to raise new support tickets and to access open or historic support tickets.
Telephone Support	Access to the Calligo Service Desk via the issued telephone contact numbers during regional Business Hours only.
First Line Fix	Access to the Calligo L1 Service Desk Analysts for first line fix or resolution.

4.6.2. Exclusions

CO-ITSM-SD	
Exclusion Item	**Description**
24/7 Telephone Support	This is a chargeable addition.
Onsite support	All support delivered via the Service Desk offering is remote.

5. Roles and Responsibilities

The table below provides a responsibility matrix for the core Managed Network Device elements:

Service Activities – Core Elements	**Calligo**	**Customer**

CO-ITSM-PFWL (as required)		
Firewall management (policies, networking, security services)	R, A	C, I
Policy definitions (permitted/denied network access)	R, C, I	R, A
Remote VPN access	R, A	R, A
Firmware updates	R, A	C, I
CO-ITSM-PSW (as required)		
Switch management (policies, LAN networking)	R, A	C, I
Inter-VLAN routing definitions (rules), LAG, DHCP	R, C, I	R, A
Remote Access to switch	R, A	R, A
Firmware updates	R, A	C, I
CO-ITSM-WAP (as required)		
WAP management (QoS policies, SSID management RADIUS)	R, A	C, I
Remote Troubleshooting WAP/Wi-Fi performance issues	R, A	R, C, A
Remote Access to WAP/Controller	R, A	R, A
Firmware updates	R, A	C, I
CO-ITSM-UPS (as required)		
UPS management (software)	R, A	C
Monitoring Policies	R, A	I
Visual checks	R, A	R, A
Environmental management	C, I	R, A
On-prem preventative maintenance	R, A	I
System testing	R, A	I
Firmware updates	R, A	C, I
CO-ITSM-UPS (as required) - Client with Register Electrical Contractor onsite		
UPS management (software)	R, A	
Monitoring Policies	R, A	C
Visual checks	R, A	I
Environmental management	C, I	R, A, C
On-prem preventative maintenance	R, A	R, C
System testing	R, A	R, C
Firmware updates	R, A	
CO-ITSM-SD		
Raising support requests	R	R, A
Contacting Calligo Service Desk via telephone for P1 Support Requests	I	R, A
Correctly assigned the right category and priority to all incoming support requests	R, A	C, I
Providing full and detailed information when creating new support requests	I	R, A
Providing detailed and regular ticket updates	R, A	I
Responding to all ticket updates where additional information or testing is requested from Calligo Service Desk	I	R, A
Providing prompt confirmation of ticket closure agreements.	I	R, A

R=Responsible, A=Accountable, C=Consulted, I=Informed

6. Reporting

The table below provides details on the additional Monthly Reporting and Analytics for Managed Network Device that are included in the core service:

Service Item	Reporting Item	Description	Frequency
CO-ITSM-PFWL	Executive Summary	Summary report of blocked sites/attacks/categories, top endpoints, etc.	1/month as requested
CO-ITSM-PFWL	Per-client	Summary of device activity	1/month as requested
CO-ITSM-PFWL	Web	Activity, most popular domains, and categories	1/month as requested
CO-ITSM-PFWL	Services	Summary report of UTM feature activity	1/month as requested
CO-ITSM-PFWL	Detailed Services	Detailed report of UTM feature activity	1/month as requested
CO-ITSM-PFWL	Device	Firewall health and activity summary	1/month as requested
CO-ITSM-PSW	Switch Health and Performance	Report confirming health and performance of the switch.	Based on schedule of service management reporting
CO-ITSM-PSW	Switch Firmware/Software recommendations	Notification/recommendations for new switch software/firmware	Based on schedule of service management reporting
CO-ITSM-WAP	WAP Health and Performance	Report confirming health and performance of the WAP (if supported by controller).	Based on schedule of service management reporting
CO-ITSM-WAP	WAP Firmware/Software recommendations	Notification/recommendations for new switch software/firmware	Based on schedule of service management reporting
CO-ITSM-UPS	Executive Summary	Summary report	1/quarter as requested
CO-ITSM-UPS	Per-client	Summary of device activity	1/quarter as requested
CO-ITSM-UPS	Services	Summary report of feature activity	1/quarter as requested
CO-ITSM-UPS	Detailed Services	Detailed report of feature activity	1/quarter as requested
CO-ITSM-UPS	Device	Device health and activity summary	1/quarter as requested

7. Data Residency

Calligo Data Residency

8. Service Requirements

Service Item	Requirements Item
CO-ITSM-PFWL	Access to admin / support credentials for supported asset. Secure remote access to the firewall to manage the appliance. Access to physical asset location.
CO-ITSM-PSW	Asset under management must be within the current product support lifecycle and be eligible for required patching / updates / revisions. Any SFP/+ modules/DAC cables must be vendor certified. Logging and reporting may require a separate log server
CO-ITSM-WAP	Asset under management must be within the current product support lifecycle and be eligible for required patching / updates / revisions. WAP Controller under management must be within the current product support lifecycle and be eligible for required patching / updates / revisions. On-site technical resource to assist with testing/troubleshooting. Logging and reporting may require a separate log server Dependent on Managed Firewall/Physical Switch Service
Co-ITSM-UPS	A Registered Electrical Contractor (REC) must be nominated by the Client. Asset under management must be within the current product support lifecycle and be eligible for required patching / updates / revisions. Some UPS features require additional license subscription. Logging and reporting may require a separate log server.
CO-ITSM-SD	Client is provided information on support access methods

CO-ITSM-SD	All Priority 1 incidents are logged, and the client must follow up with a telephone call into support.

9. Access Requirements

Requirements Item
Access to admin / support credentials for supported asset. Secure remote access to the firewall or switch or WAP to manage the appliances.
Access to physical asset location.
Administrative access to all assets in scope as required for remediation actions
Assistance of a Registered Electrical Contractor (REC) whilst on-site.

10. Support Locations

Calligo Support Locations

11. Service Catalogue Request Items

Catalogue Item	Fulfilment Time	Qualifying Criteria	Included Requests
New firewall policy	24BHR	Add a policy to the firewall. Source and destination address(es) and port(s), and action (allow or deny)	1/week
Amend existing policy	24BHR	Existing policy name or description, source, and destination address(es) and port(s) to amend	1/week
Configure UTM features	24BHR	Enable and configure an available UTM feature	1/week
Amend UTM feature	24BHR	Adjust thresholds, exempt or deny source/destination addresses, modify actions of UTM features	1/week
Configure WAN	24BHR	Add new WAN interface or configure existing, adjust SD-WAN thresholds, configure failover/multi-WAN	1/month
Site-to-site VPN	24BHR	Configure VPN gateway and tunnel between two or more sites	1/month
Client VPN	24BHR	Configure secure VPN server for client connectivity	1/month
DHCP Server configuration	24BHR	Configure the firewall as a DHCP server for a LAN segment	1/month
DNS Server configuration	24BHR	Configure the firewall as a DNS responder and forwarder	1/month
VLAN configuration	24BHR	Configure VLAN ID on the firewall	1/month
NTP configuration	24BHR	Configure the firewall as a trusted time source	1/month
Traffic shaping	24BHR	Define QoS and bandwidth policies to prioritize and optimize network utilization	1/week
Firewall Update	24BHR	Install the latest available firmware and OS updates	1/month
Malfunction	24BHR	Investigate and remediate a device crash or malfunction	1/week
Monitoring Report	24BHR	Report of network activity	1/month
New Switch Configuration (Remote)	24BHR	Configure a new switch for a LAN segment	1/month
New Inter-VLAN Routing Configuration	24BHR	Setup new Inter-VLAN routing/rules/rules on a supported switch	1/month
Update Inter-VLAN Routing	24BHR	Amend existing Inter-VLAN routing on a supported switch	1/month

Catalogue Item	Fulfilment Time	Qualifying Criteria	Included Requests
VLAN Configuration	24BHR	Configure/Update VLANs	1/month
Configure Spanning Tree	24BHR	Configure/update Spanning Tree configuration	1/month
Configure LAG	24BHR	Configure/update port ling aggregation	1/month
Switch Firmware/Software Update	24BHR	Install the latest firmware/software	1/month
DHCP Server Configuration	24BHR	Configure the switch a DHCP server for a LAN segment	1/month
Replacement WAP Configuration (Remote)	24BHR	Configure a replacement WAP	1/month
New SSID Profile	24BHR	New SSID profile configuration	4/year
Update SSID Profile	24BHR	Update existing SSID Profile	1/month
Update RADIUS Configuration	24BHR	Update existing RADIUS configuration	1/month
Update Wireless Performance (QoS, Bandwidth profiles)	24BHR	Configure/update Spanning Tree configuration	1/month
WAP Firmware/Software Update	24BHR	Install the latest firmware/software	4/year
New UPS monitoring policy	24BHR	Add a policy to Datto. Configure or amend reporting.	1/month
Amend existing policy	24BHR	Change policy in Datto. Configure or amend reporting.	1/month
Configure or amend UPS Management software	24BHR	Enable and configure an available feature	1/month
Monitoring Report	24BHR	Report of monitoring activity	1/quarter
Visual check	24BHR	For warning lights, alarms etc	2/year
Environmental check	24BHR	For excess heat, loose connections etc	2/year
Operational test	24BHR	Checklist agreed in advance with client, carried out in conjunction with REC	1/year
Firmware Update	24BHR	Install the latest available firmware	1/quarter
Software Update	24BHR	Install the latest available software.	1/quarter
Malfunction	24BHR	Investigate and remediate a device crash or malfunction	1/week

12. Standard SLO's

Service-Level-Agreement.pdf (calligo.io)

13. Related Documents

Supporting documents for this service:

Any clients onboarding to Calligo will require the following document as an introduction to service.

Calligo – Welcome to Support for Clients

14. Optional Services

In addition to the Managed Network Device service, Calligo can provide the following service items as optional add on services for Managed Network Device:

Service Item	Service Item Reference	Description
Licensing	CO-SW-LICENCE	Licencing services
Cloud Protect Email Hygiene	CO-CP-EH	Email Hygiene services
Cloud Protect Web Filtering (Firewall)	CO-CP-WFF	Firewall web filtering
Onsite Support	CO-ITSM-ONSITE	Onsite support requirements
Service Delivery Manager	CO-ITSM-SDM	The Service Delivery Manager will be responsible for the business as usual and account management relationship. This will include service reviews, point of escalation, responsible for Information Technology Infrastructure Library (ITIL) practice adherence, interfacing with third-party suppliers also participating under the customer's Service Integration and Management model and ensuring that Calligo meets or exceeds Service Level Objective (SLO) targets.
Technical Account Manager	CO-ITSM-TAM	The Technical Account Manager will be responsible for the technical collaboration between the customer and Calligo support teams and will play a key role in technical service improvement, managing deployment of new services or configuration changes, ensuring optimal performance and uptime of the application stack, and interfacing with third-party suppliers as required under the customer's support model.

15. Auxiliary Services

15.1. Service Onboarding & Transition

To launch Managed Network Device service successfully, service design, onboarding and transition will be required to prepare and test both the environment and the managed services processes. Calligo will undertake several workshops to discuss and confirm each element of the service to ensure all parties are aware of roles and responsibilities in advance of service launch.

Service transition and onboarding covers areas such as ticket management setup, platform readiness with knowledge share, and finalising all ITIL practices. A test and acceptance criteria are captured and signed off, to allow for the Managed Network Device service to commence.

After service launch, Calligo uses a formal service transition framework as the basis to carry out acceptance into service procedures, for new services landing into managed services. We typically engage at the initial stages of a project to ensure service operation adoption and readiness is planned and carried out correctly. This materializes as follows:

- To review designs, build and test artefacts to ensure supportability.
- Attend change review boards to gain early sight of changes by way of knowledge acquisition.
- To witness and validate designs and builds are delivered as proposed and intended.
- Complete operational into service documentation, training, and runbook enablement, which is required as part of the service hand-over.

15.2. Change Request and Change Control Process:

All infrastructure changes introducing risk to the environment will require change control which includes, but not limited to, Microsoft Security Patching, Infrastructure Upgrades, Deployments, Configuration Item status change. This can be generated from maintenance or an event such as an upgrade required on the system released by Third Party vendors, requested by the customer, or from a monthly release of security patches.

Where possible Standard Changes will be used with minimal risk, repeatable implementation steps, and prior approval from the customer in the form of an email.

An Emergency, or unplanned, change process will be raised to resolve a Priority 1 or 2 incident or to implement an emergency Security Patch. This accelerates the time to implement and resolve.

All Requests for Change will be reviewed internally, assessed internally, and authorized or rejected through Calligo ITSM tool.