



Service Specification

Cisco SD WAN with SASE Managed Service



Contents

Table of Contents

Definitions	3
Overview	3
Service Hours	4
Standard Service Packages	4
Responsibilities	5
Service / Change Request Management	8
Service Request Points Entitlement Overview	8
Service Reporting	9
Customer Responsibilities	9
Dependencies	10
Exclusions	10
Service Request	11
Service Types	12

Definitions

The following expressions will have the following meanings unless inconsistent with the context:

SD-WAN	Software Defined – Wide Area Network
WAN	Wide Area Network
DIA	Direct Internet Access
MPLS	Multiprotocol Label Switching A routing technique that directs data from one node to the next based on short path labels
Broadband	A wide bandwidth data transmission method which uses a wide range of frequencies and Internet traffic types, used in fast internet connections
Underlay	The transport layer that the SD-WAN utilises. This includes MPLS, Internet (DIA), Broadband and 4G mobile data.
Cisco Meraki	Definition to be added
Cisco Catalyst SD-WAN	Cisco SD-WAN product that was previously called Viptella.
SASE	Secure Access Service Edge

Overview

A Software-defined Wide Area Network (SD-WAN) is a virtual WAN architecture that works through a centralized platform, detaching the management of the network from the hardware itself which allows customers to leverage any combination of underlying transport services – including DIA, MPLS, LTE and broadband internet services, to securely connect users to applications. SD WAN enables a secure local Internet breakout of IaaS and SaaS application traffic from a customer location providing the highest levels of management and performance while protecting the customer's estate from security threats.

The Cisco SD-WAN service uses a vendor provided centralized control function, either the Cloud based Cisco Meraki management portal, a hosted implementation of Cisco vManage or Cisco Cloud hosted vManage stack to securely and intelligently direct traffic across a Customers Circuit underlay.

The SCC Cisco SD-WAN Managed Service offers a set of standardized support services to the range of Cisco Meraki MX and Z3 devices as well as Catalyst SD-WAN (formerly Viptella) networking appliances. The service utilises the unique capabilities of Cisco Meraki Cloud delivered or vManage network management underpinned by SCC's Cisco certified managed service resources. This will provide Cloud provisioning into a customer tenancy, incident management, service requests, change management, regular firmware and feature upgrades, network visibility and pro-active remote troubleshooting to deployments of any size.

SD-WAN enables a convergence of security and network connectivity technologies for business enterprise users, Secure Access Service Edge (SASE) is a security framework supporting this convergence of networking and network security to meet the challenges of digital business

transformation, edge computing, and workforce mobility. SASE is a standard component included as part of the SCC Cisco SD-WAN managed service.

The standard technologies covered under this Service are as follows:

- Cloud Managed SD-WAN (Cisco Meraki) or vManage (Cisco Catalyst SD-WAN, formerly Viptella)
- Hosted vManage (Cisco Catalyst SD-WAN, formerly Viptella)
- Managed SASE services (Cisco Umbrella)

Service Hours

24 x 7 x 365

P1 resolution 24x7

Standard Service Packages

The table below is for information purposes only and equipment, connectivity and licensing are not part of the deliverables under this Service Description.

Feature	Use Cases				
	Teleworker / Kiosk	Small Office	Medium / Low Office	Medium / High Office	Head Office / Data Centre
Device Throughput	Up to 50Mbps	Up to 300Mbps	Up to 500Mbps	Up to 800Mbps	Up to 1Gbps
Client and Site to Site VPN	Up to 2	Up to 50	Up to 75	Up to 500	Up to 1000
Primary Connectivity	Internet	Internet	Internet	Internet	Dual Internet
Secondary Connectivity ¹	LTE	Internet or LTE	Internet	Internet	Dual Internet
Number of users/devices per location	Up to 2	Up to 50 Users	Up to 200 Users	Up to 500 Users	Up to 2000 Users
Components	Meraki Z4 Inbuilt WIFI or C8000V	Meraki MX68CW or Catalyst C8200L	Meraki MX85 or Catalyst C8200L	Meraki MX105 or Catalyst C8300	2 x Meraki MX250 (HA Pair) ² or Catalyst C8500
Options	LTE (4G)	HA device/dual connectivity	HA device/dual connectivity	HA device/dual connectivity	
License Level (Network Wide) ³	Advantage Enterprise features + On-Prem UTM and Umbrella Integration				
Umbrella Package	DNS Essentials DNS Layer Security				

¹ Where HA devices / Dual connectivity is taken, Secondary Connectivity is optional

² In Dual DC deployment, can run across Data Centres if required

³ Only Enterprise License is available for Z4; this does NOT preclude using Advanced Security for rest of network

Responsibilities

The following table defines the responsibilities of SCC within the scope of this Service. Please note certain Customer Responsibilities identified within this Service description may be superseded either in part or entirely by SCC as part of other SCC Services that the Customer has contracted for under this Agreement.

Feature	SCC Activities
SD-WAN Support & Administration	SCC will Identify and resolve Incidents relating to the pre-agreed scope of SD-WAN Managed infrastructure as detailed in the Customers contract technical specification.
	SCC will implement software and firmware updates for the managed Cisco Meraki MX appliances or Cisco Catalyst Routers where required for Incident Resolution.
	SCC is responsible for remote deployment and configuration of any agents or tools required for this Service within the Customer's environment.
	For service impacting faults that are identified as a P1 by the SCC Operations team, perform out of hours resolution.
	Where SCC determine it is appropriate as part of Incident Resolution apply any appropriate software, firmware patches or configuration restores for Service restoration.
	If a critical error cannot be resolved by SCC using the normal support tools and processes, the problem may require escalation to Cisco. SCC will manage the escalation and resulting outcome.
Underlay circuit support	SCC will monitor the WAN interface of the Cisco Meraki MX or Catalyst SD-WAN Router Equipment for availability. In the event of any changes of state to the interface an alert will be generated and investigated.
	SCC will investigate and triage alerts reporting an issue with an Underlay circuit used by the managed Cisco SD-WAN
	Log an incident with the third-party circuit provider to investigate and resolve. Regularly check with the third-party circuit provider the resolution status of the incident.
Event and Alert Management	Proactive device monitoring of the Cisco Meraki hardware under the scope of this Service via the Meraki Dashboard or Catalyst SD-WAN router via vManage Router
	Notify the Customer when allocated capacity is approaching limits and there is a risk of service performance degradation.
	Take action to investigate and remediate a reported degradation of Cisco SD-WAN performance beyond agreed Customer thresholds.
	Make proactive recommendations to prevent possible service degradation of the Cisco SD-WAN performance beyond agreed

	Customer thresholds.
	Action changes to monitoring thresholds or alerts raised as a Service Request.
Capacity and Availability Reporting	Ensure the customer's read only access to the Cisco Meraki reporting dashboard or vManage Console access is maintained.
	As part of the Service reporting package provide availability, performance, uptime, and capacity reporting for the managed Cisco SD-WAN infrastructure as detailed in the Customers contract technical specification.
	Provide a high-level overview of total traffic across all devices monitored and managed as part of the Cisco SD-WAN Service as detailed in the Customers contract technical specification over an agreed period.
License management	Report quarterly on the licensing status of the Cisco SD-WAN and compliance within the management portal. Where Cisco Meraki or Catalyst SD-WAN DNA licenses are included as part of the Service Charges, SCC will maintain license compliance for the term of the Order. When the Customer is responsible for the procurement of Cisco Meraki or Catalyst SD-WAN DNA licenses SCC will report license term end dates to the Customer 60 days before they expire.
Portal	SCC will manage the Customer's read only default view of their managed SD WAN infrastructure through the Cisco Meraki Enterprise or vManage portal for up to three (3) user accounts.
SD-WAN & traffic shaping	SCC will manage Customer requested updates or changes to the SD WAN infrastructure in scope of the managed service. This includes and is limited to the following features: • SD-WAN policies • Traffic shaping rules • Flow preferences • WAN traffic load balancing Where applicable updates will be applied on a per application basis.
On Device Security	SCC will manage Customer requested updates or changes to the SASE functionality in scope of the managed service. This includes and is limited to the following On-Box security features: • Enterprise Firewall • IDS/IPS • Content Filtering (Cisco Meraki specific categories) • Advanced Malware Protection (AMP) For Catalyst SD-WAN, we will include all relevant features available as part of the solution or additional Cisco technologies required to provide the right posture and design as required. Note that any additional features will be charged for accordingly
Device software update	A bi-annual assessment is performed of the software and firmware version to ensure full system stability is maintained of the managed Cisco SD-WAN, SCC may recommend that the latest stable Operating System or feature updates be applied to all managed Cisco devices specified in the Technical Specification. The recommended updates for each bi-annual assessment will be

	applied on no more than three separate dates / times of the Customer's choosing over a three-week period. These updates will be managed by SCC in accordance with the Customers Change management processes. Where a customer requires a different patching schedule to be implemented, i.e. within a certain amount of time of release of a patch from the equipment manufacturer, this will incur an additional supplementary service charge for each affected Cisco device. Supported Equipment that fails after an upgrade will be resolved in accordance with the terms of the Equipment Maintenance Service.
Active Directory	For those Customers with integration configured between their Active Directory installation and the SCC managed Cisco Meraki or vManage management portal, SCC will support the trouble shooting of Active Directory authentication issue in relation to those accounts only.
SASE Support and Administration	Manage Customer web filtering by domain or category using the SD-WAN service.
Cisco Catalyst SD-WAN vManage platform (Client Hosted)	If required SCC will perform mandatory software upgrades to ensure system stability, security and compatibility with the SCC monitoring and management platforms. A bi-annual assessment is performed on the vManage software version to ensure full system security and stability is maintained; SCC may recommend that the latest stable firmware upgrades be applied to the Cisco Catalyst SD-WAN vManage appliance(s) specified in the Technical Specification. Any update will have to be compatible with the firmware release running on the SD-WAN Catalyst routers. The update will be managed by SCC in accordance with the Customers Change management processes.
	Manage and maintain DNS control policies such as block domains with malware, phishing, botnet, or other high-risk items in line with the Customers security policy.
	Where Incidents cannot be resolved by SCC raise and manage an Incident with the software vendor
	Manage and maintain DNS Layer Security procedures and policies in accordance with the Customer's security policy.
	Manage and maintain customised block pages and bypass options in accordance with the customer's security policy.
	Manage the Proxy and inspect web traffic (incl. decryption of SSL (HTTPS) traffic) and the SSL certificate for SSL encryption. ⁴
	Release blocked files and content identified by the Umbrella AV Engine and malware defence, at the Customers request.
SASE Service Reporting	As part of the monthly service reporting SCC will provide an agreed set of compliance reports by either network or device which will include: • Security overview (totals) • Security activity (detail of activities undertaken)

	Application discovery (DNS score by application) and Top threats (mitigated).
Cisco Umbrella licensing	SCC will manage the Service security application user license compliance. It is the Customers responsibility to report to SCC any changes in SD-WAN user numbers across the managed infrastructure that may impact compliance.
Configuration Change Requests	All policy and template configuration changes to SD WAN or SASE service may be requested through the Service Desk. Design changes or changes that require architectural assistance are required to be raised as projects due to risk and effort and will be subject to additional Charges.

Notes

⁴Feature not available as part of standard Umbrella service provided. Available if DNS Advantage or SiG Essentials editions purchased.

Service / Change Request Management

Detail on how to make requests is provided in your Operations Manual.

Requests specific to this Service, include, but are not limited to the following, and should be logged as a Service Request through the SCC Service Desk:

- Additional reporting, and
- All Service Request Catalogue items.

If you require any changes or additions to any of the above, your requests will be reviewed by us and confirmed with you. Following agreement by both Parties, we will implement all configuration changes agreed upon with you via the Change Request procedure. If the changes required are deemed to be significant changes to the Service or require a professional services engagement due to your bespoke or detailed requirements, additional Charges will be discussed with you before any change is implemented and applied at our prevailing rates or as otherwise agreed with you in your applicable Service Request.

Within the SCC Vision Services Hub Portal, you can view:

- 24/7 any requests you raise and their detail;
- the list of possible Service Requests ("Service Request Catalogue"); and
- Your available and consumed Service Request Points.

Complex Design changes that require architectural assistance or changes which fall outside the scope of Service Description will be raised as projects due to risk and effort required to implement. These requests will be assessed and if implemented will be charged in addition to the charges for this Service.

Complex design changes include but are not limited to:

- Redesign of the SD-WAN service network architecture
- Adding a new hub site and configuring routing policies

- Integrating of the SD-WAN Service with a new Public Cloud site
- Integration of the SD-WAN Service with a new Data centre

Less complex changes, small works requests will be assessed and if implemented will be charged in addition to the charges for this Service.

- Installing a new site on to the SD-WAN
- Decommission an SD-WAN site.

Service Request Points Entitlement Overview

A Customer accrues Service Request points based on their total managed services spend, excluding Public Cloud and one-off charges.

For every £1000 of spend this entitles the customer to 5 points per month of Service Request spend.

New points are allocated from the service commencement date and reset every 30 days thereafter until the end of the contract term. If any of the monthly points entitlement is not used during each 30-day cycle, the remain balanced is wiped and will not be carried over.

In the event that the monthly balance of Service Request points is fully consumed, and the Customer requires further changes to be made before the next 30-day allocation of points an On-Demand change will have to be raised which is charged at the prevailing hourly rate published on the SCC Services Portal, Vision.

Service Reporting

SCC will provide any reporting included as part of the Service within 2 weeks of the end of the relevant reporting period, where this falls on a non-Working Day then the required reports will be provided by the next Working Day.

Report Type	Frequency
Monitoring Reports	Monthly
Capacity & Availability Reports	Monthly / Ad hoc

Customer Responsibilities

- The Customer is responsible for ensuring End Users raise Service Requests and Incidents to SCC's Service desk in accordance with the processes detailed in that Service Description
- For the management of encrypted proxy traffic, the Customer shall provide an up-to-date SSL certificate with a term period of at least one year, when requested by SCC⁵
- Installation and configuration of Umbrella client software on equipment not managed by SCC.
- Where the Meraki Dashboard is not managed via SCC's MSP portal, the Customer must provide unrestricted access to their Meraki dashboard to deliver this Service.
- Participation in change control process as required due to any actions arising as result of Event & Alert Management.

- A default threshold of 70% of capacity will be put in place unless specific measures, alerts and corresponding remedial actions are advised and provided by the Customer.
- Where changes to monitoring thresholds or alerts are required raise these through the Service Desk as a Service Request.
- Where the Service Underlay is not supplied by SCC, the Customer is required to provide details of where Client end of each circuit terminated (including postcode).
- Where the Service Underlay is not supplied by SCC, the Customer is responsible for configuring their end of each circuit and associated equipment forming the Underlay.
- Ensure that a Joiners/Leavers/Process is in place that makes use of an implemented RBAC model required to deliver Portal access to the Customer.
- Raise all changes to reports via the SCC Service Desk.
- Agree a schedule for service unavailability (maintenance windows) to allow critical maintenance to take place.
- Ensure the SD WAN Network device hosting locations and environment must meet the recommendations of the vendor for any remote locations not under SCC's control.
- Maintain and support the cabling infrastructure for any remote locations not under SCC's control.
- The Customer will inform SCC of any uplift in user numbers which may impact the licensing of this Service.

Notes

⁵ Only required if Web proxy edition of Cisco Umbrella used as part of the managed service

Dependencies

- Incident, Major Incident (required to support Enhanced service), Problem, Change Management and Hardware Maintenance services (unless Customer provided and managed)
- A physical Underlay is required either Customer provided service provision or an SCC Underlay service.
- All Customers who require access to Meraki Reporting Dashboards are required to provide a valid Customer domain e-mail address and have Multi Factor authentication enabled.

Exclusions

- The Customer acknowledges that Cisco is responsible for the availability and quality of service of the Meraki Cloud based components of this Service
- Support, Integration or Management of a Customer's Active Directory unless taken as part of another Service.
- Provision and Management of any Underlay, leased lines, network connectivity required for this Service to operate unless provided by SCC as part of another service
- Remediation activities by SCC, required because of degradation or failure of the Equipment or Hardware by parties other than SCC are excluded and shall be subject to additional Charges from SCC.

- Provision of Hardware required to operate this service

Service Request

The table below lists the inclusive Service Request types available as part of this service and there associated points consumption:

Category	Service Request	Points
General	Add/remove device or term licenses.	1
	Add/remove read only Administrator accounts.	1
Monitoring and reporting	Add/remove/modify alerts	1
	Change alert destination email address	1
	Configure Webhooks with Pre-defined alerts.	1
	Add/remove a device from the SCC monitoring service.	1
	Perform a device auto-discovery of the organisation.	3
Security (Meraki MX) – firewall / Catalyst SD-WAN router	Add/remove/modify the enablement and/or denial of relevant	3
	Add/remove/modify Firewall rules for applications through layer 3,4 and 7	3
	Add/remove/modify geo-IP based firewall rules (enabling source country rules)	3
	Add/remove/modify port forwarding rules	3
	Add/remove/modify 1:1 NAT forwarding rules	3
Security (Meraki MX) Catalyst SD-WAN router - Appliance Features	Addressing and VLANs	3
	Add/remove/modify traffic shaping	3
	DHCP	5
	Firewall policies	1
	Configure Auto VPNs	5
	Configure Site to Site VPNs	5
	Active Directory	3
	Configure SD-WAN hubs	5
	Threat Protection	5
	Access Control	3
	Add/remove/modify Splash page	5
	Wireless concentrator	5
Security – network and reporting	Run WAN optimisation report (Requires SD-WAN Plus License or Insight license)	3
Security – content and security filtering	Add/remove/modify content filtering (add and amend blocked website categories)	1
	Add/remove/modify URL whitelisting	1
	Add/remove/modify URL blacklisting	1
	Add/remove/modify HTTPS filtering	1
	Add/remove/modify assignment of device or user	1

	to an existing group policy	
	Add/remove/modify security filtering	3
	Add/remove/modify Advanced Malware Protection	3

Service Types

SCC can offer two service levels for SD-WAN customers:

Secure – standard secure service using accredited UK and near-shore capability for day-to-day management.

- Management control plane may be either dedicated or shared, depending on the requirement.
- Hosted within a UK SCC Data Centre or Customer's own hosting facility.

Secure Plus – secure plus offering, using only UK based, accredited and cleared resources (such as SC, NPPV3 and/or DV) in a shared or dedicated service model.

- Management control plane may be either dedicated or shared, depending on the requirement.
- Hosted within a UK SCC Data Centre or Customer's own UK hosting facility.

