Cisco Powered Services Portfolio

Requirements Document v9.2
February 2023

Contents

Introduction

This document outlines the requirements for Cisco Powered Services related to the Provider Role of the Cisco Partner Program. We recommend using this as a reference when preparing for Cisco Powered Service(s) audits.

The provider must have the following general capabilities to offer Cisco Powered service(s)

- Service provisioning
- Change management
- Proactive monitoring
- Remote troubleshooting
- Network Operations Center (NOC)
- Service-level agreement with the end customer

In addition, the Provider must also meet the requirements specified in this document for the relevant Cisco Powered Service(s).

Partner has the option to be audited against the previous audit document version up to 90-days after the latest audit document version is published.

Role sharing is allowed unless otherwise specified.

Note: Obtaining a Cisco Powered Service designation does not grant the Provider permission to purchase or deliver restricted products. Please refer to the territory-specific requirements, specified in the Provider's Cisco Partner Agreement, for the desired products. Examples of such requirements are Specialization, Enrollment, and Training requirements.

X1 Secure Access Services Edge (SASE)

Introduced: August 2021
Last updated: February 2023

Overview

Cisco Powered SASE gives Cisco partners the ability to deliver a rich, integrated set of cloud-based networking and security offers to end customers as a managed service. A Managed Service Provider can centrally operate its managed SASE service to address key customer needs via the following general use cases:

- Cisco Secure Cloud Edge
    - Streamline connectivity to apps across office locations
    - Provision SD-WAN fabric across thousands of users and locations
    - Secure access to apps and direct internet access
    - Identify and resolve issues across ISPs, SaaS, public and private apps
- Cisco Secure Remote Worker
    - Give remote workers secure access to applications and data, from anywhere
    - Secure access to internet and cloud hosted applications and private DC applications.
    - Authenticate users and ensure device health before establishing connection
    - Deliver the best connectivity and application experience for every remote worker and branch office

Partners may choose to achieve the Cisco Powered SASE designation by addressing the Secure Cloud Edge, Secure Remote Worker, or both use cases with their managed service offer. In doing so, they can monetize Cisco's broad portfolio of security products, streamline operations with a complete management system, and optimize financial (CapEx or OpEx) investments in the data center, on customer premises, and in the cloud, to provide the highest standard of networking and security for their customers.

The Cisco SASE portfolio includes the following Cisco products and solutions and outcomes:

- Umbrella Secure Internet Gateway (SIG)
    - Cloud RA and security functions (DNS, SWG, L4FW) delivering secure connectivity for cloud-based apps (IaaS, PaaS, SaaS)
- Duo MFA
    - Two factor authentication for access across all apps delivering layered zero-trust security to protect apps and endpoints
- Secure Client Connectivity (Anyconnect with roaming capability)
    - Client-based IPSec services providing access to always-on, outbound VPN's and access to private and external apps
    - Agent-based controls for DNS and Web (SWG) providing secure remote access to for SaaS and cloud apps

- SD-WAN

  SD-WAN and cloud delivered security services providing secure connectivity for users and application in the cloud, on-prem, or provided via SaaS.

  - Meraki SD-WAN (see Meraki SD-WAN section of this document for details):

    Meraki MX product family and associated licenses
  - Cisco SD-WAN (see Cisco SD-WAN section of this document for details):

    Catalyst 8000 product families

    ISR product families

    Industrial Routers and gateways

    Associated DNA licenses

Prerequisites

	Requirement	Evidence
X1.PR.1	**Customer References** • Reference customers must be under existing contractual relationships • One customer may serve as a reference to multiple Cisco Powered Services designations • One customer with multiple sites satisfies the requirement for a **single** reference, as the intent is to ensure that the Provider has proven and repeatable service practices • Two customer references are required only once: either with a new Cisco Powered Service application or upon first-year renewal • Use the Customer Reference Validation form to either submit references or to indicate references will be provided upon first year renewal	Customer Reference Validation Form uploaded into the Provider application
X1.PR.2	**Cisco Certifications** Cisco Certified individuals are responsible for designing and delivering modernized network solutions based on Cisco technologies. • Two individuals with a CCIE Enterprise Infrastructure or CCNP Enterprise certification The Provider must have a total of **two** individuals with either certification. And • Two individuals with a CCIE Security or CCNP Security certification. The Provider must have a total of **two** individuals with either certification. Two individuals with both certifications will also meet this requirement. For more information, visit Cisco Certifications.	Evidence of CCIE Enterprise Infrastructure **or** CCNP Enterprise certification for Individual 1
		Evidence of CCIE Enterprise Infrastructure **or** CCNP Enterprise certification for Individual 2
		Evidence of CCIE Security **or** CCNP Security certification for Individual 1
		Evidence of CCIE Security **or** CCNP Security certification for Individual 2

	Requirement	Evidence
X1.PR.3	**SD-WAN Designation (Required when selecting the Secure Cloud Edge use case)** SASE is described as a combination of SD-WAN and cloud delivered security. In order to achieve the SASE Cisco Powered Services designation, the Provider MUST have **one** of the SD-WAN designations: • Cisco SD-WAN (Viptela) • Meraki SD-WAN Providers may concurrently apply for and audit for **both** SASE and the SD-WAN designation of choice. If a Provider already holds an SD-WAN Cisco Powered Services designation, then the Provider may apply for the SASE designation without being required to repeat the audit for the SD-WAN Cisco Powered Services designation.	• Partner Locator will be used to confirm the Provider has achieved the Cisco Powered Services designation for either Cisco SD-WAN or Meraki SD-WAN • Provider will complete the audit process for **either** the Cisco SD-WAN or Meraki SD-WAN Cisco Powered designation, at the same time as the SASE audit
X1.PR.4	**Included Use Case(s)** Specify a minimum of **one** use case that your managed service supports • Secure Cloud Edge • Secure Remote Worker within the notes section of the Provider application when submitting, or email: certification-team@cisco.com	A minimum of one Use Case must be specified in the Provider application or emailed to certification-team@cisco.com
X1.PR.5	**Training Evidence** Upload evidence of completion for all Training required for this Cisco Powered Service.	Evidence of training must be uploaded into the Provider application. Refer to requirements in sections X1.SP.1 to X1.SP.4

Service Offer

	Requirement	Evidence
X1.SO.1	**Service Level Agreements** Service performance is committed through Service-Level Agreements (SLAs) between the Provider and End Customers, which are backed by processes to measure and report on whether those commitments are met. Service performance elements covered by the SLA may include: • Platform availability: infrastructure (e.g., CPE), orchestration and service interfaces • Network availability: the network operated by the Provider Partner that is used to provide connectivity from the Internet or private WAN, involved data centers, and/or a third party used to provide network connectivity • Mean Time to Notify (MTTN): MTTN measures the average time taken to notify a customer of an issue with the subscribed service. The measurement encompasses the time that an alert is generated to the time the customer is notified, which can be by any method of communication agreed upon with the customer • Mean Time to Restore Service (MTRS): MTRS measures the total elapsed time from the start of a resource outage to the time the service is restored. This is also known as Mean Time to Restore/Repair (MTTR). The turnaround time for implementing changes requested by the customer. Must be within 48 hours for standard changes. Access rules are used to define the network security policy; they control the traffic that flows through a firewall device. Access rules are recognized in the form of an ordered list. A firewall device processes rules from first to last. When a rule matches the network traffic that a firewall device is processing, the firewall device uses that rule's action to decide if traffic is permitted. Rules at the top of the list are therefore considered a higher priority. Priority rules must be changed within 4 hours.	One of: • Executed Service Level Agreement • Service Level Agreement template
X1.SO.2	**Security Operations Function** Security Operations are a centralized function, often referred to as a Security Operations Center (SOC), employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents. Partner must document the operation of a Security Operations Function for incident prevention, detection, and response capabilities. Partner can also use a 3rd party white label SOC provider. In this case, the sub-contracted SOC provider must participate in the audit.	Both of: • Documentation of security event detection, escalation, and remediation processes consistent with Provider's SLA • Documentation or demonstration of people, processes, and tools specific to the Security Operations Function

	Requirement	Evidence
X1.SO.3	**Service Requirements** Formal requirements help align the business on a definition of success. These documents, such as a Marketing Requirements Document (MRD) or a Product Requirements Document (PRD) ensure that the various stakeholders' requirements are cataloged and addressed, increasing the likelihood of market success dramatically. The Provider must show evidence of a MRD or PRD for this service. At a minimum, these documents should address: • Target customer segments and clearly defined use cases • Service packaging and pricing structure • Customer value proposition of the service	A table of contents or redacted version of one of • Marketing Requirements Document (MRD) • Product Requirements Document (PRD) of the service
X1.SO.4	**Service Description** The Service Description is an End-User facing document which explains the service features, benefits, and business outcomes to a potential customer. Typically, a Service Description would include an outline of the different tiers of service such as bronze, silver, or gold, and the features available at each tier.	Service Description document

Service Delivery

Managed SASE Use Case: Secure Cloud Edge

	Requirement	Evidence
X1.SD.1	**Service Architecture** The Provider must provide a Service Architecture document which describes the key technology components, how they are integrated, and how End-Users access the service. It should cover: • SD-WAN control-plane and data-plane based on Cisco or Meraki SDWAN technology • branch connectivity • access to cloud-security • egress to external (managed or unmanaged) cloud/SaaS services The Provider must provide an architecture design as evidence of this requirement. The Provider must also describe how the availability and health of the service is monitored.	• Cisco Powered Managed SD-WAN designation OR both of: • Service Architecture document • Description of how the availability and health of the service is monitored

	Requirement	Evidence
X1.SD.2	**Integrated Cloud Security** (Secure tunnel from SD-WAN service to cloud security service) Cisco SD-WAN and Meraki MX routers can support SD-WAN, routing, security, and other LAN access features that can be managed centrally. These routers can integrate with Cisco Umbrella Secure Internet Gateways (SIG) which does the majority of the processing to secure enterprise traffic for external traffic flows. When Cisco Umbrella SIG is enabled, all client traffic, based on routing or policy, is forwarded to Cisco Umbrella SIG. In addition, Cisco Umbrella SIG can also protect roaming users, mobile users, and BYOD use-cases. The outcome is the ability to connect and secure access to applications, data, and the internet for remote workers, fixed locations, any internet-facing devices, and workloads. The Provider must provide evidence that their managed SASE offer provides for manual or automated tunnelling to Cisco Umbrella SIG. The Provider must also describe how the availability and health of the service is monitored.	• Service Description document **and** One of: • Service Architecture document • Screenshots of tunnel configuration from the SD-WAN (Viptela or Meraki) and Umbrella user interfaces
X1.SD.3	**Secure DNS Protection** By enforcing security at the DNS and IP layers, Umbrella blocks requests to malicious and unwanted destinations before a connection is even established – stopping threats over any port or protocol before they reach your network or endpoints. DNS protection provides: • The visibility needed to protect internet access across all network devices, office locations, and roaming users • Detailed reporting for DNS activity by type of security threat or web content and the action taken • Ability to retain logs of all activity as necessary • Fast rollout to thousands of locations and users to provide immediate return on investment This level of protection is enough for some locations and users, yet others need additional visibility and control to meet compliance regulations and further reduce risk. The Provider must provide evidence that their managed SASE offer uses Cisco Umbrella for secure DNS protection services	• Service Description document **and** One of: • Service Architecture document • Screenshot of DNS or Domain policy settings from the Umbrella user interface

	Requirement	Evidence
X1.SD.4	**Secure Web Browsing** (Full web proxy with content filtering) Cisco Umbrella includes a cloud-based full web proxy that can log and inspect all of your web traffic for greater transparency, control, and protection. IPsec tunnels, PAC files and proxy chaining can be used to forward traffic for full visibility, URL and application-level controls, and advanced threat protection. The full proxy with web filtering provides: • Content filtering by category or specific URLs to block destinations that violate policies or compliance regulations • The ability to efficiently scan all uploaded and downloaded files for malware and other threats using the Cisco Secure Endpoint (formerly Cisco AMP) engine and third-party resources • Cisco Secure Malware Analytics (formerly Threat Grid) rapidly analyzes suspicious files (unlimited samples) • File type blocking (e.g., block download of .exe files) • Full or selective SSL decryption to further protect your organization from hidden attacks and time-consuming infections • Granular app controls to block specific user activities in select apps (e.g., file uploads to Dropbox, attachments to Gmail, post/shares on Facebook) • Detailed reporting with full URL addresses, network identity, allow or block actions, plus the external IP address The Provider must provide evidence that their managed SASE offer uses Cisco Umbrella for secure web browsing services.	• Service Description document **and** One of: • Screenshot of Web policy settings from the Umbrella user interface • SLA agreements • Activity Search Report
X1.SD.5	**Cloud Delivered Firewalling (L3/4)** The Umbrella cloud-delivered firewall provides visibility and control for traffic that originated from requests going to the internet, across all ports and protocols. Cloud firewall protection provides: • Deployment, management, and reporting through the Umbrella single, unified dashboard • Customizable policies (IP, port, protocol, application and IPS policies) • Layer 3/4 firewall to log all activity and block unwanted traffic using IP, port, and protocol rules • Intrusion prevention system (IPS)* to examine network traffic flows and prevent vulnerability exploits with an added layer of threat prevention using SNORT 3 technology and signature-based detection. • Detection and blocking of vulnerability exploitation • Scalable cloud compute resources eliminate appliance capacity concerns • Cisco Talos threat intelligence to detect and block more threats The Provider must provide evidence that their managed SASE offer uses Cisco Umbrella for L3/4 cloud delivered firewall services.	• Service Description document **and** One of: • Screenshot of Firewall policies from the Umbrella user interface • SLA agreements • Activity Search Report

	Requirement	Evidence
X1.SD.6	**Layer 7 Cloud Firewall (optional)** With layer 7 application visibility and control, Umbrella recognizes non-web applications and takes appropriate action to block/allow them. The cloud-delivered firewall employs signature detection to identify and block 2,800 applications (more added on a regular basis). This extends the application detection and blocking already performed with Umbrella's DNS-layer security and secure web gateway. The L7 cloud firewall provides the ability to: • Block shadow IT applications over non-Web ports to stop use of unapproved SaaS applications • Block insecure applications on non-standard ports • Block unsanctioned traffic over non-web ports The Provider must provide evidence that their managed SASE offer uses Cisco Umbrella for L7 cloud firewall services.	*Optional* • Service Description document **and** One of: • Firewall policy setting showing application rules from the Umbrella user interface • SLA agreements Activity Search report showing application details
X1.SD.7	**Multi Factor Authentication (optional)** Multi-factor authentication (MFA) is a layered approach to securing data and applications where a system requires a user to present a combination of two or more credentials to verify a user's identity for login. MFA increases security because even if one credential becomes compromised, unauthorized users will be unable to meet the second authentication requirement and will not be able to access the targeted physical space, computing device, network, or database. The added security offered by MFA can simplify the user login process by using single sign-on where practicable. A single sign-on system enables authenticated users access to an environment from which they can use multiple covered applications without needing to log in separately each time. The Provider must provide evidence that their managed SASE offer uses a suitable Duo package supporting MFA for multi-factor authentication services.	*Optional* • Service Description document **and** One of: • Screenshot of authentication policy showing Enforce 2FA enabled • SLA agreements Current 'Authentication Log' detailing 'second factor' information
X1.SD.8	**Support Service** A Provider Partner must act as single point of first line support for the service, covering all aspects of incident response for hardware and software. In the case of private cloud infrastructure that is based on both Cisco and 3rd party solutions, the partner must be the single point of contact of first line support and co-ordinate the support among solution providers.	One of: • Service Description document • Service Operation Guide/ Runbook
X1.SD.9	**Managed Service** A Provider partner must provide day 2 managed service to end customers for the service, to ensure infrastructure is up to date on firmware, latest OS, security patches, performance tune-up, proactive monitoring/alerting service with proper SLA defined.	One of: • Service Description document • Service Operation Guide/ Runbook

Service Delivery (continued)

Managed SASE Use Case: Secure Remote Worker

	Requirement	Evidence
X1.SD.10	**Remote Access Service** The partner must choose to support at least one of the below access models: User access to privately hosted applications (such as an existing local data center) and depending on the topology, SaaS and cloud applications externally hosted by the organization. • A traditional head-end based approach using: ◦ Cisco ASA, Cisco NGFW, or Meraki MX ◦ The Cisco Secure Client (Anyconnect) VPN software User access to SaaS and Cloud applications • Umbrella is integrated with the Cisco Secure Client with the Umbrella Roaming Security Module for AnyConnect. The Cisco Umbrella Roaming Security module provides always-on security on any network, anywhere, any time—both on and off your corporate VPN. The Roaming Security Agent enforces security at the DNS layer to block malware, phishing, and command and control callbacks over any port. The SWG Agent enforces security at the URL layer, to provide security and visibility for web traffic.	• Service Description document **and** One of: • SLA agreements • Architecture document denoting VPN head-end (for option 1) and cloud security elements
X1.SD.11	**Secure DNS Protection** By enforcing security at the DNS and IP layers, Umbrella blocks requests to malicious and unwanted destinations before a connection is even established – stopping threats over any port or protocol before they reach your network or endpoints. DNS protection provides: • The visibility needed to protect internet access across all network devices, office locations, and roaming users • Detailed reporting for DNS activity by type of security threat or web content and the action taken • Ability to retain logs of all activity as long as needed • Fast rollout to thousands of locations and users to provide immediate return on investment This level of protection is enough for some locations and users, yet others need additional visibility and control to meet compliance regulations and further reduce risk. The Provider must provide evidence that their managed SASE offer uses Cisco Umbrella for secure DNS protection services	• Service Description document **and** One of: • Service Architecture document • Screenshot of DNS or Domain policy settings from the Umbrella user interface

	Requirement	Evidence
X1.SD.12	**Secure Web Browsing** (Full web proxy with content filtering) Cisco Umbrella includes a cloud-based full web proxy that can log and inspect all of your web traffic for greater transparency, control, and protection. IPsec tunnels, PAC files and proxy chaining can be used to forward traffic for full visibility, URL and application-level controls, and advanced threat protection. The full proxy with web filtering provides: • Content filtering by category or specific URLs to block destinations that violate policies or compliance regulations • The ability to efficiently scan all uploaded and downloaded files for malware and other threats using the Cisco Secure Endpoint (formerly Cisco AMP) engine and third-party resources • Cisco Secure Malware Analytics (formerly Threat Grid) rapidly analyzes suspicious files (unlimited samples) • File type blocking (e.g., block download of .exe files) • Full or selective SSL decryption to further protect your organization from hidden attacks and time-consuming infections • Granular app controls to block specific user activities in select apps (e.g., file uploads to Dropbox, attachments to Gmail, post/shares on Facebook) • Detailed reporting with full URL addresses, network identity, allow or block actions, plus the external IP address The Provider must provide evidence that their managed SASE offer uses Cisco Umbrella for secure web browsing services.	• Service Description document **and** One of: • Screenshot of Web policy settings from the Umbrella user interface • SLA agreements • Activity Search Report
X1.SD.13	**Cloud Delivered Firewalling (L3/4)** The Umbrella cloud-delivered firewall provides visibility and control for traffic that originated from requests going to the internet, across all ports and protocols. Cloud firewall protection provides: • Deployment, management, and reporting through the Umbrella single, unified dashboard • Customizable policies (IP, port, protocol, application and IPS policies) • Layer 3/4 firewall to log all activity and block unwanted traffic using IP, port, and protocol rules • Intrusion prevention system (IPS)* to examine network traffic flows and prevent vulnerability exploits with an added layer of threat prevention using SNORT 3 technology and signature-based detection. • Detection and blocking of vulnerability exploitation • Scalable cloud compute resources eliminate appliance capacity concerns • Cisco Talos threat intelligence to detect and block more threats The Provider must provide evidence that their managed SASE offer uses Cisco Umbrella for L3/4 cloud delivered firewall services.	• Service Description document **and** One of: • Screenshot of Firewall policies from the Umbrella user interface • SLA agreements • Activity Search Report

	Requirement	Evidence
X1.SD.14	**Remote Access VPN Client** The Cisco Secure Client (Cisco AnyConnect) is a security endpoint solution that empowers remote workers with frictionless, highly secure access to the internet or the enterprise network from any device, at any time, in any location while protecting the organization. It also provides the visibility and the control you need to identify who, and which devices are accessing the extended enterprise. Cisco AnyConnect's wide range of security services include functions such remote access, posture enforcement, web security features, and roaming protection.	• Service Description document **and** One of: • Demonstration of remote access VPN using Cisco Secure Client • SLA agreements
X1.SD.15	**Off-network Protection – Roaming** A secure roaming services can be offered to extend Web and DNS protections for offnet, remote and hybrid workers. The Cisco Umbrella Roaming Security module provides always-on security on any network, anywhere, any time—both on and off your corporate VPN. When you install the Roaming Security module, it installs two services Cisco AnyConnect Umbrella Roaming Security Agent and Cisco AnyConnect Secure Web Gateway (SWG) Agent. The Roaming Security Agent enforces security at the DNS layer to block malware, phishing, and command and control callbacks over any port. The SWG Agent enforces security at the URL layer, to provide security and visibility for web traffic. However, while installed, the SWG Agent is only enabled for Umbrella Secure Internet Gateway (SIG) platform users, which is dependent on your current subscription package. The AnyConnect Roaming Security Agent can replace your existing Umbrella roaming client if you already have AnyConnect configured. The roaming module allows for full update control, and the Roaming Security Agent offers an option to disable automatically behind a full tunnel VPN connection. The Roaming Security Agent and offers an option to disable on a trusted network.	• Service Description document **and** One of: • Screenshot of, or sample "Identities Report", with "Identity Type" of "Roaming Computers" • SLA agreements
X1.SD.16	**Multi Factor Authentication (optional)** Multi-factor authentication (MFA) is a layered approach to securing data and applications where a system requires a user to present a combination of two or more credentials to verify a user's identity for login. MFA increases security because even if one credential becomes compromised, unauthorized users will be unable to meet the second authentication requirement and will not be able to access the targeted physical space, computing device, network, or database. The added security offered by MFA can simplify the user login process by using single sign-on where practicable. A single sign-on system enables authenticated users access to an environment from which they can use multiple covered applications without needing to log in separately each time. The Provider must provide evidence that their managed SASE offer uses a suitable Duo package supporting MFA for multi-factor authentication services.	• Service Description document **and** One of: • Screenshot of authentication policy showing Enforce 2FA enabled • SLA agreements • Current 'Authentication Log' detailing 'second factor' information"
X1.SD.17	**Support Service** A Provider partner must act as single point of first line support for the service, covering all aspects of incident response for hardware and software. In the case of private cloud infrastructure that is based on both Cisco and 3rd party solutions, the partner must be the single point of contact of first line support and co-ordinate the support among solution providers.	One of: • Service Description document • Service Operation Guide/ Runbook

	Requirement	Evidence
X1.SD.18	**Managed Service** A Provider partner must provide day 2 managed service to end customers for the service, to ensure infrastructure is up to date on firmware, latest OS, security patches, performance tune-up, proactive monitoring/alerting service with proper SLA defined.	One of: • Service Description document • Service Operation Guide/ Runbook

Service Marketing

	Description	Evidence
X1.SM.1	**Digital presence** Most buyers will complete their research online before engaging with the Provider's sales team. Online presence may include a web page, micro site, social media, podcast, and marketing events.	One of: • Demonstrate a service-specific online presence with service specific marketing content, • A marketing plan across various marketing channels and platform
X1.SM.2	**Align digital marketing to the buyer journey** Prospective customers complete the majority of purchasing decision research before engaging a Provider's sales contacts. It is a best practice to ensure that rich digital marketing content with clearly defined use cases is in place through the buyer's journey. This may include a micro web site, social media, podcasts, and interactive marketing events such as webinars.	Buyer Journey Map document

Sales Operations

	Description	Evidence
X1.SP.1	**SASE Sales Training** Stage 1 1. Complete **Stage 1** under **SASE Sales** This requirement waived for Provider partners that have achieved the Cisco SASE Solution Specialization	Evidence of completion for Sales Person 1 Evidence of completion for Sales Person 2
X1.SP.2	**SASE Pre-Sales Training** Stage 1 This requirement waived for Provider partners that have achieved the Cisco SASE Solution Specialization	Evidence of completion for Pre-Sales Engineer 1 Evidence of completion for Pre-Sales Engineer 2

	Description	Evidence
X1.SP.3	**SASE Pre-Sales Training** Stage 2 This requirement waived for Provider partners that have achieved the Cisco SASE Solution Specialization	Evidence of completion for Pre-Sales Engineer 1 Evidence of completion for Pre-Sales Engineer 2
X1.SP.4	**DUO Pre-Sales Engineering Training (Required only for optional Multi-factor Authentication)** Stage 2 1. Select **Visibility & Segmentation** 2. Complete the **Visibility & Segmentation – Duo – Quiz** This requirement waived for Provider partners that have achieved the Cisco SASE Solution Specialization	Evidence of completion for Pre-Sales Engineer 1 Evidence of completion for Pre-Sales Engineer 2
X1.SP.5	**Sales Training** Provider must have a process to formally train both sales representatives and sales engineers for the service	Sales Training Plan document
X1.SP.6	**Sales Enablement** Provider must provide evidence of an **End Customer-facing pitch deck** and at least two of the following sales enablement materials: • Services at-a-glance • Service brochure or video • Battle card/sales reference card • Sales playbook • Call script • Email template • Demo For examples, please reach out to your Cisco Partner Account Team	• End Customer-facing pitch deck and at least **two** of: • Services at-a-glance • Service brochure or video • Battle card/sales reference card • Sales playbook • Call script • Email template • Demo
X1.SP.7	**Sales Compensation policy** Provider must have a sales compensation policy that incentivizes and rewards the involved teams for selling the service.	Sales Compensation Policy document

Customer Success

	Requirement	Evidence
X1.CS.1	**Customer Success Practice** Customer Success is the function within a Provider organization responsible for managing the relationship between the Provider and its customers. The goals of Customer Success are to: • Maximize customer value • Increase service adoption • Ensure ease of use • Increase customer satisfaction • Drive service renewal For Evidence Option #2 (Customer Success Practice documentation): Provider must demonstrate processes and metrics that support each of the following elements of a customer success practice: • Customer on-boarding and service activation process • Service renewal process • Service renewal rate measurement • Dispute and escalation handling processes • Ongoing customer communications • Regular business review process to periodically assess business requirements and change management needs	One of: 1. Customer Success Practice documentation 2. Customer Experience or Advanced Customer Experience Specialization (no further evidence required if the Specialization is held)
X1.CS.2	**User Guide** A User Guide is a document provided to customers showing how to access the customer service portal for self-service capabilities which may include service activation, on-boarding, configuration, and reporting for the audited service.	User guide document
X1.CS.3	**Customer Ticketing System** A ticketing system should be in place for tracking customer change requests and system generated incidents. A ticketing system may be part of a larger IT Systems Manager (ITSM) or Customer Relationship Management (CRM) system. Reports from this system should include metrics and summaries of incidents including details such as quantity, status, average time to resolve past incidents, and how the incidents were resolved.	Demonstration of the Customer ticketing system

X2 Managed Full-Stack Observability (FSO)

Introduced: December 2022
Updated: February 2023

Overview

Cisco Powered Full-Stack Observability (FSO) is a platform that enables Cisco partners with a blueprint to evolve their Managed Services businesses from a predominantly infrastructure-based, event driven operation, to an observable data-driven user experience that correlates telemetry and provides valuable insights linked to business outcomes. A Managed Service Provider can leverage a managed FSO service to address key customer needs via the following general use cases:

Cisco Platforms	Hybrid Application Monitoring	Modern Application Monitoring	Customer Digital Experience Monitoring	Application Dependency Monitoring	Hybrid Cost Optimization	Application Resource Optimization	Application Security
AppDynamics	●		●			●	
AppDynamics Cloud		●					
Cisco Secure Application							●
ThousandEyes			●	●			
Intersight Workload Optimizer					●	●	

The Provider can monetize Cisco's broad portfolio of products, applications, and services to assure the highest standard of application, infrastructure, security, cloud managed services for its customers.

Note: For those partners that were following the ENAA (Enterprise Network Assurance and AIOps) optional requirement in section D1.SO.4 of "D1 Cisco SD-WAN" in CPS 9.1, please follow the "Application Dependency Monitoring" use case.

Training

Providers are required to build at minimum (1) Managed Full Stack Observability use-case to achieve Cisco Powered status. To successfully build a Managed Full Stack Observability service with one or more uses, specific training is required for at minimum (2) individuals on staff utilizing the matrix below. All evidence of completed training must be uploaded to the provider application which will be validated through a 3rd party audit process.

Required Use-Case Training	Managed Full Stack Observability Use-Cases						
	Hybrid Application Monitoring	Modern Application Monitoring	Customer Digital Experience Monitoring	Application Dependency Monitoring	Hybrid Cost Optimization	Application Resource Optimization	Application Security
Full Stack Observability Sales Stage 1 (link)	●	●	●	●	●	●	●
Full Stack Observability Pre-Sales Stage 1 (link)	●	●	●	●	●	●	●
Full Stack Observability Pre-Sales Stage 2 (link)	●	●	●	●	●	●	●
AppDynamics Performance Analyst (link)	▲	▲	●			▲	▲
AppDynamics Implementation (link)	▲	▲	●			▲	▲
AppDynamics Associate Administrator (link)	●	●	●			●	●
ThousandEyes Pre-Sales Stage 1 (link)			●	●			
ThousandEyes Pre-Sales Stage 2 (link)			●	●			
ThousandEyes Deployment Stage 1 (link)			●	●			
Intersight Pre-Sales Stage 1 (link)					●	●	
Intersight Pre-Sales Stage 2 (link)					●	●	

● Required training ▲ Required secondary training (see provided example below)

Example: If a Provider is applying for the Hybrid Application Monitoring use-case:

1) a minimum of two individuals must provide evidence of the Full-Stack Observability sales and pre-sales Black-Belt training and

2) a minimum of two individuals must provide evidence of the AppDynamics Associate Administrator Certification along with either the AppDynamics Performance Analyst Certification or the AppDynamics Implementation Certification.

Note: If a provider is applying for more than one use-case the same individuals may be used to meet the training qualifications of the additional use-cases.

Prerequisites

	Requirement	Evidence
X2.PR.1	**Customer References** • Reference customers must be under existing contractual relationships • One customer may serve as a reference to multiple Cisco Powered Service designations • One customer with multiple use cases satisfies the requirement for a single reference, as the intent is to ensure that the Provider has proven and repeatable service practices • Two customer references are required only once: either with a new Cisco Powered Service application or upon first-year renewal • Use the Customer Reference Validation form to either submit references or to indicate references will be provided upon first year renewal	Customer Reference Validation Form uploaded into the Provider application
X2.PR.4	**Managed Full Stack Observability Use-Cases** The provider must have a minimum of **one** use-case operationalized in market as a managed service and specified in the provider application: 1. Hybrid Application Monitoring 2. Modern Application Monitoring 3. Customer Digital Experience Monitoring 4. Application Dependency Monitoring (aka Network Observability) 5. Hybrid Cost Optimization 6. Application Resource Optimization 7. Application Security	A minimum of one use-case must be specified in the Provider application
X2.PR.9	**Training Evidence** • Upload evidence of completion for all Training required for this Cisco Powered Service.	Evidence of training must be uploaded into the Provider application. Refer to requirements in Training section above based on Use case.

Service Offer

	Requirement	Evidence
X2.SO.1	**Service Level Agreements** Service performance is committed through Service-Level Agreements (SLAs) between the Provider and End Customers, which are backed by processes to measure and report on whether those commitments are met. Service performance elements covered by the SLA may include: • Platform availability: ability for the applicable FSO Elements to process the required functions, orchestration, and service interfaces/integrations • Mean Time to Notify (MTTN): MTTN measures the average time taken to notify a customer of an issue with the subscribed service. The measurement encompasses the time that an alert is generated to the time the customer notified, which can be by any method of communication agreed upon with the customer • Mean Time to Restore Service (MTRS): MTRS measures the total elapsed time from the start of a resource outage to the time the service is restored. This is also known as Mean Time to Restore/Repair (MTTR). The turnaround time for implementing changes requested by the customer. Must be within 48 hours for standard changes.	• Evidence of Service-Level Agreements (SLAs) must be uploaded into the Provider application One of: • Executed Service Level Agreement • Service Level Agreement template
X2.SO.2	**Operations Function** Operations are a centralized function, often referred to as a Network Operations Center (NOC) or an Application Operations Center (AOC), employing people, processes, and technology to continuously monitor and improve the Partner's customer environment or application(s) while preventing, detecting, analyzing, and responding to incidents. Partner must document the operation of their NOC/AOC Function for incident prevention, detection, business relevancy and response capabilities.	*Waived for Gold Providers* Evidence of operations function documentation must be uploaded into the Provider application
X2.SO.3	**Service Requirements** The Provider must show evidence of a MRD or PRD for this service. At a minimum, these documents should address: • Target customer segment and clearly defined use cases • Service packaging and pricing structure • Customer value proposition of the service Formal requirements help align the business on a definition of success. These documents, such as a Marketing Requirements Document (MRD) or a Product Requirements Document (PRD) ensure that the various stakeholders' requirements are cataloged and addressed, increasing the likelihood of market success dramatically.	Evidence of service requirements documentation must be uploaded into the Provider application
X2.SO.4	**Service Description** The Service Description is an End-User facing document which explains the service features, benefits, and business outcomes to a potential customer. Typically, a Service Description would include an outline of the different tiers of service such as bronze, silver, or gold, and the features available at each tier.	Evidence of service delivery documentation must be uploaded into the Provider application

Service Delivery

	Requirement	Evidence
X2.SD.1	**Service Delivery Function** For use-case(s) specified in section X2.PR.4, the Provider must provide a Service Architecture document which describes the key technology components, how they are integrated, and how End-Users access the service. It should cover: • Cisco platform integrations with Provider tools • End-customer and Provider Access and security control/measures • Best practice for integrating to Provider end-customer environments (private/public) • Customer on-boarding process • Service Offering Matrix including offer packages (e.g., Small-Medium-Large) and tiers (e.g. good-better-best)	Evidence of service delivery must be uploaded into the Provider application. **Requirements:** • Service Architecture document • Description of how the availability and health of the service is monitored • Service Offering Matrix (standard scoping and tiering)

Customer Success

	Requirement	Evidence
X2.CS.1	**Customer Success Practice** Customer Success is the function within a Provider organization responsible for managing the relationship between the Provider and its customers. The goals of Customer Success are to • maximize customer value • increase service adoption • ensure ease of use • increase customer satisfaction • drive service renewal Provider must demonstrate processes and metrics that support each of the following elements of a customer success practice: • Customer on-boarding and service activation process • Service renewal process • Service renewal rate measurement • Dispute and escalation handling processes • Ongoing customer communications • Regular business review process to periodically assess business requirements and change management needs	*Waived for Gold Providers* Customer Success Practice Description document
X2.CS.2	**User Guide** A User Guide is a document provided to customers showing how to access the customer service portal for self-service capabilities which may include service activation, on-boarding, configuration and reporting for the audited service.	User guide document

	Requirement	Evidence
X2.CS.3	**Customer Ticketing System** A ticketing system should be in place for tracking customer change requests and system generated incidents. A ticketing system may be part of a larger IT Systems Manager (ITSM) or Customer Relationship Management (CRM) system. Reports from this system should include metrics and summaries of incidents including details such as quantity, status, average time to resolve past incidents, and how the incidents were resolved.	*Waived for Gold Providers* Demonstration of the Customer ticketing system

Recommended Best Practices

In addition to the core requirements for Cisco Powered Services validation above, the following section includes several noteworthy Best Practices that have been shown to greatly contribute to the market success of Managed Service offerings. While these Best Practices will not be inspected during the validation process, Cisco strongly recommends that Providers implement them.

Recommendation
Digital presence • Most buyers will complete their research online before engaging with the Provider’s sales team. Online presence may include a web page, micro site, social media, podcast, and marketing events.
Align digital marketing to the buyer journey Prospective customers complete the majority of purchasing decision research before engaging a Provider’s sales contacts. It is a best practice to ensure that rich digital marketing content with clearly defined use cases is in place through the buyer’s journey. This may include a micro web site, social media, podcasts, and interactive marketing events such as webinars.
Sales Compensation policy It is recommended for the provider to have a sales compensation policy that incentivizes and rewards the involved teams for selling the service.
Sales Training It is recommended for the provider to have a process to train both sales representatives and sales engineers for the service
Sales Enablement It is recommended for the provider to develop sales enablement materials: • Battle card • Call script • Email template • Demo portal • Demo video Please reach out to your Cisco Account Team. for examples of these materials.

X3 Sovereign Cloud

Introduced: December 2022
Last updated: February 2023

Overview

The Cisco Powered Sovereign Cloud service is defined as a provider-delivered managed service or as-a-service offering that provides on-premise private or air-gapped cloud service, delivered by a Cisco Provider. Cisco Sovereign Cloud solutions enable in-country providers to deliver sovereign cloud services in the following areas:

- Meets local sovereignty and jurisdiction compliance around data privacy, access and control
- Fully air-gapped managed private cloud service operated from within tightly secured facilities
- Deployed from provider owned service catalog and operated through entirely in-country staff

Cisco Sovereign Cloud solutions enable in-country providers to deliver Sovereign cloud services in the following areas:

	Managed Sovereign Cloud Use-Cases			
Cisco Platforms	Sovereign Cloud Operations	Sovereign Cloud Infrastructure	Data Center Networking	Data Center Fabric (SDN)
Intersight Private Virtual Appliance	●			
Intersight Infrastructure Service	●			
Intersight Cloud Orchestrator	●			
Intersight Workload Optimizer	●			
UCS Computing Infrastructure		●		
HyperFlex Infrastructure		●		
Nexus Dashboard			●	
Nexus Data Center Networking			●	
Application Centric Infrastructure (ACI) On-Prem				●

The Provider can monetize Cisco's broad portfolio of products, applications, and services to assure the highest standard of application, infrastructure, security, cloud managed services for its customers.

Training

Providers are required to build Cisco Sovereign Cloud Infrastructure utilizing Cisco Sovereign Cloud Operations solutions to achieve Cisco Powered status. To successfully build a Managed Sovereign Cloud service, specific training is required for at minimum (2) individuals on staff utilizing the matrix below. All evidence of completed training must be uploaded to the provider application which will be validated through a 3rd party audit process.

	Managed Sovereign Cloud Components			
Required Trainings	Sovereign Cloud Operations	Sovereign Cloud Infrastructure	Data Center Networking	Data Center Fabric (SDN)
Intersight Pre-Sales Stage 1 (link)	●	●		
Intersight Pre-Sales Stage 2 (link)	●	●		
UCS Deployment Stage 1 (link)	●	●		
UCS Deployment Stage 2 (link)	●	●		
Hyperflex Deployment Stage 1 (link)		▲		
Hyperflex Deployment Stage 2 (link)		▲		
Nexus Dashboard Deployment Stage 1 (link)			●	
Nexus Dashboard Deployment Stage 2 (link)			●	
ACI Deployment Stage 1 (link)				▲
ACI Deployment Stage 2 (link)				▲
Nexus Switching Deployment Stage 1 (link)			●	
Nexus Switching Deployment Stage 2 (link)			●	

● Required training ▲ Optional training

Example: If a Provider is applying for the Sovereign Cloud Operations use-case:

1) a minimum of two individuals must provide evidence of the Pre-Sales and Deployment Black-Belt training and

2) a minimum of two individuals must provide evidence of the CCIE Data Center certifications.

Note: if a provider is applying for more than one use-case the same individuals may be used to meet the training qualifications of the additional use-cases.

Prerequisites

	Requirement	Evidence
X3.PR.1	**Sovereign Operations** Member must be the legal entity ("Operating Entity") that (a) will operate, manage, market, and sell the Member's Sovereign Cloud Offering; and (b) is located and incorporated in the applicable sovereign territory where such offering will be made available. For clarity, the European Union will be considered a single sovereign territory. Operating Entity must be an autonomous legal entity, i.e., no affiliate or any corporate relationship with any corporate entity located outside the applicable sovereign territory, where the Sovereign Cloud Offering is made available.	Provider must sign self-attest requirements validation document and must be uploaded into the Provider application
X3.PR.2	**Customer References** • Reference customers must be under existing contractual relationships • One customer may serve as a reference to multiple Cisco Powered Service designations • One customer with multiple use cases satisfies the requirement for a **single** reference, as the intent is to ensure that the Provider has proven and repeatable service practices • Two customer references are required only once: either with a new Cisco Powered Service application or upon first-year renewal • Use the Customer Reference Validation form to either submit references or to indicate references will be provided upon first year renewal	Customer Reference Validation Form uploaded into the Provider application
X3.PR.3	**Cisco Certifications** Cisco Certified individuals are responsible for designing and delivering modernized hybrid cloud solutions based on Cisco technologies. **Two** individuals must **each hold a Cisco Expert-Level certification**: • CCIE Data Center Certification For more information, visit Cisco Certifications	Evidence of Cisco Certification must be uploaded into the Provider application • Evidence for Individual 1 • Evidence for Individual 2
X3.PR.4	**Managed Sovereign Cloud Use-Cases** The provider must have Private Cloud Infrastructure utilizing Sovereign Cloud Operations in market as a managed service and specified in the provider application: 1. Sovereign Cloud Operations 2. Sovereign Cloud Infrastructure 3. Data Center Networking 4. Data Center Fabric (SDN)	A minimum of one use-case must be specified in the Provider application

	Requirement	Evidence
X3.PR.5	**Training Evidence** Upload evidence of completion for all Training required for this Cisco Powered Service.	Evidence of training must be uploaded into the Provider application.

Service Offer

	Requirement	Evidence
X3.SO.1	**Service Level Agreements** Service performance is committed through Service-Level Agreements (SLAs) between the Provider and End Customers, which are backed by processes to measure and report on whether those commitments are met. Service performance elements covered by the SLA may include: • Platform availability: ability for the applicable FSO Elements to process the required functions, orchestration, and service interfaces/integrations • Mean Time to Notify (MTTN): MTTN measures the average time taken to notify a customer of an issue with the subscribed service. The measurement encompasses the time that an alert is generated to the time the customer notified, which can be by any method of communication agreed upon with the customer • Mean Time to Restore Service (MTRS): MTRS measures the total elapsed time from the start of a resource outage to the time the service is restored. This is also known as Mean Time to Restore/Repair (MTTR). The turnaround time for implementing changes requested by the customer. Must be within 48 hours for standard changes.	Evidence of Service-Level Agreements (SLAs) must be uploaded into the Provider application One of: • Executed Service Level Agreement • Service Level Agreement template
X3.SO.2	**Operations Function** Operations are a centralized function, often referred to as a IT Operations Center employing people, processes, and technology to continuously monitor and improve the Partner's customer environment or application(s) while preventing, detecting, analyzing, and responding to incidents. Partner must document the operation of their IT Ops Function for incident prevention, detection, business relevancy and response capabilities.	*Waived for Gold Providers* Evidence of operations function documentation must be uploaded into the Provider application

	Requirement	Evidence
X3.SO.3	**Service Requirements** The Provider must show evidence of a MRD or PRD for this service. At a minimum, these documents should address: • Target customer segment and clearly defined use cases • Service packaging and pricing structure • Customer value proposition of the service Formal requirements help align the business on a definition of success. These documents, such as a Marketing Requirements Document (MRD) or a Product Requirements Document (PRD) ensure that the various stakeholders' requirements are cataloged and addressed, increasing the likelihood of market success dramatically.	Evidence of service requirements documentation must be uploaded into the Provider application
X3.SO.4	**Service Description** The Service Description is an End-User facing document which explains the service features, benefits, and business outcomes to a potential customer. Typically, a Service Description would include an outline of the different tiers of service such as bronze, silver, or gold, and the features available at each tier.	Evidence of service delivery documentation must be uploaded into the Provider application

Service Delivery

	Requirement	Evidence
X3.SD.1	**Service Delivery Function** For use-case(s) specified in section X3.PR.4, the Provider must provide a Service Architecture document which describes the key technology components, how they are integrated, and how End-Users access the service. It should cover: • Cisco platform integrations with Provider tools • End-customer and Provider Access and security control/measures • Best practice for integrating to Provider end-customer environments (private/public) • Customer on-boarding process Service Offering Matrix including offer packages (e.g., Small-Medium-Large) and tiers (e.g., good-better-best)	Evidence of service delivery must be uploaded into the Provider application. **Requirements:** • Service Architecture document • Description of how the availability and health of the service is monitored • Service Offering Matrix (standard scoping and tiering)

Customer Success

	Requirement	Evidence
X3.CS.1	**Customer Success Practice** Customer Success is the function within a Provider organization responsible for managing the relationship between the Provider and its customers. The goals of Customer Success are to • maximize customer value • increase service adoption • ensure ease of use • increase customer satisfaction • drive service renewal Provider must demonstrate processes and metrics that support each of the following elements of a customer success practice: • Customer on-boarding and service activation process • Service renewal process • Service renewal rate measurement • Dispute and escalation handling processes • Ongoing customer communications • Regular business review process to periodically assess business requirements and change management needs	*Waived for Gold Providers* Customer Success Practice Description document
X3.CS.2	**User Guide** A User Guide is a document provided to customers showing how to access the customer service portal for self-service capabilities which may include service activation, on-boarding, configuration and reporting for the audited service.	User guide document

Recommended Best Practices

In addition to the core requirements for Cisco Powered Services validation above, the following section includes several noteworthy Best Practices that have been shown to greatly contribute to the market success of Managed Service offerings. While these Best Practices will not be inspected during the validation process, Cisco strongly recommends that Providers implement them.

Recommendation
Digital presence Most buyers will complete their research online before engaging with the Provider's sales team. Online presence may include a web page, micro site, social media, podcast, and marketing events.
Align digital marketing to the buyer journey Prospective customers complete the majority of purchasing decision research before engaging a Provider's sales contacts. It is a best practice to ensure that rich digital marketing content with clearly defined use cases is in place through the buyer's journey. This may include a micro web site, social media, podcasts, and interactive marketing events such as webinars.
Sales Compensation policy It is recommended for the provider to have a sales compensation policy that incentivizes and rewards the involved teams for selling the service.
Sales Training It is recommended for the provider to have a process to train both sales representatives and sales engineers for the service
Sales Enablement It is recommended for the provider to develop sales enablement materials: • Battle card • Call script • Email template • Demo portal • Demo video Please reach out to your Cisco Account Team. for examples of these materials.

D1 Cisco SD-WAN

Introduced: February 2017
Last updated: February 2023

Overview

Cisco SD-WAN gives Providers the ability to deliver secure, automated WAN performance services to customers as a cloud-based managed service.

A Cisco Powered Cisco SD-WAN Service is delivered via the Provider's cloud or third-party IaaS provider. The customer consumes a set of SD-WAN services enabling the use of hybrid WAN, performance routing, load balancing, or application visibility and control from the Provider.

Relevant Products:

- Catalyst 8000 product families
- ISR product families
- vEdge product families
- Associated DNA licenses for the above

Supported Platforms:

- Cisco ASR 1000 Series Aggregation Services Routers
- Cisco ISR 1000 Series Integrated Services Routers
- Cisco ISR 4000 Series Integrated Services Routers
- Cisco Catalyst 8000V Edge Software
- Cisco 5000 Series Enterprise Network Compute System
- Cisco UCS E Series M2 servers
- Cisco UCS E Series M3 servers
- Cisco ISR1101 Integrated Services Router Rugged
- Cisco Catalyst 8200 Series Edge Platforms
- Cisco Catalyst 8300 Series Edge Platforms
- Cisco Catalyst 8500 Series Edge Platforms
- Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers
- Cisco vEdge Devices

Prerequisites

	Requirement	Evidence
D1.PR.1	**Customer References** • Reference customers must be under existing contractual relationships • One customer may serve as a reference to multiple Cisco Powered Service designations • One customer with multiple sites satisfies the requirement for a **single** reference, as the intent is to ensure that the Provider has proven and repeatable service practices • Two customer references are required only once: either with a new Cisco Powered Service application or upon first-year renewal • Use the Customer Reference Validation form to either submit references or to indicate references will be provided upon first year renewal	Customer Reference Validation Form uploaded into the Provider application
D1.PR.2	**Cisco Certifications** Cisco Certified individuals are responsible for designing and delivering modernized network solutions based on Cisco technologies. **Two** individuals must **each** have **one** of: • CCIE Enterprise Infrastructure • CCNP Enterprise The Provider must have a total of **two** individuals with either certification. For more information, visit Cisco Certifications.	Evidence of CCIE Enterprise Infrastructure **or** CCNP Enterprise certification for Individual 1
		Evidence of CCIE Enterprise Infrastructure **or** CCNP Enterprise certification for Individual 2

	Requirement	Evidence
D1.PR.3	Cisco Networking Specialization (Recommended) Cisco Master Networking Specialization is the highest level for Cisco Networking solutions, the exclusive Master Networking Specialization will ensure you have the expertise to help your customers manage their business by providing context, visibility, and insight into their networks. Partners will be required to fulfill special requirements for this Master Specialization including a full audit for first time applicants. Partners going through a full audit are required to complete the steps below: Step 1: Pre-Audit • Advanced Enterprise Networks Architecture Specialization (link) • A Networking CCIE – See table below • Fire Jumper status in Network Security focus area • Customer References or POVs (Proof of Value) Step 2: Technical Evaluation • After a Cisco Certification Program Manager validates your application, the manager will forward your application to the third-party auditing firm who will contact you to arrange an Evaluation audit date. Normally carried out virtually (Webex) Step 3: Foundation and Sales Onsite Evaluation • After a Cisco Certification Program Manager validates your application, the manager will forward your application to the third-party auditing firm who will contact you to arrange an Evaluation audit date. For information, visit Cisco Partner Architecture Specializations.	Evidence of Cisco Master Networking Specialization must be uploaded into the Provider application.
D1.PR.4	**Training Evidence** Upload evidence of completion for all Training required for this Cisco Powered Service.	Evidence of training must be uploaded into the Provider application. Refer to requirements in sections D1.SD.6, D1.SD.7, and D1.SP.1 to D1.SP.3.

Service Offer

	Requirement	Evidence
D1.SO.1	**Service Level Agreements** Service performance is committed through having Service-Level Agreements (SLAs) in place between the Provider and End-User which are backed by processes to measure and report on whether those commitments are being met. Service performance elements covered by the SLA may include: • Platform availability: infrastructure (e.g., CPE), orchestration and service interfaces • Network availability: the network operated by the Provider that is used to provide connectivity from the Internet or private WAN, involved data centers, and/or a third party used to provide network connectivity • Mean Time to Notify (MTTN): MTTN measures the average time taken to notify a customer of an issue with the subscribed service. The measurement encompasses the time that an alert is generated to the time the customer notified, which can be by any method of communication agreed upon with the customer • Mean Time to Restore Service (MTRS): MTRS measures the total elapsed time from the start of a resource outage to the time the service is restored. This is also known as Mean Time to Restore/Repair (MTTR). In some cases, a cloud-based service, brokered by a third party, may not have a platform availability SLA. The Provider must still provide SLA parameters such as MTTN to the customer.	One of: • Executed Service Level Agreement • Service Level Agreement template
D1.SO.2	**Service Requirements** Formal requirements help align the business on a definition of success. These documents, such as a Marketing Requirements Document (MRD) or a Product Requirements Document (PRD) ensure that the various stakeholders' requirements are cataloged and addressed, increasing the likelihood of market success dramatically. The Provider must show evidence of a MRD or PRD for this service. At a minimum, these documents should address: • Target customer segment and clearly defined use cases • Service packaging and pricing structure • Customer value proposition of the service	A table of contents or redacted version of one of • Marketing Requirements Document (MRD) • Product Requirements Document (PRD) of the service
D1.SO.3	**Service Description** The Service Description is an End-User facing document which explains the service features, benefits, and business outcomes to a potential customer. Typically, a Service Description would include an outline of the different tiers of service such as bronze, silver, or gold, and the features available at each tier.	Service Description document
D1.SO.4	**Artificial Intelligence Operations (AI Ops) Function** **This optional requirement is no longer available. Partners interested in ENAA should evaluate the "Application Dependency Monitoring" use case in CPS 9.2 Full-Stack Observability Designation.**	• Not Applicable

Service Delivery

	Requirement	Evidence
D1.SD.1	**Service Architecture** The Provider must provide a Service Architecture document which describes the key technology components, how they are integrated, and how End-Users access the service. The Provider must also describe how the availability and health of the service is monitored.	Both of: • Service Architecture document • Description of how the availability and health of the service is monitored
D1.SD.2	**Application-Aware Routing** Application-aware routing tracks network and path characteristics of the data plane tunnels between cEdge and vEdge routers and uses the collected information to compute optimal paths for data traffic. These characteristics include packet loss, latency, and jitter, and the load, cost, and bandwidth of a link. The ability to consider factors in path selection other than those used by standard routing protocols—such as route prefixes, metrics, link-state information, and route removal on the edge router—offers a number of advantages to an enterprise: • In normal network operation, the path taken by application data traffic through the network can be optimized, by directing it to WAN links that support the required levels of packet loss, latency, and jitter defined in an application's SLA. • In the face of network brownouts or soft failures, performance degradation can be minimized. The tracking of network and path conditions by application-aware routing in real time can quickly reveal performance issues, and it automatically activates strategies that redirect data traffic to the best available path. As the network recovers from the brownout or soft failure conditions, application-aware routing automatically readjusts the data traffic paths. • Network costs can be reduced because data traffic can be more efficiently load-balanced. • Application performance can be increased without the need for WAN upgrades.	Architectural diagram or live demonstration of how Application-Aware Routing capabilities are provided through vManage and aligned to the Provider's SLAs
D1.SD.3	**Cisco CPE** The Cisco SD-WAN managed service must be based on the following CPE and/or virtual CPE: • Supported cEdge product families, including the Catalyst 8000 product family • Supported vEdge product families Provider must acquire the necessary licenses to operate the CPE.	Demonstration of the use of the required products in the vManage Dashboard, and the necessary licenses
D1.SD.4	**Enterprise Network Assurance for AIOps** This optional requirement is no longer available. Partners interested in ENAA should evaluate the "Application Dependency Monitoring" use case in CPS 9.2 Full-Stack Observability Designation.	• Not Applicable

	Requirement	Evidence
D1.SD.5	**Customer Service Portal** The Provider must offer a secure web portal to present an operational view of the managed SD-WAN service, for multiple audiences, designed to give a view of the network and device status. The customer service portal must include specific to the Cisco Powered Cisco SD-WAN service: • Real-time status map • Path Control monitoring report • Usage report • Device Inventory This requirement can be met via the vManage portal or third-party portal.	Demonstration of the secure web portal to communicate status and performance
D1.SD.6	**Deployment Training** SD-WAN Deployment Stages 1, 2, 3 1. In **All Technology** dropdown, Select **SD-WAN** 2. Complete **SD-WAN Deployment Stages 1, 2 & 3** **Exception: Cisco Master Networking Specialization requirements in section D1.PR.3 may be substituted for Cisco Black Belt training requirements in this section.**	One of: 1. Email confirmations for Deployment Engineer 1 2. Cisco Master Networking Specialization in section D1.PR.3
		One of: 1. Email confirmations for Deployment Engineer 2 2. Cisco Master Networking Specialization in section D1.PR.3
D1.SD.7	**Support Training** SD-WAN Support Stages 1,2,3 1. In **All Technology** dropdown, Select **SD-WAN** 2. Complete **SD-WAN Support Stages 1, 2 & 3** a. Do not choose SD-WAN Support (PSS) **Exception: Cisco Master Networking Specialization requirements in section D1.PR.3 may be substituted for Cisco Black Belt training requirements in this section.**	One of: 1. Email confirmation for Support Person 1 2. Cisco Master Networking Specialization in section D1.PR.3
		One of: 1. Email confirmation for Support Person 2 2. Cisco Master Networking Specialization in section D1.PR.3

Service Marketing

	Description	Evidence
D1.SM.1	**Digital presence** Most buyers will complete their research online before engaging with the Provider's sales team. Online presence may include a web page, micro site, social media, podcast, and marketing events.	One of: • Demonstrate a service-specific online presence with service specific marketing content, • A marketing plan across various marketing channels and platform
D1.SM.2	**Align digital marketing to the buyer journey** Prospective customers complete the majority of purchasing decision research before engaging a Provider's sales contacts. It is a best practice to ensure that rich digital marketing content with clearly defined use cases is in place through the buyer's journey. This may include a micro web site, social media, podcasts, and interactive marketing events such as webinars.	Buyer Journey Map document

Sales Operations

	Description	Evidence
D1.SP.1	**Cisco SD-WAN Sales Training** BlackBelt - EN Sales Stage 1 1. Select **Stage 1: Sales Associate** 2. Select **IBN** in the Enterprise Networks section 3. Complete **EN Sales Stage 1**	One of: 1. Email confirmation for Sales Person 1 2. Cisco Master Networking Specialization in section D1.PR.3
	BlackBelt – EN SD-WAN Sales Stage 2 1. Select **Stage 2: Sales Specialist** 2. Select **IBN** in the Enterprise Networking section 3. Complete **EN SD-WAN Sales Stage 2** **Exception: Cisco Master Networking Specialization requirements in section D1.PR.3 may be substituted for Cisco Black Belt training requirements in this section.**	One of: 1. Email confirmation for Sales Person 2 2. Cisco Master Networking Specialization in section D1.PR.3

D1.SP.2	**Pre-Sales Engineer Training** Black Belt SD-WAN Presales Stage 1, 2, 3 1. In **All Technology** dropdown, Select **SD-WAN** 2. Complete **SD-WAN Pre-Sales Stages 1, 2 & 3** **Exception: Cisco Master Networking Specialization requirements in section D1.PR.3 may be substituted for Cisco Black Belt training requirements in this section.**	One of: 1. Email confirmations for Pre-Sales Engineer 1 2. Cisco Master Networking Specialization in section D1.PR.3
		One of: 1. Email confirmations for Pre-Sales Engineer 2 2. Cisco Master Networking Specialization in section D1.PR.3
D1.SP.3	**Enterprise Network Assurance for AIOps Sales Training** This optional requirement is no longer available. Partners interested in ENAA should evaluate the "Application Dependency Monitoring" use case in CPS 9.2 Full-Stack Observability Designation.	Not Applicable
D1.SP.4	**Sales Training** Provider must have a process to formally train both sales and sales engineers for the service	Sales Training Plan document
D1.SP.5	**Sales Enablement** Provider must provide evidence of an **End Customer-facing pitch deck** and at least two of the following sales enablement materials: • Services at-a-glance • Service brochure or video • Battle card/sales reference card • Sales playbook • Call script • Email template • Demo Please reach out to your Cisco Account Team for examples of these materials.	• End Customer-facing pitch deck and at least **two** of: • Services at-a-glance • Service brochure or video • Battle card/sales reference card • Sales playbook • Call script • Email template • Demo
D1.SP.6	**Sales Compensation policy** Provider must have a sales compensation policy that incentivizes and rewards the involved teams for selling the service	Sales Compensation Policy document

Customer Success

	Requirement	Evidence
D1.CS.1	**Customer Success Practice** Customer Success is the function within a Provider organization responsible for managing the relationship between the Provider and its customers. The goals of Customer Success are to: • Maximize customer value • Increase service adoption • Ensure ease of use • Increase customer satisfaction • Drive service renewal For Evidence Option #2 (Customer Success Practice documentation): Provider must demonstrate processes and metrics that support each of the following elements of a customer success practice: • Customer on-boarding and service activation process • Service renewal process • Service renewal rate measurement • Dispute and escalation handling processes • Ongoing customer communications Regular business review process to periodically assess business requirements and change management needs	One of: 1. Customer Success Practice documentation 2. Customer Experience or Advanced Customer Experience Specialization (no further evidence required if the Specialization is held)
D1.CS.2	**User Guide** A User Guide is a document provided to customers showing how to access the customer service portal for self-service capabilities which may include service activation, on-boarding, configuration, and reporting for the audited service.	User guide document
D1.CS.3	**Customer Ticketing System** A ticketing system should be in place for tracking customer change requests and system generated incidents. A ticketing system may be part of a larger IT Systems Manager (ITSM) or Customer Relationship Management (CRM) system. Reports from this system should include metrics and summaries of incidents including details such as quantity, status, average time to resolve past incidents, and how the incidents were resolved.	Demonstration of the Customer ticketing system

D4 Meraki SD-WAN

Introduced: February 2017
Last updated: February 2023

Overview

Cisco Powered Meraki SD-WAN Services are managed services that deliver automated, hybrid WAN services to business customers via a cloud-based, multitenant solution.

Meraki SD-WAN services are delivered and managed from the Provider's cloud. Through the managed service, end customers benefit from a rich set of SD-WAN capabilities including hybrid WAN, performance routing, load balancing, application visibility and control capabilities.

Furthermore, Meraki SD-WAN enables Providers to deliver SD-WAN at a high scale, with extreme efficiency, and in an automated fashion. End customers may additionally leverage self-service capabilities for configuring, monitoring, and reporting via a cloud-based service portal.

Relevant Products:

- Meraki MX family or Meraki virtual MX (vMX)
- Associated licenses for the above

Prerequisites

	Requirement	Evidence
D4.PR.1	**Customer References** • Reference customers must be under existing contractual relationships • One customer may serve as a reference to multiple Cisco Powered Service designations • One customer with multiple sites satisfies the requirement for a single reference, as the intent is to ensure that the Provider has proven and repeatable service practices • Two customer references are required only once: either with a new Cisco Powered Service application or upon first-year renewal • Use the Customer Reference Validation form to either submit references or to indicate references will be provided upon first year renewal	Customer Reference Validation Form uploaded into the Provider application
D4.PR.2	**Training Evidence** Upload evidence of completion for all Training required for this Cisco Powered Service.	Evidence of training must be uploaded into the Provider application. Refer to requirements in sections D4.SD.10, D4.SD.11, and D4.SP.1 to D4.SP.3.

Service Offer

	Requirement	Evidence
D4.SO.1	**Service Level Agreements** Service performance is committed through having Service-Level Agreements (SLAs) in place between the Provider and End-User which are backed by processes to measure and report on whether those commitments are being met. Service performance elements covered by the SLA may include: • Platform availability: infrastructure, orchestration, and service interfaces • Network availability: the network operated by the Provider that is used to provide connectivity from the Internet or private WAN, involved data centers, and/or a third party used to provide network connectivity • Mean Time to Notify (MTTN): MTTN measures the average time taken to notify a customer of an issue with the subscribed service. The measurement encompasses the time that an alert is generated to the time the customer notified, which can be by any method of communication agreed upon with the customer • Mean Time to Restore Service (MTRS): MTRS measures the total elapsed time from the start of a resource outage to the time the service is restored. This is also known as Mean Time to Restore/Repair (MTTR). In some cases, a cloud-based service, brokered by a third party, may not have a platform availability SLA. The Provider must still provide SLA parameters such as MTTN to the customer.	One of: • Executed Service Level Agreement • Service Level Agreement template
D4.SO.2	**Service Requirements** Formal requirements help align the business on a definition of success. These documents, such as a Marketing Requirements Document (MRD) or a Product Requirements Document (PRD) ensure that the various stakeholders' requirements are cataloged and addressed, increasing the likelihood of market success dramatically. The Provider must show evidence of a MRD or PRD for this service. At a minimum, these documents should address: • Target customer segment and clearly defined use cases • Service packaging and pricing structure • Customer value proposition of the service	A table of contents or redacted version of one of: • Marketing Requirements Document (MRD) • Product Requirements Document (PRD) of the service
D4.SO.3	**Service Description** The Service Description is an End-User facing document which explains the service features, benefits, and business outcomes to a potential customer. Typically, a Service Description would include an outline of the different tiers of service such as bronze, silver, or gold, and the features available at each tier.	Service Description document
D4.SO.4	**Artificial Intelligence Operations (AI Ops) Function** **This optional requirement is no longer available. Partners interested in ENAA should evaluate the "Application Dependency Monitoring" use case in CPS 9.2 Full-Stack Observability Designation.**	• Not Applicable

Service Delivery

	Requirement	Evidence
D4.SD.1	**Service Architecture** The Provider must provide a Service Architecture document which describes the key technology components, how they are integrated, and how End-Users access the service. The Provider must also describe how the availability and health of the service is monitored.	Both of: • Service Architecture document • Description of how the availability and health of the service is monitored
D4.SD.2	**Hybrid WAN** This design allows Meraki intelligent path control to performance policy-based routing based on application requirements, priority and source or destination IP addresses. And this design supports dynamic path control on per application basis based on real time network performance, selecting the best WAN path for applications based on application requirements, policy and network performance. This design has the capability to use two transport circuits from the following. These two links could use the same transport (e.g., 2 Internet circuits) or mix of any two-different transport (MPLS + Internet, or Internet + LTE). • MPLS transport • Direct Internet access • 4G LTE transport; and • Use the intelligent path control capability to select a transport circuit for particular application traffic or both for load balancing. For a SD-WAN domain associated with an organization, this hybrid WAN design must be implemented at a number of sites such as headquarter sites or large branch sites. Some sites with single transport uplink within this organization are allowed.	Architectural diagram or live demonstration of how **Hybrid WAN** capabilities are provided through the managed service
D4.SD.3	**Secure VPN** Meraki SD-WAN creates a secure VPN overlay using Meraki AutoVPN technology. AutoVPN is IPsec based VPN controlled and managed from Meraki cloud. AutoVPN ensures secure connectivity between sites within an SD-WAN domain.	Demonstration of how **AutoVPN** capabilities are provided through the managed service, in the Meraki dashboard

	Requirement	Evidence
D4.SD.4	**Intelligent Path Control** Intelligent path control maximizes the value of multiple network paths (like dual MPLS access or dual Service Providers or MPLS + Internet) by ensuring the optimum usage of each available path between sites. Intelligent Path Control consists of: • Policy based routing (PbR) capability that configure preferred VPN paths for different traffic flow based on application, source, destination IP addresses and ports. • Dynamic path control capability that configures performance criteria for different types of traffic. And path selection decision is made based on application performance requirements and real-time network performance such as jitter, delay, loss and the available bandwidth. Demonstration should cover flow preference, SD-WAN policies and traffic shaping rules.	Demonstration of how **Intelligent Path Control** capabilities is provided through the managed service, in the Meraki dashboard
D4.SD.5	**Application visibility and reporting** Application visibility and reporting are a set of service capabilities that allow the discovery and classification of all applications flowing over the network and provide reports on application network usage and performance via the Meraki dashboard.	Both of: • Service description referencing the **Application visibility and reporting** capabilities • Demonstration of **Application visibility and reporting** capabilities in use via the Meraki Dashboard
D4.SD.6	**Meraki CPE** Cloud Managed Meraki SD-WAN Service requires Meraki CPE and/or virtualized CPE (vCPE). The Provider must offer Cloud Managed Meraki SD-WAN based on following CPE and/or virtual CPE: • Meraki MX family, or • Meraki virtual MX (vMX) Provider must acquire the necessary licenses to operate the CPE.	Demonstration of the use of the required products in the Meraki Dashboard, and the necessary licenses
D4.SD.7	**License Management** The Provider must ensure a valid software license is applied to CPE devices used for service delivery. Failure to properly manage the software license expiration could result is a service outage for the customer.	Demonstration of the license management process
D4.SD.8	**Enterprise Network Assurance for AIOps** **This optional requirement is no longer available. Partners interested in ENAA should evaluate the "Application Dependency Monitoring" use case in CPS 9.2 Full-Stack Observability Designation.**	• Not Applicable

	Requirement	Evidence
D4.SD.9	**Customer Service Portal** The Provider is to offer a secure web portal to present an operational view of the managed SD-WAN service, for multiple audiences, designed to give a view of the network and device status. The customer service portal must include specific to the Cisco Powered Meraki SD-WAN service: • Real-time status map • Path Control monitoring report • Usage report • Device Inventory This requirement can be met via the Meraki portal or third-party portal.	Demonstration of the secure web portal to communicate status and performance
D4.SD.10	**Deployment Training** Black Belt Meraki Deployment Stage 1, 2, 3 1. In **All Technology** dropdown, Select **Meraki** 2. Complete **Meraki Deployment Stages 1, 2, and 3**	Email confirmations for Deployment Engineer 1
		Email confirmations for Deployment Engineer 2
D4.SD.11	**Support Training** Black Belt Meraki Support Stage 1,2,3 1. In **All Technology** dropdown, Select **Meraki** 2. Complete **Meraki Support Stages 1, 2, and 3**	Email confirmation for Support Person 1
		Email confirmation for Support Person 2

Service Marketing

	Description	Evidence
D4.SM.1	**Digital presence** Most buyers will complete their research online before engaging with the Provider's sales team. Online presence may include a web page, micro site, social media, podcast, and marketing events.	One of: • Demonstrate a service-specific online presence with service specific marketing content, • A marketing plan across various marketing channels and platform
D4.SM.2	**Align digital marketing to the buyer journey** Prospective customers complete the majority of purchasing decision research before engaging a Provider's sales contacts. It is a best practice to ensure that rich digital marketing content with clearly defined use cases is in place through the buyer's journey. This may include a micro web site, social media, podcasts, and interactive marketing events such as webinars.	Buyer Journey Map document

Sales Operations

	Description	Evidence
D4.SP.1	**Cisco Sales Training** Black Belt Meraki Sales Stage 1 1. Select **Stage 1: Sales Associate** 2. Under **Enterprise Networks**, Complete **Meraki**	Email confirmation for Sales Person 1 Email confirmation for Sales Person 2
D4.SP.2	**Pre-Sales Engineer Training** Black Belt Meraki Presales Stage 1, 2, 3 1. In **All Technology** dropdown, Select **Meraki** 2. Complete **Meraki Presales Stages 1, 2, and 3**	Email confirmations for Presales Engineer 1 Email confirmations for Presales Engineer 2
D4.SP.3	**Sales Training** Provider must have a process to formally train both sales and sales engineers for the service	Sales Training Plan document
D4.SP.4	**Sales Enablement** Provider must provide evidence of an **End Customer-facing pitch deck** and at least two of the following sales enablement materials: • Services at-a-glance • Service brochure or video • Battle card/sales reference card • Sales playbook • Call script • Email template • Demo Please reach out to your Cisco Account Team for examples of these materials.	• End Customer-facing pitch deck and at least **two** of: • Services at-a-glance • Service brochure or video • Battle card/sales reference card • Sales playbook • Call script • Email template • Demo
D4.SP.5	**Sales Compensation policy** Provider must have a sales compensation policy that incentivizes and rewards the involved teams for selling the service	Sales Compensation policy document

Customer Success

	Requirement	Evidence
D4.CS.1	**Customer Success Practice** Customer Success is the function within a Provider organization responsible for managing the relationship between the Provider and its customers. The goals of Customer Success are to: • Maximize customer value • Increase service adoption • Ensure ease of use • Increase customer satisfaction • Drive service renewal For Evidence Option #2 (Customer Success Practice documentation): Provider must demonstrate processes and metrics that support each of the following elements of a customer success practice: • Customer on-boarding and service activation process • Service renewal process • Service renewal rate measurement • Dispute and escalation handling processes • Ongoing customer communications Regular business review process to periodically assess business requirements and change management needs	One of: 1. Customer Success Practice documentation 2. Customer Experience or Advanced Customer Experience Specialization (no further evidence required if the Specialization is held)
D4.CS.2	**User Guide** A User Guide is a document provided to customers showing how to access the customer service portal for self-service capabilities which may include service activation, on-boarding, configuration, and reporting for the audited service.	User guide document
D4.CS.3	**Customer Ticketing System** A ticketing system should be in place for tracking customer change requests and system generated incidents. A ticketing system may be part of a larger IT Systems Manager (ITSM) or Customer Relationship Management (CRM) system. Reports from this system should include metrics and summaries of incidents including details such as quantity, status, average time to resolve past incidents, and how the incidents were resolved.	Demonstration of the Customer ticketing system

D5 Meraki Security

Introduced: July 2019
Last updated: February 2023

Overview

Meraki Security allows the provider to leverage Cisco Meraki cloud offerings to create and manage flexible, dynamic pools of physical and virtual security appliances that can be shared efficiently and securely among multiple tenants. It also provides orchestration to reduce resource provisioning and improves time to market for managed security services.

Meraki Security technologies enable Providers to create subscription-based "as a service" offers utilizing hosted and managed models. Providers can monetize Cisco Meraki's broad portfolio of security products, streamline operations with a complete management system, and optimize their capital investments in the data center, on customer premises, and in hosted SaaS offerings, to assure the highest security and for their customers.

Relevant Products:

- Meraki MX
- Enterprise license: Next Generation Firewall and Auto VPN
- Advanced license: Content filtering, AMP for Endpoints, and intrusion detection/prevention

Prerequisites

	Requirement	Evidence
D5.PR.1	**Customer References** • Reference customers must be under existing contractual relationships • One customer may serve as a reference to multiple Cisco Powered Service designations • One customer with multiple sites satisfies the requirement for a single reference, as the intent is to ensure that the Provider has proven and repeatable service practices • Two customer references are required only once: either with a new Cisco Powered Service application or upon first-year renewal • Use the Customer Reference Validation form to either submit references or to indicate references will be provided upon first year renewal	Customer Reference Validation Form uploaded into the Provider application
D5.PR.2	**Training Evidence** Upload evidence of completion for all Training required for this Cisco Powered Service.	Evidence of training must be uploaded into the Provider application. Refer to requirements in sections D5.SD.13, D5.SD.14, D5.SP.1 and D5.SP.2.

Service Offer

	Requirement	Evidence
D5.SO.1	**Service Level Agreements** Service performance is committed through having Service-Level Agreements (SLAs) in place between the Provider and End-User which are backed by processes to measure and report on whether those commitments are being met. Service performance elements covered by the SLA may include: • Platform availability: infrastructure, orchestration, and service interfaces • Network availability: the network operated by the Provider that is used to provide connectivity from the Internet or private WAN, involved data centers, and/or a third party used to provide network connectivity • Mean Time to Notify (MTTN): MTTN measures the average time taken to notify a customer of an issue with the subscribed service. The measurement encompasses the time that an alert is generated to the time the customer notified, which can be by any method of communication agreed upon with the customer • Mean Time to Restore Service (MTRS): MTRS measures the total elapsed time from the start of a resource outage to the time the service is restored. This is also known as Mean Time to Restore/Repair (MTTR). In some cases, a cloud-based service, brokered by a third party, may not have a platform availability SLA. The Provider must still provide SLA parameters such as MTTN to the customer.	One of: • Executed Service Level Agreement • Service Level Agreement template
D5.SO.2	**Service Requirements** Formal requirements help align the business on a definition of success. These documents, such as a Marketing Requirements Document (MRD) or a Product Requirements Document (PRD) ensure that the various stakeholders' requirements are cataloged and addressed, increasing the likelihood of market success dramatically. The Provider must show evidence of a MRD or PRD for this service. At a minimum, these documents should address: • Target customer segment and clearly defined use cases • Service packaging and pricing structure • Customer value proposition of the service	A table of contents or redacted version of one of: • Marketing Requirements Document (MRD) • Product Requirements Document (PRD) of the service
D5.SO.3	**Service Description** The Service Description is an End-User facing document which explains the service features, benefits, and business outcomes to a potential customer. Typically, a Service Description would include an outline of the different tiers of service such as bronze, silver, or gold, and the features available at each tier.	Service Description document

Service Delivery

	Requirement	Evidence
D5.SD.1	**Service Architecture** The Provider must provide a Service Architecture document which describes the key technology components, how they are integrated, and how End-Users access the service. The Provider must also describe how the availability and health of the service is monitored.	Both of: • Service Architecture document • Description of how the availability and health of the service is monitored
D5.SD.2	**Security Event Monitoring and Triaging** Provider must document the operation of a Security Event Monitoring and Triaging Center for incident prevention, detection, and response capabilities. This requirement may be fulfilled by Network Operations Center / Security Operations Center (NOC/SOC) monitoring and triaging of security events, or a 3rd party white label SOC provider. In this case, the sub-contracted SOC provider must participate in the audit.	Both of: • Documentation of security event detection, escalation, and remediation processes consistent with SLAs • Evidence of people, processes, and tools specific to the Security Event Monitoring and Triaging Center
D5.SD.3	**Cloud Orchestration Software** Policy deployment and service orchestration at scale and not on a device-by-device basis are core capabilities of Cloud Managed Security Services. Provider may deploy the cloud orchestration software in its data center or consume such capabilities from the cloud to orchestrate the service capabilities. It provides service management and configuration, zero-touch deployment of CPE or datacenter virtualized appliances, and policy management and deployment to those appliances.	Demonstration the **Cloud Orchestration Software** via the Meraki dashboard or third-party software
D5.SD.4	**Security Services** The Cloud Managed Security services are aimed at Providers offering a range of security capabilities to protect their customer from a variety of security threats. The Provider must deliver **two** of the following services: • Firewall as a Service • VPN as a Service • Content Filtering • Threat Protection Services must be delivered using Meraki MX and/or vMX.	Specify the two security services selected for the audit
D5.SD.5	**Customer Service Portal** The Provider is to offer a secure web portal to present an operational view of the managed service, for multiple audiences, designed to give a view of the network and device status. If the Provider does not provide direct access to the Cisco Meraki Dashboard and/or Meraki APIs, the Provider must provide a third-party portal integrated with the Meraki APIs.	Both of: • Demonstration of the secure web portal • User Guide that includes information on the portal

	Requirement	Evidence
D5.SD.6	**Event log retention** Security events are stored in a log for regulatory and analysis purposes. Must be retained for a period of time established with the customer.	Demonstration that event logs can be stored and made accessible via the portal.
D5.SD.7	**Service Dashboard** Summary-level dashboard to communicate key performance criteria, including: • Real-time status • Monitoring report • Usage report For firewall as a service, web security as a service and email security as a service, the security dashboard must include: • Top five attacked or visited sites of the month/week including the number of events and the associated percentage • Top five alerts of the month/week: The top five most received alerts, including the number of occurrences and the associated percentage • Historical charts (day, week, month, year) For VPN services, the security dashboard must include: • Network traffic • VPN tunnels history Network delays: round trip time (RTT) and time to live (TTL)	Demonstration of summary-level dashboard
D5.SD.8	**Service Availability reports** Service availability reporting on the overall services, separate infrastructure services, separate network services, separate managed devices level services are provided including details of the service downtime over a defined period of time. Web-based reporting via a customer web portal is considered a best practice and allows the Providers to differentiate themselves from other Providers.	One of: • Sample reports • Demonstration of the report from the customer web portal.
D5.SD.9	**Device Inventory reports** Reporting of devices under management for the customer, providing data that is relevant to the customer regarding the inventory of equipment or WAN services used in delivering the service.	One of: • Sample reports • Demonstration of the report from the customer web portal.
D5.SD.10	**Incident Management reports** Reports summarizing customer change request activities and system generated incidents (e.g., utilization warnings) are made available to the customer. These should include metrics on the incidents, such as number, status, average time to resolve past incidents, and how the incidents were resolved.	One of: • Sample reports • Demonstration of the report from the customer web portal.

	Requirement	Evidence
D5.SD.11	**Exception reports** Reports generated by customer-specified thresholds or ranges; provide ability for customers to self-select parameters on individual devices and determine thresholds for the raising of exception reports.	One of: - Sample reports - Demonstration of the report from the customer web portal.
D5.SD.12	**Security reports** Security reporting capabilities must include: Number of security incidents that occurred over a pre-determined period - Types of incidents - Time to respond - Most frequent types of attacks - Most frequently attacked hosts or sites - Identified sources of attack	One of: - Sample reports - Demonstration of the report from the customer web portal
D5.SD.13	**Deployment Training** Black Belt Meraki Deployment Stage 1, 2, 3 1. Complete **Meraki Deployment Stages 1, 2, and 3**	Email confirmations for Deployment Engineer 1 Email confirmations for Deployment Engineer 2
D5.SD.14	**Support Training** Black Belt Meraki Support Stage 1,2,3 1. Complete **Meraki Support Stages 1, 2, and 3**	Email confirmation for Support Person 1 Email confirmation for Support Person 2

Service Delivery: Firewall as a Service

	Requirement	Evidence
D5.F.1	**Support for Network Address Translation (NAT)** Network Address Translation allows hiding of internal addressing, also known as obfuscation. This prevents external attackers from guessing the internal addressing and attempting to access those devices. It enables private IP networks that use unregistered IP addresses to connect to the Internet. NAT operates on the firewall; usually connecting two networks together and translates the private (not globally unique) addresses in the internal network into legal addresses, before packets are forwarded to another network. As part of this capability, NAT can be configured to advertise only one address for the entire network to the outside world. This provides additional security by effectively hiding the entire internal network behind that address.	Both of: - Evidence of the firewall service capabilities such as: ◦ Policy settings ◦ Report ◦ SLA agreements ◦ Service descriptions ◦ Service architecture - Explanation of the key benefits of the service and how it can be used to block traffic from the Internet into the customer network

	Requirement	Evidence
D5.F.2	**Layer 3 Firewall Based on IP Address and Port** Layer 3 Firewall rules provide an administrator granular access control of outbound client traffic. A layer 3 firewall rule on the MX appliance can be based on protocol, source IP address and port, and destination IP address (or FQDN) and port.	Demonstration of the ability to create Layer 3 Firewall Rules
D5.F.3	**Layer 7 Firewall Based Application Inspection and Control (optional)** Layer 7 Firewall rules are used to deny certain traffic based on traffic type. Where most firewall rules only inspect headers at layer 3 (IP address), 4 (Transport), and 5 (Port), a layer 7 rule inspects the payload of packets to match against known traffic types. An example of this would be encrypted P2P traffic.	*Optional* Demonstration of the ability to create Layer 7 Firewall Rules /
D5.F.4	**Dual firewall support with stateful failover (optional)** Stateful failover enables the firewall to continue processing and forwarding session packets after a planned or unplanned outage occurs. A backup (secondary) firewall is employed that automatically takes over the tasks of the active (primary) firewall if the active firewall loses connectivity for any reason. This process is transparent and does not require adjustment or reconfiguration of any remote peer.	*Optional* One of: • Policy settings • Report • SLA agreements • Service descriptions • Service architecture

Service Delivery: VPN as a Service

	Requirement	Evidence
D5.V.1	**Support for internet site-to-site VPN** The Provider must offer a site-to-site VPN termination service from its cloud infrastructure that allows secure site-to-site connectivity the end customer network and the Provider hosted security cloud infrastructure.	Service architecture document demonstrating implementation of Meraki Auto VPN for site-to-site VPN service

Service Delivery: Content Filtering

	Requirement	Evidence
D5.C.1	**Content Filtering** Provide content filtering service with the following capabilities: • Blocking web sites based on categories • Web search filtering Creating black or white list of URLs based on pattern or specific name	Both of: • Evidence of the content filtering service capabilities such as: ◦ Policy settings ◦ Report ◦ SLA agreements ◦ Service descriptions ◦ Service architecture • Explanation of the key benefits of the service and how it can be used to protect the customer
D5.C.2	**High Availability (optional)** Active-active or active-passive high availability for the web security function allows the Provider to continue service delivery during a planned or unplanned outage.	*Optional* Documentation or demonstration of high availability capability based on load balancing between web security appliances.

Service Delivery: Threat Protection

	Requirement	Evidence
D5.T.1	**Intrusion detection and prevention capabilities** Networks are exposed to a wide range of attacks, including viruses, worms, spyware, botnets, and spam. Intrusion Prevention Systems inspect all traffic for intrusions and exploits. It combines signature-, protocol-, and anomaly-based inspection methods to deliver comprehensive protection from attacks. The service includes the ability to monitor network traffic and respond based on defined policies. An intrusion policy examines decoded packets for attacks based on patterns and can block or alter malicious traffic. This monitoring will consist of event correlation, rating and filtering, and reporting through the customer web portal.	Both of: • Evidence of the Intrusion detection and prevention capability such as: ◦ Policy settings ◦ Report ◦ SLA agreements ◦ Service descriptions ◦ Service architecture • Evidence of procedures to implement customer policies such as operational or training documentation

	Requirement	Evidence
D5.T.2	**Intrusion monitoring and incident handling** Cisco Meraki intrusion monitoring has a choice of three levels: 1. **Connectivity:** Contains rules from the current year and the previous two years for vulnerabilities with a CVSS score of 10 2. **Balanced:** Contains rules that are from the current year and the previous two years, are for vulnerabilities with a CVSS score of 9 or greater, and are in one of the following categories: ◦ *Malware-CNC* Rules for known malicious command and control activity for identified botnet traffic. This includes call home, downloading of dropped files, and exfiltration of data. ◦ *Blacklist* Rules for URIs, user agents, DNS hostnames, and IP addresses that have been determined to be indicators of malicious activity. ◦ *SQL Injection* Rules that are designed to detect SQL Injection attempts. ◦ *Exploit-kit* Rules that are designed to detect exploit kit activity. 3. **Security:** Contains rules that are from the current year and the previous three years, are for vulnerabilities with a CVSS score of 8 or greater, and are in one of the following categories: ◦ *Malware-CNC* Rules for known malicious command and control activity for identified botnet traffic. This includes call home, downloading of dropped files, and exfiltration of data. ◦ *Blacklist* Rules for URIs, user agents, DNS hostnames, and IP addresses that have been determined to be indicators of malicious activity. ◦ *SQL Injection* Rules that are designed to detect SQL Injection attempts. ◦ *Exploit-kit* Rules that are designed to detect exploit kit activity. ◦ *App-detect* Rules that look for and control the traffic of certain applications that generate network activity. The **Balanced** ruleset will be selected by default. The Provider must set this to **Balanced** or **Security**.	• Evidence of the selection of either the **Balanced** or **Security** ruleset such as: ◦ Policy settings ◦ Report ◦ SLA agreements ◦ Service descriptions ◦ Service architecture

	Requirement	Evidence
D5.T.3	**Network-based AMP** Network-based Advanced Malware Protection solution inspects network traffic for threats in a multitude of file types, and it protects against zero-day and targeted file-based threats by: • File reputation – the appliance captures a fingerprint of each file and sends it to Cisco AMP cloud threat intelligence service or private AMP Cloud to obtain the reputation of known files whereby malicious files can be automatically blocked • File analysis – analyzing behavior of certain files that are not yet known to the reputation service • File retrospection - Continuously evaluating emerging threats as new information becomes available, and notifying end customers about files that are determined to be threats after they have entered their network, indicating who on their network may have been infected and when	Demonstration of this service being enabled on the Meraki dashboard

Service Marketing

	Description	Evidence
D5.SM.1	**Digital presence** Most buyers will complete their research online before engaging with the Provider's sales team. Online presence may include a web page, micro site, social media, podcast, and marketing events.	One of: • Demonstrate a service-specific online presence with service specific marketing content, • A marketing plan across various marketing channels and platform
D5.SM.2	**Align digital marketing to the buyer journey** Prospective customers complete the majority of purchasing decision research before engaging a Provider's sales contacts. It is a best practice to ensure that rich digital marketing content with clearly defined use cases is in place through the buyer's journey. This may include a micro web site, social media, podcasts, and interactive marketing events such as webinars.	Buyer Journey Map document

Sales Operations

	Description	Evidence
D5.SP.1	**Cisco Sales Training** Black Belt Meraki Sales Stage 1 1. Select **Stage 1: Sales Associate** 2. Complete **Meraki**	Email confirmation for Sales Person 1
		Email confirmation for Sales Person 2

	Description	Evidence
D5.SP.2	**Presales Engineer Training** Black Belt Meraki Presales Stage 1, 2, 3 1. Complete **Meraki Presales Stages 1, 2, and 3**	Email confirmation for Presales Engineer 1 Email confirmation for Presales Engineer 2
D5.SP.3	**Sales Training** Provider must have a process to formally train both sales and sales engineers for the service	Sales Training Plan document
D5.SP.4	**Sales Enablement** Provider must provide evidence of an **End Customer-facing pitch deck** and at least two of the following sales enablement materials: • Services at-a-glance • Service brochure or video • Battle card/sales reference card • Sales playbook • Call script • Email template • Demo Please reach out to your Cisco Account Team for examples of these materials.	• End Customer-facing pitch deck and at least **two** of: • Services at-a-glance • Service brochure or video • Battle card/sales reference card • Sales playbook • Call script • Email template • Demo
D5.SP.5	**Sales Compensation policy** Provider must have a sales compensation policy that incentivizes and rewards the involved teams for selling the service	Sales Compensation policy document

Customer Success

	Requirement	Evidence
D5.CS.1	**Customer Success Practice** Customer Success is the function within a Provider organization responsible for managing the relationship between the Provider and its customers. The goals of Customer Success are to: • Maximize customer value • Increase service adoption • Ensure ease of use • Increase customer satisfaction • Drive service renewal For Evidence Option #2 (Customer Success Practice documentation): Provider must demonstrate processes and metrics that support each of the following elements of a customer success practice: • Customer on-boarding and service activation process • Service renewal process • Service renewal rate measurement • Dispute and escalation handling processes • Ongoing customer communications Regular business review process to periodically assess business requirements and change management needs	One of: 1. Customer Succes Practice documentation 2. Customer Experience or Advanced Customer Experience Specialization (no further evidence required if the Specialization is held)
D5.CS.2	**User Guide** A User Guide is a document provided to customers showing how to access the customer service portal for self-service capabilities which may include service activation, on-boarding, configuration, and reporting for the audited service.	User guide document
D5.CS.3	**Customer Ticketing System** A ticketing system should be in place for tracking customer change requests and system generated incidents. A ticketing system may be part of a larger IT Systems Manager (ITSM) or Customer Relationship Management (CRM) system. Reports from this system should include metrics and summaries of incidents including details such as quantity, status, average time to resolve past incidents, and how the incidents were resolved.	Demonstration of the Customer ticketing system

D3 Meraki Access

Introduced: November 2017
Last updated: February 2023

Overview

An access network connects the users and devices to other devices on the local area network and wide area networks for communication and accessing business applications. It is a critical layer of networking that delivers high performance, secure, wired or wireless connectivity to the applications and information. The access layer of the network consists of switches, wireless access points, controllers, and a suite of management software that configures the associated equipment, manages the associated policies, and continuously monitors the performance and quality of services. Meraki Access enables Providers to offer managed wireless LAN (WLAN) and managed LAN services to interconnect end users and devices with layer 2 switching, layer 3 routing with security and quality of services with a cloud-based controller and management.

A Cisco Powered Meraki Access Service is a managed local area network (LAN) service, a managed wireless LAN (WLAN) service, or both, that is orchestrated from the cloud and managed by the Provider, using Cisco Meraki network solutions, together with support services, a Service Level Agreement, and proactive monitoring. End customers consume a set of access network services including managed LAN, managed WLAN, and other value-added services, such as presence analytics service and proximity marketing services. With Meraki Access, the Provider is able to control the infrastructure efficiently from the cloud, with the help of multi-tenancy and automation features aimed at delivering a compelling user experience, at scale. Furthermore, the Provider may make status and reporting capabilities, as well as self-service capabilities, available to End Customer administrators.

Relevant Products:

- Cisco Meraki MR series products
- Cisco Meraki MX series products with WiFi capability
- Cisco Meraki MS product family
- Associated licenses for the above

Prerequisites

	Requirement	Evidence
D3.PR.1	**Customer References** - Reference customers must be under existing contractual relationships - One customer may serve as a reference to multiple Cisco Powered Service designations - One customer with multiple sites satisfies the requirement for a **single** reference, as the intent is to ensure that the Provider has proven and repeatable service practices - Two customer references are required only once: either with a new Cisco Powered Service application or upon first-year renewal - Use the Customer Reference Validation form to either submit references or to indicate references will be provided upon first year renewal	Customer Reference Validation Form uploaded into the Provider application
D3.PR.2	**Training Evidence** Upload evidence of completion for all Training required for this Cisco Powered Service.	Evidence of training must be uploaded into the Provider application. Refer to requirements in sections D3.SD.11, D3.SD.12, and D3.SP.1 to D3.SP.3.
D3.PR.3	**Included Services** Specify whether you are offering Managed LAN, Managed Wireless LAN (WLAN), or both within the notes section of the Provider application when submitting, or email: certification-team@cisco.com	Selected services must be specified in the Provider application or emailed to certification-team@cisco.com

Service Offer

	Requirement	Evidence
D3.SO.1	**Service Level Agreements** Service performance is committed through having Service-Level Agreements (SLAs) in place between the Provider and End-User which are backed by processes to measure and report on whether those commitments are being met. Service performance elements covered by the SLA may include: • Platform availability: infrastructure, orchestration and service interfaces • Network availability: the network operated by the Provider that is used to provide connectivity from the Internet or private WAN, involved data centers, and/or a third party used to provide network connectivity • Mean Time to Notify (MTTN): MTTN measures the average time taken to notify a customer of an issue with the subscribed service. The measurement encompasses the time that an alert is generated to the time the customer notified, which can be by any method of communication agreed upon with the customer • Mean Time to Restore Service (MTRS): MTRS measures the total elapsed time from the start of a resource outage to the time the service is restored. This is also known as Mean Time to Restore/Repair (MTTR). In some cases, a cloud-based service, brokered by a third party, may not have a platform availability SLA. The Provider must still provide SLA parameters such as MTTN to the customer.	One of: • Executed Service Level Agreement • Service Level Agreement template
D3.SO.2	**Service Requirements** Formal requirements help align the business on a definition of success. These documents, such as a Marketing Requirements Document (MRD) or a Product Requirements Document (PRD) ensure that the various stakeholders' requirements are cataloged and addressed, increasing the likelihood of market success dramatically. The Provider must show evidence of a MRD or PRD for this service. At a minimum, these documents should address: • Target customer segment and clearly defined use cases • Service packaging and pricing structure • Customer value proposition of the service	A table of contents or redacted version of one of: • Marketing Requirements Document (MRD) • Product Requirements Document (PRD) of the service
D3.SO.3	**Service Description** The Service Description is an End-User facing document which explains the service features, benefits, and business outcomes to a potential customer. Typically, a Service Description would include an outline of the different tiers of service such as bronze, silver, or gold, and the features available at each tier.	Service Description document
D3.SO.4	**Artificial Intelligence Operations (AI Ops) Function** **This optional requirement is no longer available. Partners interested in ENAA should evaluate the "Application Dependency Monitoring" use case in CPS 9.2 Full-Stack Observability Designation.**	• Not Applicable

Service Delivery

	Requirement	Evidence
D3.SD.1	**Service Architecture** The Provider must provide a Service Architecture document which describes the key technology components, how they are integrated, and how End-Users access the service. The Provider must also describe how the availability and health of the service is monitored.	Both of: • Service Architecture document • Description of how the availability and health of the service is monitored
D3.SD.2	**WLAN Management** The Provider must offer WLAN management services including: • SSID management including network naming and authentication • Access control policy management • Splash page management • Firewall rules at layer 3 and layer 7 application layer (optional) and • Traffic shaping management (optional) The Provider can make some or all of these management capabilities available for end customer self-service via the Cisco Meraki Dashboard.	*Required if **Managed WLAN** is included (refer to D3.PR.3)* Both of: • Demonstration of how **WLAN Management** capabilities are provided through the managed service • Service Description document reflecting the **WLAN management and reporting** capabilities
D3.SD.3	**WLAN Analytics and Reporting** The Provider must offer WLAN analytics to end customers via the customer service portal. This should include: • Number of visitors, passersby • Capture rate • Time that visitors spent • Number of return visitors • Top clients of the network in terms of traffic • Top applications of the network in terms of amount traffic • Information of devices on the wireless network The Provider must demonstrate these management capabilities as evidence of meeting this requirement. Additionally, these capabilities should be reflected in the Service Description document.	*Required for **Managed WLAN** is included (refer to D3.PR.3)* Both of: • Demonstration of how **WLAN management and reporting** capabilities are provided through the managed service • Service Description document reflecting the **WLAN management and reporting** capabilities

	Requirement	Evidence
D3.SD.4	**LAN Management** The Provider must offer the following management capabilities to customers: • Switch chassis management • Port management • VLAN management • Access control policy management • Switch stacking management The Provider can make some or all of these management capabilities available for end customer self-service. The Provider must demonstrate these management capabilities as evidence of meeting this requirement. Additionally, these capabilities should be reflected in the Service Description document.	*Required for **Managed LAN** is included (refer to D3.PR.3)* Both of: • Demonstration of how **LAN management** capabilities are provided through the managed service • Service Description document reflecting the **LAN management** capabilities
D3.SD.5	**LAN Analytics and Reporting** The Provider must provide analytics and reporting capabilities related to network topology, network usage report at switch, port level including: • Network level usage • Top device by usage • Top clients by usage • Top application by usage • Port level statistics such as top usage, clients and application utilization The Provider must demonstrate these management capabilities as evidence of meeting this requirement. Additionally, these capabilities should be reflected in the Service Description document.	*Required for **Managed LAN** is included (refer to D3.PR.3)* Both of: • Demonstration of **LAN analytics and reporting** capabilities in use via the Meraki Dashboard • Service description referencing the **LAN analytics and reporting** capabilities
D3.SD.6	**Meraki CPE** Cloud Managed Meraki Access Service requires Meraki CPE. The Provider must offer Cloud Managed Meraki Access based on the following CPE, applicable to the services offered (WLAN and/or LAN): • Cisco Meraki MR series products, for managed WLAN • Cisco Meraki MX series products with WiFi capability, for managed WLAN • Cisco Meraki MS product family, for managed LAN Provider must acquire the necessary licenses to operate the CPE.	Demonstration of the use of the required products in the Meraki Dashboard, and the necessary licenses
D3.SD.7	**Software License Management** The Provider must ensure a valid software license is applied to CPE devices used for service delivery. Failure to properly manage the software license expiration could result is a service outage for the customer.	Demonstration of the license management process

	Requirement	Evidence
D3.SD.8	**Proactive Monitoring of the Managed WLAN or Managed LAN Service** The Provider must offer proactive monitoring as part of cloud managed WLAN or LAN service. The access point or switching device is proactively monitored for availability and health from the Provider's operation center rather than waiting for the customer to notify the Provider of a problem. The Provider must provide an operations procedure document or demonstration of the network management systems where the status of end customer devices can be viewed as evidence of meeting this requirement.	One of: • Operations procedure document • Demonstration of the network management systems showing the status of end customer devices
D3.SD.9	**Artificial Intelligence Operations (AI Ops) Function** **This optional requirement is no longer available. Partners interested in ENAA should evaluate the "Application Dependency Monitoring" use case in CPS 9.2 Full-Stack Observability Designation.**	• Not Applicable
D3.SD.10	**Customer Service Portal** The Provider is to offer a secure web portal to present an operational view of the managed service, for multiple audiences, designed to give a view of the network and device status. If the Provider does not provide direct access to the Cisco Meraki Dashboard and/or Meraki APIs, the Provider must provide a third-party portal integrated with the Meraki APIs.	Both of: • Demonstration of the secure web portal • User Guide that includes information on the portal
D3.SD.11	**Deployment Training** Black Belt Meraki Deployment Stage 1, 2, 3 1. Complete **Meraki Deployment Stages 1, 2, and 3**	Email confirmations for Deployment Engineer 1 Email confirmations for Deployment Engineer 2
D3.SD.12	**Support Training** Black Belt Meraki Support Stage 1,2,3 1. Complete **Meraki Support Stages 1, 2, and 3**	Email confirmation for Support Person 1 Email confirmation for Support Person 2

Service Marketing

	Description	Evidence
D3.SM.1	**Digital presence** Most buyers will complete their research online before engaging with the Provider's sales team. Online presence may include a web page, micro site, social media, podcast, and marketing events.	One of: • Demonstrate a service-specific online presence with service specific marketing content, • A marketing plan across various marketing channels and platform

	Description	Evidence
D3.SM.2	**Align digital marketing to the buyer journey** Prospective customers complete the majority of purchasing decision research before engaging a Provider's sales contacts. It is a best practice to ensure that rich digital marketing content with clearly defined use cases is in place through the buyer's journey. This may include a micro web site, social media, podcasts, and interactive marketing events such as webinars.	Buyer Journey Map document

Sales Operations

	Description	Evidence
D3.SP.1	**Cisco Sales Training** Black Belt Meraki Sales Stage 1 1. Select **Stage 1: Sales Associate** 2. Complete **Meraki**	Email confirmation for Sales Person 1 Email confirmation for Sales Person 2
D3.SP.2	**Pre-Sales Engineer Training** Black Belt Meraki Presales Stage 1, 2, 3 1. Complete **Meraki Presales Stages 1, 2, and 3**	Email confirmations for Presales Engineer 1 Email confirmations for Presales Engineer 2
D3.SP.3	**Enterprise Network Assurance for AIOps** **This optional requirement is no longer available. Partners interested in ENAA should evaluate the "Application Dependency Monitoring" use case in CPS 9.2 Full-Stack Observability Designation.**	• Not Applicable
D3.SP.4	**Sales Training** Provider must have a process to formally train both sales and sales engineers for the service	Sales Training Plan document
D3.SP.5	**Sales Enablement** Provider must provide evidence of an **End Customer-facing pitch deck** and at least two of the following sales enablement materials: • Services at-a-glance • Service brochure or video • Battle card/sales reference card • Sales playbook • Call script • Email template • Demo Please reach out to your Cisco Account Team for examples of these materials.	• End Customer-facing pitch deck and at least **two** of: • Services at-a-glance • Service brochure or video • Battle card/sales reference card • Sales playbook • Call script • Email template • Demo

	Description	Evidence
D3.SP.6	**Sales Compensation policy** Provider must have a sales compensation policy that incentivizes and rewards the involved teams for selling the service	Sales Compensation Policy document

Customer Success

	Requirement	Evidence
D3.CS.1	**Customer Success Practice** Customer Success is the function within a Provider organization responsible for managing the relationship between the Provider and its customers. The goals of Customer Success are to: • Maximize customer value • Increase service adoption • Ensure ease of use • Increase customer satisfaction • Drive service renewal For Evidence Option #2 (Customer Success Practice documentation): Provider must demonstrate processes and metrics that support each of the following elements of a customer success practice: • Customer on-boarding and service activation process • Service renewal process • Service renewal rate measurement • Dispute and escalation handling processes • Ongoing customer communications Regular business review process to periodically assess business requirements and change management needs	One of: 1. Customer Success Practice documentation 2. Customer Experience or Advanced Customer Experience Specialization (no further evidence required if the Specialization is held)
D3.CS.2	**User Guide** The User Guide is a document provided to customers showing how to access the customer service portal for self-service capabilities which may include service activation, on-boarding, configuration and reporting for the audited service.	User guide document
D3.CS.3	**Customer Ticketing System** A ticketing system should be in place for tracking customer change requests and system generated incidents. A ticketing system may be part of a larger IT Systems Manager (ITSM) or Customer Relationship Management (CRM) system. Reports from this system should include metrics and summaries of incidents including details such as quantity, status, average time to resolve past incidents, and how the incidents were resolved.	Demonstration of the Customer ticketing system

D6 Secure Access

Introduced: September 2020
Last updated: February 2023

Overview

A Cisco Powered Secure Access Service is a managed local area network (LAN) or managed wireless LAN (WLAN) service that is built on a Cisco DNA secure access network, including switches, APs, and wireless controllers, that are managed by Cisco DNA Center or a Provider network management solution that leverage Cisco DNA Center APIs. Cisco DNA Center is a powerful network management platform that enables network operation automation, visibility, analytics, service assurance, security, software defined access with secure segmentation and policy management.

This designation requires the Provider to offer the secure access as a managed service to End-Users with a clearly defined service description, supported by a service level agreement (SLA), and backed by Cisco DNA trained sales, operation teams, and customer success teams.

Relevant Products:

- DNA Center appliances
- Catalyst 9000 Switches
- Catalyst 9000 Wireless Lan Controllers
- Catalyst 9000 Access Points
- Cisco DNA Software

Prerequisites

	Requirement	Evidence
D6.PR.1	**Customer References** • Reference customers must be under existing contractual relationships • One customer may serve as a reference to multiple Cisco Powered Service designations • One customer with multiple sites satisfies the requirement for a **single** reference, as the intent is to ensure that the Provider has proven and repeatable service practices • Two customer references are required only once: either with a new Cisco Powered Service application or upon first-year renewal • Use the Customer Reference Validation form to either submit references **or** to indicate references will be provided upon first year renewal	Customer Reference Validation Form uploaded into the Provider application

	Requirement	Evidence
D6.PR.2	**Cisco Certifications** The Cisco Certified Network Professional Enterprise certification is for network engineers, systems engineers, and network specialists who are responsible for designing and delivering modernized enterprise network solutions based on Cisco technologies. Each of **two** individuals must have **one** of: • CCNP Enterprise • CCIE Enterprise Infrastructure • CCIE Enterprise Wireless For information, visit Cisco Certifications.	Evidence of one certification for Individual 1 Evidence of one certification for Individual 2
D6.PR.3	**Cisco Networking Specialization (Recommended)** Cisco Master Networking Specialization is the highest level for Cisco Networking solutions, the exclusive Master Networking Specialization will ensure you have the expertise to help your customers manage their business by providing context, visibility, and insight into their networks. Partners will be required to fulfill special requirements for this Master Specialization including a full audit for first time applicants. Partners going through a full audit are required to complete the steps below: Step 1: Pre-Audit • Advanced Enterprise Networks Architecture Specialization (link) • A Networking CCIE • Fire Jumper status in Network Security focus area • Customer References or POVs (Proof of Value) Step 2: Technical Evaluation • After a Cisco Certification Program Manager validates your application, the manager will forward your application to the third-party auditing firm who will contact you to arrange an Evaluation audit date. Normally carried out virtually (Webex) Step 3: Foundation and Sales Onsite Evaluation • After a Cisco Certification Program Manager validates your application, the manager will forward your application to the third-party auditing firm who will contact you to arrange an Evaluation audit date. For information, visit Cisco Partner Architecture Specializations.	Evidence of Cisco Master Networking Specialization must be uploaded into the Provider application.
D6.PR.4	**Training Evidence** Upload evidence of completion for all Training required for this Cisco Powered Service.	Evidence of training must be uploaded into the Provider application. Refer to requirements in sections D6.SD.9, D6.SD.10, and D6.SP.1 to D6.SP.2.

Service Offer

	Requirement	Evidence
D6.SO.1	**Service Level Agreements** Service performance is committed through having Service-Level Agreements (SLAs) in place between the Provider and End-User which are backed by processes to measure and report on whether those commitments are being met. Service performance elements covered by the SLA may include: • Platform availability: infrastructure, orchestration, and service interfaces • Network availability: the network operated by the Provider that is used to provide connectivity from the Internet or private WAN, involved data centers, and/or a third party used to provide network connectivity • Mean Time to Notify (MTTN): MTTN measures the average time taken to notify a customer of an issue with the subscribed service. The measurement encompasses the time that an alert is generated to the time the customer notified, which can be by any method of communication agreed upon with the customer • Mean Time to Restore Service (MTRS): MTRS measures the total elapsed time from the start of a resource outage to the time the service is restored. This is also known as Mean Time to Restore/Repair (MTTR). In some cases, a cloud-based service, brokered by a third party, may not have a platform availability SLA. The Provider must still provide SLA parameters such as MTTN to the customer.	One of: • Executed Service Level Agreement • Service Level Agreement template
D6.SO.2	**Service Requirements** Formal requirements help align the business on a definition of success. These documents, such as a Marketing Requirements Document (MRD) or a Product Requirements Document (PRD) ensure that the various stakeholders' requirements are cataloged and addressed, increasing the likelihood of market success dramatically. The Provider must show evidence of a MRD or PRD for this service. At a minimum, these documents should address: • Target customer segment and clearly defined use cases • Service packaging and pricing structure • Customer value proposition of the service	A table of contents or redacted version of one of: • Marketing Requirements Document (MRD) • Product Requirements Document (PRD) of the service
D6.SO.3	**Service Description** The Service Description is an End-User facing document which explains the service features, benefits, and business outcomes to a potential customer. Typically, a Service Description would include an outline of the different tiers of service such as bronze, silver, or gold, and the features available at each tier.	Service Description document

	Requirement	Evidence
D6.SO.4	**Managed Service Tiers (optional)** The Provider may offer several tiers of managed LAN/WLAN services, which may include the following options: • infrastructure design and deployment service • Cisco DNA Advantage or Premier licenses to provide Assurance services such as network health, device health, client health and application performance • software defined access (SD-Access) with secure segmentation Provider must provide infrastructure management services including inventory management, infrastructure status monitoring, technical support, and software image management	*Optional* Service Description document
D6.SO.5	**Artificial Intelligence Operations (AI Ops) Function (optional)** This optional requirement is no longer available. Partners interested in ENAA should evaluate the "Application Dependency Monitoring" use case in CPS 9.2 Full-Stack Observability Designation.	*Not Applicable*

Service Delivery

	Requirement	Evidence
D6.SD.1	**Service Architecture** The Provider must provide a Service Architecture document which describes the key technology components, how they are integrated, and how End-Users access the service. The document shall also describe how the availability and health of the service is monitored by the Provider and how the service is based on Cisco Catalyst switches, APs, Wireless LAN Controller (WLCs) and Cisco DNA Center.	Service Architecture document
D6.SD.2	**Proactive Management** Provider must proactively monitor the devices and platforms that comprise the managed service. The APs, WLCs, switches, or DNA Center appliances must be monitored for availability and health from the Provider's operation center, rather than only reacting when an End Customer notifies the Provider of a problem.	One of: • Demonstration of the Network Management System (NMS) used to monitor the End-User environments • Demonstration of the operational processes related to the practice
D6.SD.3	**Device Inventory Reporting** The Provider must provide End Customers with reports of services relevant to the devices under management.	One of: • Screen shots of the reports • Demonstration of the reporting platform

	Requirement	Evidence
D6.SD.4	Enterprise Network Assurance for AIOps (Optional) **This optional requirement is no longer available. Partners interested in ENAA should evaluate the "Application Dependency Monitoring" use case in CPS 9.2 Full-Stack Observability Designation.**	*Not Applicable*
D6.SD.5	**Cisco Infrastructure** The managed LAN or managed WLAN service must be based on Cisco switching and wireless infrastructure with Cisco DNA software. At a minimum, a valid Cisco DNA Essential subscription license is required for the network devices within this service offering.	Demonstration of the use of the required products in the DNA Center and the necessary licenses
D6.SD.6	**Cisco DNA Center** The managed service must be delivered with Cisco DNA Center to manage the infrastructure	Service Architecture Document
D6.SD.7	**Secure Management Platform** When the Provider manages the network via on-prem DNA Center or hosted DNA Center, proper security must be in place to protect the management such as using a firewall to protect the DNA Center and the management network.	Service Architecture Document illustrating the security practice
D6.SD.8	**Secure Web Portal** The Provider must offer a secure web portal to present an operational view of the managed service, for multiple audiences, designed to give a view of the network and device status.	Demonstration of the secure web portal to communicate network and device status
D6.SD.9	**Deployment Training (Required)** Black Belt Switching Deployment - Stages 1, 2, and 3 1. In **All Technology** dropdown, Select **Switching** 2. Complete **Switching Deployment Stages 1, 2, and 3** Black Belt Wireless Deployment - Stages 1, 2, and 3 1. In **All Technology** dropdown, Select **Wireless** 2. Complete **Wireless Deployment Stages 1, 2, and 3** Black Belt DNA Deployment - Stages 1, 2, and 3 1. In **All Technology** dropdown, Select **Cisco DNA** 2. Complete **DNA Deployment Stages 1, 2, and 3** **Exception: Cisco Master Networking Specialization requirements in section D6.PR3 may be substituted Cisco Black Belt training requirements in this section.**	One of: • Email Confirmation for Deployment Person 1 • Cisco Master Networking Specialization in section D6.PR3

	Requirement	Evidence
D6.SD.10	**Support Training (Required)** Black Belt Switching Support - Stages 1, 2, and 3 1. In **All Technology** dropdown, Select **Switching** 2. Complete **Switching Support Stages 1, 2, and 3** Black Belt Wireless Support - Stages 1, 2, and 3 1. In **All Technology** dropdown, Select **Wireless** 2. Complete **Wireless Support Stages 1, 2, and 3** Black Belt DNA Presales - Stages 1, 2, and 3 1. In **All Technology** dropdown, Select **Cisco DNA** 2. Complete **DNA Support Stages 1, 2, and 3** **Exception: Cisco Master Networking Specialization requirements in section D6.PR3 may be substituted Cisco Black Belt training requirements in this section.**	One of: - Email Confirmation for Support Person 1 - Cisco Master Networking Specialization in section D6.PR3

Service Marketing

	Description	Evidence
D6.SM.1	**Digital presence** Most buyers will complete their research online before engaging with the Provider's sales team. Online presence may include a web page, micro site, social media, podcast, and marketing events.	One of: - Demonstrate a service-specific online presence with service specific marketing content, - A marketing plan across various marketing channels and platform
D6.SM.2	**Align digital marketing to the buyer journey** Prospective customers complete the majority of purchasing decision research before engaging a Provider's sales contacts. It is a best practice to ensure that rich digital marketing content with clearly defined use cases is in place through the buyer's journey. This may include a micro web site, social media, podcasts, and interactive marketing events such as webinars.	Buyer Journey Map document

Sales Operations

	Description	Evidence
D6.SP.1	**Cisco Sales Training (Required)** Black Belt - EN Sales Stage 1 1. Select **Stage 1: Sales Associate** 2. Complete **IBN** under **Enterprise Networking** **Exception: Cisco Master Networking Specialization requirements in section D6.PR3 may be substituted Cisco Black Belt training requirements in this section.**	One of: • Email Confirmation for Sales Person 1 • Cisco Master Networking Specialization in section D6.PR3
D6.SP.2	**Pre-Sales Engineer Training (Required)** Black Belt Switching Presales - Stages 1, 2, and 3 1. In **All Technology** dropdown, Select **Switching** 2. Complete **Switching Pre-Sales Stages 1, 2, and 3** Black Belt Wireless Presales - Stages 1, 2, and 3 1. In **All Technology** dropdown, Select **Wireless** 2. Complete **Wireless Pre-Sales Stages 1, 2, and 3** Black Belt DNA Presales - Stages 1, 2, and 3 1. In **All Technology** dropdown, Select **Cisco DNA** 2. Complete **DNA Pre-Sales Stages 1, 2, and 3** **Exception: Cisco Master Networking Specialization requirements in section D6.PR3 may be substituted Cisco Black Belt training requirements in this section.**	One of: • Email Confirmation for Pre-Sales Person 1 • Cisco Master Networking Specialization in section D6.PR3
D6.SP.3	**Enterprise Network Assurance for AIOps Sales Training (Optional)** **This optional requirement is no longer available. Partners interested in ENAA should evaluate the "Application Dependency Monitoring" use case in CPS 9.2 Full-Stack Observability Designation.**	*Not Applicable*
D6.SP.4	**Sales Training** Provider must have a process to formally train both sales and sales engineers for the service	Sales Training Plan document

	Description	Evidence
D6.SP.5	**Sales Enablement** Provider must provide evidence of an **End Customer-facing pitch deck** and at least two of the following sales enablement materials: • Services at-a-glance • Service brochure or video • Battle card/sales reference card • Sales playbook • Call script • Email template • Demo Please reach out to your Cisco Account Team for examples of these materials.	• End Customer-facing pitch deck and at least **two** of: • Services at-a-glance • Service brochure or video • Battle card/sales reference card • Sales playbook • Call script • Email template • Demo
D6.SP.6	**Sales Compensation policy** Provider must have a sales compensation policy that incentivizes and rewards the involved teams for selling the service	Sales Compensation policy document

Customer Success

	Requirement	Evidence
D6.CS.1	**Customer Success Practice** Customer Success is the function within a Provider organization responsible for managing the relationship between the Provider and its customers. The goals of Customer Success are to: • Maximize customer value • Increase service adoption • Ensure ease of use • Increase customer satisfaction • Drive service renewal For Evidence Option #2 (Customer Experience or Advanced Customer Experience Specialization): Provider must demonstrate processes and metrics that support each of the following elements of a customer experience practice: • Customer on-boarding and service activation process • Service renewal process • Service renewal rate measurement • Dispute and escalation handling processes • Ongoing customer communications • Regular business review process to periodically assess business requirements and change management needs	One of: 1. Customer Success Practice documentation 2. Customer Experience or Advanced Customer Experience Specialization (no further evidence required if the Specialization is held)

	Requirement	Evidence
D6.CS.2	**User Guide** A User Guide is a document provided to customers showing how to access the customer service portal for self-service capabilities which may include service activation, on-boarding, configuration and reporting for the audited service.	User guide document
D6.CS.3	**Customer Ticketing System** A ticketing system should be in place for tracking customer change requests and system generated incidents. A ticketing system may be part of a larger IT Systems Manager (ITSM) or Customer Relationship Management (CRM) system. Reports from this system should include metrics and summaries of incidents including details such as quantity, status, average time to resolve past incidents, and how the incidents were resolved.	Demonstration of the Customer ticketing system

D7 Webex for BroadWorks

Introduced: September 2020
Last updated: August 2021

Overview

Webex for BroadWorks is a brandable, strategic collaboration app available through Providers. Webex for BroadWorks leverages the full range of Webex technology, including Webex Meetings and Webex Teams messaging, combined with the Provider's BroadWorks call control to deliver a complete modern collaboration solution in a single unified app. The unified client that provides all the necessary collaboration capabilities is Webex Teams.

Webex for BroadWorks is delivered to Providers in three flexible packages that range from a Basic softphone and messaging package up to a Premium package that provides meetings for up to 200 users. Providers will manage, provision, support and administer the service on behalf of their customers through Cisco's Webex Control Hub platform. Webex for BroadWorks is optimized for the SMB customer from a price and feature perspective.

The Cisco Powered Webex for BroadWorks designation is defined as a managed collaboration service that is based on the Webex for BroadWorks offer, where the call control is hosted by the service provider's BroadWorks calling platform while messaging, meetings and soft phone capabilities are delivered from the Cisco Webex cloud.

Prerequisites

	Requirement	Evidence
D7.PR.1	**Customer References** • Reference customers must be under existing contractual relationships • One customer may serve as a reference to multiple Cisco Powered Service designations • One customer with multiple sites satisfies the requirement for a single reference, as the intent is to ensure that the Provider has proven and repeatable service practices • Two customer references are required only once: either with a new Cisco Powered Service application or upon first-year renewal • Use the Customer Reference Validation form to either submit references or to indicate references will be provided upon first year renewal	Customer Reference Validation Form uploaded into the Provider application

	Requirement	Evidence
D7.PR.2	**Cisco Certifications** Cisco Certified individuals are responsible for designing and delivering modernized network solutions based on Cisco technologies. The Provider is required to have **two** staff members who **each** meet **both** of the requirements: • Webex for BroadWorks Administration • Webex for BroadWorks Sales Refer to Webex Education Catalog for Partners for more information.	Evidence of certification for Individual 1
		Evidence of certification for Individual 2
D7.PR.3	**Training Evidence** Upload evidence of completion for all Training required for this Cisco Powered Service.	Evidence of training must be uploaded into the Provider application. Refer to requirements in section D7.SP.2.

Service Offering

	Requirement	Evidence
D7.SO.1	**Service Level Agreement** Service performance is committed through having Service-Level Agreements (SLAs) in place between the Provider and End-User which are backed by processes to measure and report on whether those commitments are being met. Service performance elements covered by the SLA may include: • Platform availability: infrastructure, orchestration, and service interfaces • Network availability: the network operated by the Provider that is used to provide connectivity from the Internet or private WAN, involved data centers, and/or a third party used to provide network connectivity • Mean Time to Notify (MTTN): MTTN measures the average time taken to notify a customer of an issue with the subscribed service. The measurement encompasses the time that an alert is generated to the time the customer notified, which can be by any method of communication agreed upon with the customer • Mean Time to Restore Service (MTRS): MTRS measures the total elapsed time from the start of a resource outage to the time the service is restored. This is also known as Mean Time to Restore/Repair (MTTR). In some cases, a cloud-based service, brokered by a third party, may not have a platform availability SLA. The Provider must still provide SLA parameters such as MTTN to the customer.	One of: • Executed Service Level Agreement • Service Level Agreement template

	Requirement	Evidence
D7.SO.2	**Service Requirements** Formal requirements help align the business on a definition of success. These documents, such as a Marketing Requirements Document (MRD) or a Product Requirements Document (PRD) ensure that the various stakeholders' requirements are cataloged and addressed, increasing the likelihood of market success dramatically. The Provider must show evidence of a MRD or PRD for this service. At a minimum, these documents should address: • Target customer segment and clearly defined use cases • Service packaging and pricing structure • Customer value proposition of the service	A table of contents or redacted version of one of: • Marketing Requirements Document (MRD) • Product Requirements Document (PRD) of the service
D7.SO.3	**Service Description** The Service Description is an End-User facing document which explains the service features, benefits, and business outcomes to a potential customer. Typically, a Service Description would include an outline of the different tiers of service such as bronze, silver, or gold, and the features available at each tier. For Cisco Powered Webex for BroadWorks this would include calling, messaging, and meeting capabilities, and perhaps advanced collaboration features such as wireless device pairing and sharing.	Service Description document

Service Delivery

	Requirement	Evidence
D7.SD.1	**Service Architecture** The Provider must provide a Service Architecture document which describes the key technology components, how they are integrated, and how End-Users access the service. The Provider must provide an architecture design as evidence of this requirement. The Provider must also describe how the availability and health of the service is monitored.	Service Architecture document
D7.SD.2	**Utilize the Webex Teams application to deliver an improved customer experience** The Webex for BroadWorks service is consumed by End-Users via the Cisco Webex Teams unified application. Webex Teams supports calling via the Provider's BroadWorks implementation, messaging, meetings, device pairing and wireless sharing. The Provider may co-brand the app using their colors and logo.	Demonstration of using the Webex Teams application leveraging Webex for BroadWorks Platform

	Requirement	Evidence
D7.SD.3	**Cisco Collaboration devices (optional)** The Provider shall include Cisco devices with this service such as Cisco IP Phone Models 6800, 7800 and 8800 with Multiplatform firmware, 500 Series Headsets, personal video devices, or room kits.	*Optional* Demonstration of Devices working with BroadWorks Platform
D7.SD.4	**Bring your own PSTN for meeting dial in numbers** The Provider must provide its own PSTN for the meeting so the meeting guests can join the audio via PSTN.	Network Diagram including PSTN Integration
D7.SD.5	**Integration of Provider's BroadWorks calling platform with Cisco Webex** The Provider must follow the Cisco Webex integration guide and be responsible for the integration of its Cisco BroadWorks calling platform with Cisco Webex. This shall be shown in a technical document such as an Operational Processes and Procedures Runbook. The Provider must share this document, a portion of this document, or the table of contents of this document as evidence of meeting this requirement.	One of: • technical document • portion of document • table of contents of document showing the technical integration
D7.SD.6	**Meet documented security requirements** The Provider must meet XSP security requirements listed in the Webex for BroadWorks Solution Guide, including: • Using CA-signed certificate to authenticate clients • Support for TLS v1.2 • Using a proper cipher suite (DHE, ECDHE, AES, GCM).	Screenshot of the command line view that demonstrates the requirements have been met
D7.SD.7	**Protect the environment with a network firewall** The Provider shall follow the Webex for BroadWorks Solution Guide to setup proper firewall policy to allow communication between the Cisco Webex Teams clients, Provider's network and the Cisco Webex cloud.	Service Architecture document indicating the use of high availability firewalls
D7.SD.8	**Perform testing and validate service readiness in a staging environment** The Provider must follow the staging process described in Cisco Webex Reseller Guide and demonstrate this in an integration plan.	Integration plan
D7.SD.9	**Provide End-User support** Provider is responsible for providing the first line of support for WebEx for BroadWorks. There shall be support staff resources in place and support contact information for this service published to End Users. Providers must have a process documented to go through basic trouble isolation procedures including: receiving support request from End Users, conducting preliminary diagnosis, utilizing tools provided by Webex for BroadWorks for initial troubleshooting and problem resolution.	Document describing how first line support staff members are trained
D7.SD.10	**Secure web portal to communicate status and performance** The Provider must employ a secure portal to present End Users with a service status view.	Demonstration of the secure web portal

Service Marketing

	Description	Evidence
D7.SM.1	**Digital presence** Most buyers will complete their research online before engaging with the Provider's sales team. Online presence may include a web page, micro site, social media, podcast, and marketing events.	One of: • Demonstrate a service-specific online presence with service specific marketing content • A marketing plan across various marketing channels and platform
D7.SM.2	**Align digital marketing to the buyer journey** Prospective customers complete the majority of purchasing decision research before engaging a Provider's sales contacts. It is a best practice to ensure that rich digital marketing content with clearly defined use cases is in place through the buyer's journey. This may include a micro web site, social media, podcasts, and interactive marketing events such as webinars.	Buyer Journey Map document

Sales Operations

	Description	Evidence
D7.SP.1	**Sales Training** To successfully sell a Cisco Powered Webex for BroadWorks service, a Provider must gain the confidence and motivation of their sales force. The Provider must demonstrate that it has a sales training process in place for the Webex for BroadWorks as evidence of meeting this requirement. This process should include: • A process to formally train both sales and sales engineers (SEs) specific to this service • A demonstration training process for SEs to show potential customers the experience	Sales Training Plan document
D7.SP.2	**Cisco Sales Training** Completion of Webex for BroadWorks Sales training and provide the proof of completion of training course Refer to Cisco BroadSoft Training Certifications for more information.	Evidence of course completion for one individual

	Description	Evidence
D7.SP.3	**Sales Enablement** Provider must provide evidence of at least **two** of the following sales enablement materials: • Battle card • Call script • Email template • Demo portal • Demo video	**Two** sales enablement materials
D7.SP.4	**Sales Compensation policy** Provider must have a sales compensation policy that incentivizes and rewards the involved teams for selling the service	Sales Compensation policy document

Customer Success

	Requirement	Evidence
D7.CS.1	**Customer Success Practice** Customer Success is the function within a Provider organization responsible for managing the relationship between the Provider and its customers. The goals of Customer Success are to: • Maximize customer value • Increase service adoption • Ensure ease of use • Increase customer satisfaction • Drive service renewal Provider must demonstrate processes and metrics that support each of the following elements of a customer success practice: • Customer on-boarding and service activation process • Service renewal process • Service renewal rate measurement • Dispute and escalation handling processes • Ongoing customer communications Regular business review process to periodically assess business requirements and change management needs	Customer Success Practice document
D7.CS.2	**User Guide** The User Guide is a document provided to customers showing how to access the customer service portal for self-service capabilities which may include service activation, on-boarding, configuration, and reporting for the audited service.	User guide document

	Requirement	Evidence
D7.CS.3	**Customer Ticketing System** A ticketing system should be in place for tracking customer change requests and system generated incidents. A ticketing system may be part of a larger IT Systems Manager (ITSM) or Customer Relationship Management (CRM) system. Reports from this system should include metrics and summaries of incidents including details such as quantity, status, average time to resolve past incidents, and how the incidents were resolved.	Demonstration of the Customer ticketing system

D2 Cloud Managed Security

Introduced: May 2014
Last Updated: May 2022

Overview

Cloud Managed Security uses a multi-tenant cloud infrastructure to host a suite of managed security services. Requirements in this section include solution requirements and service offering requirements that must be met by a Provider to obtain the Cisco Powered designation.

Cloud Managed Security allows the Provider to leverage Cisco cloud offerings and create and manage flexible, dynamic pools of physical and virtual security appliances that can be shared efficiently and securely among multiple tenants. It also provides orchestration to reduce resource provisioning and improves time to market for managed security services.

Cloud Managed Security is based on Cisco security technologies and provides a Provider the opportunity to create subscription-based “as a service” offers utilizing hosted and managed models. The Provider can monetize Cisco’s broad portfolio of security products, streamline operations with a complete management system, optimize their capital investments in the data center, on customer premises, and hosted SaaS offerings, to assure the highest security and for their customers.

Relevant Products:

- Secure Email Cloud Mailbox (formerly Email Security)
- Umbrella DNS Security
- Umbrella SIG Essentials
- Umbrella SIG Advantage
- Secure Endpoint (formerly AMP for Endpoints)
- Secure Network Analytics (formerly Stealthwatch)
- Secure Cloud Analytics (formerly Stealthwatch Cloud)
- Secure Malware Analytics (Threat Grid)
- Secure Web Appliance (WSA or WSAv)
- Firepower product family
- ASA product family
- Next-generation firewall (NGFW)

D2.1 Prerequisites

The Provider must meet the following prerequisites to apply for this service designation.

Requirement	Description
D2.1.1 Submit at least two customer references for the service.	Reference Customers • Reference customers must be under existing contractual relationships • One customer may serve as a reference to multiple designations • One customer with multiple sites satisfies the requirement for a single reference, as the intent is to ensure that the Provider has proven and repeatable service practices • Two customer references are required only once: either with a new service application or upon first-year renewal • Use the Customer Reference Validation form to either submit references or to indicate references will be provided upon first year renewal Evidence: Customer Reference Validation Form uploaded into the Provider application.
D2.1.2 Maintain at least one CCNP Security certified individual on staff	The Cisco CCNP Security certification validates advanced knowledge and skills required to secure Cisco networks. A Cisco CCIE certification, of any technology specialization, supersedes and fulfills the certification requirements for this service. For more information, see Cisco Certifications.

D2.2 Service Design (Build)

The following section describes the key requirements needed to deliver Cloud Managed Security services, which include a range of services that a Provider can deliver using Cisco's rich security product portfolio and cloud-based orchestration and management at scale.

Requirement	Description
D2.2.1 Provide the following documents unique to the service: • Service-level agreement (SLA) • Marketing Service Description (MSD) • Architecture Diagram	Service performance is monitored through having Service-Level Agreements (SLAs) in place and effective processes to measure and report on whether they are being met. The Provider must provide an actual SLA with an existing customer or SLAs for multiple customers. Please refer to section D2.3 for the detailed requirements. The Marketing Service Description is a document produced by the Provider that describes the service capabilities, service packages and benefits it provides. The MSD must be a published document. The architectural diagram(s) must show how the service delivery components are connected along with how a customer will gain access to services via network connectivity.

Requirement	Description
D2.2.2 Dedicated Security Operations Center (SOC)	Provider must document the operation of a Security Operations Center (SOC) for incident prevention, detection, and response capabilities. Provider can also use a 3rd party white label SOC provider. In this case, the sub-contracted SOC provider must participate in the audit. The Provider must provide documentation of security event detection, escalation, and remediation processes consistent with their SLA. The Provider must also show evidence of people, processes, and tools specific to the SOC. Each of these should be distinct from the Network Operations Center.
D2.2.3 Cloud Orchestration Software	Policy deployment and service orchestration at scale and not on a device-by-device basis are core capabilities of Cloud Managed Security Services. A Service Provider may deploy the cloud orchestration software in its data center or consume such capabilities from the cloud to orchestrate the service capabilities defined in D2.2.1. It provides service management and configuration, zero-touch deployment of CPE or datacenter virtualized appliances, and policy management and deployment to those appliances. Examples of this functionality could be provided by Cisco Network Services Orchestrator (NSO), Cisco Defense Orchestrator (CDO), Cisco Firepower Management Console (FMC), and Service Provider or third-party software.

Requirement	Description
D2.2.4 Must offer at least two Cisco-based security services	The Cloud Managed Security services are aimed at Providers offering a range of security capabilities to protect their customer from a variety of security threats. The Provider must deliver a minimum of two of the following services: • Firewall as a Service • Managed Cloud Firewall *using Umbrella SIG* • Next Generation Firewall as a Service • Web Security as a Service • Managed Web Security *using Umbrella SIG* • Email Security as a Service • DNS Monitoring Service *using Umbrella DNS* • DNS Monitoring Service *using Umbrella SIG* • Managed Endpoint Security • Secure Cloud Analytics • VPN as a Service Services must be delivered using any of the following: • Secure Email Cloud Mailbox (formerly Email Security) • Umbrella DNS Security • Umbrella SIG Essentials • Umbrella SIG Advantage • Secure Endpoint (formerly AMP for Endpoints) • Secure Network Analytics (formerly Stealthwatch) • Secure Cloud Analytics (formerly Stealthwatch Cloud) • Secure Malware Analytics (Threat Grid) • Secure Web Appliance (WSA or WSAv) • Firepower product family • ASA product family • Next-generation firewall (NGFW)

D2.2.4 Firewall as a Service

The following section describes the basic functions of the Firewall as a Service offering. The Provider must provide evidence of the firewall service capabilities and explain the key benefits of the service and how it can be used to block traffic from the Internet into the customer network.

Requirement	Description
D2.2.4.1 Support for Network Address Translation (NAT)	Network Address Translation allows hiding of internal addressing, also known as obfuscation. This prevents external attackers from guessing the internal addressing and attempting to access those devices. It enables private IP networks that use unregistered IP addresses to connect to the Internet. NAT operates on the firewall; usually connecting two networks together and translates the private (not globally unique) addresses in the internal network into legal addresses, before packets are forwarded to another network. As part of this capability, NAT can be configured to advertise only one address for the entire network to the outside world. This provides additional security by effectively hiding the entire internal network behind that address.
D2.2.4.2 Support for De-Militarized Zones (DMZs) *(optional)*	This security service option is only applicable when Service Providers are delivering or plan to deliver value added security services such as web security as a service, email protection as a Service. Virtual security appliances will be provisioned in the DMZ for the delivery of these services.
Stateful Inspection The following section describes key stateful firewall features that provide advanced protection of the data traversing the firewall. Direct demonstration of the stateful inspection features can be provided as evidence. The Provider may also show a customer portal with the ability to configure these parameters or provide examples of customer designs that incorporate these capabilities. If the market segment in which the service is offered does not yet demand this capability from a firewall service, the Provider will need to show that they will have the required expertise to implement these features when demanded by the market by explaining the value of the feature and how it is delivered on the related Cisco technology.	
D2.2.4.3 Stateful firewall inspection engine	Stateful firewall inspection tracks the state of a flow or connection in order to allow legitimate traffic to pass through from the Internet to the corporate network. A “stateful” firewall capability permits this by monitoring established connections from the internal network to the Internet and only allowing traffic through if this is the case. This requires monitoring not just at the packet level but also the state of a flow or connection. An example of this for TCP is to monitor for synchronization (SYN) and SYN-ACK messages to check if a connection is established. Evidence of stateful firewall inspection engine can be demonstrated using a TCP session emulator. Or having the TCP client and agent on either side of the firewall to generate the necessary TCP packets to be able to show that the firewall is working effectively to block TCP traffic that is not part of a session generated from within the internal network.
D2.2.4.4 Support for user-based policy authentication *(optional)*	User-based policy authentication is a security service option that allows network administrators to create specific security policies for each user with dynamic, per-user authentication and authorization. Per-user policy can now be downloaded dynamically to the virtual appliance from a Terminal Access Controller Access Control System (TACACS+) or Remote Authentication Dial-In User Service (RADIUS) authentication server using authentication, authorization, and accounting (AAA) services. Users can log into the cloud services or onto the Internet via HTTP, and their specific access profiles will automatically be downloaded. Appropriate dynamic individual access privileges are available as required, protecting against more general policy that is applied across multiple users.

Requirement	Description
Application Inspection and Control The following section describes capabilities offered by the service to enable more effective control of applications traversing the firewall. Direct demonstration of the application-centric features can be provided as proof of support. The Provider may also show a customer portal with the ability to configure these parameters or provide examples of customer designs that incorporate these capabilities. If the market segment in which the service is offered does not yet demand this capability from a firewall service, the Provider will need to show that they will have the required expertise to implement these features when demanded by the mark.	
D2.2.4.5 Instant Messenger (IM) blocking *(optional)*	Instant Messenger blocking offers per-service control to block or allow instant messaging applications. It allows service restriction to text chat only, blocking voice and video chat and file transfer.
D2.2.4.6 Peer-to-peer control *(optional)*	Peer-to-peer control individually blocks access to BitTorrent, Gnutella, KaZaA, and eDonkey file-sharing networks.
D2.2.4.7 Protocol conformance checking	Enforces protocol conformance for HTTP, Simple Mail Transfer Protocol (SMTP), Extended SMTP (ESMTP), Internet Mail Access Protocol (IMAP), and Post Office Protocol 3 (POP3). It facilitates detection and prevention of unwanted traffic on desired application service ports.
D2.2.4.8 Inspect Internet Control Message Protocol (ICMP)	Allows responses to ICMP packets (i.e., ping and traceroute) originating from inside the firewall to return through while still denying other ICMP traffic.
Voice Security Features Support (Optional) The following section describes capabilities for managing the flow of IP-based voice traffic across the firewall. When delivering Unified Communication as a Service (UCaaS) based on HCS to customers from the same service architecture, the Provider must exhibit an understanding of the capabilities and ensure they are activated.	
D2.2.4.9 Session Initiation Protocol (SIP) inspection	SIP inspection is described in RFC 2543 and RFC 3261, which are both used by Cisco HCS. The SIP inspect functionality provides SIP packet inspection and pinhole opening (allowing traffic through the firewall for the duration of a session) as well as checking for protocol conformance and application security, giving the users a more granular control on what policies and security checks to apply to SIP traffic.
D2.2.4.10 Skinny local traffic support	Skinny Client Control Protocol (SCCP) is a protocol used in VoIP networks between Cisco IP phone and Cisco HCS. Skinny application inspection help ensures that all SCCP signaling, and media packets can traverse the security device.
D2.2.4.11 H.323 V1 to V4 support	H.323 inspection provides support for H.323 compliant applications such as Cisco Unified Communications Manager. The security appliance supports H.323, Version 1 through Version 4, including H.323 v3 feature Multiple Calls on One Call Signaling Channel. With H323 inspection enabled, the security appliance supports multiple calls on the same call signaling channel, a feature introduced with H.323 Version 3 to reduce call setup time. The two major functions of H.323 inspection are as follows: • Network Address Translation (NAT): the necessary embedded IPv4 addresses in the H.225 and H.245 messages • Dynamically allocate the negotiated H.245 and RTP/RTCP connections

Requirement	Description
Availability The following section describes features that can be incorporated into the design of the service for a customer if there is a requirement to enhance the availability of the service or a particular site. Showing the features that are incorporated into the service can exhibit these requirements or evidence can be provided in a published service description that includes the required features.	
D2.2.4.12 Dual firewall support with stateful failover *(optional)*	Stateful failover enables the firewall to continue processing and forwarding session packets after a planned or unplanned outage occurs. A backup (secondary) firewall is employed that automatically takes over the tasks of the active (primary) firewall if the active firewall loses connectivity for any reason. This process is transparent and does not require adjustment or reconfiguration of any remote peer.
D2.2.4.13 Configuration backup	Storage of configurations of all virtual devices used in the firewall service with ability to provide restoration. Provider must demonstrate how configuration backup statuses are monitored and existence of processes for restoring configurations when required.
Customer Premises Equipment (CPE) The following section describes operational procedures that must be incorporated as best practices for the design and implementation of service delivered from Cisco CPE, such as ISR and ASR Series router, Cisco ASA, Firepower appliances, CSP2100, or ENCS. Example best practices documents are available in the Cisco Guide to Harden IOS Devices. The Provider must provide evidence that these procedures are being followed. This can be proven by a demonstration of the features being used or by presenting a design and implementation guide that incorporates these capabilities and is shown to be in use. The following requirements must be met if using a Cisco IOS platform.	
D2.2.4.14 Management Plane Security	The management plane provides access, configuration, and management of a device, as well as monitors its operations and the network on which it is deployed. The Provider must provide evidence of the operational procedures in place to protect the device management plane.
D2.2.4.15 Data Plane Security	The data plane is responsible for moving data from source to destination. The Provider must provide evidence of the operational procedures in place to protect the device data plane.
D2.2.4b Managed Cloud Firewall using Umbrella SIG	
Service Delivery requirements	
D2.2.4b.1 Directing Traffic to Cisco Umbrella Secure Internet Gateway	Provider must explicitly direct customer traffic to the Umbrella cloud by pointing network traffic to an Umbrella head-end IP Address. Provider must provide evidence that customer traffic is being directed to the Cisco Umbrella cloud service through one of: • Demonstration • Service Description Document • Service Architecture Documentation

Requirement	Description
D2.2.4b.2 Firewall Services	The Umbrella cloud-delivered firewall provides visibility and control for traffic that originated from requests going to the internet, across all ports and protocols. Cloud firewall protection provides: • Deployment, management, and reporting through the Umbrella single, unified dashboard • Customizable policies (IP, port, protocol, application and IPS policies) • Layer 3/4 firewall to log all activity and block unwanted traffic using IP, port, and protocol rules • Intrusion prevention system (IPS)* to examine network traffic flows and prevent vulnerability exploits with an added layer of threat prevention using SNORT 3 technology and signature-based detection. • Detection and blocking of vulnerability exploitation • Scalable cloud compute resources eliminate appliance capacity concerns • Cisco Talos threat intelligence to detect and block more threats Provider must provide evidence that its Managed Cloud Firewall offer uses Cisco Umbrella for L3/4 cloud delivered firewall service through **both** of: • Evidence of the firewall service capabilities such as: ◦ Policy settings ◦ Report ◦ SLA agreements ◦ Service Description Document ◦ Service Architecture Document • Explanation of the key benefits of the service and how it can be used to block traffic from the Internet into the customer network
D2.2.4b.3 Application Inspection and Control	**ICMP Inspection** (required) Allows responses to ICMP packets (i.e., ping and traceroute) originating from inside the firewall to return through while still denying other ICMP traffic. **IM blocking** *(optional)* Instant Messenger blocking offers per-service control to block or allow instant messaging applications. It allows service restriction to text chat only, blocking voice and video chat and file transfer. **P2P controls** *(optional)* Peer-to-peer control individually blocks access to P2P services such as the BitTorrent, Gnutella, KaZaA, and eDonkey file-sharing networks. Provider must demonstrate the Application Inspection and Control capabilities: • The Provider may also show a customer portal with the ability to configure these parameters or provide examples of customer designs that incorporate these capabilities. • If the market segment in which the service is offered does not yet demand this capability from a firewall service, the Provider will need to show that they will have the required expertise to implement these features when demanded

Requirement	Description
D2.2.4b.4 Network Tunnel Failover	Cisco Umbrella implements automatic failover of IPsec tunnels when a data center is unavailable. When this occurs, tunnels automatically move from one data center in a region to the other. Provider must show evidence of tunnel failover support via **one** of: • Demonstration • Service Description Document • Service Architecture Document
D2.2.4b.5 Two Factor Authentication	It is considered a best practice to enable two-factor authentication for access to the Umbrella Secure Internet Gateway administrative dashboard. Two-step verification is the ability to add a second factor of authentication to your login. This combines something you know (your password) with something you have (your mobile phone), and whenever you log into your account, you'll need to enter both your password and a security code from your mobile device Provider must demonstrate that two-factor enabled dashboard administrator login is enabled.
D2.2.5 Email Security as a Service The following section describes the basic functions of Email Security as a service offering. The Provider must provide evidence of the email protection service capabilities and explain the key benefits of the service and how it can be used to protect email servers and email content. The protection service can be delivered to protect email servers located at the customer's premises or to protect email services hosted in the Service Provider's cloud. This service may be delivered via Cisco Secure Email.	
D2.2.5.1 Reputation scoring and anti-spam	Internet abusers constantly evolve techniques to penetrate an organization's defenses. Email threats have expanded beyond simply annoying unwanted marketing email messages to dangerous phishing and fraudulent spam. The Provider must explain how the technology removes most unsolicited email whether it is malicious (e.g., targeted phishing message) or not (e.g., traditional unwanted marketing messages) before it hits the email server, and the benefits that this can provide in increasing security, employee productivity, and preventing waste of network bandwidth and storage. By using Cisco Secure Email, the Provider is able to filter SMTP >99% of spam email traffic through a combination of proactive reputation filtering and antispam content scanning for optimal detection and industry leading false positive rate.
D2.2.5.2 Antivirus	The scale and complexity of recent virus attacks highlight the importance of a vigorous, secure messaging platform. The Provider must explain how the service can combat this threat by using Cisco Secure Email to detect incoming infected messages and filter SMTP traffic for optimal detection rates and security.
D2.2.5.3 Inbound email content filtering	Businesses may have specific policies about emails entering their company. The Provider must also be able to explain how they help customers enforce acceptable usage policies: rules on users, file types, file sizes, keyword searches and dictionaries, credit card information, social security numbers, etc. and comply with regulations such as Payment Card Industry Data Security Standard (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley (SOX), and the Data Protection Act.

Requirement	Description
D2.2.5.4 Quarantine	Quarantines are special repositories used to hold and process messages. Messages in quarantines can be delivered or deleted, based on service policies. Quarantine policies can be set up for anti-spam, Antivirus, message and content filters. The Provider must explain how their service for incoming or outgoing messages can place those messages in quarantine.
D2.2.5.5 Enhanced email security with Advanced Malware Protection *(optional)*	Advanced Malware Protection (AMP) service option protects against zero-day and targeted file-based threats in email attachments by: • File reputation - the email security gateway captures a fingerprint of each file and send it to AMP cloud threat intelligence service to obtain the reputation of known files., with the result malicious files can be automatically blocked • File analysis - analyzing behavior of certain files that are not yet known to the reputation service • File retrospection - continuously evaluating emerging threats as new information becomes available, and notifying end customers about files that are determined to be threats after they have entered their network, indicating who on their network may have been infected and when These service options are available only for incoming messages. Files attached to outgoing messages are not evaluated. The file reputation service and the file analysis service are available as either Cisco public-cloud or private-cloud services delivered from the Provider Cloud Managed Security infrastructure. The private-cloud file reputation service is provided through the use of Cisco AMP Virtual Private Cloud appliance. The private-cloud file analysis service is provided using Cisco AMP Threat Grid appliance deployed in the Service Provider Cloud Managed Security infrastructure. The Provider must explain how the solution provides Advanced Malware Protection by using a combination of file reputation, file sandboxing, or retrospective file analysis to identify and block suspicious files where no known signature exists.
Outbound Email Security (Optional)	
D2.2.5.6 Antivirus	Businesses may have specific policies to avoid sending email corrupted with viruses outside their company. The Provider must explain how the service can deliver this capability by: Using Cisco Secure Email to detect outgoing infected messages and filter SMTP traffic for optimal detection rates and security.
D2.2.5.7 Outbound content filtering	Businesses may have specific policies about emails exiting their company. The Provider must also be able to explain how they help customers enforce acceptable usage policy: rules on users, file types, file sizes, keyword searches and dictionaries, credit card information, social security numbers, etc. and comply with regulations such as Payment Card Industry Data Security Standard (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley (SOX), and the Data Protection Act.

Requirement	Description
D2.2.5.8 Data Loss Prevention	Businesses must prevent the malicious or unintentional distribution of sensitive and proprietary information over the Internet. The Provider must also be able to explain how protect customer's information and intellectual property and enforce compliancy using Cisco Secure Email based on either: • RSA Email DLP: A solution local to the Email Security appliance that includes an integrated data loss prevention (DLP) scanning engine and DLP policy templates designed by RSA Security Inc. to identify and protect sensitive data; or • RSA Enterprise Manager: Customer using RSA's Enterprise Manager can use Provider's Email Security service with their Enterprise Manager software and use RSA's DLP technologies to scan outgoing message.
Availability The following section describes features that can be incorporated into the design of the service for a customer if there is a requirement to enhance the availability of the service or a particular site. Showing the features that are incorporated into the service can exhibit these requirements or evidence can be provided in a published service description that includes the required features.	
D2.2.5.9 High Availability *(optional)*	Active-active or active-passive high availability for the email security function allows service delivery to continue after a planned or unplanned outage occurs. The Provider should be able to explain to explain high availability capability based on either Cisco Secure Email clustering capability for active-active or traffic redirection to a standby virtual appliance fore active passive.
D2.2.5.10 Configuration backup	Storage of configurations of all virtual devices used in the email security service with ability to provide restoration.
D2.2.6 Web Security as a Service The following section describes the basic functions of a Web Security as a Service offering. The Provider must provide evidence of the web protection service capabilities and explain the key benefits of the service and how it can be used to protect end user accessing internet public web site. This service can be delivered to customer accessing the internet, the Service Provider cloud, or via their corporate sites.	
Real time threat protection services	
D2.2.6.1 Web reputation filtering	The number of security threats introduced by web traffic has reached epidemic proportions. The speed, variety, and damage potential of malware attacks highlight the importance of a robust, secure platform to protect the enterprise network perimeter. The Provider must explain how the solution: • Analyzes web traffic and network-related parameters to accurately evaluate a URL's trustworthiness • Quickly and accurately detects and blocks a full range of known and emerging threats • Provides a powerful outer layer of defense against the latest bot sites and exploited legitimate sites by using Cisco Secure Web appliance

Requirement	Description
D2.2.6.2 Malware scanning	The Provider must explain how the solution provides protection against the widest variety of web-based malware ranging from commercially invasive adware applications to malicious Trojans, system monitors, and phishing attacks.
Acceptable use services	
D2.2.6.3 URL filtering	The Provider must explain how the solution provides user access control based on the web server category of a particular HTTP or HTTPS requests.
D2.2.6.4 Application Visibility and Control	The Provider must explain how the solution provides industry-leading visibility and protection from web use violations.
D2.2.6.5 Software as a Service (SaaS) access policy control *(optional)*	The Provider must explain how the solution provides SaaS Application Authentication Policy control to determine whether or not a user is allowed access to the Software as a Service application.
D2.2.6.6 Transparent user authentication	The Provider must explain how the solution when interfaced with end customer's user identity servers such as LDAP, Active Directory can provide transparent user authentication and IP to username mapping.
Advanced Malware Protection (Optional)	
D2.2.6.7 Web Security with Advanced Malware Protection	Advanced Malware Protection service option protects against zero-day and targeted file-based threats that end user may download when visiting public web site by: • File reputation – the web security gateway captures a fingerprint of each file and send it to Cisco AMP cloud threat intelligence service or private AMP Cloud to obtain the reputation of known files, with the result malicious files can be automatically blocked • File analysis – analyzing behavior of certain files that are not yet known to the reputation service • File retrospection - continuously evaluating emerging threats as new information becomes available, and notifying end customers about files that are determined to be threats after they have entered their network, indicating who on their network may have been infected and when The file reputation service and the file analysis service are available as either Cisco public-cloud or private-cloud services delivered from the Service Provider Cloud Managed Security infrastructure. The private-cloud file reputation service is provided through the use of Cisco AMP Virtual Private Cloud appliance. The private-cloud file analysis service is provided using Cisco AMP Threat Grid appliance deployed in the Service Provider Cloud Managed Security infrastructure. The Provider must explain how the solution provides Advanced Malware Protection by using a combination of file reputation, file sandboxing, or retrospective file analysis to identify and block suspicious files where no known signature exists.

Requirement	Description
Advanced policy control services (Optional)	
D2.2.6.8 Granular access control	The Provider must explain how the solution provides differentiated security policies to individual users or group of users.
D2.2.6.9 Remote access (mobile) user	The Provider must explain how the solution provides the capability to distinguish remote users from local users, create specific policies for remote users and can transparently authenticate remote users (single sign-on).
Availability The following section describes features that can be incorporated into the design of the service for a customer if there is a requirement to enhance the availability of the service or a particular site. Showing the features that are incorporated into the service can exhibit these requirements or evidence can be provided in a published service description that includes the required features.	
D2.2.6.10 Optional high availability	Active-active or active-passive high availability for the web security function allows the Provider to continue service delivery during a planned or unplanned outage. The Provider must be able to explain to explain high availability capability based on either using Web Cache Communication Protocol (WCCP) redirection or load balancing between web security appliances.
D2.2.6.11 Configuration backup	The Provider must explain how the configurations of all virtual devices used in the Web security service are captured and stored with ability to provide restoration upon device failure or corruption.
D2.2.6b Managed Web Security with Umbrella SIG	
Service Delivery requirements	
D2.2.6b.1 Web protection service	The web protection service can be delivered to customer accessing the internet, the Service Provider cloud, or via their corporate sites. Provider must show both of: • Evidence of the web protection service capabilities such as: ◦ Policy settings ◦ Service descriptions ◦ Service architecture • Explanation of the key benefits of the service and how it can be used to protect the customer
D2.2.6b.2 DNS Layer Security	The service must include DNS Layer Security implemented via Umbrella SIG. Provider must show evidence of implementation of DNS Layer Security via **one** of: • Policy settings • Service descriptions • Service architecture

Requirement	Description
D2.2.6b.3 Web Reputation Filtering	The number of security threats introduced by web traffic has reached epidemic proportions. The speed, variety, and damage potential of malware attacks highlight the importance of a robust, secure platform to protect the enterprise network perimeter. The Provider must explain how the solution: • Analyzes web traffic and network-related parameters to accurately evaluate a URL's trustworthiness • Quickly and accurately detects and blocks a full range of known and emerging threats • Provides a powerful outer layer of defense against the latest bot sites and exploited legitimate sites. Provider must show evidence of implementation of Web Reputation Filtering via **one** of: • Policy settings • Service descriptions • Service architecture
D2.2.6b.4 URL Filtering	The service must provide user access control based on the web server category of a particular HTTP or HTTPS requests Provider must provider an explanation of how the service provides user access control based on the web server category of a particular HTTP or HTTPS requests
D2.2.6b.5 Transparent User Authentication	Provisioning user and group identities from Active Directory requires the deployment of an Umbrella Active Directory Connector. This connector securely retrieves non-sensitive user and computer group information from the AD domain controller and communicates that information to Umbrella. This enables the Provider to create and enforce AD group-based rules or policies and view AD user-based reports. The Provider must explain how the solution is interfaced with the end customer's user identity servers, such as LDAP or Active Directory, to provide transparent user authentication and IP to username mapping. Provider must show evidence of implementation of Transparent User Authentication via **one** of: • Demonstration • Service architecture
D2.2.6b.6 Two Factor Authentication	It is considered a best practice to enable two-factor authentication for access to the Umbrella Secure Internet Gateway administrative dashboard. Two-step verification is the ability to add a second factor of authentication to your login. This combines something you know (your password) with something you have (your mobile phone), and whenever you log into your account, you'll need to enter both your password and a security code from your mobile device Provider must demonstrate that two-factor enabled dashboard administrator login is enabled.

Requirement	Description
D2.2.6b.7 Cloud Malware Scanning *(optional)*	Cloud Malware Scanning provides the ability to detect and remediate malicious files in sanctioned cloud applications. With the addition of this feature, security admins can investigate the reported malware- at-rest found by Cisco AMP and other Umbrella AV tools and secure their environment by choosing to quarantine or delete those files. Cloud Malware Detection allows organizations to: • Safely share and support cloud transformation • Prevent the spread of cloud malware infections • Report on cloud malware incidents Provider must provide an explanation of how the service provides protection against the widest variety of web-based malware ranging from commercially invasive adware applications to malicious Trojans, system monitors, and phishing attacks.
D2.2.6b.8 Application Visibility and Control *(optional)*	Umbrella's Application settings organize application-based destinations into categories based on the type of processes or services provided (for example, shopping, education, or human resources). As well as configuring Application settings within Web policy ruleset's rules, you can create Web Application settings through Umbrella's policy component. Once saved, these Application settings are globally available to all of your DNS policies or Web policy ruleset's rules. Provider must provide an explanation of how the service provides industry-leading visibility and protection from web use violations.
D2.2.6b.9 Software as a Service (SaaS) access policy control *(optional)*	Umbrella's Tenant Controls setting control identity access to software as a service (SaaS) applications in the cloud. To control identity access to SaaS applications, you can add a Tenant Control setting to Umbrella and then select it when a Web policy ruleset. The advantage to adding a Tenant Control setting is that you can reuse this setting across multiple rulesets. The Provider can add a Tenant Controls setting for the following cloud-based applications and suites: • Microsoft 365 • Google G Suite • Slack Provider must give an explanation of how the service provides SaaS Application Authentication Policy control to determine whether or not a user is allowed access to the Software as a Service application
D2.2.7 Next Generation Firewall as a Service The following section describes the basic functions of a Next Generation Firewall (NGFW) service. Next Generation Firewall as a Service extends standard firewall capabilities by adding Intrusion Prevention System (IPS) and Application Control protection. The Provider must provide evidence of the next generation firewall service capabilities and explain the key benefits of the service and how it can be used to control application usage from the Internet into the customer network.	
D2.2.7.1 Support for standard firewall capabilities	Provider must support standard firewall capabilities, such as network-address translation (NAT) and stateful protocol inspection as specific in section D2.2.4.1 and D2.2.4.3 of this document.

Requirement	Description
Application Visibility and Control Support The following section describes key features of the NGFW that provides advanced visibility, detection, and control for the service.	
D2.2.7.2 Application discovery and visibility	The NGFW discovers application protocols transiting from customer's network to the internet and cloud applications hosted in virtual private cloud zone and collects information about hosts, operating systems, applications, users, files, networks, geo-location information, and vulnerabilities. Provider implements network discovery policies to monitor traffic and collect host, application, and non-authoritative user data. By accessing the Provider's cloud customer web portal, network administrators gain visibility into discovered applications running in their networks and their network usage, top talkers, top sites, and related statistics. Provider must present evidence how these features are delivered to their customers using their cloud-based service delivery platform.
D2.2.7.3 Optional advanced visibility	The Provider can provide the following services options: • Development and use of custom server or client fingerprints to help recognize operating system on hosts or clients • Active detection of host information collected from scanning services such as NMAP, QUALYS, or others • User awareness, integration with end customer Active Directory (direct or via Cisco Identity Service Engine) in order to collect authoritative user data.
D2.2.7.4 Application access control	Provide centralized Application based policy enforcement including the following functions: • Block, Allow, rate limit Traffic based on either of the additional criteria: ◦ user, user group (integration with AD, ISE), ◦ security TAG group, endpoint profile, endpoint location (integration with Cisco Identity Service Engine - ISE) • File control: detect and block end customer's users from uploading (sending) or downloading (receiving) files of specific types over specific application protocols. • Security Intelligence filtering: blacklist, deny traffic to and from specific IP addresses, URLs, and DNS domain names, before the traffic is subjected to analysis by access control rules
D2.2.7.5 SSL inspection *(optional)*	Secure Socket Layer (SSL) inspection allows handling encrypted traffic without decryption or decrypting encrypted traffic for further access control inspection. Public key certificates and paired private keys can be used to decrypt encrypted traffic, then inspect the decrypted traffic with access control. If the system does not block the decrypted traffic post-analysis, it re-encrypts the traffic before passing it to the destination host. Log details about encrypted connections can be provided to the customers.

Requirement	Description
Next Generation Intrusion Prevention System (NGIPS) (Optional) The following section describes the functions of NGIPS service options. The Provider must provide evidence of the Next Gen IPS capabilities, explain the key benefits of the service and how it can be used to detect, prevent, and report on intrusions, and analyze intrusion information in order to prevent recurrence.	
D2.2.7.6 Intrusion detection and prevention capabilities	Networks are exposed to a wide range of attacks, including viruses, worms, spyware, botnets, and spam. Intrusion Prevention Systems inspect all traffic for intrusions and exploits. It combines signature-, protocol-, and anomaly-based inspection methods to deliver comprehensive protection from attacks. The service includes the ability to monitor network traffic and respond based on defined policies. An intrusion policy examines decoded packets for attacks based on patterns and can block or alter malicious traffic. This monitoring will consist of event correlation, rating and filtering, and reporting through the customer web portal. The Provider must provide evidence of the intrusion detection and prevention capability and provide evidence of procedures to implement customer policies.
D2.2.7.7 Implementation and profiling service	To enable an effective intrusion detection and prevention solution, Provider must be able to gain an understanding of the customer network and application environment. Contextual awareness can be built by compiling data about the composition and behavior of networks, applications, and users. Advanced visibility options described above in D2.2.5.3 is therefore a pre-requisite, since inventorying the network not only ensures that all end devices are adequately patched, but also helps with alarm classification and enables Service Provider consultants to provide security policy recommendation. Vulnerability scanning services can either be provided as a separate service or as a part of the NGIPS service. Provider performs traffic profiling capability to create a profile of end customer's normal network traffic that is then used as a baseline against which to detect and track anomalous behavior. Provider uses correlation policies to generate events and trigger responses (such as alerts or external remediation) to specific types of connections or traffic profile changes.

Requirement	Description
D2.2.7.8 Intrusion monitoring and incident handling	The service must provide the following functionality: • Comprehensive reporting: customer access to preconfigured and perhaps customizable reporting to support a range of operational objectives such as troubleshooting, attack trending, and presentations • Real-time alerting: automated warnings by email, or a Simple Network Management Protocol (SNMP) trap • Real-time attack response: Provider creates event-focused rules and actions to block suspicious traffic and trigger inspections and remediation for a targeted system in customer's environment The Provider must provide the capability to process the multiple events that are generated, correlation them, and turning those correlations into a few meaningful events. Event correlation allows for simplified root cause analysis to be carried out. This analysis activity can then lead to long-term fixes, which may be a new signature, an ACL, a blocking action, or other configuration changes.
D2.2.7.9 Rules management	NGIPS uses rules as the primary mechanism to detect known attacks; just as with antivirus, the quality of NGIPS service is dependent on the rules database being up to date in order to provide the capability to protect customer environment from emerging. Cisco® Talos Security Intelligence and Research Group (Talos) writes and publish IPS rules every hour of the day to combat new and evolving threats. The Provider must provide evidence of an effective process for rules management that ensures that new Cisco NGIPS operating system and Talos published rules are implemented via an agreed upon process with the customer.

Requirement	Description
Advanced Malware Protection (AMP) Service for Network The following section describes the functions of Advanced Malware Protection for Network service option for Next Generation Firewall as a Service, Email security as a Service and Web Security as a Service. Provider must provide evidence of the Advanced Malware Protection for Network capabilities, explain the key benefits of the service and how it can be used to detect, track, capture, analyze, and optionally block the transmission of files (including malware files and nested files inside archive files) in network traffic.	
D2.2.7.10 Network-based AMP	Network-based Advanced Malware Protection solution inspects network traffic for threats in a multitude of file types, and it protects against zero-day and targeted file-based threats by: • File reputation – the NGFW appliance captures a fingerprint of each file and sends it to Cisco AMP cloud threat intelligence service or private AMP Cloud to obtain the reputation of known files whereby malicious files can be automatically blocked • File analysis – analyzing behavior of certain files that are not yet known to the reputation service • File retrospection - Continuously evaluating emerging threats as new information becomes available, and notifying end customers about files that are determined to be threats after they have entered their network, indicating who on their network may have been infected and when The file reputation service and the file analysis service are available as either Cisco public-cloud or private-cloud services delivered from the Service Provider Cloud Managed Security infrastructure. The private-cloud file reputation service is provided through the use of Cisco AMP Virtual Private Cloud appliance. The private-cloud file analysis service is provided using Cisco AMP Threat Grid appliance deployed in the Service Provider Cloud Managed Security infrastructure.
Availability	
D2.2.7.11 Optional redundancy	Service must include the ability to recover from a device failure without service disruption. This is achieved by deploying two NGFW appliances in active/standby failover mode.
D2.2.7.12 Configuration backup	The Provider must explain how the configurations of all devices used in the NGFW service are captured and stored with ability to provide restoration upon device failure or corruption.

Requirement	Description
D2.2.8 Advanced Malware Protection (AMP) Service for Endpoints The following section describes the functions and requirements of Advanced Malware Protection for Endpoints service. Provider can use Cisco Secure Endpoint MSSP public cloud service or host private AMP and Cisco Threat Grid to offer the service to end customers. Provider must provide evidence such as a Market Service Description document that describes the Advanced Malware Protection for Endpoints capabilities, explains the key benefits of the service and how it can be used to protect their customers against the advanced threats with the service.	
D2.2.8.1 Secure Endpoint Service Capabilities	Secure Endpoint service blocks, detects, contains, and remediates the advanced malware with the following capabilities: • File reputation – the local client captures a fingerprint of each file and sends it to Cisco AMP cloud threat intelligence service or private AMP Cloud to obtain the reputation of known files whereby malicious files can be automatically blocked • Continuous analysis – Once a file lands on the endpoint, Secure Endpoint continues to watch, analyze, and record all file activities • File retrospection - Continuously evaluating emerging threats as new information becomes available, and notifying end customers about files that are determined to be threats after they have entered their network, indicating who on their network may have been infected and when • AV Detection – Malware and Antivirus protection bundled into a single lightweight client • Proactive Protection – Identifies vulnerability patterns, with the ability to analyze and stop suspicious executables quickly • File and Device Trajectory – Identifies root causes of infection and initial point of entry • Vulnerabilities – identify vulnerable software and show a list of hosts that contain vulnerable software • Outbreak control - control over suspicious files or outbreaks, and quickly and surgically control and remediate an infection without waiting for a content update
D2.2.8.2 Responsible for the managed service life cycle	Provider must be responsible for end-to-end Secure Endpoint service including: • Cisco SSFAMP training for a minimum of two SOC analysts • Service activation and customer on-boarding: account creation, customer vetting, • License management • Security assessment in term of the flavors of endpoints, customer IT setting, applications to determine the service needs • Service provisioning, setting AMP policies, installation of AMP connectors • Service staging to fine tuning the policies and configuration • On-going monitoring or management and threat detection and response • End to end customer support • Providing reports to customers • Service termination

Requirement	Description
D2.2.9 DNS Monitoring Service using Umbrella DNS Cisco Umbrella DNS provides the first line of defense against threat on the Internet. It uses DNS to stop threats over all communication ports and protocols. Provider can deliver Cisco Umbrella as a managed secure Internet gateway service to its customers by enforcing policies to prevent users from visiting malicious web sites, providing a complete real-time picture of internet activity for on-network and roaming devices with reports on security, usage, compliance, and cloud services.	
D2.2.9.1 Offer Cisco Umbrella DNS layer security service	Provider can offer several tiers of secure internet gateway services based on Cisco Umbrella to customers. Provider must provide evidence such as a service description document or via policy setting on the service portal to demonstrate that DNS layer security service is offered, i.e., at DNS layer to block Malware, Command and Control Callbacks and Phishing attacks categories.
D2.2.9.2 Offer network level enforcement and visibility	DNS security policies can be enforced at multiple layers, entire network behind a public IP address, sub networks identified by WLAN SSIDs or VLAN tag. Provider must provide evidence that security policies are enforced on customers' network to whom the Provider provides a managed service. Device level and user level enforcement is optional.
D2.2.9.3 Block page	Provider can choose to use the default Cisco Umbrella block page or Provider's customized block page or provide capability to let customers customize their own block pages.
D2.2.9.4 Content category filtering *(optional)*	As a service option, Provider can offer Cisco Umbrella content category filtering to customers to enforce acceptable usage policies.
D2.2.9.5 Roaming user protection *(optional)*	As a service option, Provider can offer Cisco Umbrella roaming protection capability to protect users while they are off the network which protected by the service. In this case, Provider must be responsible for the process of deployment of Umbrella roaming clients or Cisco AnyConnect clients on users' device or provide documentation to end customers for self-deployment of the clients.
D2.2.9.6 Intelligent proxy for risky domains *(optional)*	As a service option, Provider can offer Cisco Umbrella intelligent proxy capability for risky domains, which host both malicious and safe content. Intelligent proxy supports URL inspection based on Cisco Talos and 3rd party threat intelligence and file inspection using Antivirus engine and Cisco AMP.
D2.2.9.7 Offer global policies or per customer policies *(optional)*	As a managed service provider, Provider can offer pre-defined global level security policies to its entire customer based or a sub-set of customers. Provider can also choose to offer the capability to allow end customers to define and customize their own policies via the service portal.

Requirement	Description
D2.2.9.8 Responsible for the entire managed service life cycle	Provider must provide evidence via a Service Description document or operation procedure document to demonstrate that it is responsible for the entire managed secure Internet gateway service life cycle for its customers, including: • Customer on-boarding: account creation, customer vetting • License management to ensure the customer have valid licenses for the offer. • Policies setting such as security category, content filtering setting. • Service deployment such as changing DNS setting to point to Cisco Umbrella and roaming client deployment. • Enforcement of the security at network, device, and user level • Provide regular security report to customers when applicable • Provide technical support to customers • Customer service termination
D2.2.9b DNS Monitoring Service using Umbrella SIG	
D2.2.9b.1 Web protection service	The web protection service can be delivered to customer accessing the internet, the Service Provider cloud, or via their corporate sites. Provider must show **both** of: • Evidence of the web protection service capabilities such as: ◦ Policy settings ◦ Service Description Document ◦ Service Architecture Document • Explanation of the key benefits of the service and how it can be used to protect the customer
D2.2.9b.2 DNS Layer Security	The service must include DNS Layer Security implemented via Umbrella SIG. Provider must show evidence of DNS Layer Security via **one** of: • Policy settings • Service Description Document • Service Architecture Document
D2.2.9b.3 Direct Traffic to Umbrella	To use Umbrella, Provider must explicitly point customer DNS services in operating system or hardware firewall/router to Umbrella's name server IP addresses. Provider must demonstrate the policy settings on the service portal to demonstrate that customer DNS requests are being resolved by Cisco Umbrella.
D2.2.9b.4 Network Level Enforcement and Visibility	Provider must provide evidence that security policies are enforced on customers' network to whom the Provider provides a managed service. Explanation of how the service provides user access control based on the web server category of a particular HTTP or HTTPS requests.

Requirement	Description
D2.2.9b.5 Block Page	Provider can choose to use the default Cisco Umbrella block page or Provider's customized block page or provide capability to let customers customize their own block pages. Provider must show evidence of implementation of a Block Page via **one** of: • Demonstration • Service Description Document • Operations Procedure Document
D2.2.9b.6 Two Factor Authentication	It is considered a best practice to enable two-factor authentication for access to the Umbrella Secure Internet Gateway administrative dashboard. Two-step verification is the ability to add a second factor of authentication to your login. This combines something you know (your password) with something you have (your mobile phone), and whenever you log into your account, you'll need to enter both your password and a security code from your mobile device Provider must demonstrate that two-factor enabled dashboard administrator login is enabled.
D2.2.9b.7 Content category filtering *(optional)*	As a service option, Provider may offer Cisco Umbrella content category filtering to customers to enforce acceptable usage policies. Provider must provide evidence of content category filtering via **one** of: • Block Page Demonstration • Service Description Document • Operations Procedure Document • Demonstration of DNS Policy with content category check box selected in dashboard
D2.2.9b.8 Roaming user protection *(optional)*	As a service option, Provider can offer Cisco Umbrella roaming protection capability to protect users while they are off the network which protected by the service. In this case, Provider must be responsible for the process of deployment of Umbrella roaming clients or Cisco AnyConnect clients on users' device or provide documentation to end customers for self-deployment of the clients. Provider must provide evidence of implementation of roaming user protection via **one** of: • Service Description Document • Operations Procedure Document

Requirement	Description
D2.2.9b.9 Intelligent proxy for risky domains *(optional)*	As a service option, Provider can offer Cisco Umbrella intelligent proxy capability for risky domains, which host both malicious and safe content. Umbrella's intelligent proxy intercepts and proxies requests for URLs, potentially malicious files, and domain names associated with certain uncategorized or "grey" domains. With the intelligent proxy, Umbrella avoids the need to proxy requests to domains that are already known to be safe or bad. Most phishing, malware, ransomware, and other threats are hosted on domains that are classified as malicious Provider must provide evidence of implementation of intelligent proxy for risky domains via **one** of: • Service Description Document • Operations Procedure Document
D2.2.9b.10 Offer global policies or per customer policies *(optional)*	As a managed service provider, Provider can offer pre-defined global level security policies to its entire customer based or a sub-set of customers. Provider can also choose to offer the capability to allow end customers to define and customize their own policies via the service portal Provider must provide evidence of implementation of global policies or per customer policies via **one** of: • Service Description Document • Operations Procedure Document
D2.2.10 Secure Cloud Analytics Private Network Monitoring and Public Cloud Monitoring Service Cisco Secure Cloud Analytics is a public cloud service that uses behavior-modelling approach to detect threats posed by compromised network devices and endpoints across private networks, branch offices and public cloud infrastructures like Amazon AWS. It provides comprehensive visibility and high precision alerts with low noise. Providers can provide Secure Cloud Analytics as a managed security service offer to detect threats in real time, identify indicators of compromise and assess the customer's security posture. Providers must provide evidence, such as a service description document, that following requirements are met.	
D2.2.10.1 Offer at least one of two services • Private Network Monitoring (PNM) • Public Cloud Monitoring (PCM)	Secure Cloud Analytics supports two primary offerings. Provider must provide evidence such as a service description document that it provides at least one of these two offerings to the customers. • Private Network Monitoring (PNM) provides visibility and threat detection for the on-premises network. It works by deploying one or more free virtual appliances, called "sensors" on customer private network. Sensors can consume a variety of native sources of telemetry or extract metadata from network packet flow. Sensors encrypt this metadata and sends it to the Secure Cloud Analytics platform for analysis. • Public Cloud Monitoring (PCM) provides visibility and threat detection in Amazon Web Services (AWS), Google Computer Platform (GCP) and Microsoft Azure infrastructures. In AWS, it relies on native AWS sources of telemetry such as its Virtual Private Cloud (VPC) flow logs.

Requirement	Description
D2.2.10.2 Responsible for the entire managed service life cycle	Provider must provide evidence via a Service Description document or operation procedure document to demonstrate that it is responsible for the entire managed Secure Cloud Analytics service life cycle for its customers, including: • Provider training as required by Cisco • Customer vetting to ensure that customer meet the requirements defined in Cisco Secure Cloud Analytics agreement • Customer on-boarding: account creation and service activation including coordinating orders with Cisco. • License management to ensure the customer have valid licenses for the offer and endpoints • Policies setting such as alert priorities, watch lists, IP rules, country level blacklist • Deploying the sensors and ensure the availability and secure access of these sensors • Continuously monitoring the alerts and act upon those alerts for the customers • Providing tier 1 support to the customers • Providing regular security status report to customers
D2.2.10.3 Integration with SIEM *(optional)*	Provider can choose to use Secure Cloud Analytics API and integrate Secure Cloud Analytics with its security information and event management (SIEM) application such as IBM QRadar® or Splunk®.
2.2.11 VPN as a Service Capabilities The following section describes the basic functions of site-to-site and remote access Internet Virtual Private Network (VPN) services, delivering secured connectivity. The Provider must provide evidence of the VPN service capabilities. The site-to-site VPN service option is required when the hosted security services are delivered over internet connectivity, the remote access VPN service option is required to support remote (mobile) users for web and email protection services.	
Site to Site VPN	
D2.2.11.1 Support for internet site-to-site VPN	The Provider must offer a site-to-site VPN termination service from its cloud infrastructure that allows secure site-to-site connectivity the end customer network and the Provider hosted security cloud infrastructure. The Provider must present evidence of how this is delivered using a Cisco platform such as architectural or topology diagrams.
D2.2.11.2 Data encryption algorithms	Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), or Advanced Encryption Standard (AES) (where permitted) must be used for IPsec encryption. The Provider must provide evidence that they support one or more of these protocols. The Provider must present evidence of how this requirement is delivered on a Cisco platform, such as labeling on an architectural diagram or via configuration examples.

Requirement	Description
Remote Access VPN (Optional)	
D2.2.11.3 Internet remote access VPN	The Provider must offer a remote access VPN termination service from its cloud infrastructure to protect end customer mobile users. The Provider must present evidence of how this is delivered using a Cisco platform, such as architectural or topology diagrams.
D2.2.11.4 Remote access IP VPN technologies	The Provider must support at least one of the following remote access VPN deployment solutions: • Remote access IPsec-based VPN • Remote access SSL-based VPN The Provider must present evidence of how this requirement is delivered on a Cisco platform, such as architectural or topology diagrams.
D2.2.11.5 Remote access IPsec Network Address Translation (NAT) transparency	IPsec and NAT have numerous incompatibilities that do not allow IPsec connections to function through NAT devices. With this feature, IPsec peers can establish a connection through a NAT device via a Cisco coauthored Internet Engineering Task Force (IETF) standard. The Provider must present evidence of how this requirement is delivered on a Cisco platform, such as architectural or topology diagrams.
D2.2.11.6 Authentication, Authorization, and Accounting (AAA) options	The service must support methods for ensuring only authorized users can gain access to a VPN and that appropriate accounting information is available. For example, a RADIUS server (e.g., Cisco Access Registrar), at either the customer or the Provider, may be used to authenticate and authorize remote-access clients. Customer-managed RADIUS servers typically store per-user information (such as user authentication). At the Provider site, a RADIUS server can store all AAA and configuration information, or the information can be split across two servers. For this component, the Provider may use any RADIUS server that understands Cisco AV pairs to authenticate and authorize remote access clients. If a two-factor, secure-ID-based authentication is required, an RSA or like server must be installed on the service-provider management network for local AAA or on the customer premises for proxy authentication. The Provider must present evidence of how this requirement is delivered, such as architectural or topology diagrams.
Availability The following section describes features that can be incorporated into the design of the service for a customer if there is a requirement to enhance the availability of the service or a particular site. Showing the features that are incorporated into the service can exhibit these requirements or evidence can be provided in a published service description that includes the required features.	
D2.2.11.7 Dual VPN gateway support with stateless failover *(optional)*	Stateless failover enables the VPN service to continue processing and forwarding session packets after a planned or unplanned outage occurs. A backup (secondary) VPN gateway is employed to reestablish VPN connections when connections are lost with primary VPN gateway for any reason. This process is transparent and does not require adjustment or reconfiguration of any remote peer.

Requirement	Description
D2.2.11.8 Dual VPN gateway support with stateful failover *(optional)*	Stateful failover enables the VPN gateway to continue processing and forwarding packets after a planned or unplanned outage occurs. A backup (secondary) VPN Gateway is employed that automatically takes over the tasks of the active (primary) VPN Gateway if the active VPN Gateway loses connectivity for any reason. This process is transparent and does not require adjustment or reconfiguration of any remote peer.
D2.2.11.10 Configuration backup	Storage of configurations of all virtual devices used in the firewall service with ability to provide restoration. The Provider must present evidence of how this requirement is delivered, such as a screen shot from the configuration backup system.

D2.3 Service-Level Management Requirements

Requirement	Description
Service-Level Agreement (SLA) Components This section describes the SLAs that the Provider is willing to contract for as part of the service. These are normally available as part of the service description. Existing customer contracts that include the relevant SLAs may also be presented as evidence of meeting these requirements.	
D2.3.1 Mean Time to Notify (MTTN)	The average time taken to notify a customer of an issue. Measured from the time that an alarm is generated to the time the customer is notified, which can be by any method of communication agreed with the customer.
D2.3.2 Mean Time to Restore Service (MTRS)	The average time taken to restore service after a failure. Measured from when the service failure is reported to the time it is fully restored and delivering its normal functionality. Sometimes known as MTTR. Guidelines for restoring services to the previous known working configuration based on priority levels are as follows: • P1: 4 hours • P2: 24 hours • P3: 2 business days • P4: 5 business days
D2.3.3 Turnaround time for customer-initiated changes	The turnaround time for implementing changes requested by the customer. Must be within 48 hours for standard changes.
D2.3.4 Change request for rules	**Access rules are used to define the network security policy; they control the traffic that flows through a firewall device. Access rules are recognized in the form of an ordered list. A firewall device processes rules from first to last. When a rule matches the network traffic that a firewall device is processing, the firewall device uses that rule's action to decide if traffic is permitted. Rules at the top of the list are therefore considered higher priority.** Priority rules must be changed within 4 hours.

Requirement	Description
D2.3.5 Notification of security update and bug fixes	The average turnaround time for notification of security updates and bug fixes.
Customer Web Portal The following section describes the online facilities that must be made available to the customer to view the current and historical performance of their service. May be proven by a demonstration of the portal from customer viewpoint, including real-time view of connectivity and status. Mechanisms may include password protection or similar restrictions to access the online web portal for downloading reports. The Provider must also be able to show that event logs can be stored and made accessible via the portal. If a Provider chooses to use a Cisco cloud service portal or API from these services for integration, including Secure Endpoint MSSP, Umbrella, or Secure Email Security, or Secure Cloud Analytics to offer managed security services to its end customers, the following customer web portal requirements are satisfied.	
D2.3.6 Secure web portal	A secure, customer web portal is used to communicate the current status and performance, including specific reports available online as agreed with the customer. It provides an operational view for multiple audiences; designed to give a quick view of the network status, including current availability, reliability, and security for managed devices.
D2.3.7 Event log retention	Security events are stored in a log for regulatory and analysis purposes. Must be retained for a period of time established with the customer.
D2.3.8 Summary-level dashboard to communicate key performance criteria, including: • Real-time status • Monitoring report • Usage report	For firewall as a service, web security as a service and email security as a service, the security dashboard must include: • Top five attacked or visited sites of the month/week including the number of events and the associated percentage • Top five alerts of the month/week: The top five most received alerts, including the number of occurrences and the associated percentage • Historical charts (day, week, month, year) For VPN services, the security dashboard must include: • Network traffic • VPN tunnels history • Network delays: round trip time (RTT) and time to live (TTL)
External Reporting The following section describes the reports that are to be made available to the customer via customer portal. Example reports must be provided or a view of customer web portal with ability to select reports listed. Web-based reporting via a customer web portal is considered a best practice and allows the Providers to differentiate themselves from other Providers.	
D2.3.9 Service Availability reports	Service availability reporting on the overall services, separate infrastructure services, separate network services, separate managed devices level services are provided including details of the service downtime over a defined period of time.

Requirement	Description
D2.3.10 Device Inventory reports	Reporting of devices under management for the customer, providing data that is relevant to the customer regarding the inventory of equipment or WAN services used in delivering the service.
D2.3.11 Incident Management reports	Reports summarizing customer change request activities and system generated incidents (e.g., utilization warnings) are made available to the customer. These should include metrics on the incidents, such as number, status, average time to resolve past incidents, and how the incidents were resolved.
D2.3.12 Exception reports	Reports generated by customer-specified thresholds or ranges; provide ability for customers to self-select parameters on individual devices and determine thresholds for the raising of exception reports.
D2.3.13 Security reports	Security reporting capabilities must include: • Number of security incidents that occurred over a pre-determined period • Types of incidents • Time to respond • Most frequent types of attacks • Most frequently attacked hosts or sites • Identified sources of attack
Internal Performance Reporting The following section describes reports that are to be internally created and reviewed. May be proven by provisioning of example reports or demonstration of reporting tool with ability to select reports listed.	
D2.3.14 Customer-related reports/internal performance metrics	Reports on metrics used to measure trends of service performance, including: • SLA violations • Performance against internal targets (typically more stringent than those agreed with the customer)
Infrastructure Reporting (applies only to organizations providing virtualized infrastructure for delivery of the service) The following section describes reports that are to be internally created and reviewed and that relate specifically to the performance of the infrastructure used to deliver the service across the Internet. May be proven by provision of example reports or a demonstration of the reporting tool with ability to select reports listed. For non-service affecting incidents, Provider must provide evidence of a process to investigate reported problems as necessary in order to prevent them from affecting service to the customer.	
D2.3.15 Infrastructure/network-related reports	Reports relating to the overall performance of the network infrastructure used to provide the service covering key areas of potential concern. May include: • Overall trend in traffic loads: Monitored to ensure adequate capacity is maintained to meet contracted Service-Levels • Peak loads: Signifies potential areas or times of concern that may warrant further investigation • Non-service affecting incidents: Includes incidents such as hardware or link failures on network devices that were successfully routed around

D8 Webex Contact Center

Introduced: September 2020
Last updated: August 2021

Overview

Cisco Webex Contact Center (Webex CC) provides Providers with a native contact center as a service solution, enabling security, visibility, flexibility, and scalability. The solution brings together all of a customer's interactions (voice, email, and chat), into a unified environment for a seamless experience.

Cisco Powered Webex CC enables Providers to provide:

- 360° customer journey analytics, helping to better understand the customer experience through the entire lifecycle, across all channels.
- Predictive analytics-based routing, to anticipate customer need based on their stage of the customer journey and match them with the best available agent for that need.
- Expert collaboration and communications via on-demand voice and chat collaboration with other agents, managers, and subject matter experts.
- An optional Workforce Optimization (WFO) suite, including dynamic scheduling with agent participation, quality management, and "voice of the customer" insights through speech and desktop analytics.
- Optional Outbound Campaigns, with preview and progressive dialing and management

Prerequisites

	Requirement	Evidence
D8.PR.1	**Customer References** • Reference customers must be under existing contractual relationships • One customer may serve as a reference to multiple Cisco Powered Service designations • One customer with multiple sites satisfies the requirement for a single reference, as the intent is to ensure that the Provider has proven and repeatable service practices • Two customer references are required only once: either with a new Cisco Powered Service application or upon first-year renewal • Use the Customer Reference Validation form to either submit references or to indicate references will be provided upon first year renewal	Customer Reference Validation Form uploaded into the Provider application.
D8.PR.2	**Cisco Specializations** Provider must have Webex Contact Center Specialization. For information, visit Partner Architecture Specializations.	Partner Locator will be used to confirm the Provider has achieved the Webex Contact Center Specialization.

Service Offer

	Requirement	Evidence
D8.SO.1	**Service Level Agreements** Service performance is committed through having Service-Level Agreements (SLAs) in place between the Provider and End-User which are backed by processes to measure and report on whether those commitments are being met. Service performance elements covered by the SLA may include: • Platform availability: infrastructure, orchestration, and service interfaces • Network availability: the network operated by the Provider that is used to provide connectivity from the Internet or private WAN, involved data centers, and/or a third party used to provide network connectivity • Mean Time to Notify (MTTN): MTTN measures the average time taken to notify a customer of an issue with the subscribed service. The measurement encompasses the time that an alert is generated to the time the customer notified, which can be by any method of communication agreed upon with the customer • Mean Time to Restore Service (MTRS): MTRS measures the total elapsed time from the start of a resource outage to the time the service is restored. This is also known as Mean Time to Restore/Repair (MTTR). In some cases, a cloud-based service, brokered by a third party, may not have a platform availability SLA. The Provider must still provide SLA parameters such as MTTN to the customer.	One of: • Executed Service Level Agreement • Service Level Agreement template
D8.SO.2	**Service Requirements** Formal requirements help align the business on a definition of success. These documents, such as a Marketing Requirements Document (MRD) or a Product Requirements Document (PRD) ensure that the various stakeholders' requirements are cataloged and addressed, increasing the likelihood of market success dramatically. The Provider must show evidence of a MRD or PRD for this service. At a minimum, these documents should address: • Target customer segment and clearly defined use cases • Service packaging and pricing structure • Customer value proposition of the service	A table of contents or redacted version of one of • Marketing Requirements Document (MRD) • Product Requirements Document (PRD) of the service
D8.SO.3	**Service Description** The Service Description is an End-User facing document which explains the service features, benefits, and business outcomes to a potential customer. Typically, a Service Description would include an outline of the different tiers of service such as bronze, silver, or gold, and the features available at each tier.	Service Description document

Service Delivery

	Requirement	Evidence
D8.SD.1	**Service Architecture Document** The Service Architecture document must • describe the key technology components, how they are integrated, and how End-Users access the service. • show the available deployment models with PSTN interconnection options and Telephony platforms supported within the offer • describe how the availability and health of the service is monitored	Architecture design document
D8.SD.2	**Bring your own PSTN for meeting dial in numbers** Provider must provide PSTN resources for inbound and outbound calls into Webex Contact Center. This may be fulfilled using Cisco PSTN bundles, where available.	Documentation of PSTN options in the service description
D8.SD.3	**Integration of Provider's BroadWorks calling platform with Cisco Webex** Provider is responsible for the integration of provider or customer telephony platform with Cisco Webex Contact Center. The Provider must support the integration of the underlying telephony platform with the Cisco Webex Contact Center infrastructure.	Description of the available architectural options
D8.SD.4	**Perform testing and validate service readiness in a staging environment** Provider must have an active Gold Tenant in the staging platform.	Description of the Gold Tenant architecture and implementation

Service Marketing

	Description	Evidence
D8.SM.1	**Digital presence** Most buyers will complete their research online before engaging with the Provider's sales team. Online presence may include a web page, micro site, social media, podcast, and marketing events.	One of: • Demonstrate a service-specific online presence with service specific marketing content • A marketing plan across various marketing channels and platform
D8.SM.2	**Align digital marketing to the buyer journey** Prospective customers complete the majority of purchasing decision research before engaging a Provider's sales contacts. It is a best practice to ensure that rich digital marketing content with clearly defined use cases is in place through the buyer's journey. This may include a micro web site, social media, podcasts, and interactive marketing events such as webinars.	Buyer Journey Map document

Sales Operations

	Description	Evidence
D8.SP.1	**Sales Training** Provider must have a process to formally train both sales and sales engineers for the service	Sales Training Plan document
D8.SP.2	Provider must provide evidence of at least **two** of the following sales enablement materials: • Battle card • Call script • Email template • Demo portal • Demo video	**Two** sales enablement materials
D8.SP.3	**Sales Compensation policy** Provider must have a sales compensation policy that incentivizes and rewards the involved teams for selling the service	Sales Compensation policy document

Customer Success

	Requirement	Evidence
D8.CS.1	**Customer Success Practice** Customer Success is the function within a Provider organization responsible for managing the relationship between the Provider and its customers. The goals of Customer Success are to: • Maximize customer value • Increase service adoption • Ensure ease of use • Increase customer satisfaction • Drive service renewal Provider must demonstrate processes and metrics that support each of the following elements of a customer success practice: • Customer on-boarding and service activation process • Service renewal process • Service renewal rate measurement • Dispute and escalation handling processes • Ongoing customer communications Regular business review process to periodically assess business requirements and change management needs	Customer Success Practice Description document

	Requirement	Evidence
D8.CS.2	**User Guide** A User Guide is a document provided to customers showing how to access the customer service portal for self-service capabilities which may include service activation, on-boarding, configuration and reporting for the audited service.	User guide document
D8.CS.3	**Customer Ticketing System** A ticketing system should be in place for tracking customer change requests and system generated incidents. A ticketing system may be part of a larger IT Systems Manager (ITSM) or Customer Relationship Management (CRM) system. Reports from this system should include metrics and summaries of incidents including details such as quantity, status, average time to resolve past incidents, and how the incidents were resolved.	Demonstration of the Customer ticketing system
D8.CS.4	**Provide End User Support** Provider is responsible for the first line of support for Cisco Webex Contact Center. Support staff must be in place and support contact information for this service must be published to End Users. Provider must have a documented process describing basic trouble isolation procedures including: • Receiving support request from End Users • Conducting preliminary diagnosis • Initial troubleshooting Problem resolution or escalation	Documentation describing first line support staff training process

C2 Unified Communications as a Service Based on HCS

Introduced: September 2011
Last updated: August 2021

Overview

Cisco UC as a Service Based on HCS (HCS) is based on Cisco's Hosted Collaboration Solution (HCS) which is part of Cisco's Unified Collaboration technologies and provides a Provider the opportunity to create subscription-based "as a service" offers utilizing hosted and managed models.

The Provider can monetize Cisco's broad portfolio of applications, streamline operations with complete management system, optimize their capital investments in the data center through virtualization, and assure the highest quality of experience for their customers.

UC as a Service Based on HCS can be delivered on the Hybrid Cloud platform architectures aligned to the C8 Hybrid Cloud Cisco Powered Service designations, using VMware vSphere as the hypervisor.

Refer to Cisco Hosted Collaboration Solution for additional information.

C2.1 Prerequisites

The Provider must meet the following prerequisites to apply for this service designation.

Requirement	Description
C2.1.1 Submit at least two customer references for the service	Reference Customers • Reference customers must be under existing contractual relationships • One customer may serve as a reference to multiple Cisco Powered Service designations • One customer with multiple sites satisfies the requirement for a single reference, as the intent is to ensure that the Provider has proven and repeatable service practices • Two customer references are required only once: either with a new Cisco Powered Service application or upon first-year renewal Use the Customer Reference Validation form to either submit references or to indicate references will be provided upon first year renewal Evidence: Customer Reference Validation Form uploaded into the Provider application

Requirement	Description
C2.1.2 Completed an Assessment to Quality for Hosted Collaboration Solution Phase 3	The Assessment to Quality (A2Q) for Hosted Collaboration Solution Phase 3 is required prior to the audit for UC as a Service based on HCS. The Provider must present evidence that the A2Q review was completed successfully with no open issues, within the prior three months of the audit. Note: If a Provider has a valid approved phase 3 A2Q, they are not required to submit an A2Q for Provider annual renewal.
C2.1.3 Employ at least one CCNP Collaboration certified individual and at least one CCNP Data Center certified individual on staff where the HCS service originates	The CCNP Voice Professional and the CCNP Data Center must be located where the HCS service originates to ensure a high quality of experience for end user customers. Optimally, these individuals would be on staff in the data center where HCS service originates; however, at a minimum they must reside in the country and have remote access into the data center. A Cisco CCIE certification, of any technology specialization, supersedes and fulfills the certification requirements for this service. Refer to Cisco Certifications for more information. The Provider must provide evidence that there are certified individuals on staff where the HCS service originates.
C2.1.4 Maintain Master Collaboration Specialization or Advanced Collaboration Architecture Specialization in country where HCS service originates	The Provider must maintain one of the following in the country where the UCaaS service originates: • Master Collaboration Specialization • Advanced Collaboration Architecture Specialization Refer to Collaboration Specializations for more information. The Provider must provide evidence of the Specialization compliance in country where HCS service originates.
C2.1.5 Have a commercial agreement in place with Cisco	HCS requires a contractual commitment between the Provider and Cisco that outlines the licensing agreements and any volume commitment. The Provider must provide evidence that a buying agreement addendum has been added to the Provider's reseller agreement. For assistance in executing the addendum, contact the Cisco Account Team.

C2.2 Provider System/Solution Requirements (Build)

Requirement	Description
Service Capabilities The following section describes the basic functions of the Service Provider's cloud infrastructure service as a foundation to HCS. The Provider must explain how each of the functions listed are provided, and the benefits this delivers to the customer by providing a flexible, reliable, and secure infrastructure to create services on. These functions can be provided with multiple Cisco platforms.	

Requirement	Description
C2.2.1 Provide the following documents unique to the service: • Marketing Service Description • Technical Service Description • Operational Processes and Procedures • Architectural diagram	The Marketing Service Description (MSD) is a document produced by the Provider which explains to a potential customer what the service is, what features are included, and the benefits the service provides. The MSD must be a published document which is available to customers and prospective customers. The Technical Service Description (TSD) provides documentation on how services are delivered, specific features the customer should expect, often differing by service tier, and who is responsible for what activities related to service delivery. The TSD is often an attachment or amendment to a services agreement between the Provider and the customer. The Operational Processes and Procedures, sometimes referred to as a runbook, is the set of Provider internal documentation detailing customer support and capacity management related to the service. The architectural diagram(s) must show how the compute, storage, and networking components are connected along with how a customer will gain access to Virtual Machines (VMs) via network connectivity. The Provider must provide examples of the MSD, the TSD, and architectural diagram(s) as evidence of this requirement. Proving the existence of the Operational Processes and Procedures is required, but the Provider does not have to upload or share specific details.
C2.2.2 Deliver from a Cisco Powered Infrastructure as a Service or Hybrid Cloud environment	The HCS solution must be delivered from an audited cloud infrastructure environment. As such the Provider is required to hold a Cisco Powered Service designation for Cisco Powered Hybrid Cloud (C8). VMware vSphere must be used as cloud computing virtualization platform. The Provider may also opt to meet the requirements in C1.1 and C1.2 without holding the abovementioned designations to fulfill this requirement.
C2.2.3 Server virtualization	Compute must comply to the Cisco supported options: • UC on UCS Tested Reference Configuration (TRC) • UC on UCS Specs-based • Third-party Server Specs-based The Provider must provide evidence that the data center design is based on these models and is in compliance with the version of VMware vSphere (vCenter or vCSA and ESXi) along with UC application compatibility being utilized. References: • UCS Hardware and Software Compatibility • VMware Compatibility Guide • Collaboration Virtualization Hardware • Unified Communications VMware Requirements • Unified Communications Virtualization Supported Applications

Requirement	Description
C2.2.4 Storage virtualization	The Provider must meet and provide evidence as described within the Hybrid Cloud Requirement section. In addition, and if deployed, the Provider must provide evidence that the Storage Array is compliant with the version of VMware vSphere (vCenter or vCSA and ESXi), and meets the IOPS, Capacity and Performance requirements of the UC apps deployed. References: • VMware Compatibility Guide • Cisco UC Virtualization Storage System Design Requirement
Provider VoIP Infrastructure The following section describes the key requirements needed within the Voice Over IP (VoIP) infrastructure to conform to HCS requirements. The Provider must explain the infrastructure they have deployed to support each function. Where options are given and one of the suggested platforms is not being used, then the Provider must explain how the necessary function is achieved and show that Cisco and Provider have agreements in place that indicate the Provider has taken responsibility for the performance of the particular aspect of the solution.	
C2.2.5 IP Demarcation Layer	The Provider must have an IP Demarcation Layer. The Session Boarder Controller (SBC) also functions as a Network Address Translation (NAT) firewall, media, and signaling anchoring device. In the Aggregation Layer, the SBC is used as a Cisco HCS demarcation, which normalizes all the communication between the Cisco HCS and the outside world, either a different IP network or the IP Multimedia Subsystem (IMS) cloud. The architectural diagram can be used as evidence of this requirement.
C2.2.6 Signaling Aggregation Layer	The Aggregation Layer provides connection to the Provider cloud and/or at the customer premises and acts as a point of interconnect for off-net calling to and from the public switched telephone network (PSTN) and mobile networks, handoff to emergency services, and lawful intercept (LI). The aggregation function can be realized in several ways: Cisco ASR, appropriate customer premises gateway router, or a third-party soft switch that is approved as part of the solution. Any of these components can be used as a signaling aggregation node. The Provider must explain the architectural approach they have adopted for the Aggregation Layer and which products have been deployed to provide this function. It must also be illustrated on the architectural diagram.
C2.2.7 Security	The service design must include firewalls to separate the customer premises-based components and UC applications instances in the data center. The firewalls must be deployed in a redundant mode from the Provider's cloud. Additionally, there must be a firewall between the UC applications and management domain. The architectural diagram can be used as evidence of this requirement.

Requirement	Description
Network Management The following section describes the network management function, which is an integral part of HCS to ensure a consistent and reliable user experience of the service. The overall architecture consists of multiple applications that have been integrated together to create the integrated and scalable management infrastructure required to deliver the flexibility and speed of service deployment offered by HCS. The Provider must be able to describe the overall management solution being used for HCS, incorporating each of the applications listed below that have been tested as part of the solution, and describe their function and the customer benefits of this architectural approach to service management.	
C2.2.8 Service management	Service management enables customized service definition, catalog, inventory, provisioning, activation, and workflows, as well as provisioning portals for subscribers, customer administrators, Service Providers, and service designers. This platform coordinates the functions of underlying provisioning domain managers. The Provider must explain the architectural approach adopted for the service management layer and which products have been deployed to provide this function.
C2.2.9 Fulfillment Integration Layer	For HCS deployments with Cisco UC Domain Manager (CUCDM): • The Provider must use HCM-F. For HCS deployments without CUCDM: • The Provider must provide evidence that the main features of their service offering are reliable, as well as offering different levels of service availability according to customer needs.
C2.2.10 Unified Communications application monitoring	The Provider must provide evidence that the main features of their service offering are reliable, as well as offering different levels of service availability according to customer needs.
C2.2.11 Call quality and performance monitoring	The Provider must provide evidence that the main features of their service offering are reliable, as well as offering different levels of service availability according to customer needs.
C2.2.12 Unified Communications provisioning	The Provider must provide evidence that the main features of their service offering are reliable, as well as offering different levels of service availability according to customer needs.
C2.2.13 Data center infrastructure monitoring	VMWare vCenter or like tools are used to monitor the status, health, and capacity of the virtual data center infrastructure, which is required to maintain service quality of the applications operating on that infrastructure. The Provider must provide evidence that tools and processes are employed to ensure to measure and alert on the availability, performance, and capacity of the virtual data center infrastructure.
Collaboration Service Features The following section describes the collaboration software features required to be offered on customer request. The Provider must be able to provide evidence of the business communications capabilities, explain the key benefits of the service and how it can be used to deliver enhanced business communications for the customer.	

Requirement	Description
C2.2.14 IP communications service core functions	The foundation of the service is IP-PBX call control functionality for Voice over IP (VoIP) and video telephony, using Cisco Unified Communications Manager (CUCM), version 10.6 or later. The Provider must present evidence that all of the features below are supported as part of their service, in the form of a customer demonstration: • Call features: Call forward, call hold/resume, call transfer • Phone features: hands free, visual line ring indication • Conferencing: multi-party meet me/ad hoc conferencing • Incoming/outgoing call routing • Extension mobility
C2.2.15 Voice and integrated messaging	The Provider must present evidence of support for the key features of Cisco Unity Connection 10.6 or later, including the below as part of their service description, in the form of a customer demonstration: • Address voicemails to multiple recipients • Tag as urgent, private, or regular • Search facilities to locate specific messages • Recording of conversations with recording sent to mailbox • View messages on phone display • Integration with email systems such as Outlook to allow users to manage voicemails from their mail client • SMS alerts when voicemail arrives • Speech-enabled messaging, email and calendar access • Secure messaging (no playback when sent outside company) • Auto Attendant • Speech-to-text transcription of voicemail messages The Provider must present evidence that at least six of the above messaging capabilities of the solution are supported and explain the benefits of the various features.

Requirement	Description
C2.2.16 Presence and Instant Messaging	The Provider must provide evidence that Presence and Instant Messaging (IM) capabilities are available to customers. The Provider must present evidence that the IM features below are supported and explain how they benefit the customer, in the form of a customer demonstration: • Group chat • Persistent chat • Support for multiple devices: desktop, mobile, and optionally web The Provider must present evidence that at least two of the Presence features below are supported and explain how they benefit the customer, in the form of a customer demonstration: • Always on telephony presence • Always on calendar presence • Third-party presence application integration • Network enforced presence policy • Phone presence (desktop client)
C2.2.17 Mobility and client desktop applications	An important aspect of the Collaboration service is enhancing mobility for the user. The increased use of smartphones and tablets requires that they be integrated into the overall Collaboration solution to provide maximum benefits for the customer. The Provider must present evidence that at least four of the listed mobility capabilities of the solution are supported, in the form of a customer demonstration: • Mobile to desktop, allowing a user to switch the call between devices without disruption • Dual mode calling for both iOS and Android devices (and optionally others), allowing calls to use the most cost-effective network depending on location and seamlessly hand off calls as necessary to maintain connectivity • Single number reach • Video calling via the IP-PBX • Desk phone control • Integration with other collaboration applications such as Cisco Webex • Integration of mobile presence with Cisco Unified Presence • A virtual phone (soft phone) to run on both Microsoft Windows and Mac desktops and provide office number portability via a VPN connection from any remote site

Requirement	Description
C2.2.18 Unified messaging	Messages for users may arrive in multiple formats and may need to be accessed via different methods. To enhance productivity for the user it is important to understand the capabilities of the solution and how they may be applied. The Provider must present evidence that at least three of the below Unified Messaging capabilities are supported, in the form of a customer demonstration: • Receiving faxes in email inboxes • Playing voice messages via email systems such as Microsoft Outlook • Visual voicemail via Microsoft Windows, Mac, iOS, and Android devices • Secure voice messaging: Ability to play back messages encrypted with Cisco Unity Connection through Microsoft Windows, Mac, iOS, and Android clients • Options for localized or central voicemail support
C2.2.19 Secure collaboration	Security is a key enabler for extending Unified Communications services to remote users and inter-business collaboration. Cisco Security for UC provides interoperability services that allow for more open and collaborative systems while at the same time protecting those systems from threats and improper use. The Provider must present evidence of how security is achieved in the UC architecture. At least three of the following capabilities must be utilized, in the form of a customer demonstration: • Password and PIN policy • Call restriction tables to prevent toll fraud • Secure private messaging • Voice message aging policies • Security event logging
C2.2.20 Internet access to services	If a Provider offers access of the Internet as part of their service offering, then the following devices must be supported: • Expressway: The Cisco Expressway enables remote access over the Internet for TelePresence endpoints and Jabber. The Provider must deploy at least one pair of Cisco Expressway (C and E) per customer and add more Expressway clusters to meet the scaling needs. • Session Border Controller (SBC): The SBC is used as a Network Address Translation (NAT) firewall and media anchoring network device. It performs address translation and media anchor role for inter-enterprise calls. • For Local Trunk breakout, the Provider must deploy Cisco TDM-IP Gateway or similar for all customer inbound calls.

C2.3 Customer Requirements

Requirement	Description
Customer VoIP Infrastructure Each customer is supported with the customer's unique instance of the required applications. The Provider must be able to explain the design solution for a typical customer, products deployed and benefits of the HCS approach in terms of feature flexibility, integration of the collaboration software deployed as well as reliability and scale of the overall solution to meet customer demands.	
C2.3.1 Customer premises layer	This layer connects customer endpoints (phones, mobile devices, local gateways, etc.) to the IP network, and provides end user interfaces to network management software. Customer premises are deployed with Survivable Remote Site Telephony (SRST) CPE, switch, and end devices only. The Cisco IP phone portfolio includes a range of phones that provide a rich feature set when controlled by Session Initiation Protocol (SIP), which is required as part of HCS. The Provider must present evidence that the design of the customer premises solution incorporating these features and explain the benefit of the solution for the customer. Solution must be delivered on a Cisco platform.
C2.3.2 Call routing	The Hosted Collaboration Solution licensed Cisco Unified Communications Manager (CUCM) will route internal calls across the network and off-net calls via a SIP trunk to the Provider's SIP network. The Provider must present evidence that this is deployed as part of the solution, and that it is delivered on a Cisco platform.
C2.3.3 Customer migration plan	The Provider must present evidence that the capability to build a clear migration plan that allows the customer to move over to the new service while interoperating with the existing service. The plan must take into consideration the customer's existing infrastructure and business priorities and ensure continuity of service throughout the migration, demonstrating the added value to the customer of each stage.

C2.4 Service-Level Management Requirements (Operate)

Requirement	Description
Service-Level Agreement (SLA) Components This section describes the SLAs that the Provider must contract for as part of the service. These are normally available as part of the service description. Existing customer contracts that include the relevant SLAs may also be presented as evidence of meeting these requirements.	
C2.4.1 Mean Time to Notify (MTTN)	If the customer experiences any resource or performance-affecting event the Provider must notify the customer of the issue. May vary according to customer agreements. MTTN measures the average time taken to notify a customer of an issue. Measured from the time that an alarm is generated to the time the customer notified, which can be by any method of communication agreed with the customer.

Requirement	Description
C2.4.2 Mean Time to Restore Service (MTRS)	If there is a disruption to the performance or availability of resources allocated to a customer, the Provider must provide an expectation of restoration time. May vary according to customer agreements. MTRS measures the total elapsed time from the start of a service outage to the time the service is restored. Also known as Mean Time to Restore (MTTR). Suggested guidelines for restoring services to the previous known working configuration based on priority levels are as follows: • P1: 4 hours • P2: 24 hours • P3: 2 business days • P4: 5 business days
C2.4.3 Existing user changes	Changing a user profile may be the responsibility of the Provider, or the customers may be given access to do this themselves. If the customer carries out these changes, the Provider must present evidence of how access is provided. If changes are the responsibility of the Provider, published service description or example existing customer documentation must be provided showing what agreement is in place for how quickly user changes will be implemented.
C2.4.4 User addition to service	The addition of new subscribers may be the responsibility of the Provider or of the customer. If the customer carries out these changes, the Provider must provide evidence of how access is provided. If changes are the responsibility of the Provider, published service description or example existing customer documentation must be provided showing what agreement is in place for how quickly users will be added.
Customer Web Portal The following section describes the online facilities that must be made available to the customer to view their service. May be proven by a demonstration of portal from customer viewpoint, including real-time view of connectivity and status. Mechanisms may include password protection or similar restrictions to access the online web portal for downloading reports. The Provider must also be able to demonstrate that event logs can be stored and made accessible. If for some reason the Provider chooses not to provide a customer web portal, evidence must be provided of how the required information and features are provided to the customers and the delivery method. The lack of a customer web portal does not waive any of the requirements.	
C2.4.5 Service role-based portal	Provide an operational view for multiple audiences, providing functionality and visibility based on the role of the person, such as service administrators, responsible for setting up customers and managing HCS resources. The Provider must demonstrate the provided portal and how various user roles are implemented.
C2.4.6 Self-Care Customer Portal	Provides capabilities for subscribers to amend the services that they subscribe to, based on the service capabilities for which they are licensed.

Requirement	Description
External Reporting The following section describes the reports that are to be made available to the customer via customer portal. Example reports must be provided or a view of customer web portal with ability to select reports listed. If for some reason the Provider chooses not to provide reporting via a customer web portal, evidence must be provided of the reports available and the delivery method. The lack of a portal does not waive any of the requirements. Web-based reporting via a customer web portal is considered a best practice and allows Providers to differentiate themselves from other Providers.	
C2.4.7 Service availability reports	Provide a summary view of service availability which may allow for details down to specific sites and/or equipment.
C2.4.8 Device inventory reports	Provide reports of devices under management for the customer, including data that is relevant to the customer regarding inventory of equipment or WAN services used in delivering the Collaboration service.
C2.4.9 Incident management reports	Provide reports detailing the current work activities to correct incidents on the customer network, and metrics on the management of incidents, such as number of incidents, average time to resolve, and common causes identified.
Internal Performance Reporting The following section describes reports that are to be internally created and reviewed. May be proven by provision of example reports or demonstration of reporting tool with ability to select reports listed.	
C2.4.10 Customer-related reports with internal performance metrics	Generator and review reports on metrics related to service performance, including: • SLA violations • Performance against internal Service-Level Objectives (SLOs), which are typically more stringent than those agreed with the customer

C3 Contact Center as a Service Based on HCS

Introduced: October 2010
Last updated: August 2021

Overview

Cisco Powered Contact Center as a Service Based on HCS (HCS_CC) delivers a connected digital experience, used to improve the end customers' journey, and is delivered as a cloud service from the Provider. There are two viable platforms which can be used to deliver the service: Cisco Unified Contact Center Enterprise (UCCE) and Cisco Unified Contact Center Express (UCCX). UCCE is highly scalable, and it is designed for companies with up to 12,000 concurrent knowledge workers or agents per Cisco Contact Center instance. Cisco Unified Contact Center Express (UCCX) with HCS enables Providers to host UCCX in the HCS environment when using HCS with the Open Provisioning Architecture.

C3.1 Prerequisites

The Provider must meet the following prerequisites to apply for this service designation.

Requirement	Description
C3.1.1 Submit at least two customer references for the service	Reference Customers • Reference customers must be under existing contractual relationships • One customer may serve as a reference to multiple Cisco Powered Service designations • One customer with multiple sites satisfies the requirement for a single reference, as the intent is to ensure that the Provider has proven and repeatable service practices • Two customer references are required only once: either with a new Cisco Powered Service application or upon first-year renewal • Use the Customer Reference Validation form to either submit references or to indicate references will be provided upon first year renewal Evidence: Customer Reference Validation Form uploaded into the Provider application
C3.1.2 Meet Unified Communications as a Service Based on HCS (HCS) requirements	Refer to the Unified Communications as a Service Based on HCS (section C2) for requirements. Unified Communications as a Service Based on HCS and Contact Center as a Service Based on HCS may be audited at the same time. If audited separately, Cisco's Partner Locator will be used to confirm the Provider has achieved the designations for Unified Communications as a Service Based on HCS.

Requirement	Description
C3.1.3 Have a commercial agreement in place with Cisco	HCS requires a contractual commitment between the Provider and Cisco that outlines the licensing agreements and any volume commitment. The Provider must provide evidence that a buying agreement addendum has been added to the Provider's reseller agreement. For assistance in executing the addendum, contact the Cisco Account Team.

C3.2 Provider System/Solution Requirements (Build)

UCCE based Requirement	Description
Service Capabilities The following two sections describes the basic functions of a Contact Center as a Service Based on UCCE HCS for CC and UCCX Based offering. Section C3.2.3.x are requirements to deploy the UCCE based HCS for CC solution, and section C.3.2.4.x are requirements to deploy UCCX based deployments. The Provider must provide evidence of the Contact Center as a Service Based on HCS capability for technology being offered (section C3.2.3.x for UCCE based offerings, section C3.2.4.x for UCCX based offerings, or both should Provider chose) and must explain the key benefits of the service and how it can be used to deliver the benefits of the Cisco Contact Center solution as a managed service.	
C3.2.1 Deployment that adheres to one of the four reference architectures when using UCCE or adhere to UCCX design guidelines for HCS with UCCX	Reference architectures for HCS-CC can be found in the Install and Upgrade Guides document. Design guidelines for UCCX with HCS is found in the UCCX Solution Design Guide. Any deviation from the reference architecture models must be disclosed at the time of audit or renewal.
C3.2.2 Provide the following documents unique to the service: • Service-Level Agreement (SLA) • Marketing Service Description (MSD)	Service performance is monitored through having Service-Level Agreements (SLAs) in place and effective processes to measure and report on whether they are being met. The Provider must provide an actual SLA with an existing customer or SLAs for multiple customers. The Marketing Service Description (MSD) is a document produced by the Provider that explains to a potential customer what the service is and what features and benefits it provides. The MSD must be a published document.
C3.2.3 Ensure Technical Proficiency on technology (UCCE based HCS-CC or UCCX)	To Offer UCCE based solution: • Unified Contact Center Enterprise 9.0 and later is required. • The Provider must hold the UCCE Authorization or have personnel that have completed the UCCE Deployment Engineer/TAC Support (DE/TS) and Customer Voice Portal Developer training. To Offer UCCX based Technology: • The Provider must have the Advanced Collaboration Specialization. • The Provider must have deployed a minimum of 5 Unified Contact Center Express solutions (including Enterprise customers) in the previous 2 years. See Specializations for more information.

UCCE based Requirement	Description
C3.2.3.1 Call control platform	All calls must be routed via HCS Cisco UCM to contact center agents as detailed in the UCCE Install and Upgrade Guides.
C3.2.3.2 Customer Voice Portal as network Interactive Voice Response	The Interactive Voice Response (IVR) feature provides information to callers and collects information from callers before they speak to a live agent. The Provider must demonstrate of how Customer Voice Portal is supported.
C3.2.3.3 Deployment type	Unified Contact Center Administration deployment type selection, must be one of the following: • HCS-CC 500 Agents • HCS-CC 2000 Agents • HCS-CC 4000 Agents (includes Small Contact Center) • HCS-CC 12000 Agents Provider must provide evidence that all deployment rules and capacity info have passed validation (using the Unified CC Administration deployment page).
C3.2.3.4 Agent IP phone support	Provider must show compliance within HCS UCM for IP phone models as listed in HCS-CC Design Guide – under Operating Considerations. Agent IP phones must support Built-in-Bridge (BIB) and Computer Telephony Integration (CTI) controlled features under SIP control. SCCP phones are not supported.
C3.2.3.5 Network routing with Computer Telephony Integration	The network-based Automatic Call Distributor (ACD) function is combined with CTI services to deliver data to the agent desktop. Agent Desktop must be either Cisco Finesse or Cisco CTIOS. The Provider must provide evidence of how ACD is supported.
C3.2.3.6 Agent support	Provides support for agents in offices or homes using one or more of the four options below: • Remote office with agents and local trunk breakout • Remote office with MPLS connectivity and CC Agents • Cisco CVO Home Agents with broadband • Mobile Agent with PSTN phone The Provider must provide evidence of how agents are supported, such as architectural or topology diagrams.
C3.2.3.7 Remote Silent Monitoring	Remote Silent Monitoring enables a caller to dial into and listen to an agent conversation. The Provider must provide evidence of how Remote Silent Monitoring is supported, if included as part of the Provider's offering.

UCCE based Requirement	Description
C3.2.3.8 Intelligent Call Routing	Calls are routed between contact centers based on call context information (dialed number and caller ID), caller entered digits, agent availability, and customer information from databases. The Provider must provide evidence of how Intelligent Call Routing is supported.
C3.2.3.9 In-bound call routing	For SIP Trunks are being aggregated into a Session Border Controller (SBC). The Provider must deploy either CUBE (SP) or Metaswitch Perimeta for HCS for CC. The SBC is used as a Network Address Translation (NAT) firewall and media anchoring network device. It performs address translation and media anchor role for inter-enterprise calls. For Local Trunk breakout, the Provider must deploy either Cisco TDM-IP Gateway or CUBE-E for all customer inbound calls.
C3.2.3.10 Integration of Cisco Unified Customer Voice Portal (CVP)	Delivers intelligent, personalized self-service over the phone. Cisco Unified Customer Voice Portal (CVP) enables customers to efficiently retrieve the information they need from the contact center. Customers can use touchtone signals or their own voice to request self-service information. If they request live agent assistance, Unified CVP can place a call in-queue until an appropriate agent is available and then transfer information given by the customer directly to the agent along with the call itself to provide a seamless customer service experience. In addition, Unified CVP can support video interactions, including self-service, queuing, and agent across mobile devices and kiosks. The Provider must demonstrate the use Cisco Unified Customer Voice Portal (CVP).
C3.2.3.11 Multi-channel support	The Provider must show the support for enterprise chat and email. The Provider must provide evidence of support for these applications, if included as part of the Providers offering.
C3.2.3.12 Customer Relationship Manager integration (optional)	If Customer Relationship Manager (CRM) is offered, CRM integration is only supported through the Cisco CTI server. The Provider must provide evidence of CRM integration if offered.
C3.2.3.13 Outbound dialing	The Provider must support outbound dialing capability. 100 outbound (dialer) ports per customer instance are included with agent licenses. If more than 100 ports per customer instance are required, the Provider can order additional transferable outbound dialer licenses. The Provider must provide evidence of support for outbound dialing, if included as part of the Provider's offering.

UCCX based Requirement	Description
C3.2.4.1 Call control platform	All calls must be routed via HCS Cisco UCM to contact center agents as detailed in the UCCX SRND.
C3.2.4.2 Agent IP phone support	Provider must show compliance within HCS UCM for IP phone models as listed in the Cisco Hosted Collaboration Solution for Contact Center Design Guide – under Operating Considerations. Agent IP phones must support Built-in-Bridge (BIB) and Computer Telephony Integration (CTI) controlled features under SIP control. SCCP phones are not supported.
C3.2.4.3 Network routing with Computer Telephony Integration (CTI)	The network-based Automatic Call Distributor (ACD) function is combined with CTI services to deliver data to the agent desktop (Cisco Finesse). The Provider must provide evidence of how ACD is supported.
C3.2.4.4 Agent support	Provides support for agents in offices or homes using one or more of the four options below: • Remote office with agents and local trunk breakout • Remote office with MPLS connectivity and CC Agents • Cisco CVO Home Agents with broadband • Mobile Agent with PSTN phone The Provider must provide evidence of how agents are supported, such as architectural or topology diagrams.
C3.2.4.5 Intelligent Call Routing	Calls are routed between contact centers based on call context information (dialed number and caller ID), caller entered digits, agent availability, and customer information from databases. The Provider must provide evidence of how Intelligent Call Routing is supported.
C3.2.4.6 In-bound call routing	For SIP Trunks are being aggregated into a Session Border Controller (SBC). The Provider must deploy either CUBE (SP) or Metaswitch Perimeta for HCS for CC. The SBC is used as a Network Address Translation (NAT) firewall and media anchoring network device. It performs address translation and media anchor role for inter-enterprise calls. For Local Trunk breakout, the Provider must deploy either Cisco TDM-IP Gateway or CUBE-E for all customer inbound calls.
C3.2.4.7 Multi-channel support	The Provider must show the support for chat and email integrations with SocialMiner. The Provider must provide evidence of support for these applications, if included as part of the Providers offering.
C3.2.4.8 Customer Relationship Manager integration (optional)	The Provider must provide evidence of CRM integration if offered.

UCCX based Requirement	Description
C3.2.4.9 Outbound dialing	The Provider must support outbound dialing capability. The Provider can order outbound dialer licenses if these capabilities are required. The Provider must provide evidence of support for outbound dialing, if included as part of the Provider's offering.
C3.2.4.10 Workforce Optimization (WFO) usage	If WFO, which includes Compliance Recording, Quality Management and Workforce Management, is provided, Provider must demonstrate integration of Solutions Plus (or other provider) use of WFO technology.
C3.2.4.11 Use of Open Provisioning Architecture	The Provider must demonstrate that UCCX with HCS is being used exclusively with HCS Open Provisioning Architecture and is not used with the Cisco Unified Communications Domain Manager.

Requirement	Description
Infrastructure The following section describes the requirements for a service which is delivered over infrastructure owned by the Provider, and some of the call control function is located within the network rather than on the customer site.	
C3.2.5 Must use HCS Unified Communications Manager for call control	The only call control supported is provided through the HCS solution. Contact Center as a Service Based on HCS is not supported with a Hosted Collaboration Solution (Micro Node) deployment.
C3.2.6 Quality of service (QoS) assurance for remote operators	The Provider must explain how QoS is supported for remote operator calls and agent desktops, when the call and data are routed over a WAN infrastructure; for example, QoS support for Cisco Powered MPLS VPN connections.
C3.2.7 Antimalware protection for servers	There are many servers that may be used in support of the delivery of this managed service. The Provider must provide evidence that processes are in place to keep all such servers protected from malware by running some form of protection application which receives product updates and definition updates, if applicable, on a periodic basis.
Network Management The following section describes operational procedures that must be incorporated as best practices for the design and implementation of the Unified Contact Center service. The Provider must provide evidence that these procedures are being followed. This can be proven by a demonstration of the features being used or by presenting a design and implementation guide that incorporates these capabilities and is shown to be in use.	
C3.2.8 Reporting platform	Provider must have an extensible reporting engine that allows for reporting of the Contact Center activity. This can also be extended to customer administration and supervisors. The Provider can deploy one of the following: • Cisco Unified Intelligence Center • Exony VIM • Third party reporting solution The Provider must provide evidence of the reporting solution used.

Requirement	Description
C3.2.9 Contact Center Application monitoring	For version 10.0 and later: the Provider must either use Cisco Prime Collaboration for Assurance, which monitors Contact Center applications and devices for fault management or demonstrate use of another product.
C3.3.10 Contact Center Call Quality and Performance monitoring	For version 10.0 and later: the Provider must either use Cisco Prime Collaboration for Assurance (PCA), which provides and evaluates quality of the Contact Center service and performance associated with agents in a monitored network or demonstrate use of another assurance product.
C3.2.11 Contact Center Domain Manager	Contact Center Domain Manager is an extensible web portal that allows for multi-level administration of the contact center. The Provider must support Contact Center Domain Manager.
C3.2.12 Event log retention	Provider must show the capability to store events, in a log for regulatory and analysis purposes for a minimum of 13 months.

C3.3 Customer Requirements

The Provider must be able to explain the design solution for a typical customer, products deployed and benefits of the HCS approach in terms of feature flexibility, integration of the Collaboration software deployed as well as reliability and scale of the overall solution to meet customer demands.

Requirement	Description
C3.3.1 Agent Desktop hardware	The Provider must provide the customer with the hardware requirements for the agent desktops, to ensure that they are compatible with Finesse and/or CTIOS. The Provider must provide the documentation on the agent desktop hardware requirements.

C3.4 Service-Level Management Requirements

Requirement	Description
Service-Level Agreement (SLA) Components This section describes the service-level agreements that the Provider must contract for as part of the service. These are normally available as part of the service description. Existing customer contracts that include the relevant service-level agreements may also be presented as evidence of meeting these requirements.	
C3.4.1 Proper call handling SLA	The availability of the contact center agents, correct call routing, and accuracy of customer information is a critical component of the service, regardless of where the agents are located. The Provider must offer an SLA that ensures proper call handling.

Requirement	Description
External Reporting The following section describes the reports that are to be made available to the customer via customer portal. Example reports must be provided or a view of customer web portal with ability to select reports listed. If for some reason the Provider chooses not to provide reporting via a customer web portal, evidence must be provided of the reports available and the delivery method. The lack of a portal does not waive any of the requirements.	
C3.4.2 Contact Center specific reports	Reports providing agent and overall service performance; for example: • Call queuing delay • Performance against agreed Service-Levels • Average talk time • Average calls per hour • Time spent on after call work • Percentage of calls resolving customer issues • Number of calls abandoned

C8 Hybrid Cloud

Introduced: December 2022
Last Updated: February 2023

Overview

The Cisco Powered Hybrid Cloud service is defined as a Provider-delivered managed service or as-a-service offering that provides on-premise private cloud or hybrid cloud service, delivered by a Cisco Provider. The Hybrid cloud service can be centrally managed to enable interoperability for various high-value use cases, such as seamless workload and application portability and the extension of common networking and security policies across clouds.

Cisco Hybrid Cloud solutions enable in-country providers to deliver Hybrid cloud services in the following areas:

	Managed Hybrid Cloud Use-Cases				
Cisco Platforms	**Hybrid Cloud Operations**	**Private Cloud Infrastructure**	**Data Center Networking**	**Data Center Fabric (SDN)**	**Cloud Networking**
Intersight Infrastructure Service	●				
Intersight Cloud Orchestrator	●				
Intersight Workload Optimizer	●				
UCS Computing Infrastructure		●			
HyperFlex Infrastructure		●			
Nexus Dashboard			●	▲	
Nexus Cloud			▲		
Nexus Data Center Networking			●		
Application Centric Infrastructure (ACI)				●	
Cloud Network Controller					●
Application Services Engine					●

The Provider can monetize Cisco's broad portfolio of products, applications, and services to assure the highest standard of application, infrastructure, security, cloud managed services for its customers.

Training

Providers are required to build Cisco Private Cloud Infrastructure utilizing Cisco Hybrid Cloud Operations solutions to achieve Cisco Powered status. To successfully build a Managed Hybrid Cloud service, specific training is required for at minimum (2) individuals on staff utilizing the matrix below. All evidence of completed training must be uploaded to the provider application which will be validated through a 3rd party audit process.

	Managed Hybrid Cloud Use-Cases				
Required Trainings	Hybrid Cloud Operations	Private Cloud Infrastructure	Data Center Networking	Data Center Fabric (SDN)	Cloud Networking
Intersight Pre-Sales Stage 1 (link)	●	●			
Intersight Pre-Sales Stage 2 (link)	●	●			
UCS Deployment Stage 1 (link)	●	●			
UCS Deployment Stage 2 (link)	●	●			
Hyperflex Deployment Stage 1 (link)		▲			
Hyperflex Deployment Stage 2 (link)		▲			
Nexus Dashboard Deployment Stage 1 (link)			●		
Nexus Dashboard Deployment Stage 2 (link)			●		
ACI Deployment Stage 1 (link)				▲	▲
ACI Deployment Stage 2 (link)				▲	▲
Nexus Switching Deployment Stage 1 (link)			●		
Nexus Switching Deployment Stage 2 (link)			●		

● Required training ▲ Optional training

Example: If a Provider is applying for the Hybrid Cloud Operations use-case:

1) a minimum of two individuals must provide evidence of the Data Center and Pre-Sales Black-Belt training and
2) a minimum of two individuals must provide evidence of the AppDynamics Associate Administrator Certification along with either the AppDynamics Performance Analyst Certification or the AppDynamics Implementation Certification.

Note: if a provider is applying for more than one use-case the same individuals may be used to meet the training qualifications of the additional use-cases.

Prerequisites

	Requirement	Evidence
	Cloud Service Provider Program Alignment Cloud Services are a critical requirement for any hybrid cloud solution and is why Cisco requires program alignment with AWS, Google Cloud, or Microsoft Azure. Provider must be a registered partner at one major cloud service provider listed below. Provider must be registered as top tier or level partner and be registered in the respective Cloud Service Provider's Manager Service Provider Program. **AWS** • Premier Managed Service Provider Program **Google** • Premier Managed Service Provider Program **Microsoft Azure** • Expert Managed Service Provider Program For more information, visit AWS Partner Program For more information, visit Google Cloud Partner Program For more information, visit Microsoft Azure Partner Program	Provider must provide evidence of current enrollment in one of three specified Cloud Service provider MSP Programs at the time of audit
C8.PR.1	**Customer References** • Reference customers must be under existing contractual relationships • One customer may serve as a reference to multiple Cisco Powered Service designations • One customer with multiple use cases satisfies the requirement for a single reference, as the intent is to ensure that the Provider has proven and repeatable service practices • Two customer references are required only once: either with a new Cisco Powered Service application or upon first-year renewal • Use the Customer Reference Validation form to either submit references or to indicate references will be provided upon first year renewal	Customer Reference Validation Form uploaded into the Provider application
	Cisco Certifications Cisco Certified individuals are responsible for designing and delivering modernized hybrid cloud solutions based on Cisco technologies. **Two** individuals must **each hold a Cisco Expert-Level certification**: • CCIE Data Center Certification **For more information, visit Cisco Certifications**	Evidence of Cisco Certification must be uploaded into the Provider application • Evidence for Individual 1 • Evidence for Individual 2

	Requirement	Evidence
C8.PR.4	**Managed Hybrid Cloud Use-Cases** The provider must have Private Cloud Infrastructure utilizing Hybrid Cloud Operations in market as a managed service and specified in the provider application: 1. Hybrid Cloud Operations 2. Private Cloud Infrastructure 3. Data Center Networking 4. Data Center Fabric (SDN) 5. Cloud Networking	A minimum of one use-case must be specified in the Provider application
C8.PR.9	**Training Evidence** Upload evidence of completion for all Training required for this Cisco Powered Service.	Evidence of training must be uploaded into the Provider application.

Service Offer

	Requirement	Evidence
C8.SO.1	**Service Level Agreements** Service performance is committed through Service-Level Agreements (SLAs) between the Provider and End Customers, which are backed by processes to measure and report on whether those commitments are met. Service performance elements covered by the SLA may include: • Platform availability: ability for the applicable FSO Elements to process the required functions, orchestration, and service interfaces/integrations • Mean Time to Notify (MTTN): MTTN measures the average time taken to notify a customer of an issue with the subscribed service. The measurement encompasses the time that an alert is generated to the time the customer notified, which can be by any method of communication agreed upon with the customer • Mean Time to Restore Service (MTRS): MTRS measures the total elapsed time from the start of a resource outage to the time the service is restored. This is also known as Mean Time to Restore/Repair (MTTR). The turnaround time for implementing changes requested by the customer. Must be within 48 hours for standard changes.	Evidence of Service-Level Agreements (SLAs) must be uploaded into the Provider application One of: • Executed Service Level Agreement • Service Level Agreement template
C8.SO.2	**Operations Function** Operations are a centralized function, often referred to as a IT Operations Center employing people, processes, and technology to continuously monitor and improve the Partner's customer environment or application(s) while preventing, detecting, analyzing, and responding to incidents. Partner must document the operation of their IT Ops Function for incident prevention, detection, business relevancy and response capabilities.	*Waived for Gold Providers* Evidence of operations function documentation must be uploaded into the Provider application

	Requirement	Evidence
C8.SO.3	**Service Requirements** The Provider must show evidence of a MRD or PRD for this service. At a minimum, these documents should address: • Target customer segment and clearly defined use cases • Service packaging and pricing structure • Customer value proposition of the service Formal requirements help align the business on a definition of success. These documents, such as a Marketing Requirements Document (MRD) or a Product Requirements Document (PRD) ensure that the various stakeholders' requirements are cataloged and addressed, increasing the likelihood of market success dramatically.	Evidence of service requirements documentation must be uploaded into the Provider application
C8.SO.4	**Service Description** The Service Description is an End-User facing document which explains the service features, benefits, and business outcomes to a potential customer. Typically, a Service Description would include an outline of the different tiers of service such as bronze, silver, or gold, and the features available at each tier.	Evidence of service delivery documentation must be uploaded into the Provider application

Service Delivery

	Requirement	Evidence
C8.SD.1	**Service Delivery Function** For use-case(s) specified in section C8.PR.4, the Provider must provide a Service Architecture document which describes the key technology components, how they are integrated, and how End-Users access the service. It should cover: • Cisco platform integrations with Provider tools • End-customer and Provider Access and security control/measures • Best practice for integrating to Provider end-customer environments (private/public) • Customer on-boarding process Service Offering Matrix including offer packages (e.g., Small-Medium-Large) and tiers (e.g. good-better-best)	Evidence of service delivery must be uploaded into the Provider application. **Requirements:** • Service Architecture document • Description of how the availability and health of the service is monitored • Service Offering Matrix (standard scoping and tiering)

Customer Success

	Requirement	Evidence
C8.CS.1	**Customer Success Practice** Customer Success is the function within a Provider organization responsible for managing the relationship between the Provider and its customers. The goals of Customer Success are to • maximize customer value • increase service adoption • ensure ease of use • increase customer satisfaction • drive service renewal Provider must demonstrate processes and metrics that support each of the following elements of a customer success practice: • Customer on-boarding and service activation process • Service renewal process • Service renewal rate measurement • Dispute and escalation handling processes • Ongoing customer communications • Regular business review process to periodically assess business requirements and change management needs	*Waived for Gold Providers* Customer Success Practice Description document
C8.CS.2	**User Guide** A User Guide is a document provided to customers showing how to access the customer service portal for self-service capabilities which may include service activation, on-boarding, configuration and reporting for the audited service.	User guide document

Recommended Best Practices

In addition to the core requirements for Cisco Powered Services validation above, the following section includes several noteworthy Best Practices that have been shown to greatly contribute to the market success of Managed Service offerings. While these Best Practices will not be inspected during the validation process, Cisco strongly recommends that Providers implement them.

Recommendation
Digital presence Most buyers will complete their research online before engaging with the Provider’s sales team. Online presence may include a web page, micro site, social media, podcast, and marketing events.
Align digital marketing to the buyer journey Prospective customers complete the majority of purchasing decision research before engaging a Provider’s sales contacts. It is a best practice to ensure that rich digital marketing content with clearly defined use cases is in place through the buyer’s journey. This may include a micro web site, social media, podcasts, and interactive marketing events such as webinars.
Sales Compensation policy It is recommended for the provider to have a sales compensation policy that incentivizes and rewards the involved teams for selling the service.
Sales Training It is recommended for the provider to have a process to train both sales representatives and sales engineers for the service
Sales Enablement It is recommended for the provider to develop sales enablement materials: • Battle card • Call script • Email template • Demo portal • Demo video Please reach out to your Cisco Account Team. for examples of these materials.

C10 Cloud Calling

Introduced: December 2018
Last Updated: December 2022

Overview

Note: Cloud Calling was previously named Webex Calling SP.

Cisco Powered **Cloud Calling** Services are delivered from a robust cloud infrastructure and enable Providers to significantly reduce time-to-market for delivering Unified Communication (UC) services. Cloud Calling is comprised of a comprehensive collaboration portfolio that complements other Cisco collaboration technologies, including Webex Meetings and Webex Teams. Unified Communications as a Service based on Cisco Webex Calling provides an industry leading set of capabilities to subscribers enabled by cloud-native rapid feature enhancements and improvements to the user experience.

Prerequisites

	Requirement	Evidence
C10.PR.1	**Customer References** • Reference customers must be under existing contractual relationships • One customer may serve as a reference to multiple Cisco Powered Service designations • One customer with multiple sites satisfies the requirement for a **single** reference, as the intent is to ensure that the Provider has proven and repeatable service practices • Two customer references are required only once: either with a new Cisco Powered Service application or upon first-year renewal • Use the Customer Reference Validation form to either submit references or to indicate references will be provided upon first year renewal	Customer Reference Validation Form uploaded into the Provider application
C10.PR.2	**Collaboration SaaS Specialization** The Provider must hold the Collaboration SaaS Specialization. Partner Locator will be used to confirm the Provider has achieved the Collaboration SaaS Specialization.	Partner Locator will be used to confirm the Provider has achieved the Collaboration SaaS Specialization.
C10.PR.3	**Advanced Collaboration Architecture Specialization (Required only for C10.SD.6: Dedicated Instance)** In order to deliver the Dedicated Instance option (C10.SD.6), the Provider must hold the Advanced Collaboration Architecture Specialization.	Partner Locator will be used to confirm the Provider has achieved the Advanced Collaboration Architecture Specialization

	Requirement	Evidence
C10.PR.4	**Training Evidence** Upload evidence of completion for all Training required for this Cisco Powered Service.	Evidence of training must be uploaded into the Provider application. Refer to requirements in sections C10.SD.8 and C10.SP.1

Service Offer

	Requirement	Evidence
C10.SO.1	**Service Level Agreements** Service performance is committed through having Service-Level Agreements (SLAs) in place between the Provider and End-User which are backed by processes to measure and report on whether those commitments are being met. Service performance elements covered by the SLA may include: • Platform availability: infrastructure, orchestration, and service interfaces • Network availability: the network operated by the Provider that is used to provide connectivity from the Internet or private WAN, involved data centers, and/or a third party used to provide network connectivity • Mean Time to Notify (MTTN): MTTN measures the average time taken to notify a customer of an issue with the subscribed service. The measurement encompasses the time that an alert is generated to the time the customer notified, which can be by any method of communication agreed upon with the customer • Mean Time to Restore Service (MTRS): MTRS measures the total elapsed time from the start of a resource outage to the time the service is restored. This is also known as Mean Time to Restore/Repair (MTTR). In some cases, a cloud-based service, brokered by a third party, may not have a platform availability SLA. The Provider must still provide SLA parameters such as MTTN to the customer.	One of: • Executed Service Level Agreement • Service Level Agreement template
C10.SO.2	**Service Requirements** Formal requirements help align the business on a definition of success. These documents, such as a Marketing Requirements Document (MRD) or a Product Requirements Document (PRD) ensure that the various stakeholders' requirements are cataloged and addressed, increasing the likelihood of market success dramatically. The Provider must show evidence of a MRD or PRD for this service. At a minimum, these documents should address: • Target customer segment and clearly defined use cases • Service packaging and pricing structure • Customer value proposition of the service	A table of contents or redacted version of one of: • Marketing Requirements Document (MRD) • Product Requirements Document (PRD) of the service

	Requirement	Evidence
C10.SO.3	**Service Description** The Service Description is an End-User facing document which explains the service features, benefits, and business outcomes to a potential customer. Typically, a Service Description would include an outline of the different tiers of service such as bronze, silver, or gold, and the features available at each tier.	Service Description document
C10.SO.4	**PSTN Operations** Partner must document its PSTN implementation strategy for its customers. Partner may leverage the PSTN capabilities of: • a Cisco CCP Provider, or • The partner's own PSTN capabilities if they offer them directly or through direct partnerships with other PSTN vendors. Partner should describe how PSTN capabilities are integrated with the Partner's managed services operations.	Both of: • Documentation of incident prevention, detection, and response processes consistent with Provider's SLA • Documentation of the provisioning processes and support specific to the PSTN capabilities

Service Delivery

	Requirement	Evidence
C10.SD.1	**Service Architecture** The Provider must provide a Service Architecture document which describes the key technology components, how they are integrated, and how End-Users access the service. The Provider must also describe how the availability and health of the service is monitored.	Both of: • Service Architecture document including the key technology components, how they are integrated, and how End-Users access the service • Description of how the availability and health of the service is monitored
C10.SD.2	**Implementation and Migration** Provider is responsible for the implementation and migration processes included in the service delivery. To demonstrate these capabilities, the Provider must provide examples of implementation and migration process and procedures, including data collection of customer requirements, provisioning processes and rollout of the services, including any phone/device rollout plans.	Both of: • Sample rollout plan/SOW • Documented implementation process, including data collection of customer requirements, provisioning processes and rollout of the services, including any phone/device rollout plans
C10.SD.3	**Support service** Provider must act as single point of first line support of the Cloud calling service covering all aspects of incident response and escalation processes.	Both of: • Service Description document • Service Operation Guide/Runbook

	Requirement	Evidence
C10.SD.4	**Software License Management** The Provider must ensure a valid software license is applied to CPE devices used for service delivery. Failure to properly manage the software license expiration could result is a service outage for the customer.	Demonstration of the license management process
C10.SD.5	**Proactive Monitoring of the Cloud Calling Service** The Provider must offer proactive monitoring as part of the cloud managed calling service. The CPE device is proactively monitored for availability and health from the Provider's operation center rather than waiting for the customer to notify the Provider of a problem. **The Provider must provide an operations procedure document or demonstration of the network management systems where the status of end customer devices can be viewed as evidence of meeting this requirement.**	One of: • Operations procedure document • Demonstration of the network management systems showing the status of end customer devices
C10.SD.6	**Dedicated Instance (optional)** The Provider may optionally offer support for Webex Calling Dedicated Instance, in addition to base support for the multi-tenanted Cloud Calling offer. The provider must perform the following Dedicated Instance tasks: • Initiate the DI automation build process by answering customer specific questions related to their calling requirements • Establish private DI peering between customer premise to Webex Calling DI Cloud • Migrate existing customer deployment to Webex Calling DI Cloud leveraging Provider's existing UCM best practices and methods of operations	*Optional* Both of: • Service Description document • Service Architecture document
C10.SD.7	**Customer Provider Service Portal** The Provider is to offer a secure web portal to present an operational view of the managed service, for multiple audiences, designed to give a view of the network and device status must have their partner view in Control Hub operationalized to manage their customers from a single pane of glass. Additionally, the provider may optionally provide a ticketing system front end for customers through the Service Portal.	Both of: • Demonstration of the secure web portal • User Guide that includes information on the portal
C10.SD.8	**Technical Training** The Provider is required to have two staff members who are Cisco Webex Calling Admin Certified. Refer to Cisco BroadSoft Training Certifications for more information. As evidence of this requirement, the Provider must provide scanned copies of the certificates received from the training courses.	Email confirmations for Engineer 1 Email confirmations for Engineer 2

Service Marketing

	Description	Evidence
C10.SM.1	**Digital presence** Most buyers will complete their research online before engaging with the Provider's sales team. Online presence may include a web page, micro site, social media, podcast, and marketing events.	One of: • Demonstrate a service-specific online presence with service specific marketing content, • A marketing plan across various marketing channels and platform
C10.SM.2	**Align digital marketing to the buyer journey** Prospective customers complete the majority of purchasing decision research before engaging a Provider's sales contacts. It is a best practice to ensure that rich digital marketing content with clearly defined use cases is in place through the buyer's journey. This may include a micro web site, social media, podcasts, and interactive marketing events such as webinars.	Buyer Journey Map document

Sales Operations

	Description	Evidence
C10.SP.1	**Webex Calling Sales Training** The Provider is required to have two staff members who are Cisco Webex Calling Sales Certified Refer to Cisco BroadSoft Training Certifications for more information. As evidence of this requirement, the Provider must provide scanned copies of the certificates received from the training courses.	Email confirmation for Sales Person 1 Email confirmation for Sales Person 2
C10.SP.2	**Sales Training** Provider must have a process to formally train both sales and sales engineers for the service	Sales Training Plan document

	Description	Evidence
C10.SP.3	**Sales Enablement** Provider must provide evidence of an **End Customer-facing pitch deck** and at least two of the following sales enablement materials: • Services at-a-glance • Service brochure or video • Battle card/sales reference card • Sales playbook • Call script • Email template • Demo Please reach out to your Cisco Account Team for examples of these materials.	• End Customer-facing pitch deck and at least **two** of: • Services at-a-glance • Service brochure or video • Battle card/sales reference card • Sales playbook • Call script • Email template • Demo
C10.SP.4	**Sales Compensation policy** Provider must have a sales compensation policy that incentivizes and rewards the involved teams for selling the service	Sales Compensation Policy document

Customer Success

	Requirement	Evidence
C10.CS.1	**Customer Success Practice** Customer Success is the function within a Provider organization responsible for managing the relationship between the Provider and its customers. The goals of Customer Success are to: • Maximize customer value • Increase service adoption • Ensure ease of use • Increase customer satisfaction • Drive service renewal For Evidence Option #2 (Customer Success Practice documentation): Provider must demonstrate processes and metrics that support each of the following elements of a customer success practice: • Customer on-boarding and service activation process • Service renewal process • Service renewal rate measurement • Dispute and escalation handling processes • Ongoing customer communications Regular business review process to periodically assess business requirements and change management needs	One of: 1. Customer Success Practice documentation 2. Customer Experience or Advanced Customer Experience Specialization (no further evidence required if the Specialization is held)

	Requirement	Evidence
C10.CS.2	**User Guide** The User Guide is a document provided to customers showing how to access the customer service portal for self-service capabilities which may include service activation, on-boarding, configuration and reporting for the audited service.	User guide document
C10.CS.3	**Customer Ticketing System** A ticketing system should be in place for tracking customer change requests and system generated incidents. A ticketing system may be part of a larger IT Systems Manager (ITSM) or Customer Relationship Management (CRM) system. Reports from this system should include metrics and summaries of incidents including details such as quantity, status, average time to resolve past incidents, and how the incidents were resolved.	Demonstration of the Customer ticketing system

M6 Business Communications

Introduced: October 2007
Last updated: August 2021

Overview

Cisco Powered Business Communications service is defined as the Provider delivering Voice over IP and key functionality enabled by the Unified Communications solution. This is a managed service delivered via CUCM that is either on the customer's premise or is dedicated to the customer. The Provider must be able to explain the key benefits of the service and how it can be used to deliver enhanced productivity and efficiencies for the customer.

M6.1 Prerequisites

The Provider must meet the following prerequisites to apply for this service designation.

Requirement	Description
M6.1.1 Submit at least two customer references for the service	Reference Customers • Reference customers must be under existing contractual relationships • One customer may serve as a reference to multiple Cisco Powered Service designations • One customer with multiple sites satisfies the requirement for a single reference, as the intent is to ensure that the Provider has proven and repeatable service practices • Two customer references are required only once: either with a new Cisco Powered Service application or upon first-year renewal • Use the Customer Reference Validation form to either submit references or to indicate references will be provided upon first year renewal Evidence: Customer Reference Validation Form uploaded into the Provider application

Requirement	Description
M6.1.2 Employ at least one CCNP Collaboration certified individual on staff where service originates	The Cisco CCNP Collaboration certification (formerly known as CCNP Voice) recognizes the increased importance placed on IT professionals of today who are responsible for integrating voice technology into underlying network architectures. Individuals who earn a CCNP Collaboration certification can help create a telephony solution that is transparent, scalable, and manageable. Earning a CCNP Collaboration certification validates a robust set of skills in implementing, operating, configuring, and troubleshooting a converged IP network. The certification content focuses on Cisco Unified Communications Manager (CUCM, formerly Unified Call Manager), quality of service (QoS), gateways, gatekeepers, IP phones, voice applications, and utilities on Cisco routers and Cisco Catalyst switches. The Provider must maintain a minimum of one CCNP Collaboration overall for all Cisco Powered UC or HCS services; it does not have to be unique to each service. A Cisco CCIE certification, of any technology specialization, supersedes and fulfills the certification requirements for this service.
M6.1.3 Maintain Advanced Collaboration Architecture Specialization in country where service originates	Must have the following specialization in host theater (where NOC is located or where the Provider is headquartered). • Advanced Collaboration Architecture Specialization See the requirements here.

M6.2 Service Design

Requirement	Description
Service Capabilities The following section describes the basic functions of a business communications service delivering voice over IP as well as key functionality enabled by the Unified Communications solution. The Provider must provide evidence of the business communications capabilities; explain the key benefits of the service and how it can be used to deliver enhanced productivity and efficiencies for the customer. The Provider must demonstrate the ability to manage the service up to the most current version of Cisco Unified Communication Manager. If the Provider has already achieved Master Unified Communications or Master Collaboration Specialization, the following requirements can be waived: M6.2.1–M6.2.17.	
M6.2.1 Deliver call management from a Cisco supported hardware platform	To qualify for this Cisco Powered managed service, the call management function must be delivered on a Cisco UC on UCS supported hardware platform, and associated security functions delivered on Cisco platforms.
M6.2.2 Provide the following documents unique to the service: • Service-level agreement (SLA) • Marketing Service Description (MSD)	Service performance is monitored through having service-level agreements (SLAs) in place and effective processes to measure and report on whether they are being met. The Provider must provide an actual SLA with an existing customer or SLAs for multiple customers. See section 9.3 for SLA requirements. The Marketing Service Description (MSD) is a document produced by the Provider that explains to a potential customer what the service is and what features and benefits it provides. The MSD must be a published document.

Requirement	Description
M6.2.3 IP Communications service: business value	The foundation of the service is IP-PBX call control functionality for VoIP and video telephony, using Cisco Unified Communications Manager. This provides capabilities including: • Call features: Call forward, call hold/resume, call transfer • Phone features: hands free, visual line ring indication • Conferencing: multi-party meet me/ad hoc conferencing, call recording • Incoming/outgoing call routing • Video telephony The Provider must provide evidence of how these features provide unique business benefits to the customer by enabling a core set of communications capabilities over an IP infrastructure based on Cisco.
M6.2.4 Voice and integrated messaging	The Provider must present evidence of support for the key features of Cisco Unity® Connection, including the below as part of their service description, in the form of a customer demonstration: The Provider must exhibit support for the key features of the voice mailbox and integrated messaging functions. Features available include: • Address voicemails to multiple recipients • Tag as urgent, private, or regular • Search facilities to locate specific messages • Recording of conversations with recording sent to mailbox • View messages on phone display • Integration with email systems such as Outlook to allow users to manage voicemails from their mail client • SMS alerts when voicemail arrives • Speech-enabled messaging, email, and calendar access The Provider must present evidence that at least six of the above messaging capabilities of the solution and explain the benefits of the various features.

Requirement	Description
M6.2.5 Presence and Instant Messaging	The Provider must provide evidence that Presence and IM capabilities are available to customers. The Provider must present evidence that the IM features below are supported and explain how they benefit the customer, in the form of a customer demonstration: • Group chat • Support for multiple devices: desktop, mobile, and optionally web • Persistent chat (optional) The Provider must present evidence that at least two of the Presence features below are supported and explain how they benefit the customer, in the form of a customer demonstration: • Always on telephony presence • Always on calendar presence • Third-party presence application integration • Network enforced presence policy • Phone presence (desktop client)
M6.2.6 Support for video telephony	The service must support the integration of video. The business communications solution offers desktop integration, dedicated video endpoints, as well as integration of video calls with applications. The Provider must provide evidence that video is supported as part of the service.
M6.2.7 Mobility and client desktop applications	An important aspect of the collaboration service is enhancing mobility for the user. The increased use of smartphones and tablets requires that they be integrated into the overall collaboration solution to provide maximum benefits for the customer. The Provider must present evidence that at least four of the listed mobility capabilities of the solution are supported, in the form of a customer demonstration: • Dual mode calling for both iOS and Android devices (and optionally others): allowing calls to use the most cost-effective network depending on location and seamlessly hand off calls as necessary to maintain connectivity • Mobile to desktop: allowing a user to switch the call between devices without disruption • Single number reach • Integration with other collaboration applications such as Cisco WebEx® • Integration of mobile presence with Cisco Unified Presence • A virtual phone (soft phone) to run on both Windows and Mac desktops and provide office number portability via a VPN connection from any remote site • Desk phone control • Video calling via the CUCM

Requirement	Description
M6.2.8 Unified Messaging	Messages for users may arrive in multiple formats and may need to be accessed via different methods. To enhance productivity for the user, it is important to understand the capabilities of the solution and how they may be applied. The Provider must present evidence that at least three of the below unified messaging capabilities are supported, in the form of a customer demonstration: • Receiving faxes in email inboxes • Playing voice messages via email systems such as Microsoft Outlook • Visual voicemail via Windows, Mac, iOS, and Android devices • Secure voice messaging: Ability to play back messages encrypted with Cisco Unity Connection through Windows, Mac, iOS, and Android clients • Options for localized or central voicemail support
M6.2.9 Application Integration	A key benefit of the business communications solution is the ability to integrate applications transparently with the customer’s business tools, enabling users to quickly reach the right people and resources. This can be enabled through a number of ways, including: • Cisco Unified Application environment • XML • Client service framework The Provider must provide evidence of how applications are integrated and provide examples of the benefits for the customer. These can be Cisco applications, such as emergency responder, unified presence and unified mobility, or third-party applications such as those typically targeted at an industry vertical.
M6.2.10 Secure collaboration	Security is a key enabler for extending Unified Communications services to remote users and inter-business collaboration. Cisco Security for UC provides interoperability services that allow for more open and collaborative systems while at the same time protecting those systems from threats and improper use. This capability is enabled by the use of devices such as the Cisco ASA. In addition, the solution supports the following capabilities: • Password and PIN policy • Call restriction tables to prevent toll fraud • Secure private messaging • Voice message aging policies • Security event logging The Provider must explain how security is incorporated into the designs for the UC architecture and the benefits it enables for mobility, presence, and remote phone support.

Requirement	Description
Service Capabilities: CPE-Based Solution The following section describes the deployment requirements for the Cisco Powered Business Communications service when using CPE-based call control. The Provider must demonstrate compliance to this section if their primary service offer uses CPE-based call control.	
M6.2.11 Service resiliency design	The business communications solution includes many features that can be used to enhance overall service availability. The Provider must exhibit an understanding of these features and explain how and where they can be used in the overall solution to meet customer expectations for service availability. These include redundancy for: • Gatekeeper • Media resources • Voicemail servers • Trunking gateways that provide connectivity to the Public Switched Telecommunications Network (PSTN) • Centralized soft switch • 1:1 or 1:2 for call processing servers • Media gateways used to connect to Public Switched Telecommunications Network (PSTN) and legacy services Network-level redundancy features include: • Hot Standby Routing Protocol (HSRP) at the distribution layer routers • Survivable Remote Site Telephony (SRST)
M6.2.12 Signaling protocols	The business communications solution supports multiple call signaling protocols to provide interoperability. These include: • Session Initiation Protocol (SIP) • H.323 • Cisco TelePresence interoperability protocol • Skinny Client Control Protocol (SCCP) • H.320 The Provider must provide evidence of support of at least three of these protocols and be able to explain the difference between them and where they would normally be applied in the solution design. This must include how and where Call Admission Control may be used to manage network resources and ensure voice and video quality. Customer references can be provided that include these protocols, or a demonstration that includes evidence of which signaling protocols are being used, such as sample configurations.

Requirement	Description
M6.2.13 Campus Quality of Service (QoS) design	The design of the campus infrastructure to support the business communications traffic must conform to the guidelines outlined in Cisco best practice design guidelines Solution Reference Network Design (SRND). This must include: • At least two VLANs at Access Layer, including a native VLAN for data traffic and a voice VLAN • Defined limitation of percentage of the link assigned to high-priority traffic based on speed, technology, interface Refer to Cisco Collaboration Solutions Design Guidance
M6.2.14 CPE deployment design	The deployment design for the customer site must include the following features: • Customer edge (CE) outbound policies: • Pre-classification of traffic into appropriate classes before CPE • Priority queuing of RTP voice packet streams into egress queues • Egress Low-Latency Queuing (LLQ) for VoIP (EF) • Class-Based Weighted Fair Queuing (CBWFQ) for Call Signaling (CS3 or CS5) • Remark Call Signaling (if necessary) Customer Edge (CE) Inbound Policies: • Trust DiffServ Code Point (DSCP) • Restore TelePresence to CS4 (if necessary) • Restore Call-Sig CS3 or CS5 (if necessary)
M6.2.15 Overall service configuration and design	Cisco provides validated design guidelines to ensure services that are designed according to these best practices will meet expected service performance. The Provider must provide evidence that the overall architectural design of the solution follows these guidelines, including: • Cisco Unified Communication Manager or Cisco Unified Communications Manager Business Edition with Cisco Unified Border Element at the edge of the customer network • Cisco Unified Communications Manager Express • Cisco UC 500 with Cisco IAD • Deployment of trunking gateway to provide PSTN connectivity • Support for centralized call control to support inter customer and off-net voice routing • Support for SIP trunking

Requirement	Description
M6.2.16 Key capabilities that are supported by the solution	The Provider must support the key features of the UC solution as a part of their service design. Key features include: • Voicemail supported by Cisco Unity, Cisco Unity Connection, or Cisco Unity Express • Emergency number support • Single number reach support • Support for SIP signaling and Internetworking with H.323 • Transcoding support
M6.2.17 Anti-virus application	There are many servers that may be used in support of the delivery of this managed service. The Provider must provide evidence of the processes in place to keep all such servers protected from viruses by running some form of antivirus application on a periodic basis, with the latest virus definition files.
Service Security: Customer Premises Equipment (CPE) The following section describes operational procedures that must be incorporated as best practices for the design and implementation of service delivered from Cisco CPE, such as ISR and ASR Series router. Best practices document available at: Cisco Guide to Harden Cisco IOS Devices. The Provider must provide evidence that these procedures are being followed. This can be proven by a demonstration of the features being used or by presenting a design and implementation guide that incorporates these capabilities and is shown to be in use. The following requirements must be met using a Cisco platform. This section applies only to Providers who are using CPE-based call control.	
M6.2.18 Control Plane Security	The control plane ensures that the management and data planes are maintained and operational. If the control plane were to become unstable during a security incident, it can be impossible for the Provider to recover the stability of the network. The Provider must provide evidence of the operational procedures in place to protect the device control plane.
M6.2.19 Management Plane Security	The management plane provides access, configuration, and management of a device, as well as monitors its operations and the network on which it is deployed. The Provider must provide evidence of the operational procedures in place to protect the device management plane.
M6.2.20 Data Plane Security	The data plane is responsible for moving data from source to destination. The Provider must provide evidence of the operational procedures in place to protect the device date plane.

M6.3 Service-Level Management Requirements

Requirement	Description
Service-Level Agreement (SLA) Components This section describes the SLAs that the Provider must contract for as part of the service. These are normally available as part of the service description. Existing customer contracts that include the relevant SLAs may also be presented as evidence of meeting these requirements.	
M6.3.1 Mean Time to Notify (MTTN)	If the customer experiences any resource or performance-affecting event the Provider must notify the customer of the issue. May vary according to customer agreements. MTTN measures the average time taken to notify a customer of an issue. Measured from the time that an alarm is generated to the time the customer notified, which can be by any method of communication agreed with the customer.
M6.3.2 Mean Time to Restore Service (MTRS)	The average time taken to restore service after a failure. Measured from when the service fails until it is fully restored and delivering its normal functionality. Sometimes known as MTTR. Guidelines for restoring services to the previous known working configuration based on priority levels are as follows: • P1: 4 hours • P2: 24 hours • P3: 2 business days • P4: 5 business days
M6.3.3 User addition to service	The addition of new users may be the responsibility of the Provider, or the customers may be given access to do this themselves. If the customer carries out these changes, the Provider must demonstrate how access is provided. If changes are the responsibility of the Provider, published service description or example existing customer documentation must be provided showing what agreement is in place for how quickly users will be added. Commitment must be at least 50 per day with 3 days' notice.
M6.3.4 Existing user changes: Must offer an SLA for existing user changes	Changing a user profile may be the responsibility of the Provider, or the customers may be given access to do this themselves. If the customer carries out these changes, the Provider must demonstrate how access is provided. If changes are the responsibility of the Provider, published service description or example existing customer documentation must be provided showing what agreement is in place for how quickly user changes will be implemented.
Customer Web Portal The following section describes the online facilities that must be made available to the customer to view the current and historical performance of their service. May be proven by a demonstration of the portal from customer viewpoint, including real-time view of connectivity and status. Mechanisms may include password protection or similar restrictions to access the online web portal for downloading reports. The Provider must also be able to show that event logs can be stored and made accessible via the portal. If for some reason the Provider chooses not to provide a customer web portal, evidence must be provided of how the required information and features are provided to the customers and the delivery method. The lack of a customer web portal does not waive any of the requirements.	

Requirement	Description
M6.3.5 Secure web portal to communicate the current status and performance, including specific reports available online as agreed with the customer	Provides an operational view for multiple audiences; designed to give executives a quick view of the network status, including current availability, reliability, and security for managed devices.
M6.3.6 Event Log retention	Events relating to any infrastructure used to support the service must be stored in a log for regulatory and analysis purposes for a period of time established with the customer.
External Reporting The following section describes the reports that are to be made available to the customer via customer portal. Example reports must be provided or a view of customer web portal with ability to select reports listed. If for some reason the Provider chooses not to provide reporting via a customer web portal, evidence must be provided of the reports available and the delivery method. The lack of a portal does not waive any of the requirements. Web-based reporting via a customer web portal is considered a best practice and allows the Provider to differentiate themselves from other Providers.	
M6.3.7 Performance Analysis reports	Historical performance analysis of the service. This would typically be available over a number of sample periods (daily, weekly, monthly) and would include data to allow the customer to understand how the overall service is performing, e.g., how heavily utilized are various Wide-Area Network (WAN) or Priority Rate Interface (PRI) links or how much traffic is being generated by a particular application.
M6.3.8 Service Availability reports	Summary views of service availability reports on the overall service availability, e.g., by site or equipment.
M6.3.9 Device Inventory reports	Reports of devices under management for the customer; provide data that is relevant to the customer regarding inventory of equipment or WAN services used in delivering the service.
M6.3.10 Incident Management reports	Reports detailing the current work activities to correct incidents on the customer network, metrics on the management of incidents, such as number of incidents, average time to resolve, common causes identified.
M6.3.11 Exception reports	Reports generated by customer-specified ranges; provide ability for customers to self-select parameters on individual devices and determine thresholds for the raising of exception reports.
M6.3.12 Call Detail reports	The Provider must have the capability provide reports on the UC calls that are made. This must include: • CUCM status and performance • Call statistics (e.g., duration, failed attempts)

Requirement	Description
Internal Performance Reporting The following section describes reports that are to be internally created and reviewed. May be proven by provision of example reports or demonstration of reporting tool with ability to select reports listed.	
M6.3.13 Customer-related reports/internal performance metrics	Reports on metrics used to measure trends of service performance, including: • SLA violations • Performance against internal targets (typically more stringent than those agreed with the customer)

M7 Unified Contact Center

Introduced: October 2007
Last updated: August 2021

Overview

Cisco Powered Unified Contact Center is a service where the partner is delivering full Call Center functions and support via an IP-based infrastructure that is either on the customer premises or dedicated to the customer.

M7.1 Prerequisites

The partner must meet the following prerequisites to apply for this service designation.

Requirement	Description
M7.1.1 Submit at least two customer references for the service	Reference Customers • Reference customers must be under existing contractual relationships • One customer may serve as a reference to multiple Cisco Powered Service designations • One customer with multiple sites satisfies the requirement for a single reference, as the intent is to ensure that the Provider has proven and repeatable service practices • Two customer references are required only once: either with a new Cisco Powered Service application or upon first-year renewal • Use the Customer Reference Validation form to either submit references or to indicate references will be provided upon first year renewal Evidence: Customer Reference Validation Form uploaded into the Provider application
M7.1.2 Meet Advanced UCCE Specialized Requirements (Invite Only)	Must meet Advanced UCCE Specialization requirements in order to purchase product and deploy this managed service.

M7.2 Service Design

Requirement	Description
Service Capabilities The following section describes the basic functions of a unified contact center service. The partner must provide evidence of the Unified Contact Center capabilities; explain the key benefits of the service and how it can be used to deliver the benefits of the Cisco Unified Contact Center solution as a managed service.	
M7.2.1 Provide the following documents unique to the service: • Service-level agreement (SLA) • Marketing Service Description (MSD)	Service performance is monitored through having service-level agreements (SLAs) in place and effective processes to measure and report on whether they are being met. The partner must provide an actual SLA with an existing customer or SLAs for multiple customers; SLA terms must be no less than one year. The Marketing Service Description (MSD) is a document produced by the partner that explains to a potential customer what the service is and what features and benefits it provides. The MSD must be a published document.
M7.2.2 Virtual call center	Calls are routed to contact center agents regardless of their location over an IP-based infrastructure.
M7.2.3 Network interactive voice response	The Interactive Voice Response (IVR) feature provides information to callers and collects information from callers before they speak to a live agent.
M7.2.4 Network routing with computer telephony integration	The network-based Automatic Call Distributor (ACD) function is combined with CTI services to deliver data to the agent desktop.
M7.2.5 Remote agent support	Uses Unified Mobile Agent to provide remote agents in branch offices or homes CTI, contact distribution, and reporting capabilities.
M7.2.6 Intelligent call routing	Calls are routed between Contact Centers based on call context information (dialed number and caller ID), caller entered digits, agent availability, and customer information from databases.
M7.2.7 Email management	Service must provide support for handling customer email inquiries submitted to company mailboxes or websites.
M7.2.8 Integration with TDM-based Contact Centers	Traditional Contact Centers may have been already deployed. Support for integration with these networks to ensure an easy migration path for the customer. The partner must demonstrate this capability either by a demonstration, an example of an installed customer design, or a published service description including this capability.
M7.2.9 Intelligent call queuing (universal queuing)	The UCC solution coordinates an agent's ability to work on multiple tasks from various channels while allowing the agent to be interrupted with high-priority tasks. Examples include: • Agent handling text sessions to accept additional text sessions • Allowing an agent dealing with email queries to accept priority voice calls • Rerouting calls based on predefined wait time

Requirement	Description
M7.2.10 Integration of Cisco Unified Customer Voice Portal (CVP)	Delivers intelligent, personalized self-service over the phone. Cisco Unified Customer Voice Portal (CVP) enables customers to efficiently retrieve the information they need from the contact center. Customers can use touchtone signals or their own voice to request self-service information. If they request live agent assistance, Unified CVP can place a call in-queue until an appropriate agent is available and then transfer information given by the customer directly to the agent along with the call itself to provide a seamless customer service experience. In addition, Unified CVP can support video interactions, including self-service, queuing, and agent across mobile devices and kiosks.
M7.2.11 Web 2.0 Integration	Support for Web 2.0 features such as: • Click to Talk • Chat room • Video links • Customer feedback
M7.2.12 Customer Relationship Manager (CRM) integration	CRM connector integrates third-party CRM applications with the UCC solution to allow agents to log in, control agent status, and conduct calls through the CRM interface. CRM information is also provided to the agent when a new call arrives. The partner must demonstrate how UCC correlates information from the incoming call and integrates information from the CRM.
M7.2.13 Voice XML support	Provides technology to deliver Interactive Voice Response (IVR) and other call control applications at the branch office or edge of the network. Voice XML browser sessions allow incoming PSTN calls to get IVR treatment from the gateway rather than burning bandwidth to process media at the centralized server.
Infrastructure (applies only to organizations providing the infrastructure for delivery of the service, e.g., carriers) The following section describes the requirements for a service that is delivered over infrastructure owned by the partner, and some of the Call Control function is located within the network rather than on the customer site. If the partner has already achieved Master Unified Communications or Master Collaboration Specialization, the following requirements can be waived: M7.2.13–M7.2.15.	
M7.2.14 The service must run over an IP transport network that is delivered on Cisco infrastructure	To qualify for this Cisco Powered managed service, the IP transport must be delivered on Cisco infrastructure, with the Provider Edge provisioned on Cisco platforms.
M7.2.15 Quality of Service (QoS) assurance for remote operators	The partner must explain how the quality of service for calls to remote operators over a WAN infrastructure is assured, for example, it runs over a Cisco Powered MPLS VPN service.
M7.2.16 All servers running antivirus application with latest virus definition files	There are many servers that may be used in support of the delivery of this managed service. The partner must demonstrate processes in place to keep all such servers protected from viruses by running some form of antivirus application on a periodic basis.

Requirement	Description
Service Security: Customer Premises Equipment (CPE) The following section describes operational procedures that must be incorporated as best practices for the design and implementation of service delivered from Cisco CPE, such as ISR and ASR Series router. Best practices document is available at: Cisco Guide to Harden Cisco IOS Devices. The partner must provide evidence that these procedures are being followed. This can be proven by a demonstration of the features being used or by presenting a design and implementation guide that incorporates these capabilities and is shown to be in use. The following requirements must be met using a Cisco platform.	
M7.2.17 Control Plane Security	The control plane ensures that the management and data planes are maintained and operational. If the control plane were to become unstable during a security incident, it can be impossible for the partner to recover the stability of the network. The partner must provide evidence of the operational procedures in place to protect the device control plane.
M7.2.18 Management Plane Security	The management plane provides access, configuration, and management of a device, as well as monitors its operations and the network on which it is deployed. The partner must provide evidence of the operational procedures in place to protect the device management plane.
M7.2.19 Data Plane Security	The data plane is responsible for moving data from source to destination. The partner must provide evidence of the operational procedures in place to protect the device date plane.

M7.3 Service-Level Management Requirements

Requirement	Description
Service-Level Agreement (SLA) Components This section describes the service-level agreements that the partner must contract for as part of the service. These are normally available as part of the service description. Existing customer contracts that include the relevant service-level agreements may also be presented as evidence of meeting these requirements.	
M7.3.1 Mean Time to Notify (MTTN)	If the customer experiences any resource or performance-affecting event the partner must notify the customer of the issue. May vary according to customer agreements. MTTN measures the average time taken to notify a customer of an issue. Measured from the time that an alarm is generated to the time the customer notified, which can be by any method of communication agreed with the customer.

Requirement	Description
M7.3.2 Mean Time to Restore Service (MTRS)	The average time taken to restore service after a failure. Measured from when the service fails until it is fully restored and delivering its normal functionality. Sometimes known as MTTR. Guidelines for restoring services to the previous known working configuration based on priority levels are as follows: • P1: 4 hours • P2: 24 hours • P3: 2 business days • P4: 5 business days
M7.3.3 Agent Availability SLA	The availability of the Contact Center agents is a critical component of the service, regardless of where they are located.
Customer Web Portal The following section describes the online facilities that must be made available to the customer to view the current and historical performance of their service. May be proven by a demonstration of the portal from customer viewpoint, including real-time view of connectivity and status. Mechanisms may include password protection or similar restrictions to access the online web portal for downloading reports. The partner must also be able to show that event logs can be stored and made accessible via the web portal. If for some reason the partner chooses not to provide a customer web portal, evidence must be provided of how the required information and features are provided to the customers and the delivery method. The lack of a customer web portal does not waive any of the requirements.	
M7.3.4 Customer web portal to communicate the current status and performance, including specific reports available online as agreed with the customer	Provides an operational view for multiple audiences; designed to give a quick view of the network status, including current availability, reliability, and security for managed devices.
M7.3.5 Event Log retention	Partner must show the capability to store events, in a log for regulatory and analysis purposes for a minimum of 13 months.
External Reporting The following section describes the reports that are to be made available to the customer via customer portal. Example reports must be provided or a view of customer web portal with ability to select reports listed. If for some reason the partner chooses not to provide reporting via a customer web portal, evidence must be provided of the reports available and the delivery method. The lack of a portal does not waive any of the requirements. Web-based reporting via a customer web portal is considered a best practice and allows partners to differentiate themselves from other partners.	
M7.3.6 Performance Analysis reports	Historical performance analysis of the service. This would typically be available over a number of sample periods (daily, weekly, monthly) and would include data to allow the customer to understand how the overall service is performing, e.g., how heavily utilized are various Wide-Area Network (WAN) or Priority Rate Interface (PRI) links or how much traffic is being generated by a particular application.
M7.3.7 Service Availability reports	Summary views of service availability reports on the overall service availability, e.g., by site or equipment.

Requirement	Description
M7.3.8 Device Inventory reports	Reports of devices under management for the customer; provide data that is relevant to the customer regarding inventory of equipment or WAN services used in delivering the service.
M7.3.9 Incident Management reports	Reports detailing the current work activities to correct incidents on the customer network, metrics on the management of incidents, such as number of incidents, average time to resolve, common causes identified.
M7.3.10 Exception reports	Reports generated by customer-specified ranges; provide ability for customers to self-select parameters on individual devices and determine thresholds for the raising of exception reports.
M7.3.11 Contact Center–specific reports (Applies to hosted solution only)	Reports providing agent and overall service performance, for example: • Call queuing delay • Performance against agreed Service-Levels • Average talk time • Average calls per hour • Time spent on after call work • Percentage of calls resolving customer issues • Number of calls abandoned
Internal Performance Reporting The following section describes reports that are to be internally created and reviewed. May be proven by provisioning of example reports or demonstration of reporting tool with ability to select reports listed.	
M7.3.12 Customer-related reports/internal performance metrics	Reports on metrics used to measure trends of service performance, including: • SLA violations • Performance against internal targets (typically more stringent than those agreed with the customer)
Infrastructure Reporting (applies only to organizations providing the infrastructure for delivery of the service, e.g., carriers) The following section describes reports that are to be internally created and reviewed and that relate specifically to the performance of the infrastructure used to deliver the service across the Internet. May be proven by provisioning of example reports or a demonstration of reporting tool with ability to select reports listed. For non-service affecting incidents, the partner must provide evidence of a process to investigate reported problems as necessary in order to prevent them from affecting service to the customer.	
M7.3.13 Infrastructure/network-related reports, including: • Traffic trend reports • Peak load reports • Non-service affecting incident reports	Reports relating to the overall performance of the network infrastructure used to provide the service covering key areas of potential concern. May include: • Overall trend in traffic loads: Monitored to ensure adequate capacity is maintained to meet contracted Service-Levels • Peak loads: Signifies potential areas or times of concern that may warrant further investigation • Non-service affecting incidents: example: hardware or link failures on network devices that were successfully routed around

Requirement	Description
Customer Agent Manager Web Portal The following section describes the online facilities that must be made available to the customer supervisor to manage Contact Center agents. May be proven by a demonstration of the portal from customer viewpoint, including real-time view of agent status. Mechanisms may include password protection or similar restrictions to access the online web portal for downloading reports. If for some reason the partner chooses not to provide a customer web portal, evidence must be provided of how the required information and features are provided to the customers and the delivery method. The lack of a customer web portal does not waive any of the requirements.	
M7.3.14 View agent status	Portal must provide the ability to: • View real-time status of all agents • View current call information • Send text messages to agents • Interrupt or intercept calls • Record conversations • Silently monitor calls • Create three-way conferencing
M7.3.15 Change agent status	Ability to change agent status, e.g., if an agent forgets to log out of or into the system.
M7.3.16 Administration	Ability to perform all UCC administration centrally, including the ability to develop or modify routing scripts, manage system configuration, monitor UCC performance, define and request reports, and verify system security.

Closed/Retired Services

M5 CLOSED TO NEW APPLICANTS: Managed Security

Closed: August 2021

C1 CLOSED TO NEW APPLICANTS: Infrastructure as a Service

Closed: August 2021

M1 RETIRED: MPLS VPN

Retired: August 2021

M3 RETIRED: Internet Service

Retired: August 2021

M8 RETIRED: Business Video

Retired: August 2021

C4 RETIRED: Video and TelePresence as a Service

Retired: August 2021

M9 RETIRED: Service Provider Wi-Fi

Retired: September 2020

C9 RETIRED: Cisco Webex SP

Retired: September 2020

M2 RETIRED: Metro Ethernet

Retired: July 2019

M4 RETIRED: IP Trunking

Retired: July 2019

C5 RETIRED: Desktop as a Service

Retired: July 2019

C6 RETIRED: Disaster Recovery as a Service

Retired: July 2019

C7 RETIRED: Cloud Cell Architecture for SAP HANA

Retired: July 2019

M11 RETIRED: Managed Intelligent WAN (IWAN)

Retired: August 2018

M10 RETIRED: Data Services over Satellite (DSoS)

Retired: November 2017

Complete Revision Log

<table>
<tr><th>Document Version</th><th>Summary of Changes</th><th>Publication Date</th></tr>
<tr><td>9.2</td><td>Added Role Sharing statement in Introduction.
Added service designations:
• X2 Full Stack Observability (FSO)
• X3 Sovereign Cloud
Changed service requirements:
<table>
<tr><th></th><th>Service</th><th>Changes</th></tr>
<tr><td>X1</td><td>SASE</td><td>Added Secure Remote Worker use case</td></tr>
<tr><td>D1</td><td>Cisco SD-WAN</td><td>Removed Enterprise Network Assurance for AIOps optional requirement</td></tr>
<tr><td>D4</td><td>Meraki SD-WAN</td><td>Removed Enterprise Network Assurance for AIOps optional requirement</td></tr>
<tr><td>D5</td><td>Meraki Security</td><td>Removed Enterprise Network Assurance for AIOps optional requirement</td></tr>
<tr><td>D3</td><td>Meraki Access</td><td>Removed Enterprise Network Assurance for AIOps optional requirement</td></tr>
<tr><td>D6</td><td>Secure Access</td><td>Removed Enterprise Network Assurance for AIOps optional requirement</td></tr>
<tr><td>C8</td><td>Hybrid Cloud</td><td>Added Hyperscaler requirement</td></tr>
</table></td><td>12/2022</td></tr>
<tr><td>9.1</td><td>Added the following policy to the document Introduction: Partner has the option to be audited against the previous audit document version up to 90-days after the latest audit document version is published.
Changed service requirements:
<table>
<tr><th></th><th>Service</th><th>Changes</th></tr>
<tr><td>X1</td><td>SASE</td><td>Removed the Assurance and Visibility (Thousand Eyes) optional requirement, as it is now included in the Cisco SD-WAN and Meraki SD-WAN requirements (again as optional)
Updated Black Belt sales training requirements to the new SASE Stage 1 Pre-sales Black Belt training
Updated the Sales Enablement requirement
Updated the Customer Success requirement to include the Customer Experience Specializations as evidence</td></tr>
</table></td><td>05/2022</td></tr>
</table>

Document Version	Summary of Changes			Publication Date
	D1	Cisco SD-WAN	Added ENAA Option and related operations and training requirements Updated Black Belt sales training requirements to include Stage 2 Updated the Sales Enablement requirement Updated the Customer Success requirement to include the Customer Experience Specializations as evidence	
	D4	Meraki SD-WAN	Added ENAA Option and related operations and training requirements Updated the Sales Enablement requirement Removed the ECMS1 requirement, as the Black Belt Deployment track has now incorporated ECMS1 training Updated the Customer Success requirement to include the Customer Experience Specializations as evidence	
	D5	Meraki Security	Updated the Sales Enablement requirement Removed the ECMS1 requirement, as the Black Belt Deployment track has now incorporated ECMS1 training Updated the Customer Success requirement to include the Customer Experience Specializations as evidence	
	D3	Meraki Access	Added ENAA Option and related operations and training requirements Updated the Sales Enablement requirement Removed the ECMS1 requirement, as the Black Belt Deployment track has now incorporated ECMS1 training Updated the Customer Success requirement to include the Customer Experience Specializations as evidence	
	D6	Secure Access	Added ENAA Option and related operations and training requirements Updated the Sales Enablement requirement Updated the Customer Success requirement to include the Customer Experience Specializations as evidence Corrected typos regarding stages 1-3 of Black Belt training	

<table>
<tr><th>Document Version</th><th>Summary of Changes</th><th>Publication Date</th></tr>
<tr><td></td><td>
<table>
<tr><td>C8</td><td>Hybrid Cloud</td><td>Added a requirement to specify UCS and/or Hyperflex in the application
Updated Black Belt sales training requirements for Sales and Pre-Sales to Cloud Experience
Updated Black Belt deployment and support training requirements – some tracks are now optional
Updated the Sales Enablement requirement</td></tr>
<tr><td>D2</td><td>Cloud Managed Security</td><td>Added service options for:
• Managed Cloud Firewall <i>using Umbrella SIG</i>
• Managed Web Security <i>using Umbrella SIG</i>
• DNS Monitoring Service <i>using Umbrella SIG</i></td></tr>
<tr><td>C10</td><td>Cloud Calling</td><td>Updated the PSTN peering requirement to include reference to the Webex Calling PSTN Interoperability Program</td></tr>
</table>
</td><td></td></tr>
<tr><td>9.0</td><td>Added service designations:
• X1 Secure Access Services Edge (SASE)
Changed service requirements:
<table>
<tr><th></th><th>Service</th><th>Changes</th></tr>
<tr><td>D1</td><td>Cisco SD-WAN</td><td>Removed reseller agreement requirement
Standardized customer references requirement
Added Cisco CPE requirement
Updated and reorganized training links
Standardized customer success practice requirement</td></tr>
<tr><td>D4</td><td>Meraki SD-WAN</td><td>Removed reseller agreement requirement
Standardized customer references requirement
Updated and reorganized training links
Standardized customer success practice requirement</td></tr>
</table>
</td><td>08/2021</td></tr>
</table>

Document Version	Summary of Changes			Publication Date
	D5	Meraki Security	Removed reseller agreement requirement Standardized customer references requirement Standardized SLA requirement Added BlackBelt training, sales training, sales enablement, compensation policy, customer success, and customer ticketing system requirements Requirements have been reorganized into five key domains • Service Offering • Service Delivery • Service Marketing • Sales Operations • Customer Success	
	D3	Meraki Access	Removed reseller agreement requirement Standardized customer references requirement Standardized SLA requirement and customer success requirement Added BlackBelt training, sales training, sales enablement, compensation policy, and customer ticketing system requirements Requirements have been reorganized into five key domains • Service Offering • Service Delivery • Service Marketing • Sales Operations • Customer Success	
	D6	Secure Access	Renamed from Secure Network Access to Secure Access Replaced CCNP Routing and Switch certification option with CCNP Enterprise Removed reseller agreement requirement Standardized customer references requirement Some requirements have been renamed or reorganized, but remain substantially the same Service tiers requirement is now explicitly optional Training links have been updated and reorganized Standardized customer success practice requirement evidence option #2	

Document Version	Summary of Changes			Publication Date
	D7	Webex for BroadWorks	Removed reseller agreement requirement Standardized customer references requirement Standardized SLA optional elements Updated training links Standardized customer success practice requirement	
	D2	Cloud Managed Security	Removed reseller agreement requirement Standardized customer references requirement Updated product names	
	C8	Hybrid Cloud	Updated to reflect the latest portfolio of Cisco Hybrid Cloud solutions that power managed hybrid cloud services: • Intersight as a hybrid cloud management platform • Intersight Workload Optimizer to maximize workload performance across hybrid cloud • AppDynamics to provide performance monitoring of hybrid cloud applications • UCS, HyperFlex, and advanced data center networking (Nexus, ACI) for cloud and on-premise locations Ready for Cisco Plus – Includes specific requirements for Providers delivering hybrid cloud services with Cisco Plus Hybrid Cloud Updated service tiers requirement for Providers to offer rich hybrid cloud services – starting from managed infrastructure services, secure hybrid cloud connectivity services and cloud experience services with application performance optimization Requirements have been reorganized into five key domains • Service Offering • Service Delivery • Service Marketing • Sales Operations • Customer Success Training links updated and reorganized Removed reseller agreement requirement Standardized customer references requirement Standardized customer success practice requirement	
	D8	Webex Contact Center	Removed reseller agreement requirement Standardized customer references requirement Standardized customer success practice requirement	

<table>
<tr><th>Document Version</th><th>Summary of Changes</th><th>Publication Date</th></tr>
<tr><td></td><td>
<table>
<tr><td>C2</td><td>Unified Communications as a Service Based on HCS</td><td>Removed reseller agreement requirement
Standardized customer references requirement
Removed Infrastructure as a Service (IaaS) option from Storage virtualization (C2.2.4) requirement</td></tr>
<tr><td>C3</td><td>Contact Center as a Service Based on HCS</td><td>Removed reseller agreement requirement
Standardized customer references requirement</td></tr>
<tr><td>C10</td><td>Cloud Calling</td><td>Renamed from Webex Calling SP to Cloud Calling
Grandfathered-in Existing PSTN Integration. For new services, partner must be a CCP Provider.
Removed CMSP requirement
Standardized customer references requirement</td></tr>
<tr><td>M6</td><td>Business Communications</td><td>Removed reseller agreement requirement
Standardized customer references requirement</td></tr>
<tr><td>M7</td><td>Unified Contact Center</td><td>UCCE Specialization requirement updated to Advanced UCCE Specialization
Removed reseller agreement requirement
Standardized customer references requirement</td></tr>
</table>
Closed service designations [Closed to new applicants]:
• C1 Infrastructure as a Service
• M5 Managed Security
Retired service designations:
• M1 MPLS VPN
• M3 Internet Service
• M8 Business Video
• C4 Video and TelePresence as a Service
</td><td></td></tr>
<tr><td>8.02</td><td>Meraki SD-WAN item D4.SD.8 now correctly specifies the Meraki dashboard instead of the vManage dashboard
Meraki Access item D3.1.2 now correctly specifies customer reference requirements</td><td>09/2020</td></tr>
<tr><td>8.01</td><td>Added Cisco Webex Calling SP audit exemption language in the Introduction of the document</td><td>09/2020</td></tr>
<tr><td>8.0</td><td>General:
• Version 8.0 marks a major update to the structure of new managed service designations, and changes to some existing services. The structure of these services will now align to Cisco Service Creation pillars, and more closely mirror partner product management deliverables.
The new requirement’s structure has been separated into five sections:
1. Service Offering
2. Service Delivery</td><td>09/2020</td></tr>
</table>

Document Version	Summary of Changes	Publication Date
	3. Service Marketing 4. Sales Operations 5. Customer Success • Material requirements such as a PRD, MSD, Architecture, and other documents that cannot be validated pre-audit have been moved from the Prerequisites section to the Service Design section across all services • Customer references are now required for new and updated service designations • Two Cisco/Meraki certified individuals are now required for new and updated service designations • Black Belt training for sales, pre-sales, operations, and support personnel is now required for new and updated service designations Retired service designations: • M9 Service Provider Wi-Fi • C9 Cisco Webex SP New Cloud Managed Service designations • Secure Access • Webex Contact Center • Webex for Broadworks C10 Cloud Calling • Cloud Calling has been renamed to Webex Calling SP to align with the underlying product name D1 Cisco SD-WAN and D4 Meraki SD-WAN • Cisco SD-WAN and Meraki SD-WAN have been revamped to align to Service Creation pillars and more closely mirror partner product management deliverables • Customer references are now required at the time of audit • Two certified individuals are now required for new service designations • Black Belt SD-WAN Presales, Deployment, and Support training is now a requirement for Sales Operations	
7.5	General • Footers with version and date information are now correct across all sections C2 Unified Communications as a Service Based on HCS • C2.1.4 – Partners with a valid phase 3 A2Q are no longer required to submit to an additional A2Q for CMSP annual renewal C9 Webex SP • C9.1.6 – Partners must now provide evidence of completing either the Cisco Customer Experience Specialization or Advanced Customer Experience Specialization requirements	03/2020

Document Version	Summary of Changes	Publication Date
	D1 Cisco SD-WAN • D1.4.5 Data Retention requirement changed to only apply if data is stored in the partner cloud D4 Meraki SD-WAN • D4.4.5 Data Retention requirement changed to only apply if data is stored in the partner cloud	
7.4.1	Maintenance release • D4.4.6 Cloud Managed Meraki SD-WAN ◦ Aligned dashboard requirements to available Meraki metrics • D4.4.12 Cloud Managed Meraki SD-WAN ◦ Aligned dashboard requirements to available Meraki metrics	09/2019
7.4	General: • Retired service designations: ◦ M2 Metro Ethernet ◦ M4 IP Trunking ◦ C5 Desktop as a Service ◦ C6 Disaster Recovery as a Service ◦ C7 Cloud Cell Architecture for SAP HANA • The Cisco Powered Cloud Managed DNA Services group has been renamed to the Cisco Powered Cloud Managed Services • Meraki now has its own SD-WAN, Security, and Access designations • Cloud Managed Access is now Meraki Access • Meraki SD-WAN designation added • Meraki Security designation added • ECMS1 certification now required for Meraki designations; CCNP requirements removed for Meraki designations C2 Unified Communications as a Service Based on HCS • C2.2.2 and C2.2.3 updated Designs now based on: ◦ IaaS and Hybrid Cloud designations ◦ Cisco Cloud and Datacenter CVDs ◦ Cisco SAFE Architecture Guides and CVDs ◦ Hardware and software restrictions removed ◦ Cisco or 3rd party specs-based hardware • C2.1.4 Assessment to Quality (A2Q) is now required D1 Cisco SD-WAN • Cloud Managed SD-WAN is now named Cisco SD-WAN • Designation is now exclusive to Cisco branded hardware, where applicable (Cisco Meraki now has its own designation)	07/2019

Document Version	Summary of Changes	Publication Date
	• D1.1.4 – Updated certification requirements from CCNP SP to CCNP Route & Switch • D1.2.2 – Updated component descriptions to align to Cisco SD-WAN documentation • D1.2.2.4 – Application Aware Routing is now required and no longer optional D2 Cloud Managed Security • Designation is now exclusive to Cisco branded hardware, where applicable (Meraki now has its own designation) • D2.2.1 – Added Stealthwatch Cloud as a service option • VPN as a Service now correctly has its own numbered section D3 Meraki Access • D3.1.5 CCNP certification removed; ECMS1 certification now required D4 Meraki SD-WAN • D3.1.4 Evidence of a Customer Success Practice now required D5 Meraki Security • New designation	
7.3	M6 Business Communications • Updated M6.1.3 to allow for UC on UCS supported hardware. C2 Unified Communications as a Services Based on HCS • Simplified infrastructure architectural requirements to align with IaaS, C1, and Hybrid Cloud, C8. C9 Webex SP • Amended to allow for a two-of-three required services approach to meet the designation requirements. • Required services include HCS using the Cisco Collaboration Flex licensing model, Cloud Connected Audio for Service Providers to complement Webex Meetings, and/or Cisco BroadCloud calling. • Moved Customer Portal requirements from Operate, C9.4, to Build, C9.2, for consistency with Cloud Calling designation. C10 Cloud Calling • Designation added. D1 Cloud Managed SD-WAN • Removed reference to ISR G2 as a viable platform. • Amended D1.2.2.1 to explicitly allow for vManage to be hosted in the Cisco cloud (in addition to other deployment options).	12/2018

Document Version	Summary of Changes	Publication Date
7.2	General: • Updated customer reference language in all services, X.x.1.2. • Removed Audit representation language from all services. Outsourcers for particular aspects of service builds and delivery are always invited to attend audits. • NOTE: These changed did not result in the modified date per service being updated. M8 • Updated the training requirements for Cisco Meeting Server. M11 Managed Intelligent WAN • Retired service designation. C2 Unified Communications as a Service Based on HCS (HCS) • Renamed service to spell out UC as Unified Communications. C3 Contact Center as a Service Based on HCS (HCS_CC) • Added Cisco Unified Contact Center Express (UCCX) as a viable architecture. C4 Video and TelePresence as a Service (TPaaS) • Updated the training requirements for Cisco Meeting Server. C9 Cisco Webex SP • Renamed service from Cisco Spark SP. • Portal requirements were updated to align with the Cisco Webex Control Hub. • Two CCNPs are now required instead of one. • C9.1.6 updated to require Life Cycle Advisor program explicitly. • Availability SLA, C9.4.1 now required. • Removed the requirement for the device inventory report, C9.4.7. D1 Cloud Managed SD-WAN • Removed Intelligent WAN (IWAN) as a viable architecture for this service. • Reflected rebranding of Virtual Managed Services (VMS) to Managed Services Accelerator (MSX). D2 Cloud Managed Security • Removed D2.1.6 requiring Point of Sales information to be provided to Cisco. This is governed by the associated product's buying program. • Substantial changes to the sub-service requirements including those around Umbrella and AMP for Endpoints.	08/2018
7.1	M8 Business Video • The Cisco Powered Business Video designation is now based on the Cisco Meeting Server (CMS). This section has changed significantly. Please review the section in its entirety to see the changes.	11/17/2017

Document Version	Summary of Changes	Publication Date
	M10 Data Services over Satellite • Retired service designation. C2 UC as a Service Based on HCS (HCS) • Removed C2.1.8 requiring Point of Sale (POS) reporting to reflect the option to consume HCS as a subscription (Cisco Spark Flex). C3 Contact Center as a Service based on HCS (HCS_CC) • Removed C3.1.2 requiring the Assessment to Quality (A2Q) process for the first three deployments. Subsequent C3.1 sections renumbered accordingly. C9 Cisco Spark SP • Removed C9.2.6, referencing the optional service, call control based on Cisco Spark Call. • Removed C9.2.9, referencing the optional service, Preferred Media Provider (PMP). D1 Cloud Managed SD-WAN • Added support for Cisco SD-WAN (Viptela) based services architecture. D3 Cloud Managed Meraki Access • Designation added.	
7.0	C1 IaaS • Removed reference to VSA • Removed “offer” language from C1.2.10 as this is operator specific. Covered layer in portal requirements. • POS reporting requirement removed. • Simplified list of network virtualization options. C8 Hosted Security as a Service (HSS) • Designation migrated to D2 Cloud Managed Security. C9 CCA-MCP -> C8 Hybrid Cloud • Renamed to Hybrid Cloud. • Becomes C8 with HSS’ migration. • Removed POS reporting requirements. • Removed requirements for named cloud platforms and software including Microsoft Hyper-V, Systems Center, and Azure Pack. • Removed the requirement that storage virtualization be “storage device-based.” C9 Cisco Spark SP • Designation added. D1 Cloud Managed SD-WAN • Added support for Meraki-based services architecture.	06/06/2017

Document Version	Summary of Changes	Publication Date
	D2 Cloud Managed Security • Designation added, transforming what was Hosted Security as a Service. • Changed requirement from one to two Cisco-based security services. • Added support for delivery of services outside of the SP datacenter. • Added support for multiple Cisco Cloud based offerings. • Removed requirement for Cisco UCS as the compute platform.	
6.0	General – Added Cloud Managed DNA Services category. M11 Managed Intelligent WAN • Renamed from Intelligent WAN as a Service (IWANaaS) to better describe the outcome. C4 Video and TelePresence as a Service (TPaaS) • C4.1.8 – Removed option for a CCIE to supersede service-specific certification exams. D1 Cloud Managed SD-WAN – New service launched.	02/17/2017
5.5	General – Removed stand-alone document summarizing the changes. M1 MPLS VPN – Clarified language. M2 Metro Ethernet (ME) – Clarified language. M3 Internet Service – Clarified language. M5 Managed Security • Replaced Cisco IronPort with Cisco Email Security Appliance. • Replaced ScanSafe with Cisco Web Security Appliance or Cisco Umbrella. • Removed option to use Trend Micro technologies in place of Cisco solutions. M11 Intelligent WAN as a Service (IWANaaS) • Introduce Intelligent Path Control (PfR) and Hybrid WAN as mandatory requirements • Clarification of Application Visibility and Control requirements C1 IaaS • Clarified language and added ACI as an architectural option. • Removed duplicate sections on virtualization and services. • Removed duplicate language related to unified fabric and UCS. • C1.2.4 – Services Layer - Added requirement that Intrusion Prevention Systems must be delivered from a Cisco platform vs. 3rd party. C2 UC as a Service Based on HCS (HCS) • Clarified language and added ACI as an architectural option. C3 Contact Center as a Service based on HCS (HCS_CC) • Clarified language.	11/30/2016

Document Version	Summary of Changes	Publication Date
	C4 Video and TelePresence as a Service (TPaaS) • The Cisco Powered Video and TelePresence as a Service offer is now based on the Cisco Meeting Server (CMS). This section has changed significantly. Please review the section in its entirety to see the changes. C5 Desktop as a Service (DaaS) • Clarified text and added ACI as an architectural option. • Removed the requirement to align with a particular third-party-based reference architecture. Any desktop management platform can be used as long as the service requirements are met. • C5.2.4 – Services Layer - Added requirement that Intrusion Prevention Systems must be delivered from a Cisco platform vs. 3rd party. • Removed the requirement for a “Multi-Data Center design” as many providers do not support DaaS deployments outside of their data center. • Removed the requirement for “Private Label Branding” as this is a business model decision and not necessary for a high-quality offering. C6 Disaster Recovery as a Service (DRaaS) • Clarified text and added ACI as an architectural option. C8 Hosted Security as a Service (HSS) • This section has changed significantly. Please review the section in its entirety to see the changes.	
5.4	Update of Career Certifications and Specialization/ATP Requirements Summary Update of MPLS VPN requirements Update of Business Communications requirements Update of Business Video requirements Update of Video and Telepresence as a Service (TPaaS) requirements Update of Disaster Recovery as a Service (DRaaS) requirements Update of Cisco Powered Architecture for the Microsoft Cloud Platform requirements (CCA-MCP) Removal of Foundation for Software as a Service (FnSaaS) Removal of BYOD as a Service (BYODaaS) The Intelligent WAN as a Service (IWANaaS) service has been moved from a Cloud Service to a Managed Service, M11	04/08/2016
5.3	Added Architecture for Microsoft Cloud Platform to Cisco Powered Cloud Services portfolio	07/31/2015
5.2	Added new offers	05/29/2015
5.1	Added new offers	11/30/2014
5.0	Added new offers	05/30/2014

Document Version	Summary of Changes	Publication Date
4.0	Added new offers	12/13/2013
3.0	Added new offers	06/14/2013
2.0	Initial Version	04/24/2013

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA SB/LW-21695 2/2023