Cisco Powered Cloud and Managed Services Portfolio: Requirements, v7.1

Table of Contents

Revision Log

Document Version	Summary of Changes	Publication Date
2.0	Initial Version	04/24/2013
3.0	Added new offers	06/14/2013
4.0	Added new offers	12/13/2013
5.0	Added new offers	05/30/2014
5.1	Added new offers	11/30/2014
5.2	Added new offers	05/29/2015
5.3	Added Architecture for Microsoft Cloud Platform to Cisco Powered Cloud Services portfolio	07/31/2015
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
5.5	• 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 o Replaced Cisco IronPort with Cisco Email Security Appliance. o Replaced ScanSafe with Cisco Web Security Appliance or Cisco Umbrella. o Removed option to use Trend Micro technologies in place of Cisco solutions. • M11 Intelligent WAN as a Service (IWANaaS) o Introduce Intelligent Path Control (PfR) and Hybrid WAN as mandatory requirements o Clarification of Application Visibility and Control requirements • C1 IaaS o Clarified language and added ACI as an architectural option. o Removed duplicate sections on virtualization and services. o Removed duplicate language related to unified fabric and UCS. o C1.2.4 – Services Layer - Added requirement that Intrusion	11/30/2016

	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.
	
	• 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.	

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.
		2/17/2017

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.
		6/6/2017

	• 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.
	
	• 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.	

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.
	
	• 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 Access
	  ○ Designation added.	

Introduction

This document outlines the Cisco® Powered Cloud and Managed Services requirements within the Cloud and Managed Services Program (CMSP) and should be used to prepare for the onsite Cisco Powered Services audit.

To qualify as a Cisco Powered Services designation, the offer must include the following capabilities:

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

The partner must also meet the requirements specified in this document for each of the Cisco Powered services that the partner is pursuing.

The partner must meet the requirements of Master or Advanced CMSP certification level as specified in the Cisco Cloud and Channel Program Audit and Policies Document in order to apply for the Cisco Powered Services designation(s).

Cisco Powered Managed Services

M1 MPLS VPN

Introduced: October 2007
Last updated: November 2016

Overview

Cisco Powered MPLS VPN Service harnesses the power of Multiprotocol Label Switching (MPLS) to create virtual private networks (VPNs). MPLS is a highly scalable, protocol agnostic, data-carrying mechanism. It allows Service Providers to deliver a service that is reliable, scalable, and secure.

M1.1 Prerequisites

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

Requirement	Description
M1.1.1 Meet all CMSP partner requirements in Cisco Channel Program Audit and Policies document	See CMSP partner requirements in Cisco Channel Program Audit and Policies document.
M1.1.2 Submit at least two customer references for the service	CMSP partners are required to have a minimum of two customer references, from existing contractual relationships, for each Cisco Powered service. One customer may serve as reference to multiple designations. A customer with multiple sites does not qualify as a second reference however. The intent is to ensure that the partner has proven and repeatable service practices. The partner must submit at least two customer references for the service at the time of the audit, or must provide evidence of the ability to deliver the service to an end customer. In the event that no customer references are available at the time of the audit, two customer references must be provided upon recertification. Refer to Customer Reference Validation template.
M1.1.3 Provide of all the infrastructure on which the service is delivered (carrier)	To meet all requirements and ensure a quality service experience, the partner applying for the service must own, provide and maintain all of the networking infrastructure on which the service is delivered (links, networking equipment, points of presence, etc. If a third party is involved providing the “Last Mile” connection, the partner must provide a signed SLA with the third party.
M1.1.4 Deliver complete end-to-end Managed MPLS VPN service	Partner must deliver a complete end-to-end managed MPLS VPN service from customer site to customer site. With the partner controlling the customer premise equipment (CPE) configuration. CPE services must be on a Cisco platform.
M1.1.5 Deliver Internet Protocol (IP) transport on Cisco infrastructure	To qualify for this Cisco Powered managed service, the IP transport and switches must be delivered on a Cisco platform.
M1.1.6 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.
M1.1.7 Employ at least one Cisco CCNP® Service Provider certified individual on staff	The Cisco CCNP Service Provider certification provides individuals working in Service Provider organizations with competencies in infrastructure IP networking solutions. CCNP Service Provider professionals have detailed understanding of networking technologies in the Service Provider arena, including IP routing, IP quality of service (QoS), Border Gateway Protocol (BGP), and MPLS. A Cisco CCIE certification, of any technology specialization, supersedes and fulfills the certification requirements for this service.

M1.1.8 Audit Representation	If the partner contracted Cisco Services or a third party to design or build the MPLS VPN service, providing some or all of the requirements. At the partner's discretion, Cisco Services or the third party must participate in the audit and provide evidence on how the requirements they have provided are fulfilled. If the partner contracted for Cisco Services to operate the MPLS VPN service, providing some or all of the requirements. At the partner's discretion, Cisco Services must participate in the audit and provide evidence on how the requirements have been fulfilled.

M1.2 Service Design

Service Capabilities

The following section describes the basic functions of a Multi-Protocol Label Switching Virtual Private Network (MPLS VPN) service.

The partner must provide evidence of the MPLS VPN service capabilities and explain the key benefits of the service and how it can be used to provide secure connectivity between customer sites using Layer 3 routing and VPN routing and forwarding tables in the Provider Edge (PE) nodes.

Requirement	Description
M1.2.1 Network foundation for Virtual Private Network (VPN) service based on Internet Protocol/Multi-Protocol Label Switching (IP/MPLS)	RFC 4364 (which replaced RFC 2547) describes a method by which a Service Provider may use an IP backbone to provide IP VPNs for its customers. The partner must provide evidence that this forms the basis for the separation of traffic across the IP backbone into customer VPNs.
M1.2.2 Connectivity provided to the Internet from the VPN	The above RFC describes a number of methods for providing connectivity from the VPN to the Internet. The partner must explain how this connectivity is achieved and the benefits provided by deploying this option.
M1.2.3 Customer ability to select a full mesh VPN option where all sites can pass traffic directly to each other	Full mesh VPN provides the ability for all customer sites to communicate directly to each other with no additional configuration apart from adding a site to the VPN. This is achieved with the IP routing capability in the VPN. Demonstration of adding a new node to an existing VPN and showing accessibility to other sites is the easiest method for meeting this requirement.
M1.2.4 Customer ability to select a design configuration option that will emulate a hub-and-spoke environment	For some customers, especially during a migration phase, the ability to emulate the current Layer 2 configuration, which is hub and spoke, is important. RFC 4364 describes a method for creating different types of VPNs using route targets. The partner must either provide evidence of this capability or explain the concepts of how it would be used. Examples of existing customer configurations that use this capability can also be provided.
M1.2.5 Extranet access to VPN	Extranet VPNs extend the VPN connectivity in a controlled and secure manner to external customers or business partners to allow communication. The partner must explain how their service enables this and how they help to maintain security.
M1.2.6 Layer 3 network reach	An important feature of the MPLS VPN is providing full mesh connectivity at Layer 3 so that traffic takes the optimum path between sites and is not subject to routing through transit nodes that could increase delay for applications such as voice and video. In order to avoid this, it is necessary to have Layer 3 routing nodes deployed within each country or region that avoids excessive "backhauling" of traffic using Layer 1 or 2 technologies to the nearest PE node. This is typically found in areas that are out of region for the partner and will reduce network performance. The partner must provide evidence that for the countries or regions for which they are claiming support for this service, they have deployed an adequate number of Points of Presence (POPs) to meet service quality requirements.
M1.2.7 Remote access via Internet	The partner must provide the ability for remote users, mobile users, or telecommuters to gain access securely to the resources in the VPN. This will typically include the creation of secure encrypted tunnel from the user across the Internet and terminated within the VPN. The partner must explain how this capability is achieved and what type of devices and access are supported.
M1.2.8 Customer option to encrypt the access link between Customer Edge (CE) and Provider	As the MPLS labels are added at the PE node, the access link from the CE device can be considered by some customers to lack sufficient security capabilities. The

Edge (PE)	partner must offer the option to encrypt traffic leaving the customer site before it reaches the PE node.
M1.2.9 Edge Quality of Service (QoS) design for customer-managed Customer Premises Equipment (CPE)	Where the CPE is not part of the Managed Service, the partner will consider the PE the "trust boundary" for honoring traffic settings, and configuration settings must be negotiated with the customer. The partner must exhibit an understanding of the following functions to ensure appropriate handling of different traffic types: • Customer to partner class of service mapping: Support for at least four classes of service at the edge. The partner must explain or demonstrate how they maintain quality for User Diagram Protocol (UDP), Transmission Control Protocol (TCP), video, and voice traffic using Cisco QoS mapping guidelines • QoS techniques such as Multilink Point-to-Point Protocol (MLPPP) to maintain service quality on low-speed links • Provisioning guidelines enforced that limit real-time traffic on CE-PE links to a defined percentage (typically 25–60%) • Routing protocols supported to include Border Gateway Protocol (BGP), static, Open Shortest Path First (OSPF) • QoS transparency support using pipe mode, or short pipe mode as defined in RFC 3270
M1.2.10 Edge Quality of Service (QoS) design for the partner-managed CPE	The demarcation point for the service is after the CE device. The QoS settings can be enforced and trusted at the CE device. In comparison to above, the incoming customer IP traffic can be reclassified according to partner policy using Differentiated Services Code Point (DSCP) settings or Access Control Lists (ACLs). The partner must exhibit an understanding of the following functions to ensure appropriate handling of different traffic types: • Customer to partner class of service mapping: Support for at least four classes of service at the Edge. The partner must explain or demonstrate how they maintain quality for User Datagram Protocol (UDP), Transmission Control Protocol (TCP), video, and voice traffic using Cisco QoS mapping guidelines • QoS techniques such as Multilink Point-to-Point Protocol (MLPPP) to maintain service quality on low-speed links • Provisioning guidelines enforced that limit real-time traffic on CE-PE links to a defined percentage (typically 25–60%) • QoS transparency is the responsibility of the partner and can be carried out at the CE device and can use MPLS to transport transparently across the network
M1.2.11 Provider Edge (PE) configuration and design that follows the design and best practices outlined in Cisco design guides	There are important design considerations for the PE node for which the partner must exhibit an understanding, including what capabilities are available and how they may be used. These considerations include: Real time traffic: • Marking as Expedited Forwarding (EF) via DSCP EF settings • Priority queuing • Verify or set queue limit • Ingress policing that drops out of contract packets • No Weighted Random Early Detection (WRED) configured on queue Business critical traffic: • Marking as Assured Forwarding using Class-Based Weighted Fair Queuing (CBWFQ) • WRED optional • Tuned queue limit to meet expected trade off of delay versus loss • Policing to limit traffic to contracted rate and optionally send out of contract traffic to a lower priority class Best effort traffic: • Appropriate marking (typically DSC or EXP 0) • Best effort queuing • WRED implemented • Policing to drop out of contract traffic The partner must explain the service classes that they support and how these features are used to provide the expected performance characteristics for each traffic type.

M1.2.12 The partner network backbone configuration and design that follows the design and best practices outlined in Cisco design guides	There are two main alternative approaches to backbone design: over-provisioning and DiffServ. Either approach can be used, although the DiffServ model provides better protection against SLA violations in the event of a problem occurring. Over-provisioning: the partner must explain how they use this approach to maintain quality of service. It is expected that the overall expected network bandwidth for all service classes of service is over-provisioned by at least a factor of two (i.e., 200% of expected peak load). Because this approach leaves the network more open to SLA violation in the event of a failure, the partner must explain what processes they have put in place to protect against failures, such as major link failures or traffic growing more quickly than forecast. DiffServ: Provides protection for each class of service from each other and allows different over-provisioning rate between service classes. Typically, with this approach a partner would support three classes of service: real time, critical, and best effort, and map the different classes at the edge into these. Similar considerations for traffic handling as described for the provider edge need to be taken into account. The partner must explain or demonstrate: • The DiffServ model that is used • How the partner expects to meet the QoS characteristics for each class of service supported, using the types of features described

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 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.

Requirement	Description
M1.2.13 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.
M1.2.14 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 partner must provide evidence of the operational procedures in place to protect the device management plane.
M1.2.15 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.

Service Security: Infrastructure

The following section describes the best practices described in Cisco Validated Design documentation for designing the network infrastructure used to transport the VPN traffic. The partner must provide evidence of adherence to the requirements as described, which include protection from Denial of Service (DoS) attacks described in the Clean Pipes architecture as well as using the features and functions of the Cisco solution to ensure that the network has been designed to meet the expected Service-Levels.

Requirement	Description
M1.2.16 In accordance with Network Foundation Protection (NFP) requirements, processes and procedures to ensure protection of data plane, management plane, and control plane	Data Plane: • Access Control Lists (ACLs): Protect devices from malicious traffic by explicitly permitting legitimate traffic. • Unicast Reverse Path Forwarding (URPF): Mitigates problems caused by the introduction of malformed or spoofed IP source addresses • Remotely Triggered Black Hole (RTBH): Drops packets based on source address and can be used while device is under attack • QoS tools: Used to protect against flooding attacks by defining QoS policies to limit bandwidth or drop offending traffic

	Control Plane: • Receive ACLs: Limits the type of traffic that can be forwarded to the processor • Control Plane Policing (CPP): Provides QoS control for the packets destined to the control plane of the device. Ensures adequate bandwidth reserved for high priority traffic such as routing protocols • Routing protection: MD5 neighbor authentication protects routing domains from spoofing attacks • Auto Secure procedures in place Management Plane: • CPU and memory threshold: Protects CPU and memory resources of IOS devices against DDoS attacks • Dual export syslog: Increases availability by exporting information to dual collectors • Procedures to prevent unauthorized management access to devices
M1.2.17 Process to baseline normal traffic loads	The partner must baseline the traffic on the network periodically, at least weekly and on a regular basis to gain an understanding of the base traffic load.
M1.2.18 Network-based mechanism to identify and classify attacks based on anomaly characteristics	The partner must provide evidence of an automated procedure to detect anomalies in traffic that may represent a denial of service attack on the infrastructure. This function can be provided by a Narus solution or similar product in the network. The partner may have implemented an alternative solution based on freeware (such as Nfsen or FlowScan).
M1.2.19 Automated or manual processes to act on and mitigate detected anomalies	The partner must provide evidence that procedures are in place to act on alarms generated by the anomaly detector, in order to mitigate the effects of the suspect traffic on the infrastructure and ensure continuity of service to the customer. This requirement can be achieved by using Cisco ASR 9000 vDDoS Protection Solution or by defined manual procedures with an assigned team to focus on attack mitigation in a timely manner.
M1.2.20 System level resiliency: Effective design process to ensure deployment where applicable to enhance device level hardware and software resiliency	System level resiliency incorporates hardware redundancy capabilities as well as features within Cisco IOS to enable high availability. Using these features enables the partner to build a reliable foundation for the service. These features include: • Nonstop Forwarding (NSF) / Stateful Switchover • In-service software upgrades • Graceful restart
M1.2.21 Network level redundancy: Effective design process to ensure use of software features to enhance network level resiliency	To ensure network level redundancy, specific routing protocol features can be enabled depending on the configuration and protocols used. These features include: • Nonstop Forwarding (NSF) awareness: Allows a router to assist NSF-capable neighbors to continue forwarding packets during a Stateful Switchover (SSO) operation • Fast convergence: Adjusts the sizing of interior gateway protocols to allow the routing tables to converge faster • IP event dampening mechanism: Suppresses the effects of excessive interface flapping events on routing protocols and routing tables in the network
M1.2.22 Physical level redundancy	There are a number of options to provide redundancy at the physical layer, depending on the technologies being deployed. These features include: • Synchronous Optical NETwork/Synchronous Digital Hierarchy (SONET/SDH) circuit protection • Access link circuit protection, e.g., Integrated Services Digital Network (ISDN), wireless • Dual homing of CPE to different PE nodes

M1.3 Service-Level Management

Service-Level Agreement (SLA) Components

This section describes the SLAs 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 SLAs may also be presented as evidence of meeting these requirements.

Requirement	Description
M1.3.1 Mean Time to Notify (MTTN): May vary according to severity levels	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.
M1.3.2 Mean Time to Restore Service (MTRS): May vary according to customer needs; must have a defined SLA with the customer	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
M1.3.3 Service Availability: Must offer an SLA for per-customer service availability	The SLA for Service Availability must be provided at the customer level and not the overall backbone network level.
M1.3.4 Last Mile Connectivity	If the partner is leveraging a third party to provide “Last Mile” connectivity to customers. The partner must have an SLA in place with the third party “Last Mile” provider; this SLA must be reflected in the overall Service Availability SLA to the customer. The partner must provide details of the SLA’s with the third-party provider.
M1.3.5 Jitter	For the service class that is to be used for support of real time traffic, an SLA must be offered that describes the maximum jitter, packet delay variation—which the traffic can expect from customer site to customer site. End customer devices have to play out the packets at the destination site and will be able to cope with small amounts of jitter, but to maintain high quality this must be kept within the stated limits. Guarantee of <30 milliseconds for real time class of service (e.g., VoIP, video, etc.).
M1.3.6 Packet Delay	For the service class that is to be used for support of real time traffic, an SLA must be offered that describes the maximum packet delay that the traffic can incur from customer site to customer site. Guarantee of <150msecs intercontinental (e.g., within Europe or U.S.) and <300 milliseconds for global (e.g., between Europe and U.S. transoceanic) for real time class of service. If service delivery is over satellite access, then the auditor shall extend the delay to accommodate the inherent latency for the transmission medium. Satellite latency can range from 40ms – 125ms, depending on the orbit.
M1.3.7 Packet Loss Ratio	For the service class that is to be used for support of real time traffic, an SLA must be offered that describes the effective delivery ratio of packets that the traffic can expect from customer site to customer site. Guarantee of 1% or less packet loss for voice, video, and business class data.

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 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 portal for at least three months. 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.	
Requirement	Description
M1.3.8 Secure web portal to communicate 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: • Real time status map • Monitoring report • Usage report
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.	
Requirement	Description
M1.3.9 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.
M1.3.10 Service Availability reports	Summary views of service availability, e.g., by site or equipment.
M1.3.11 Device Inventory reports	Reports of devices under management for the customer. Provides data that is relevant to the customer regarding inventory of equipment or WAN services used in delivering the service.
M1.3.12 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.
M1.3.13 Exception reports	Reports generated by customer-specified thresholds or ranges; provides ability for customers to self-select parameters on individual devices and determine thresholds for the raising of exception reports.
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.	
Requirement	Description
M1.3.14 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) When Managed Service Providers commit to an SLA involving latency, jitter, and/or loss, they usually maintain a margin of safety and design the network to meet tighter SLAs than what they commit to their customers. Such engineering SLAs are used for internal testing and certification purposes; these stricter latency targets may potentially be necessary in those cases where VoIP packets can be transmitted to another Service Provider network (e.g., a mobile network) with higher latency. Service Providers typically design their network to meet the stricter engineering SLAs.

Infrastructure Reporting	
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 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.	
Requirement	Description
M1.3.15 Infrastructure/network-related reports, including: • Network jitter service performance • Network latency service performance • Network packet loss service performance	In order to understand how well the network is performing against expectations and agreed Service-Levels and to identify trends that may need to be addressed, the partner must maintain regular internal reports highlighting network performance. These must include at a minimum jitter, delay (latency), and loss measurements across the network infrastructure.

Click here to return to Table of Contents

M2 Metro Ethernet (ME)

Introduced: October 2007
Last updated: November 2016

Overview

Cisco Powered Metro Ethernet allows Service Providers to offer customers a service link to local and regional offices using an established, familiar technology (Ethernet) that is being used in many existing LANs today. It can support high-speed data, Internet, voice over IP (VoIP), video, and other applications with flexible speeds.

M2.1 Prerequisites

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

Requirement	Description
M2.1.1 Meet all CMSP partner requirements in Cisco Channel Program Audit and Policies document	See CMSP partner requirements in Cisco Channel Program Audit and Policies document.
M2.1.2 Submit at least two customer references for the service	CMSP partners are required to have a minimum of two customer references, from existing contractual relationships, for each Cisco Powered service. One customer may serve as reference to multiple designations. A customer with multiple sites does not qualify as a second reference however. The intent is to ensure that the partner has proven and repeatable service practices. The partner must submit at least two customer references for the service at the time of the audit, or must provide evidence of the ability to deliver the service to an end customer. In the event that no customer references are available at the time of the audit, two customer references must be provided upon recertification. Refer to Customer Reference Validation template.
M2.1.3 Provide the infrastructure on which the service is delivered (carrier)	To meet all requirements and ensure a quality service experience, the partner applying for the service must own, provide and maintain all of the networking infrastructure on which the service is delivered (links, networking equipment, points of presence, etc.).
M2.1.4 Deliver Ethernet transport based on Cisco infrastructure	To qualify this Cisco Powered managed service, the Ethernet transport and switches must be delivered on Cisco platform.
M2.1.5 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.
M2.1.6 Employ at least one CCNP Service Provider certified individual on staff	The Cisco CCNP Service Provider certification provides individuals working in Service Provider organizations with competencies in infrastructure IP networking solutions. CCNP Service Provider professionals have detailed understanding of networking technologies in the Service Provider arena, including IP routing, IP QoS, BGP, and MPLS. A Cisco CCIE certification, of any technology specialization, supersedes and fulfills the certification requirements for this service.
M2.1.7 Audit Representation	If the partner contracted Cisco Services or a third party to design or build a Metro Ethernet service, providing some or all of the requirements. At the partner's discretion, Cisco Services or the third party must participate in the audit and provide evidence on how the requirements they have provided are fulfilled. If the partner contracted for Cisco Services to operate the Metro Ethernet service, providing some or all of the requirements. At the partner's discretion, Cisco Services must participate in the audit and provide evidence on how the requirements have

	been fulfilled.

M2.2 Service Design

Service Capabilities

The following section describes the basic functions of the Metro Ethernet service. The partner must provide evidence of the Metro Ethernet service capabilities and explain the key benefits of the service and how it can be used to deliver Layer 2 traffic either in an emulated LAN or a point-to-point service.

Requirement	Description
M2.2.1 Support for at least two of the three service types defined in the Metro Ethernet Forum (MEF) technical specification MEF 6.2 Section 10	The MEF describes the types of services that can be offered from a Metro Ethernet service using standardized terminology to reduce confusion in the marketplace as to what capabilities a service offers the customer. The partner must exhibit an understanding of the services as defined by the MEF, which of the three services their service offerings map to and the capabilities the customer can therefore expect.
M2.2.2 Ability to connect multiple Customer Premises Equipment (CPE) devices from the same site	Customers can select multiple Ethernet ports for a site, which allows them to connect different CPE devices as needed. The partner must provide evidence that this is offered to the customer, typically as part of a service description, or by displaying this functionality.
M2.2.3 Service frame transparency; deliver frames across the service without adversely affecting the format	To minimize any impact on the customer Local Area Network (LAN) infrastructure design, the service must deliver the frames across the network without making any changes to the content other than to meet design considerations, such as different Virtual Local Area Network (VLAN) headers. The partner must explain how this is achieved or provide documentation of an example customer implementation.
M2.2.4 Enhanced Local Management Interface (E-LMI) support	Enhanced LMI provides management functionality, including: • Notification of remote user to Network Interface (UNI) status to CE • Notification of EVC addition, deletion, or status (active, not active, partially active) to Customer Edge (CE) • Communication of UNI and Ethernet Virtual Connection (EVC) attributes to CE (e.g., CE-VLAN to EVC map) • CE auto-configuration The MEF 16 document describes this functionality in more detail. The partner must provide evidence that this capability is used in the network design to provide the functions described.
M2.2.5 Provision of a service that allows the customer to specify which VLAN ID they use	The ability to specify the VLAN ID used at each site provides more flexibility to the customer in terms of using the service to connect their existing infrastructure. The partner must provide evidence that the customer for each site can select this ID, either by published service description or example installed customer design that uses this feature.
M2.2.6 Ability to support hierarchal shaping, including: • Class level • VLAN level • Physical or port level	Traffic shaping allows the service to provide effective prioritization of different traffic types as it enters the network. This can be set at the class of service type, at the VLAN level, or at the physical port level, depending on customer requirements. The partner must provide evidence of these capabilities and explain where they would be used and the expected benefits to the customer.
M2.2.7 Bandwidth profile for ingress ports	MEF 10 specifies bandwidth profiles for ingress traffic that describe how to handle traffic arriving within or outside the agreed SLA. Traffic arriving within contract is subject to the SLA commitments and must be handled appropriately, while traffic arriving outside of contract can be handled separately. The partner must provide evidence of support for this capability.
M2.2.8 At least two classes of services available	Customer must be able select from at least two classes of service into which they separate their applications.

	The partner must provide evidence of this capability or provide a published service description that includes this capability, explaining what types of traffic the service classes are designed for and the expected service performance.
M2.2.9 Ability to scale bandwidth offered to the customer through remote configuration, including offering customer access to different bandwidth options over the physical link	One benefit of an Ethernet service is the ability to offer a more flexible approach to provisioning bandwidth to a customer site. After the physical link is installed, the customer must be able to select from a range of bandwidth offerings to suit their price and application requirements, with the ability to request a change to this that can be implemented remotely. The partner must explain how their service offers these capabilities, the range of options available, and any commitments they will make in terms of customer requested configuration changes, via a sample of existing customer configurations or a published service description.
M2.2.10 Support for a VLAN connected to the Internet with appropriate security support (see below)	Customer must be able to select an option for a VLAN connection to the Internet. The partner must provide evidence that this capability is offered in a published service description or by providing an example installed customer design that uses this feature.

Site Network Resiliency

The following section describes operational procedures that must be incorporated as best practices for the design and implementation of the Metro Ethernet service. The partner must provide evidence that these procedures are being followed. This can be proven with 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. These requirements are only applicable to the partner services that include management of the CPE.

Requirement	Description
M2.2.11 The partner must provide options for site network resiliency	The partner must offer the following network resiliency options to the customer: Unprotected service: Basic service with no resiliency options Fully load shared links: Traffic is load shared down redundant paths Active/passive links: One link is active and monitored. Under failure conditions the backup link is enabled The partner must provide evidence that this capability is offered in a published service description or example installed customer design that uses this feature.

M2.3 Service-Level Management

Service-Level Agreement (SLA) Components

This section describes the SLAs 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 SLAs may also be presented as evidence of meeting these requirements.

Requirement	Description
M2.3.1 Mean Time to Notify (MTTN): May vary according to severity levels	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.
M2.3.2 Mean Time to Restore Service (MTRS): May vary according to customer needs; must have a defined SLA with the customer	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

M2.3.3 Service Availability: Must offer an SLA for per-customer service availability	The SLA for Service Availability must be provided at the customer level and not the overall backbone network level.
M2.3.4 Jitter	For the service class that is to be used for support of real-time traffic, an SLA must be offered that describes the maximum jitter—or packet delay variation—that the traffic can expect from customer site to customer site. End customer devices have to play out the packets at the destination site and will be able to cope with small amounts of jitter, but to maintain high quality this must be kept within the stated limits. Guarantee of <30 milliseconds.
M2.3.5 Packet Delay	For the service class that is to be used for support of real-time traffic, an SLA must be offered that describes the maximum packet delay that the traffic can incur from customer site to customer site. Guarantee of <150msecs.
M2.3.6 Packet Loss Ratio	For the service class that is to be used for support of real-time traffic, an SLA must be offered that describes the effective delivery ratio of packets that the traffic can expect from customer site to customer site. Guarantee of 1% or less packet loss for voice, video, and business class data.

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 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 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.

Requirement	Description
M2.3.7 Secure web portal to communicate 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: • Real-time status map • Monitoring report • Usage report

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 the partner to differentiate themselves from other partners.

Requirement	Description
M2.3.8 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 Ethernet links or virtual private lines, or how much traffic is being generated by a particular application.
M2.3.9 Service Availability reports	Summary views of service availability reports on the overall service availability, e.g., by site or equipment.
M2.3.10 Device Inventory reports	Reports of devices under management for the customer; provides data that is relevant to the customer regarding inventory of equipment used in delivering the service.
M2.3.11 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.
M2.3.12 Exception reports	Reports generated by customer-specified thresholds or ranges; provides ability for customers to self-select parameters on individual devices and determine thresholds for the raising of exception reports.
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.	
Requirement	Description
M2.3.13 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)
Infrastructure Reporting	
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 network. May be proven by provision of example reports or demonstration of reporting tool with ability to select reports listed. For non–service affecting incidents, the partner must show process to investigate reported problems as necessary in order to prevent them from affecting service to the customer.	
Requirement	Description
M2.3.14 Infrastructure/network-related reports, including: • Network jitter service performance • Network latency service performance • Network packet loss service performance	In order to understand how well the network is performing against expectations and agreed Service-Levels and to identify trends that may need to be addressed, the partner must maintain regular internal reports highlighting network performance. These must include at a minimum jitter, delay (latency), and loss measurements across the network infrastructure.
M2.3.15 Real-time and historical application reports for both voice and video networks	Monitoring must include notification in the event of packet drops. Events (Syslog or SNMP traps) are generated when measurements exceed defined values. This helps to identify and isolate network problems.

Click here to return to Table of Contents

M3 Internet Service

Introduced: October 2007
Last updated: November 2016

Overview

Cisco Powered Internet Service utilizes tested and certified best practices for the design and implementation of the managed Internet Service. The service incorporates reliability, scalability, and security designs.

M3.1 Prerequisites

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

Requirement	Description
M3.1.1 Meet all CMSP partner requirements in Cisco Channel Program Audit and Policies document	See CMSP partner requirements in Cisco Channel Program Audit and Policies document.
M3.1.2 Submit at least two customer references for the service	CMSP partners are required to have a minimum of two customer references, from existing contractual relationships, for each Cisco Powered service. One customer may serve as reference to multiple designations. A customer with multiple sites does not qualify as a second reference however. The intent is to ensure that the partner has proven and repeatable service practices. The partner must submit at least two customer references for the service at the time of the audit, or must provide evidence of the ability to deliver the service to an end customer. In the event that no customer references are available at the time of the audit, two customer references must be provided upon recertification. Refer to Customer Reference Validation template.
M3.1.3 Provide the infrastructure on which the service is delivered (carrier)	To meet all requirements and ensure a quality service experience, the partner applying for the service must own, provide and maintain all of the networking infrastructure on which the service is delivered (links, networking equipment, points of presence, etc.). If a third party is involved providing the “Last Mile” connection, the partner must provide a signed SLA with the third party.
M3.1.4 Deliver complete end-to-end Internet Service	Partner must deliver a complete end-to-end managed Internet Service from customer site to customer site. With the partner controlling the customer premise equipment (CPE) configuration. CPE services must be on a Cisco platform.
M3.1.5 Deliver Internet Protocol (IP) transport on Cisco infrastructure	To qualify this Cisco Powered managed service, the IP transport and switches must be delivered on Cisco platform.
M3.1.6 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.
M3.1.7 Employ at least one CCNP Service Provider certified individual on staff	The Cisco CCNP Service Provider certification provides individuals working in Service Provider organizations with competencies in infrastructure IP networking solutions. CCNP Service Provider professionals have detailed understanding of networking technologies in the Service Provider arena, including IP routing, IP QoS, BGP, and MPLS. A Cisco CCIE certification, of any technology specialization, supersedes and fulfills the certification requirements for this service.

M3.1.8 Audit representation	If the partner has contracted Cisco Services or a third party to design or build an Internet service, providing some or all of the requirements. At the partner's discretion, Cisco Services or the third party must participate in the audit and provide evidence on how the requirements they have provided are fulfilled. If the partner has contracted for Cisco Services to operate the Internet service, providing some or all of the requirements. At the partner's discretion, Cisco Services must participate in the audit and provide evidence on how the requirements have been fulfilled.

M3.2 Service Design

Service Capabilities

The following section describes the basic functions of managed Internet service. The partner must provide evidence of the managed Internet Service capabilities and; explain the key benefits of the service and how the service can be used to deliver secure connectivity between customer sites.

M3.2.1 Service must include options for physical connectivity	The partner must support at least two different connectivity types such as: • Serial lines: E1/T1, OC3/STM-1 • xDSL • Ethernet If service delivery is over satellite access, then Ethernet connectivity is the only connection type required.
M3.2.2 Managed connectivity to the Internet must be available as an option for remote or mobile users	The partner must be able to provide connectivity to the Internet for remote users. This can be part of the MIS or a separate service.

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 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.

Requirement	Requirement
M3.2.3 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.
M3.2.4 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.
M3.2.5 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.

Service Security: Infrastructure

The following section describes the best practices described in Cisco Validated Design documentation for designing the network infrastructure used to transport the Internet traffic from the customer site to the required peering point. The partner must provide evidence of adherence to the requirements as described, which include protection from Denial of Service (DoS) attacks described in the Clean Pipes architecture.

Requirement	Description
M3.2.6 In accordance with Network Foundation Protection (NFP) requirements, processes and procedures to ensure protection of data plane, management plane, and control plane	Data plane: • Access Control Lists (ACLs): Protect devices from malicious traffic by explicitly permitting legitimate traffic • Unicast Reverse Path Forwarding (URPF): Mitigates problems caused by the introduction of malformed or spoofed IP source addresses • Remotely Triggered Black Hole (RTBH): Drops packets based on source address and can be used while device is under attack • QoS tools: Used to protect against flooding attacks Control plane: • Receive ACLs: Limits the type of traffic that can be forwarded to the processor • Control Plane Policing (CPP): Provides QoS control for the packets destined to the control plane of the device. Ensures adequate bandwidth reserved for high-priority traffic such as routing protocols • Routing protection: MD5 neighbor authentication protects routing domains from spoofing attacks • Auto Secure procedures in place Management plane: • CPU and memory threshold: Protects CPU and memory resources of Cisco IOS Software devices against DDoS attacks • Dual export syslog: Increases availability by exporting information to dual collectors • Procedures to prevent unauthorized management access to devices
M3.2.7 Process to baseline normal traffic loads	The partner must baseline the traffic on the network periodically, at least weekly and on a regular basis to gain an understanding of the base traffic load.
M3.2.8 Network-based mechanism to identify and classify attacks based on anomaly characteristics	The partner must provide evidence of an automated procedure to detect anomalies in traffic that may represent a denial of service attack on the infrastructure. This function can be provided by a Narus solution or similar product in the network. The partner may have implemented an alternative solution based on freeware (such as Nfsen or FlowScan).
M3.2.9 Automated or manual processes to act on and mitigate detected anomalies	The partner must provide evidence that procedures are in place to act on alarms generated by the anomaly detector, in order to mitigate the effects of the suspect traffic on the infrastructure and ensure continuity of service to the customer. This requirement can be achieved by using Cisco ASR 9000 vDDoS Protection Solution or by defined manual procedures with an assigned team to focus on attack mitigation in a timely manner.
M3.2.10 System-level resiliency: Effective design process to make sure of deployment where applicable to enhance device-level hardware and software resiliency	System-level resiliency incorporates hardware redundancy capabilities as well as features within Cisco IOS Software to enable high availability. Using these features enables the partner to build a reliable foundation for the service. These features include: • Nonstop Forwarding (NSF)/Stateful Switchover • In-service software upgrades • Graceful restart
M3.2.11 Network-level redundancy: Effective design process to make sure of use of software features to enhance network-level resiliency	To ensure network-level redundancy, specific routing protocol features can be enabled depending on the configuration and protocols used. These features include: • Nonstop Forwarding (NSF) awareness: Allows a router to assist NSF-capable neighbors to continue forwarding packets during a Stateful Switchover (SSO) operation • Fast convergence: Adjusts the sizing of interior gateway protocols to allow the routing tables to converge faster • IP event dampening mechanism: Suppresses the effects of excessive interface flapping events on routing protocols and routing tables in the network
M3.2.12 Physical-level redundancy	There are a number of options to provide redundancy at the physical layer, depending on the technologies being deployed. These features include: • Synchronous Optical NETwork/Synchronous Digital Hierarchy (SONET/SDH) circuit protection • Access link circuit protection, e.g., Integrated Services Digital Network (ISDN), wireless • Dual homing of CPE to different PE nodes

M3.3 Service-Level Management

Service-Level Agreement (SLA) Components

This section describes the service-level agreements (SLAs) 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.

Requirement	Description
M3.3.1 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.
M3.3.2 Mean Time to Restore Service (MTRS): May vary according to customer needs; must have a defined SLA with the customer	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
M3.3.3 Service Availability: Must offer an SLA for per-customer service availability	The SLA for Service Availability must be provided at the customer level and not the overall backbone network level.
M3.3.4 Last Mile Connectivity	If the partner is leveraging a third party to provide “Last Mile” connectivity to customers. The partner must have an SLA in place with the third party “Last Mile” provider; this SLA must be reflected in the overall Service Availability SLA to the customer. The partner must provide details of the SLA’s with the third-party provider.

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 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 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.

Requirement	Description
M3.3.5 Secure web portal to communicate 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: • Real-time status map • Monitoring report • Usage report

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 the partner to differentiate themselves from other partners.

Requirement	Description

M3.3.6 Service Availability reports	Summary views of service availability reports on the overall service availability, e.g., by site or equipment.
M3.3.7 Device Inventory reports	Reports of devices under management for the customer; provides data that is relevant to the customer regarding inventory of equipment used in delivering the service.
M3.3.8 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.
M3.3.9 Exception reports	Reports generated by customer-specified thresholds or ranges; provides ability for customers to self-select parameters on individual devices and determine thresholds for the raising of exception reports.
Internal Performance Reporting	
The following section describes reports that are to be internally created and reviewed. Example reports or demonstration reporting tool with ability to select reports listed must be shown.	
Requirement	Description
M3.3.10 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	
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. Example reports or a demonstration of the reporting tool with ability to select reports listed must be shown. For non-service affecting incidents, the partner must show a process to investigate reported problems as necessary in order to prevent them from affecting service to the customer. If for some reason the partner chooses not to provide reporting via a customer 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.	
Requirement	Description
M3.3.11 Infrastructure/network-related reports	In order to understand how well the network is performing against expectations and agreed Service-Levels, as well as to identify trends that may need to be addressed, the partner must maintain regular internal reports highlighting the network performance.

Click here to return to Table of Contents

M4 IP Trunking

Introduced: October 2007
Last updated: November 2016

Overview

Cisco Powered IP Trunking is built from the Cisco Validated Design documentation for designing the network infrastructure used to deliver the IP Trunking service. It is also described as a SIP Trunking service. One of the key benefits of the service is how it can be used to deploy and interconnect Cisco Unified Communications solutions to the network, and how it provides a single IP-based interconnect for both data and voice using Session Initiation Protocol (SIP) as the Voice over Internet Protocol (VoIP), enabling multimedia communications over IP.

M4.1 Prerequisites

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

Requirement	Description
M4.1.1 Meet all CMSP partner requirements in Cisco Channel Program Audit and Policies document	See CMSP partner requirements in Cisco Channel Program Audit and Policies document.
M4.1.2 Submit at least two customer references for the service	CMSP partners are required to have a minimum of two customer references, from existing contractual relationships, for each Cisco Powered service. One customer may serve as reference to multiple designations. A customer with multiple sites does not qualify as a second reference however. The intent is to ensure that the partner has proven and repeatable service practices. The partner must submit at least two customer references for the service at the time of the audit, or must provide evidence of the ability to deliver the service to an end customer. In the event that no customer references are available at the time of the audit, two customer references must be provided upon recertification. Refer to Customer Reference Validation template.
M4.1.3 Provide the infrastructure on which the service is delivered (carrier)	To meet all requirements and ensure a quality service experience, the partner applying for the service must own, provide and maintain all of the networking infrastructure on which the service is delivered (links, networking equipment, points of presence, etc.). If a third party is involved providing the “Last Mile” connection, the partner must provide a signed SLA with the third party.
M4.1.4 Deliver complete end-to-end Managed IP Trunking service	Partner must deliver a complete end-to-end managed IP Trunking service from customer site to customer site. With the partner controlling the customer premise equipment (CPE) configuration. CPE services must be on a Cisco platform.
M4.1.5 Deliver Internet Protocol (IP) transport on Cisco infrastructure	To qualify this Cisco Powered managed service, the IP transport and switches must be delivered on Cisco platform.
M4.1.6 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.
M4.1.7 Employ at least one CCNP Service Provider certified individual on staff	The Cisco CCNP Service Provider certification provides individuals working in Service Provider organizations with competencies in infrastructure IP networking solutions. CCNP Service Provider professionals have detailed understanding of networking technologies in the Service Provider arena, including IP routing, IP QoS, BGP, and MPLS. A Cisco CCIE certification, of any technology specialization, supersedes and fulfills

	the certification requirements for this service.
M4.1.8 Audit representation	If the partner has contracted Cisco Services or a third party to design or build an IP Trunking service, providing some or all of the IP Trunking requirements. At the partner's discretion, Cisco Services or the third party must participate in the audit and provide evidence on how the requirements have been fulfilled. If the partner has contracted Cisco Services to operate the IP Trunking Service, providing some or all of the IP Trunking requirements. At the partner's discretion, Cisco Services must participate in the audit and provide evidence on how the requirements have been fulfilled.

M4.2 Service Design

Service Capabilities

The following section describes the basic functions of an IP Trunking service. The partner must provide evidence of the IP Trunking service capabilities, explain the key benefits of the service and how it can be used to deploy and interconnect Cisco Unified Communications solutions to the network, and how it provides a single IP-based interconnect for both data and voice using Session Initiation Protocol (SIP) as the Voice over Internet Protocol (VoIP), and enables multimedia communications over IP.

Requirement	Description
M4.2.1 Compliance with RFC 3261	RFC 3261 defines the SIP Trunking standard, and as it is designed to interoperate with customer PBXs, it must comply with this standard.
M4.2.2 Support for emergency calls	Emergency calls can be supported either by continuing availability of Public Switched Telephone Network (PSTN) connectivity as a backup/alternate path for voice traffic.
M4.2.3 Compliance with RFC 3264	RFC 3264 defines a SIP offer/answer model for establishing SIP sessions. An "offer" is described in the Session Description Protocol (SDP) fields in the SIP message. The offer describes the sending device's media capabilities; the answer reciprocates with the destination details. There are two main methods: early and delayed offer. The partner must describe which of these are supported and the differences between the two approaches.
M4.2.4 Support for Managed Dial Plan Service (MDPS), including unified dial plan across multiple locations (N-digit/private dial plan with overlap between enterprises)	The management of the dial plan is an important aspect of the Managed SIP Trunking service. The Unified Communications (UC) devices may be managed by the partner, or by the customer or by a combination of both. The partner must provide evidence of effective processes to ensure that a unified dial plan is designed and implemented according to customer needs regardless of the overall deployment model.
M4.2.5 Compliance with RFC 2833 (DTMF relay)	RFC 2833 specifies in-band transportation of Dual-tone Multi-frequency (DTMF) tones, either as raw tones in the Rapid Transport Protocol (RTP) media stream or signaled tones in the RTP media stream. The IP trunking architecture must support the RTP media stream option. In addition, DTMF tones may be transported out-of-band. The partner must explain how these approaches differ, which they support directly, and what levels of interworking can be provided. This may include methods such as: ▪ Session Border Controller (SBC) to translate in-band audio signaling to RFC 2833 signaling ▪ Insertion of a Media Termination Point (MTP) to resolve transportation mismatches
M4.2.6 Support for codecs G.711 u-law and/or a-law	G.711 is a standard for encoding of voice into K 64bp/s digital format. U-law and a-law are different transcoding mechanisms used in different parts of the world.
M4.2.7 Demarcation point	Demarcation between partner network and customer network is required in order to grant the correct operational independence and security level for both networks. Cisco Validated Designs use the Cisco Unified Border Element (CUBE) as the CPE that provides this function, or an Integrated Access Device (IAD) for smaller deployments. If an alternate is used, partner must demonstrate how the two (or more) operational areas are kept separate.
M4.2.8 Edge Quality of Service (QoS) design for customer-managed Customer Premises	Where the CPE is not part of the Managed Service, the partner will consider the PE the "trust boundary" for honoring traffic settings, and configuration settings must be

Equipment (CPE)	negotiated with the customer. The partner must exhibit an understanding of the following functions to ensure appropriate handling of different traffic types: • Customer to partner class of service mapping: Support for at least four classes of service at the edge. The partner must explain or demonstrate how they maintain quality for User Datagram Protocol (UDP), Transmission Control Protocol (TCP), video, and voice traffic using Cisco QoS mapping guidelines • QoS techniques such as Multilink Point-to-Point Protocol (MLPPP) to maintain service quality on low-speed links • Provisioning guidelines enforced that limit real-time traffic on CE-PE links to a defined percentage (typically 25–60%) • Routing protocols supported to include Border Gateway Protocol (BGP), static, Open Shortest Path First (OSPF) • QoS transparency support using pipe mode, or short pipe mode as defined in RFC 3270 IP packet marking following recommended guidelines: • SIP signaling message: DiffServ PHB CS5 DSCP value 40 • RTP media: DiffServ PHB EF DSCP value 46
M4.2.9 Edge Quality of Service (QoS) design for partner-managed CPE	The demarcation point for the service is after the CE device. Because the partner has control of the CE configuration, the QoS settings can be enforced and trusted at the CE device. In comparison to above, the incoming customer IP traffic can be reclassified according to partner policy using Differentiated Services Code Point (DSCP) settings or Access Control Lists (ACLs). The partner must exhibit an understanding of the following functions to ensure appropriate handling of different traffic types: • Customer to partner class of service mapping: Support for at least four classes of service at the edge. The partner must explain or demonstrate how they maintain quality for User Diagram Protocol (UDP), Transmission Control Protocol (TCP), video, and voice traffic using Cisco QoS mapping guidelines • QoS techniques such as Multilink Point-to-Point Protocol (MLPPP) to maintain service quality on low-speed links • Provisioning guidelines enforced that limit real-time traffic on CE-PE links to a defined percentage (typically 25–60%) • QoS transparency is the responsibility of the partner and can be carried out at the CE device and can use MPLS to transport transparently across the network
M4.2.10 Provider Edge (PE) configuration and design that follows the design and best practices outlined in Cisco design guides	There are important design considerations for the PE node for which the partner must exhibit an understanding, including what capabilities are available and how they may be used. These considerations include: Real-time traffic: • Marking as Expedited Forwarding (EF) via DSCP EF settings • Priority queuing • Verify or set queue limit • Ingress policing that drops out of contract packets • No Weighted Random Early Detection (WRED) configured on queue Business-critical traffic: • Marking as Assured Forwarding using Class-Based Weighted Fair Queuing (CBWFQ) • WRED optional • Tuned queue limit to meet expected trade off of delay versus loss • Policing to limit traffic to contracted rate and optionally send out of contract traffic to a lower priority class Best effort traffic: • Appropriate marking (typically DSC or EXP 0) • Best effort queuing • WRED implemented • Policing to drop out of contract traffic The partner must explain the service classes that they support and how these features are used to provide the expected performance characteristics for each

	traffic type.
M4.2.11 The partner network backbone configuration and design that follows the design and best practices outlined in Cisco design guides	There are two main alternative approaches to backbone design: over-provisioning and DiffServ. Either approach can be used, although the DiffServ model provides better protection against SLA violations in the event of a problem occurring. Over-provisioning: the partner must explain how they use this approach to maintain quality of service. It is expected that the overall expected network bandwidth for all service classes of service is over-provisioned by at least a factor of two (i.e., 200% of expected peak load). Because this approach leaves the network more open to SLA violation in the event of a failure, the partner must explain what processes they have put in place to protect against failures, such as major link failures or traffic growing faster than forecast. DiffServ: Provides protection for each class of service from each other and allows different over-provisioning rate between service classes. Typically, with this approach a partner would support three classes of service: real time, critical, and best effort, and map the different classes at the edge into these. Similar considerations for traffic handling as described for the Provider Edge need to be taken into account. The partner must explain or demonstrate the following: • The DiffServ model that is used • How the partner expects to meet the QoS characteristics for each class of service supported, using the types of features described
M4.2.12 Wide Area Network (WAN) network outage survivability	The partner must support the following options in order to recover from failure scenarios: • If leased lines are delivered over a Synchronous Optical NETwork/Synchronous Digital Hierarchy (SONET/SDH) infrastructure, protection must be offered for the circuit • Customer option to backup a link from a site into the Virtual Private Network (VPN) • Ability to dual home the CPE into two separate nodes in the aggregation network • In case of failures, all sites must maintain capability to make calls through PSTN
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 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.	
Requirement	Requirement
M4.2.13 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.
M4.2.14 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 partner must provide evidence of the operational procedures in place to protect the device management plane.
M4.2.15 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.
Service Security: Infrastructure	

The following section describes the best practices described in Cisco Validated Design documentation for designing the network infrastructure used to deliver the IP Trunking service. The partner must provide evidence of adherence to the requirements as described, which include protection from Denial of Service (DoS) attacks described in the Clean Pipes architecture as well as using the features and functions of the Cisco solution to ensure that the network has been designed to meet the expected Service-Levels.

Requirement	Description
M4.2.16 In accordance with Network Foundation Protection (NFP) requirements, processes and procedures to ensure protection of data plane, management plane, and control plane	Data plane: • Access Control Lists (ACLs): Protects devices from malicious traffic by explicitly permitting legitimate traffic. • Unicast Reverse Path Forwarding (URPF): Mitigates problems caused by the introduction of malformed or spoofed IP source addresses • Remotely Triggered Black Hole (RTBH): Drops packets based on source address and can be used while device is under attack • QoS tools: Used to protect against flooding attacks Control plane: • Receive ACLs: Limits the type of traffic that can be forwarded to the processor • Control Plane Policing (CPP): Provides QoS control for the packets destined to the control plane of the device. Ensures adequate bandwidth reserved for high-priority traffic such as routing protocols • Routing protection: MD5 neighbor authentication protects routing domains from spoofing attacks • Procedures in place to secure the Control Plane Management plane: • CPU and memory threshold: Protects CPU and memory resources of Cisco IOS Software devices against DDoS attacks • Dual export syslog: Increases availability by exporting information to dual collectors • Procedures to prevent unauthorized management access to devices
M4.2.17 IP Trunking architecture	IP Trunking architecture must support the following best practices: • Transport Layer Security (TLS) protocol • Capability to reject non-TLS traffic if desired • MD5 Message Digest Algorithm • IP Security (IPsec) protocol • WWW-Authenticate header with “Digest” authentication as specified in RFC 3261 • HTTP authentication as specified in RFC 3261
M4.2.18 Process to baseline normal traffic loads	The partner must baseline the traffic on the network periodically, at least weekly and on a regular basis to gain an understanding of the base traffic load.
M4.2.19 Network-based mechanism to identify and classify attacks based on anomaly characteristics	The partner must provide evidence of an automated procedure to detect anomalies in traffic that may represent a denial of service attack on the infrastructure. This function can be provided by a Narus solution or similar product in the network. The partner may have implemented an alternative solution based on freeware (such as Nfsen or FlowScan).
M4.2.20 Automated or manual processes to act on and mitigate detected anomalies	The partner must provide evidence that procedures are in place to act on alarms generated by the anomaly detector, in order to mitigate the effects of the suspect traffic on the infrastructure and ensure continuity of service to the customer. This requirement can be achieved by using Cisco ASR 9000 vDDoS Protection Solution or by defined manual procedures with an assigned team to focus on attack mitigation in a timely manner.

M4.3 Service-Level Management

Service-Level Agreement (SLA) Components

This section describes the SLAs 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 SLAs may also be presented as evidence of meeting these requirements.

Requirement	Description
M4.3.1 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.
M4.3.2 Mean Time to Restore Service (MTRS): May vary according to customer needs; must have a defined SLA with the customer	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
M4.3.3 Service Availability: Must offer an SLA for per-customer service availability	The SLA for service availability must be provided at the customer level and not the overall backbone network level.
M4.3.4 Last Mile Connectivity	If the partner is leveraging a third party to provide “Last Mile” connectivity to customers. The partner must have an SLA in place with the third party “Last Mile” provider; this SLA must be reflected in the overall Service Availability SLA to the customer. The partner must provide details of the SLA’s with the third-party provider.

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 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 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.

Requirement	Description
M4.3.5 Secure web portal to communicate 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: • Real-time status map • Monitoring report • Usage report

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 partner to differentiate themselves from other partners.

Requirement	Description
M4.3.6 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.
M4.3.7 Service Availability reports	Summary views of service availability reports on the overall service availability, e.g., by site or equipment.
M4.3.8 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.
M4.3.9 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.
M4.3.10 Exception reports	Reports generated by customer-specified thresholds or ranges; provides ability for customers to self-select parameters on individual devices and determine thresholds for the raising of exception reports.
Internal Performance Reporting	
The following section describes reports that are to be internally created and reviewed. May be proven with an example of the reports or showing the reporting tool 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 customer web portal does not waive any of the requirements.	
Requirement	Description
M4.3.11 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	
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 with an example of the reports or a demonstration of the reporting tool. 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.	
Requirement	Description
M4.3.12 Infrastructure/network-related reports.	In order to understand how well the network is performing against expectations and agreed Service-Levels and to identify trends that may need to be addressed, the partner must maintain regular internal reports highlighting network performance. These must include: • Network jitter service performance • Network latency service performance • Network packet loss service performance
M4.3.13 Real-time and historical application reports for both voice and video networks	Monitoring must include notification in case of packet drops. Events (Syslog or SNMP traps) must be generated when measurements exceed certain values; this helps to identify and isolate network problems.

Click here to return to Table of Contents

M5 Managed Security

Introduced: August 2009
Last updated: November 2014

Overview

Cisco Managed Security service is defined as a partner providing a combination of standard network state full firewall functions, remote access and site-to-site virtual private network (VPN) support, secure web gateway (SWG) functionality (antimalware, URL and application control) or network intrusion prevention, focused on workstation protection.

M5.1 Prerequisites

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

Requirement	Description
M5.1.1 Meet all CMSP partner requirements in Cisco Channel Program Audit and Policies document	See CMSP partner requirements in Cisco Channel Program Audit and Policies document.
M5.1.2 Submit at least two customer references for the service	CMSP partners are required to have a minimum of two customer references, from existing contractual relationships, for each Cisco Powered service. One customer may serve as reference to multiple designations. A customer with multiple sites does not qualify as a second reference however. The intent is to ensure that the partner has proven and repeatable service practices. The partner must submit at least two customer references for the service at the time of the audit, or must provide evidence of the ability to deliver the service to an end customer. In the event that no customer references are available at the time of the audit, two customer references must be provided upon recertification. Refer to Customer Reference Validation template.
M5.1.3 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.
M5.1.4 Employ at least one CCNP Security certified individual on staff for Managed Security Services	The Cisco CCNP Security certification validates advanced knowledge and skills required to secure Cisco networks. A CCNP Security professional demonstrates the skills required to secure and manage network infrastructures to protect productivity, mitigate threats, and reduce costs. The Cisco IOS Software router (ISR) and Catalyst switch security features, Adaptive Security Appliance (ASA), secure VPN connectivity, and Intrusion Prevention Systems (IPSs) as well as techniques to optimize these technologies in a single, integrated network security solution. A Cisco CCIE certification, of any technology specialization, supersedes and fulfills the certification requirements for this service.
M5.1.5 Audit representation	If the partner contracted Cisco Services or a third party to design or build a Managed Security service, providing some or all of the Managed Security requirements. At the partner's discretion, Cisco Services or the third party must participate in the audit and provide evidence on how the requirements have been fulfilled. If the partner contracted Cisco Services to operate the Managed Security service, providing some or all of the managed security requirements. At the partner's discretion, Cisco Services must participate in the audit and provide evidence on how the requirements have been fulfilled.

M5.2 Service Design

The following section describes the key requirements needed to deliver managed security services, which include a range of services that a partner can deliver using Cisco security products deployed at the customer premises and/or in a partner's network or cloud infrastructure.

Requirement	Description
M5.2.1 Must offer Managed Firewall Service and at least one of the following services: • IPS/IDS • Web Content Security • Email Security • VPN Service	The Managed Security service is aimed at partners offering a range of security capabilities aimed at protecting the customer from a variety of security threats. Firewall is the basic component and is therefore required. The partner must also deliver at least one of the following services: IDS/IPS, Web Content Security, Email Security, and VPN Services. Firewall and VPN services must be delivered on a Cisco platform.

Firewall Service Capabilities

Core Functions

The following section describes the basic functions of a Managed Firewall service. The partner 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.

If the partner has already achieved Master Security Specialization, the following requirements can be waived: M5.2.2–M5.2.25.

Requirement	Description
M5.2.2 Support for Network Address Translation (NAT) to enable non-unique addresses to be used by the customer and to hide IP addresses from potential attackers	Network Address Translation (NAT) 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.
M5.2.3 Support for De-Militarized Zone (DMZ) or isolation LAN support	This security service option is only applicable when customers need to protect public Internet servers on a DMZ. Typically, networks are broken down into different zones, each with a different security level; for example, the inside of the network has the highest security level, and the Internet has the lowest security level. A typical firewall policy will allow connections initiated from the inside of the network to the Internet, but not the other way around. Both users from inside the network and the Internet must be able to access web servers that reside on the DMZ, which has a "medium" security level, i.e., lower than the inside network, but higher than the Internet. The DMZ must not be able to initiate connections to the inside network.

Stateful Inspection

The following section describes key features that provide business value to the end customer.

Requirement	Description
M5.2.4 Support for stateful firewall inspection engine	Stateful firewall inspection track 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 corporate zone.

M5.2.5 Support for authentication proxy	This is a Managed Security 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 router 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 network 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 the network against more general policy that is applied across multiple users. Authentication and authorization can be applied to the router interface in either direction to secure inbound or outbound extranet, intranet, and Internet usage.
M5.2.6 Support for transparent firewall support	This is a Managed Security option that provides the ability to insert firewall transparently into existing configured LAN environment and restrict traffic across the firewall to specific devices at the subnet level, i.e., of LAN traffic. This requires software bridging to be enabled. Users can allow selected devices from a subnet to traverse the firewall while denying access to other devices on the same subnet.
M5.2.7 Support for stateful inspection of encrypted traffic	This Managed Security option is applicable when customers need to protect public Internet facing servers on a DMZ. The firewall first allows encrypted traffic through to the DMZ based on standard rules. The traffic is then unencrypted within the DMZ, and a second pass through a firewall can now inspect the contents of the packets to ensure conformance to policies. After being passed, the traffic can then be re-encrypted and passed on to its destination.
Security	
The following section describes design considerations of the service that enhance the security and protection of the overall service. Firewall security can be demonstrated at the same time as the TCP emulated session, with traffic directed at the router or firewall.	
Requirement	Description
M5.2.8 Denial of Service (DoS) attack detection and prevention	The partner must exhibit an understanding of security product DoS attack prevention capability in order to implement configurations that suit the environment of each customer.
M5.2.9 User authentication and access limitation	This security service option provides the ability to limit access to corporate network resources to authenticated users. Examples are: • Support for split tunneling, which allows data to flow either inside or outside an encrypted tunnel • Limiting access to specific ports to restrict Internet traffic
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 partner may also demonstrate 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 partner will need to show that they will have the required expertise to implement these features when demanded by the market.	
Requirement	Description
M5.2.10 Instant Messenger (IM) Blocking	Instant Messenger blocking offers per-service control to block or allow Instant Messenger (IM) applications. It allows service restriction to text chat only, blocking voice and video chat and file transfer.
M5.2.11 Peer-to-peer control	Peer-to-peer control individually blocks access to BitTorrent, Gnutella, KaZaA, and eDonkey file-sharing networks.
M5.2.12 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.
M5.2.13 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.
M5.2.14 Java blocking	With the proliferation of Java applets available on the Internet, protecting networks from malicious applets has become a key issue for network managers. The Java blocking feature can be configured to filter or completely deny access to Java applets that are not embedded in archives or compressed in files.

Voice Security Features Support

The following section describes capabilities for managing the flow of IP-based voice traffic across the firewall. The partner must exhibit an understanding of the capabilities and how to ensure that they are made available to the customer. One way to prove this is to provide a sample customer design that shows how these features are made available.

If the market in which the service is offered does not yet demand this capability from a firewall service, the partner will need to exhibit that they will have the required expertise to implement these features when demanded by the market.

Requirement	Description
M5.2.15 Session Initiation Protocol (SIP) inspection	SIP inspection is described in RFC 2543 and RFC 3261, which are both used by Cisco CUCM and Call Manager Express. 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.
M5.2.16 Skinny local traffic support	Skinny Client Control Protocol (SCCP) is a protocol used in VoIP networks between Cisco IP phone and Cisco CUCM or Call Manager Express. Skinny application inspection help ensures that all SCCP signaling and media packets can traverse the security device.
M5.2.17 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

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.

Requirement	Description
M5.2.18 Dual firewall support with stateful failover	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.
M5.2.19 Configuration backup	Remote storage of configurations of all devices used in the firewall service with ability to provide remote restoration.

IDS/IPS Service Capabilities

Core Functions

The following section describes the basic functions of an IDS/IPS service. Core functionality requirements of the IDS/IPS service: the partner must provide evidence of the IDS/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.

Requirement	Description
M5.2.20 Intrusion detection capabilities	Networks are exposed to a wide range of attacks, including viruses, worms, port 80 misuse, spyware, botnets, spam, etc. An IPS device monitors transparently all traffic traversing between two interfaces. The major function of an IPS device is to compare traffic against well-known attack patterns, i.e., signatures, but also to look for heuristic attack patterns, for example, multihost scans, which could indicate a worm, and also protocol anomalies, which involves looking for deviations from a standard protocol. This is useful for identifying deviations from normal behavior, which can indicate that something is wrong, but might not be very useful for helping to decide what is wrong. This is why multiple techniques are needed; in combination this provides a higher chance of eliminating false positives. The service must include the ability to monitor network traffic and respond to

	intrusions as described above based on defined security policies. This monitoring will consist of event correlation, rating and filtering, and reporting through the customer web portal. The partner must provide evidence of the intrusion detection capability or alternatively provide evidence of procedures to map customer policies into processes executed by an event management correlation tool.
M5.2.21 Implementation and profiling service	To enable an effective intrusion detection and prevention solution, it is important to gain an understanding of the customer traffic in a “normal” or steady state environment. The partner must provide evidence of the capability to provide this either as a separate service or as a part of the IDS/IPS service. This vulnerability assessment is therefore a pre-requisite, since inventorying the network not only ensures that all end devices are adequately patched, but also enables Service Provider consultants to know where best to place the IPS devices and helps with alarm classification, if we know, for example, that an attack targeting Windows is not relevant to a subnet that only has Linux hosts.
M5.2.22 Intrusion monitoring	Includes support for the following detection methodologies: Simple pattern matching: Looks for a fixed sequence of bytes in a single packet Stateful pattern matching: Matches are made in context within the state of the data stream Alarms generated that are classified, rated, and presented to the portal in real time (an example of this would be the use of Cisco IntelliShield Alert Manager service)
M5.2.23 Signature management	IPS uses signatures as the primary mechanism to detect known attacks; just as with antivirus, the quality of IPS is dependent on the signature database being up to date. The partner must provide evidence of an effective process for signature management that ensures that new Cisco IPS operating system and signature updates are implemented via an agreed process with the customer. An example of this would be the use of Cisco IPS signature management service.
M5.2.24 Incident handling	The partner must provide as part of the service the capability to process the multiple events that are generated from event correlation and turning those into a few meaningful events so that a root cause analysis can be carried out to determine a long-term fix, which may be a new signature, an ACL, a blocking action, or other configuration changes.
M5.2.25 Redundancy	Service must include the ability to recover from a device failure without service disruption. This is achieved using the inline IPS mode, where traffic switches over to a secondary device without service disruption.

Content Security Service Capabilities

Core Functions

Cisco offers several options to provide content security technologies. Cisco Email Security Appliance provides best-in-class appliance-based technology for email security and web security. The following section describes the basic functions this solution provides and the associated benefits, which must be supported as part of the managed service.

The partner must provide evidence of the associated service capabilities and explain the key benefits and how they can be used to reduce threats from Internet traffic into the customer network. Because a managed service may not always provide both email and web security, the requirements for each of the security services appear in separate sections.

Email Security Requirements	Description
M5.2.26 Anti-spam	Internet criminals constantly evolve techniques to penetrate an organization’s defenses. Email threats have expanded beyond simply annoying spam to dangerous phishing and fraudulent spam. The partner must explain how the technology removes most unsolicited email whether it is malicious (e.g., targeted phishing message) or not (e.g., traditional spam message) before it hits the mail server, and the benefits that this can provide in increasing security, employee productivity, and preventing waste of network bandwidth and storage, by using Cisco Email Security Appliances 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.

M5.2.27 Anti-virus	The scale and complexity of recent virus attacks highlight the importance of a vigorous, secure messaging platform. The partner must explain how the solution combats those threats, by using Cisco Email Security Appliances to detect infected messages and filter SMTP traffic for optimal detection rates and security at the network perimeter.
M5.2.28 Data loss prevention and content filtering	A significant amount of information exits a company through emails. Typically, emails go largely uncontrolled and unmonitored on their way to their destinations; businesses need tools to gain better awareness of not only what is entering but also what is leaving their network. The partner must explain how their service offering provides high-performance, comprehensive data loss prevention for data and content filtering. The partner must demonstrate and explain the benefits of content filtering by enforcing rules on users, file types, file sizes, keyword searches and dictionaries, credit card information, social security numbers, etc. The partner must also be able to explain how they help customers enforce acceptable usage policy 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.
M5.2.29 Email encryption technology	The partner must explain how encryption technology helps to protect and empower the business as well as individual employees by allowing/restricting use of email encryption for sensitive communications and ensure compliance with regulations by using Cisco Email Security Appliances to encrypt identified messages for content that requires encryption (this could be TLS or message-based encryption).
Web Security Requirements	Description
M5.2.30 Anti-virus and anti-spyware	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 partner 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 Web Security Appliance to filter HTTP and optionally HTTPS traffic for optimal detection rates and security at the network perimeter • Using Cisco Umbrella technology at the Internet edge to prevent the majority of malicious code from entering the customer network from Internet
M5.2.31 URL filtering	The partner must explain how the solution provides industry-leading visibility and protection from web use violations by: • Using Cisco Web Security Appliance for a combination of list-based URL filtering, real-time dynamic categorization, and application visibility and control • Using Cisco Umbrella technology to perform URL filtering
Secure Encrypted VPN Service Capabilities	
Core Functions The following section describes the basic functions of an Internet Virtual Private Network (VPN) service based on CPE-based encryption technologies. The partner must provide evidence of the VPN service capabilities and, explain the key benefits of the service and how it can be used to deliver a secure managed IP VPN service.	
Requirement	Description
M5.2.32 Support for at least one of the required IP VPN architectures	The partner must support at least one of the following VPN deployment architectures: • IPsec-to-Multiprotocol Label Switching (MPLS): For The partners offering an MPLS VPN service, IPsec-to-MPLS deployments enable secure off-net remote access to the VPN. • IPsec-to-Layer 2 VPN using Layer 3 routing: The IPsec-to-Layer 2 VPN model

	is very similar to the IPsec-to-MPLS architecture described above, except the partner has a Layer 2 core instead of an MPLS core. • IPsec-to-Generic Routing Encapsulation (GRE): The IPsec-to-GRE deployment architecture is useful when the Service Provider has an IP backbone but still wants to provide VPN-like capability. • Provider edge-to-provider edge encryption: The provider edge-to-provider edge encryption deployment architecture enables the partner to encrypt the traffic between the provider edge devices across an MPLS network while still maintaining the traffic separation provided by MPLS. This encryption architecture can be accomplished by running label-switched path (LSP) across a GRE tunnel. All packets flowing through the GRE tunnels will be encrypted. • End-to-end encryption over MPLS VPN network: Within the MPLS VPN network, customers can also accomplish end-to-end encryption, from CPE to CPE, where CPE devices are directly connected to the MPLS network using Cisco GETVPN technology. • CPE-based site-to-site IPsec VPN: Site-to-site VPNs provide an Internet-based WAN infrastructure to extend network resources to branch offices, home offices, and business partner sites. All traffic between sites is encrypted using the IPsec protocol and integrates network features such as routing, quality of service and multicast services. The partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural or topology diagrams.
M5.2.33 CPE-based site-to-site VPN	The partner must offer a site-to-site VPN service that offers secure site-to-site connectivity. The partner must support at least two of these options. Hub-and-spoke VPN: • Enhanced easy VPN, dynamic virtual tunnel interfaces, dynamic policy push • Routed IPsec with GRE or DMVPN with dynamic routing Spoke-to-spoke VPN: • Dynamic multipoint VPN (DMVPN) • On demand VPN (Partial mesh) Any-any VPN: • Group encrypted VPN (no tunnels needed) • Multicast support • Key distribution RFC 3547 • Encrypted unicast traffic using IPsec (RFC 2401) • Support of voice and video traffic The partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural or topology diagrams.
M5.2.34 Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), and Advanced Encryption Standard (AES) (where permitted) encryption for IPsec	There are different encryption protocols that can be used to create an IPsec-based VPN service, which are all supported within Cisco IOS Software. The partner must provide evidence that they support these protocols to build IPsec VPNs. The partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural or topology diagrams.
M5.2.35 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 partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural or topology diagrams.
M5.2.36 Authentication, Authorization, and Accounting 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 partner, 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 partner site, a RADIUS server can store all AAA and configuration information, or the information can be split across two servers. For this component, the partner 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 server must be installed on the service-provider management network for local AAA or on the customer premises for proxy authentication. The partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural or topology diagrams.

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 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.

Requirement	Description
M5.2.37 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.
M5.2.38 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.
M5.2.39 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.

Service Security: Infrastructure (applies only to organizations providing the infrastructure for delivery of the service, e.g., carriers)

The following section describes design requirements for the infrastructure that the Managed Security service uses to connect to the Internet. The partner may also provide design configuration guidelines that they use for the infrastructure or provide example configurations, including the listed features from a deployed device. The partner must also be able to exhibit an understanding of resiliency and redundancy features and how they have been incorporated into the design of the service.

Requirement	Description
M5.2.40 In accordance with Network Foundation Protection (NFP) requirements, processes and procedures to ensure protection of data plane, management plane, and control plane	Data plane: • Access Control Lists (ACLs): Protect devices from malicious traffic by explicitly permitting legitimate traffic • Unicast Reverse Path Forwarding (URPF): Mitigates problems caused by the introduction of malformed or spoofed IP source addresses • Remotely Triggered Black Hole (RTBH): Drops packets based on source address and can be used while device is under attack • QoS tools: Used to protect against flooding attacks Control plane: Routing protection: MD5 neighbor authentication protects routing domains from spoofing attacks Management plane: Dual export syslog: Increases availability by exporting information to dual collectors

M5.2.41 System-level resiliency: Effective design process to ensure deployment where applicable to enhance device-level hardware and software resiliency	System-level resiliency incorporates hardware redundancy capabilities as well as features within Cisco IOS Software to enable high availability. Using these features enables the partner to build a reliable foundation for the service. These features include: • Nonstop Forwarding (NSF)/Stateful Switchover • In-service software upgrades • Graceful restart
M5.2.42 Network-level redundancy: Effective design process to ensure use of software features to enhance network-level resiliency	To ensure network-level redundancy, specific routing protocol features can be enabled depending on the configuration and protocols used. These features include: • Nonstop Forwarding (NSF) awareness: Allows a router to assist NSF-capable neighbors to continue forwarding packets during a Stateful Switchover (SSO) operation • Fast convergence: Adjusts the sizing of interior gateway protocols to allow the routing tables to converge faster • IP event dampening mechanism: Suppresses the effects of excessive interface flapping events on routing protocols and routing tables in the network

M5.3 Service-Level Management Requirements

Service-Level Agreement (SLA) Components

This section describes the SLAs 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 SLAs may also be presented as evidence of meeting these requirements.

Requirement	Description
M5.3.1 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.
M5.3.2 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
M5.3.3 Turnaround time for customer-initiated changes	The turnaround time for implementing changes requested by the customer; must be within 24 hours for standard changes.
M5.3.4 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.
M5.3.5 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 partner must also be able to show that event logs can be stored and made accessible via the 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.

Requirement	Description
M5.3.6 Secure web portal to communicate 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.
M5.3.7 Event log retention	Security events are stored in a log for regulatory and analysis purposes. Must be retained for period of time established with the customer.
M5.3.8 Summary-level dashboard to communicate key performance criteria, including: ▪ Real-time status map ▪ Monitoring report ▪ Usage report	For firewall, IDS/IPS, and web and email content security services, the security dashboard must include: • Top five attacked sites of the month/week: The top five most attacked sites, 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 performance 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.

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 the partners to differentiate themselves from other partners.

Requirement	Description
M5.3.9 Service Availability reports	Summary views of service availability reports on the overall service availability, e.g., by site or equipment.
M5.3.10 Device Inventory reports	Reports of devices under management for the customer; provide data that is relevant to the customer regarding inventory of equipment used in delivering the service.
M5.3.11 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.
M5.3.12 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.
M5.3.13 Security reports	Detailed security reports, including: • 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 provision of example reports or demonstration of reporting tool with ability to select reports listed.	
Requirement	Description
M5.3.14 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 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 provision of example reports or a demonstration of the 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.	
Requirement	Description
M5.3.15 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: Includes incidents such as hardware or link failures on network devices that were successfully routed around

Click here to return to Table of Contents

M6 Business Communications

Introduced: October 2007
Last updated: April 2016

Overview

Cisco Powered Business Communications service is defined as the partner 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 partner 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 partner must meet the following prerequisites to apply for this service designation.

Requirement	Description
M6.1.1 Meet all CMSP partner requirements in Cisco Channel Program Audit and Policies document	See CMSP partner requirements in Cisco Channel Program Audit and Policies document.
M6.1.2 Submit at least two customer references for the service	CMSP partners are required to have a minimum of two customer references, from existing contractual relationships, for each Cisco Powered service. One customer may serve as reference to multiple designations. A customer with multiple sites does not qualify as a second reference however. The intent is to ensure that the partner has proven and repeatable service practices. The partner must submit at least two customer references for the service at the time of the audit, or must provide evidence of the ability to deliver the service to an end customer. In the event that no customer references are available at the time of the audit, two customer references must be provided upon recertification. Refer to Customer Reference Validation template.
M6.1.3 Deliver call management on Cisco infrastructure	To qualify for this Cisco Powered managed service, the call management function must be delivered on the Cisco UCS platform, and associated security functions delivered on Cisco platforms.
M6.1.4 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. See section 9.3 for SLA requirements. 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.
M6.1.5 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 partner 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.
M6.1.6 Maintain Advanced Collaboration Architecture Specialization in country where	The partner must maintain the Advanced Collaboration Architecture Specialization overall for all Cisco Powered UC or HCS services; does not have to be unique to

service originates	each service.
M6.1.7 Audit representation	If the partner has contracted Cisco Services or a third party to design or build a Business Communications service, providing some or all of the Business Communications requirements. At the partner's discretion, Cisco Services or the third party must participate in the audit and provide evidence on how the requirements have been fulfilled. If the partner has contracted Cisco Services to operate the Business Communications service, providing some or all of the Business Communications requirements. At the partner's discretion, Cisco Services must participate in the audit and provide evidence on how the requirements have been fulfilled.

M6.2 Service Design

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 partner 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 partner must demonstrate the ability to manage the service up to the most current version of Cisco Unified Communication Manager.

If the partner has already achieved Master Unified Communications or Master Collaboration Specialization, the following requirements can be waived: M6.2.1–M6.2.16.

Requirement	Description
M6.2.1 Capability to build migration plan into project management for the customer	The partner must provide evidence of 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.
M6.2.2 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 partner 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.
M6.2.3 Voice and integrated messaging	The partner 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 partner 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 partner must present evidence that at least six of the above messaging capabilities of the solution and explain the benefits of the various features.

M6.2.4 Presence and Instant Messaging	The partner must provide evidence that Presence and IM capabilities are available to customers. The partner 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 partner 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)
M6.2.5 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 partner must provide evidence that video is supported as part of the service.
M6.2.6 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 partner 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
M6.2.7 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 partner 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
M6.2.8 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 partner 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.

M6.2.9 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 partner 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.
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 partner must demonstrate compliance to this section if their primary service offer uses CPE-based call control.	
Requirement	Description
M6.2.10 Service resiliency design	The business communications solution includes many features that can be used to enhance overall service availability. The partner 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)
M6.2.11 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 partner 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.

M6.2.12 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
M6.2.13 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)
M6.2.14 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 partner 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
M6.2.15 Key capabilities that are supported by the solution	The partner 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
M6.2.16 Anti-virus application	There are many servers that may be used in support of the delivery of this managed service. The partner 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 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. This section applies only to partners who are using CPE-based call control.

Requirement	Description

M6.2.17 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.
M6.2.18 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.
M6.2.19 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.

M6.3 Service-Level Management Requirements

Service-Level Agreement (SLA) Components

This section describes the SLAs 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 SLAs may also be presented as evidence of meeting these requirements.

Requirement	Description
M6.3.1 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.
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 partner, or the customers may be given access to do this themselves. If the customer carries out these changes, the partner must demonstrate how access is provided. If changes are the responsibility of the partner, 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 partner, or the customers may be given access to do this themselves. If the customer carries out these changes, the partner must demonstrate how access is provided. If changes are the responsibility of the partner, 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 partner must also be able to show that event logs can be stored and made accessible via the 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.

Requirement	Description
M6.3.5 Secure web portal to communicate 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 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 the partner to differentiate themselves from other partners.

Requirement	Description
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 partner 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)

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.

Requirement	Description
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)

Click here to return to Table of Contents

M7 Unified Contact Center

Introduced: October 2007
Last updated: May 2015

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 Meet all CMSP partner requirements in Cisco Channel Program Audit and Policies document	See CMSP partner requirements in Cisco Channel Program Audit and Policies document.
M7.1.2 Submit at least two customer references for the service	CMSP partners are required to have a minimum of two customer references, from existing contractual relationships, for each Cisco Powered service. One customer may serve as reference to multiple designations. A customer with multiple sites does not qualify as a second reference however. The intent is to ensure that the partner has proven and repeatable service practices. The partner must submit at least two customer references for the service at the time of the audit, or must provide evidence of the ability to deliver the service to an end customer. In the event that no customer references are available at the time of the audit, two customer references must be provided upon recertification. Refer to Customer Reference Validation template.
M7.1.3 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.
M7.1.4 Meet UCCE ATP requirements	Must meet UCCE ATP requirements in order to purchase product and deploy this managed service.
M7.1.5 Audit representation	If the partner contracted Cisco Services or a third party to design or build a Unified Contact Center service, providing some or all of the Unified Contact Center requirements. At the partner's discretion, Cisco Services or the third party must participate in the audit and provide evidence on how the requirements have been fulfilled. If the partner contracted Cisco Services to operate the Unified Contact Center, providing some or all of the Unified Contact Center requirements. At the partner's discretion, Cisco Services must participate in the audit and provide evidence on how the requirements have been fulfilled.

M7.2 Service Design

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.

Requirement	Description
M7.2.1 Virtual call center	Calls are routed to contact center agents regardless of their location over an IP-based infrastructure.
M7.2.2 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.
M7.2.3 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.
M7.2.4 Remote agent support	Uses Unified Mobile Agent to provide remote agents in branch offices or homes CTI, contact distribution, and reporting capabilities.
M7.2.5 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.
M7.2.6 Email management	Service must provide support for handling customer email inquiries submitted to company mailboxes or websites.
M7.2.7 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.
M7.2.8 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
M7.2.9 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.
M7.2.10 Web 2.0 Integration	Support for Web 2.0 features such as: • Click to Talk • Chat room • Video links • Customer feedback
M7.2.11 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.
M7.2.12 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.	

Requirement	Description
M7.2.13 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.
M7.2.14 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.
M7.2.15 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.

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.

Requirement	Description
M7.2.16 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.
M7.2.17 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.
M7.2.18 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

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.

Requirement	Description
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.
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.

Requirement	Description
M7.3.4 Customer web portal to communicate 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.

Requirement	Description
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.
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.	
Requirement	Description
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
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.	
Requirement	Description
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.

Click here to return to Table of Contents

M8 Business Video

Introduced: November 2008
Last updated: November 2017

Overview

Cisco Powered Business Video is a Managed Video service based on Cisco technology, where a partner is providing complete management for video infrastructure and endpoints. The equipment can either be owned by the customer or dedicated to a single customer by the partner, and the video infrastructure can be at the customer site or hosted in a partner's data center.

M8.1 Prerequisites

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

Requirement	Description
M8.1.1 Meet all CMSP partner requirements in Cisco Channel Program Audit and Policies document	See CMSP partner requirements in Cisco Channel Program Audit and Policies document.
M8.1.2 Submit at least two customer references for the service	CMSP partners are required to have a minimum of two customer references, from existing contractual relationships, for each Cisco Powered service. One customer may serve as reference to multiple designations. A customer with multiple sites does not qualify as a second reference however. The intent is to ensure that the partner has proven and repeatable service practices. The partner must submit at least two customer references for the service at the time of the audit, or must provide evidence of the ability to deliver the service to an end customer. In the event that no customer references are available at the time of the audit, two customer references must be provided upon recertification. Refer to Customer Reference Validation template.
M8.1.3 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.
M8.1.4 Meet relevant ATP requirements	Must have one of the following video designations in host theater (where NOC is located or where the partner is headquartered) and remote ATP in the theaters where partner intends to purchase product and deploy this managed service. • Express Video Specialization or Express Specialization in Video Track • Advanced Video Specialization • TelePresence Video Master ATP See the Authorized Technology Provider Requirements.
M8.1.5 Maintain method to manage all video room components	All video room components can be managed, for example, via Simple Network Management Protocol (SNMP), web interfaces, and Command Line Interface (CLI).
M8.1.6 Actively use the video solution internally	Required in order to understand the benefits of the solution and implications on the network of adding this as a service to an integrated IP network. This can be based on any of the Cisco TelePresence video products in the Cisco portfolio.
M8.1.7 Employ at least one trained/certified individual on staff	The partner must have an individual that has taken and passed the following Cisco Certification exams: • Collab150 – Cisco Meeting App Foundation • Collab350 – Cisco Meeting Server Advanced
M8.1.8 Audit representation	If the partner contracted Cisco Services or a third party to design or build a business video platform, providing some or all of the business video requirements. At the

	partner's discretion, Cisco Services or the third party must participate in the audit and provide evidence on how the requirements have been fulfilled. If the partner contracted Cisco Services to operate the Business Video platform, providing some or all of the Business Video requirements. At the partner's discretion, Cisco Services must participate in the audit and provide evidence on how the requirements have been fulfilled.

M8.2 Service Design

Service Capabilities

The following section describes the basic functions of a Managed Business Video service. The partner must demonstrate the service capabilities, and explain the key benefits of Business Video to enhance the way a customer can run their business.

Requirement	Description
M8.2.1 Cisco TelePresence multipoint service in a managed configuration, including support for key additional features of the multipoint solution	Multipoint capabilities must be delivered using Cisco Meeting Server to support HD video calling. The Cisco Meeting Server allow users to connect to multiple single screen Cisco TelePresence endpoints, three-screen Cisco TelePresence endpoints, or a mix of both in a single meeting. They will deliver voice-activated switching either site-by-site (site switching). The partner must provide evidence of these features and display an understanding of how they can be used in a customer environment to add value to the Cisco TelePresence session.
M8.2.2 Concierge services for Cisco Video endpoints and infrastructure	Integration of the immersive video service with other applications such as Cisco Unified Communications Manager and the Cisco IP Contact Center enables the partner to assign a virtual or live operator who can moderate meetings, connect participants who are using a standard phone or other video communications system, and provide additional meeting services. The partner must provide a published service description outlining features provided for the concierge service offered. Typically, the operator will be available via Cisco TelePresence, video, or audio dial-out facility and provide: • On-line training/assistance • Ad hoc addition of participants • Pre-connected and tested conferences
M8.2.3 Remote assistance	The partner must provide documentation on processes used to ensure that the service is available when required by the customer, and a training schedule to ensure that the staff understands the capabilities and limitations of the solution and the key functions used to set up and support all Cisco TelePresence session types supported.
M8.2.4 Reservation service	The partner must outline the reservation processes that are supported for the customer, which must include an automated online system.
M8.2.5 One button to push (OBTP) enabled from Microsoft Exchange or IBM Domino	The partner must demonstrate that the service includes integration with Microsoft Exchange to enable OBTP for the user from these applications for all endpoints that support it. *Note: This requirement only applies if offered as part of the service.*
M8.2.6 Gateway services	The customer may have existing infrastructure that needs to be considered when designing the solution. Examples are: • Providing end-to-end connectivity for customers on a global basis over IP • Helping migrate the customer over time from standard definition to high-definition endpoints • Providing interoperability with desktop clients • Providing firewall traversal services The partner must explain how their service can help the customer integrate the Cisco TelePresence service into their existing environment, how it can evolve from there, and the benefits that the customer will gain with the addition of each new

	capability into the service.
Design Considerations	
The following section describes the key service design functions. These can be proven as part of the demonstration or example customer designs or as part of the published service description.	
M8.2.7 Redundant and resilient service availability	Clustering technologies provide redundancy in the call control environment such that a port will fail over in the event of a call control failure without service disruption. Clustering technologies provide redundancy in the video bridging environment such that the participant will be able to rejoin the conference in the event of a calling bridge failure. The partner must provide evidence that this is an option for the customer in service design; explain how it is architected in their solution and the benefits to the customer.
M8.2.8 Unified Communications infrastructure reliability	The partner must present design best practices to ensure the reliable UC infrastructure for the managed business video service. Features that can help provide this include: • Redundancy for key services, including TFTP, DNS, DHCP, LDAP, and IP Phone Services • Redundant media resources, including conference bridges and music on hold • Hot Standby Routing Protocol (HSRP) at the distribution layer routers • Either 1:1 or 1:2 redundancies for call processing servers • For Cisco Unified Communications Manager, support for clustering of call control servers for redundancy
M8.2.9 Campus Quality of Service (QoS) design	The business video service will have an effect on the existing campus infrastructure. The partner must ensure that the design of the campus infrastructure to support the video traffic conforms to the guidelines outlined in Cisco best practice design guidelines Solution Reference Network Design (SRND). This must include: • Strict priority hardware queuing • Defined limitation of percentage of the link assigned to high-priority traffic
M8.2.10 Security best practices implemented for the overall video service	The partner must present a security design for the service that ensure at least: • Access to set up calls can be restricted • Access to management tools is restricted to authorized personnel • No security gaps are created when designing the service to gain remote access to customer located equipment The partner must describe their security procedures for the overall service; explain how it is designed to ensure the integrity of the customer environment and the benefits of the Cisco solution to the customer.
M8.2.11 Must have access to and monitor all devices within customer sites that may affect the performance of the business video service (if included within the scope of the service)	In addition to the video equipment itself, there are many potential devices within the campus, such as LAN switches and the CPE used to connect to the WAN that can affect the Cisco TelePresence service. In order to effectively isolate incidents that cause service deterioration, the partner must have visibility of all such devices. The partner must provide evidence that the campus environment is capable of supporting the video traffic. In some cases, the end customer may be managing the network that the video traverses. The partner must then show that the necessary tools and processes are in place with the end customer to ensure that the environment is monitored, including events such as configuration changes, which could adversely affect service performance.
M8.2.12 Inter-site Immersive Video traffic deployment design	To ensure a consistent user experience of the service, inter-site immersive video traffic must be appropriately handled from the egress CPE across the VPN network and across the destination campus. The partner must demonstrate how this is achieved in partnership with the MPLS VPN provider, taking into consideration: • Low-latency queuing on the CPE connected to the VPN, that uses no more than 33% of the bandwidth • Mapping of user traffic and signaling to appropriate Class of Service queues in the network • Restoration of any settings at the CPE located at the destination site (network transparency)

Design Considerations: Business Video Service with Infrastructure Located Off Premises from Customer's Network	
The following additional service capability requirements apply to off-premises Business Video service, i.e., where the partner hosts some of the equipment such as bridges that are used as part of the overall managed service.	
Requirement	**Description**
M8.2.13 Management of connectivity between customer located endpoints and equipment hosted by the partner	Connections must be provided for all customer device endpoints under management so that they can participate in multipoint conferences. The partner must explain how this is achieved to provide reliable and consistent access.
M8.2.14 Support for integration with customer-owned management system	Customer may select to run parts of the service internally and select the partner to manage other parts of the service, for example, out of region. The partner must explain how they manage the systems communications between the customer and partner solutions to ensure a seamless user experience.
M8.2.15 Connectivity between the management software and all associated endpoints and multipoint switches	The management software, e.g., TMS, must be placed in the network environment so that it has appropriate connectivity to all associated endpoints and Cisco Meeting Servers. The partner must explain how they address the security aspects of a hybrid approach such as traversal across customer firewalls for management traffic.
M8.2.16 Performance effect of off-premises solution	The deployment of bridging within the partner network may add additional delay to the performance of the service. The partner must provide evidence of how they are taking this into account with the design to ensure the customer experience is not adversely affected.
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 the business video service. 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.	
Requirement	**Description**
M8.2.17 Security best practices implemented for the Unified Communications infrastructure used by the Business Video service	These must include: • Support for device authentication • Support for signaling and media encryption

M8.3 Service-Level Management Requirements

Service-Level Agreement (SLA) Components

This section describes the SLAs 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 SLAs may also be presented as evidence of meeting these requirements.

Requirement	Description
M8.3.1 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.
M8.3.2 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. May vary according to severity levels. 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
M8.3.3 Provisioning capacity	The partner must have an agreement in place with the customer on how many video sessions can be accessed simultaneously and how much advance notice is required to reserve this capacity. The partner must provide evidence of the necessary Cisco Meeting Server capacity to support those SLAs. This SLA applies only to partners that are providing additional capacity to the customer that is not part of the video managed service dedicated to the customer.
M8.3.4 Concierge/Help-desk Agent Availability	The availability of the Business Video concierge/help desk is a critical component of the service. Video users expect immediate response when they experience problems during a video session. Must offer an SLA for agent/concierge availability, if offered as part of the video managed service.

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 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 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.

Requirement	Description
M8.3.5 Customer web portal to communicate 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: • Real-time status map • Monitoring report • Usage report

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.

Requirement	Description
M8.3.6 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) links or how much traffic is being generated by a particular application.
M8.3.7 Service Availability reports	Summary views of service availability reports on the overall service availability, e.g., by site or equipment.
M8.3.8 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.
M8.3.9 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.

M8.3.10 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.
M8.3.11 Call Detail reports	The partner must provide reports on the Cisco TelePresence calls that are made. This must include: • Call Manager status and performance • Call statistics (e.g., duration, failed attempts)
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.	
Requirement	Description
M8.3.12 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) • UC and TP endpoint peripheral failures

Click here to return to Table of Contents

M9 Service Provider Wi-Fi

Introduced: May 2013
Last Updated: May 2014

Overview

Service Providers in the mobility market continue to evolve their infrastructure; there is a need to consider alternate means for wireless coverage to address the consumption of bandwidth by customers.

One of the options to address this situation is the consideration by Mobile Network Operators (MNOs) leveraging a Service Provider Wi-Fi (SP Wi-Fi) design to provide the data bandwidth and coverage, where traditional macrocell radio footprints (2G, 3G, and 4G) have a challenge such as in-building coverage.

Another option is the consideration by Multi-System Operators (MSOs) extending their Internet access by leveraging alternate backhaul infrastructure (i.e. Cable).

The scope of the SP Wi-Fi deployments includes mobile traffic offload for Mobile Network Operators (MNOs) as well as native public Internet access for Multi-System Operators (MSOs). The criteria are based on the current solution development efforts within Cisco's Mobile Internet Technology Group (MITG) and should be used to prepare for the onsite Cisco Powered services audit process.

M9.1 Prerequisites

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

Requirement	Description
M9.1.1 Meet all CMSP partner requirements in Cisco Channel Program Audit and Policies document	See CMSP partner requirements in Cisco Channel Program Audit and Policies document.
M9.1.2 Submit at least two customer references for the service	CMSP partners are required to have a minimum of two customer references, from existing contractual relationships, for each Cisco Powered service. One customer may serve as reference to multiple designations. A customer with multiple sites does not qualify as a second reference however. The intent is to ensure that the partner has proven and repeatable service practices. The partner must submit at least two customer references for the service at the time of the audit, or must provide evidence of the ability to deliver the service to an end customer. In the event that no customer references are available at the time of the audit, two customer references must be provided upon recertification. Refer to Customer Reference Validation template.
M9.1.3 Provide the wireless infrastructure on which the service is delivered	The partner offers wireless coverage (SP Wi-Fi) for hotspot locations in order to provide Internet access to end customers. To meet all of the requirements and ensure a quality service experience, the partner needs to control the configuration of the network devices. Requirement must be met using Cisco infrastructure.
M9.1.4 Deliver Internet Protocol (IP) transport 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.
M9.1.5 Provide a Marketing Service Description (MSD) unique to the service	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.
M9.1.6 Employ have at least one CCNP Wireless certified individual on staff	The Cisco CCNP Wireless certification provides individuals working in Service Provider organizations with competencies in infrastructure IP networking solutions. CCNP Wireless professionals have detailed understanding of wireless networking technologies in the Service Provider market. See CCNP Wireless for more information. A Cisco CCIE certification, of any technology specialization, supersedes and fulfills the certification requirements for this service.

M9.1.7 Audit representation	If the partner contracted Cisco Services or a third party to design or build a Service Provider Wi-Fi service, providing some or all of the Service Provider Wi-Fi requirements. At the partner's discretion, Cisco Services or the third party must participate in the audit and provide evidence on how the requirements have been fulfilled. If the partner contracted Cisco Services to operate the Service Provider Wi-Fi) service, providing some or all of the Service Provider Wi-Fi requirements. At the partner's discretion, Cisco Services must participate in the audit and provide evidence on how the requirements have been fulfilled.

M9.2 Service Design Requirements and Recommendations

Service Capabilities

The following section describes the basic functions of an SP Wi-Fi Whole Offer based on IP transport mechanisms. The partner must provide evidence of the service capabilities, explain the key benefits of the service, and how it can be used to provide a secure, reliable interconnect service between data center sites.

Requirement	Description
M9.2.1 Network foundation for the SP Wi-Fi Managed Service must be based on IP	To provide any-any connectivity as well as to make use of the QoS characteristics available, the SP Wi-Fi service must run over an IP-based network, provisioned on Cisco platforms.
M9.2.2 Network connectivity	The partner must provide the following information related to the transport network backhaul for the overall SP Wi-Fi design review: • Layer 3/Layer 2 E2E transport network topology information: The partner must provide the typology information for the transport networks between the locations where the AP/WLCs are positioned and where the ISG and Internet connectivity are located CO (Central Office). This will be used as a general sanity check to demonstrate how the partner is providing the end-to-end connectivity for the SP Wi-Fi design. • Ability to baseline and trend transport network growth. This will be used as a general sanity check to verify that the partner has the ability to determine network usage in order to avoid potential future congestion.
M9.2.3 Network infrastructure	The infrastructure configuration and design need to follow the design and best practices outlined by the Cisco SP Wi-Fi Whole Offer Solution Team (MITG) within following document: Cisco Service Provider Wi-Fi Solution Data Sheet.
Listed below are three deployment models (Metro Wi-Fi, Hotspot and Residential Gateway). Partners are not required to deploy all three models. The partners may choose one or more of the deployment models. The partner Account Team can provide information on the deployment models during the partner audit preparation from the partner Account Team from SP Wi-Fi Solution Engineering.	
M9.2.4 Metro Wi-Fi deployment model	The following functions are *required* to be delivered as part of a service on a Cisco platform: • Intelligent Services Gateway (ISG) • Wireless LAN controller (WLC) • Access points (APs): indoor/outdoor • SW (Cisco Catalyst switches with Power over Ethernet [PoE]) The following functions are *required* to be delivered as part of a service: • RADIUS Authentication, Authorization, and Accounting (AAA) server (i.e., Cisco Access Registrar [CAR]) • Dynamic Host Configuration Protocol/Domain Name Server (DHCP/DNS Server) (i.e., Cisco Network Registrar [CNR]) The following function is *recommended* to be delivered as part of a service: • Policy Server platform (i.e., Quantum Policy Suite)

M9.2.5 Hotspot deployment model	The following functions are *required* to be delivered as part of a service on a Cisco platform: • Intelligent Services Gateway (ISG) • Wireless LAN controller (WLC) • Access points (APs): indoor/outdoor • SW (Cisco Catalyst switches with Power over Ethernet [PoE]) • Access Zone Router (AZR) The following functions are *required* to be delivered as part of a service: • RADIUS authentication, authorization, and accounting (AAA) server (i.e., Cisco Access Registrar [CAR]) • Dynamic Host Configuration Protocol/Domain Name Server (DHCP/DNS Server) (i.e., Cisco Network Registrar [CNR]) • L2TP Network Server (LNS): remote L2VPN connectivity The following function is *recommended* to be delivered as part of a service: • Policy Server platform (i.e., Quantum Policy Suite)
M9.2.6 Residential gateway model (cable operators)	The following functions are *required* to be delivered as part of a service on a Cisco platform: • Residential gateway (RG) with Mobile Access Gateway (MAG) functionality • Access points (APs): indoor/outdoor The following functions are *required* to be delivered as part of a service: • RADIUS Authentication, Authorization, and Accounting (AAA) server (i.e., Cisco Access Registrar [CAR]) • Dynamic Host Configuration Protocol/Domain Name Server (DHCP/DNS Server) (i.e., Cisco Network Registrar [CNR]) • Modular Cable Modem Termination Systems (M-CMTS) DOCSIS 3.0 (i.e., Cisco uBR10012) The following functions are *recommended* to be delivered as part of a service: • Policy Server platform (i.e., Quantum Policy Suite) • Intelligent Services Gateway (ISG)
M9.2.7 Traffic differentiation	The network configuration design must follow the design and best practices outlined by the Cisco SP Wi-Fi Whole Offer Solution Team (MITG) within the Design Implementation Guidelines (DIG) in order to handle different types of traffic (Gold, Silver, Bronze) and classify the traffic accordingly. Solution must support: • Cisco SP Wi-Fi traffic which is mapped to the correct QoS/CoS queue in order to address the individual traffic requirements such as video.
Service Security: Infrastructure	
The following section describes general guidelines to address protection of the infrastructure that is used to transport the Service Provider Wi-Fi Whole Offer services. These requirements are listed in the Network Foundation Protection (NFP) requirements. A Cisco sales engineer (SE) should be able to help validate that partner has incorporated these features into their security best practices.	
Requirement	Description
N/A	N/A
Best Practice Recommendation	Description
M9.2.8 Security Policy	With an IP-based transport design, a security policy needs to be initially addressed in order for the provider to define a security framework regarding what is considered secure and unsecure. This concept includes SP Wi-Fi Managed Service deployments. After a security policy has common agreement, general security tools can be used to address the security policy as mentioned below. The following functions are *recommended* to be delivered as part of the IP transport infrastructure: • Access Control Lists (ACLs: data plane) • Infrastructure Control Lists (ICLs: control plane) • Password protection (local, RADIUS/AAA, TACACS) • Change control (via NMS/OSS; i.e., Cisco Prime™) • MD5 authentication for routing protocols • Firewall features enabled (Denial of Service/DoS attack)

	The following functions are *recommended* to be delivered as part of Wireless LAN (WLAN) access security authentication methods: • Extensible Authentication Protocol (EAP) authentication • EAP for GSM Subscriber Identity Module (EAP-SIM) authentication • EAP Tunneled Transport Layer Security (EAP-TTLS) authentication • Web (user credentials) authentication • Web (one-click) authentication • Web (prepaid voucher) authentication • Wireless Internet Service Provider Roaming (WISPr) authentication *Note: For an SP Wi-Fi Managed Service Provider, the typical network environment is to provide basic broadband service that is considered "open." This would also influence the radio services as well (open SSID), although customers would have the ability to protect their devices by using VPN connections on top of the SP Wi-Fi service.*

M9.3 Service-Level Management Requirements and Recommendations

Service-Level Agreement (SLA) Components

This section describes the SLAs 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 SLAs may also be presented as evidence of meeting these requirements.

Requirement	Description
N/A	N/A
Best Practice Recommendation	**Description**
M9.3.1 Network Availability	The Next Generation Mobile Network committee issued a white paper related to Small Cell Backhaul outlining a proposal for the availability of the network on a 24x7x365 basis (total network hours minus downtime/total network hours multiplied by 100) when located within a macro-cell environment. The *recommended* guideline for the topic of availability is the following: Small Cell Backhaul Requirements, a White Paper by the MGMN Alliance. *Note: The value of the availability is based on the recommendations from the NGMN where the macro cell is able to provide the radio data service when the SP Wi-Fi/unlicensed small cell service is out of service.*

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.

Requirement	Description
M9.3.2 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

The following section describes reports that are to be internally created and reviewed, and 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 demonstration of reporting tool with ability to select reports listed. For non–service affecting incidents, partner must demonstrate a process to investigate reported problems as necessary in order to prevent them from affecting service to the customer.

Requirement	Description
N/A	N/A
Best Practice Recommendation	**Description**
M9.3.3 Performance reporting	In order to understand how well the network is performing against expectations and agreed Service-Levels and to identify trends that may need to be addressed, partner must maintain regular internal reports highlighting network performance. These could include parameters such as packet loss, packet errors, and packet throughput measurements across the network

	infrastructure. *Recommended* performance measuring tool: Cisco Prime Infrastructure.
M9.3.4 Analytics reporting	After the SP Wi-Fi Managed Service deployments are completed, there will be a need to gather instantaneous and historical statistics in order to address the topic of analytics reporting in order to understand the trending of the service for SP Wi-Fi. This could range from the increase of the number of customers/subscribers, length of connectivity of the customers/subscribers, or IPv4 versus IPv6 connectivity of the user end devices. *Recommended* analytics reporting tools are the following: • Cisco Prime Infrastructure • Cisco Mobility Services Engine (v7.5)
Summary Dashboard	
The following section describes the summary-level dashboard used to provide information about service status and performance. May be proven by a demonstration of summary dashboard on web portal provided to customer or description of dashboard contents provided in customer documentation.	
Requirement	Description
N/A	N/A
Best Practice Recommendation	Description
M9.3.5 Summary-level dashboard Monitoring report Usage report	The concept of a summary dashboard is to provide the visibility on how well the Service Provider Wi-Fi (SP Wi-Fi) Whole Offer deployment is working. Recommended summary dashboard tool: Cisco Prime Infrastructure.

Click here to return to Table of Contents

M10 RETIRED: Data Services over Satellite (DSoS)

Introduced: May 2014
Retired: November 2017

Click here to return to Table of Contents

M11 Managed Intelligent WAN (IWAN)

Introduced: May 2014
Updated: November 2016

Overview

Cisco Powered Managed Intelligent WAN (IWAN) is a Software Defined Wide Area Network (SD-WAN) solution that delivers secure, high-performance user experiences over any type of wide-area network. Cisco Intelligent WAN (IWAN) supports intelligent path control, application optimization, application visibility and control, secure inter-branch communication and secure direct Internet access. These IWAN software capabilities built on the following Cisco router platforms: Cisco 4000 Series Integrated Services Router (ISR), Cisco ISR Generation 2 (G2), Cisco ASR 1000 Series Aggregation Services Routers (ASR 1000), Cisco Cloud Services Router (CSR 1000V).

Managed IWAN features of the Cisco router platforms which are managed by the partner using a service delivery platform allow service subscribers to monitor their network resource usage, application performance metrics, and the application performance improvements resulting from deploying the solution.

IWAN provides additional value in terms of visibility of the applications running in the customer environment and the benefits of application optimization and acceleration. The solution provides the customer the visibility and reporting capabilities to understand which applications are using valuable resources within the network, and it provides the ability to prioritize and optimize critical applications.

M11.1 Prerequisites

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

Requirement	Description
M11.1.1 Meet all CMSP partner requirements in Cisco Channel Program Audit and Policies document	See CMSP partner requirements in Cisco Channel Program Audit and Policies document.
M11.1.2 Submit at least two customer references for the service	CMSP partners are required to have a minimum of two customer references, from existing contractual relationships, for each Cisco Powered service. One customer may serve as reference to multiple designations. A customer with multiple sites does not qualify as a second reference however. The intent is to ensure that the partner has proven and repeatable service practices. The partner must submit at least two customer references for the service at the time of the audit, or must provide evidence of the ability to deliver the service to an end customer. In the event that no customer references are available at the time of the audit, two customer references must be provided upon recertification. Refer to Customer Reference Validation template.
M11.1.3 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. 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.
M11.1.4 Maintain at least one CCNP Service Provider certified individual on staff	The Cisco CCNP Service Provider certification validates the ability to plan, implement, verify and troubleshoot local and wide-area enterprise networks and work collaboratively with specialists on advanced security, voice, wireless and video solutions. The CCNP Service Provider certification is appropriate for those with at least one year of networking experience who are ready to advance their skills and work independently on complex network solutions. Those who achieve CCNP Service Provider have demonstrated the skills required in enterprise roles such as network technician, support engineer, systems engineer or network engineer. A Cisco CCIE certification, of any technology specialization, supersedes and fulfills the certification requirements for this service.

M11.1.5 Maintain appropriate licenses on Cisco router platforms	The partner must offer Intelligent WAN service based on one or more of the following appropriately licensed Cisco technologies: • AX license on ISR G2 and ISR 4000 families • AX licenses for ISRs enable both Application Visibility and Control, PfR Path Control, ZBFW and WAAS capabilities at the most economical price point. With the correct initial hardware configuration, they enable upsell of the subscriber to the WAN Optimization service level without a truck roll. • AX or AVC license on ASR 1000. Because the ASR 1000 does not support WAAS running directly on the router, the AX license for the ASR 1000 offers a discount for the purchase of WAAS physical or virtual appliances to be used in association with the ASR 1000. • Premium license for CSR 1000V
M11.1.6 Manage the Path Control or Performance Routing Master Controller	For all IWAN deployments, the partner must host the Path Control or Performance Routing Master Controller in their cloud environment or manage as a dedicated platform at the customer premise. Cisco Performance Routing (PfR) consists of border routers (BRs) that connect to the DMVPN overlay networks for each carrier network and a master controller (MC) application process that enforces policy. The MC defines the IWAN domain and the HUB MC is the platform singled out in this requirement.
M11.1.7 Manage the WAAS Central Manager	For WAN Optimization subscribers, the partner must host virtual WAAS Central Manager in their cloud environment or WAAS Central Manager on a dedicated WAVE appliance at the customer premise with an option for a redundant configuration. Central Manager provides the following functionality: • Manages central configuration, provisioning, monitoring, fault management, logging, and reporting for up to 2500 WAVEs within a Cisco WAAS topology • Comprehensive statistics: Comprehensive logs, reports, graphs, and statistics for Cisco WAVE device functions help IT administrators to optimize system performance and troubleshooting • Monitoring, reporting, and alerts: The option for a redundant configuration would provide active/standby deployment with automatic failover, replication of Central Manager database and encryption keys
M11.1.8 Audit representation	If the partner contracted Cisco Services or a third party to design or build a Managed Intelligent WAN service, providing some or all of the Managed Intelligent WAN requirements. At the partner's discretion, Cisco Services or the third party may participate in the audit and provide evidence on how the requirements have been fulfilled. If the partner contracted Cisco Services to operate the Intelligent WAN (IWAN) service, providing some or all of the Managed Intelligent WAN requirements. At the partner's discretion, Cisco Services may participate in the audit and provide evidence on how the requirements have been fulfilled.

M11.2 Service Design (Build)

Service Capabilities

Cisco Performance Routing (PfR) improves application delivery and WAN efficiency. PfR dynamically controls data packet forwarding decisions by looking at application type, performance, policies, and path status. PfR monitors the network performance - jitter, packet loss, and delay - and makes decisions to forward critical applications over the best-performing path based on the defined application policy. PfR can intelligently load-balance traffic efficiently by using all available WAN bandwidth. IWAN intelligent path control is the key to providing a business-class WAN over Internet transport.

Requirement	Description
M11.2.1 Performance Routing	Performance Routing 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 uses Cisco router's performance routing (PfR) capability to automatically choose the best path for each application flow to maximize the application performance and availability, while optimizing the usage of each available network at the same time. Path selection is performed in real-time and

	considers connection quality parameters like network delay, jitter and loss, as well as the available bandwidth. The partner must present evidence of how this requirement is delivered to their customers.
M11.2.2 IWAN Hybrid Design Model (Required unless M11.2.3 is leveraged)	This design allows for Path Control Policies to move non-critical traffic off MPLS, which gives critical traffic better performance over the MPLS Network. It provides balanced SLA guarantees. This model has the following capabilities: • Uses at least one MPLS carrier • Uses at least one Internet carrier • Uses front-door virtual routing and forwarding (FVRF) on both MPLS and Internet links, with static default routing within the FVRF The partner must present evidence of how this requirement is delivered to their customers such as an architectural diagram.
M11.2.3 IWAN Dual Internet or MPLS Design Model (required if M11.2.2 is not leveraged)	The dual Internet or MPLS design provides the provider the align network services to support the customers SLA requirements. Dual MPLS provides the highest SLA options while dual Internet provides the lowest. This model has the following capabilities: • Uses at least two Internet Links or 2 MPLS Links • Uses front-door virtual routing and forwarding (FVRF) on both MPLS and Internet links, with static default routing within the FVRF The partner must present evidence of how this requirement is delivered to their customers.
Application Visibility and Reporting	
Application Visibility and Reporting is a set of service capabilities that allows the discovery and classification of all applications flowing over the network, provides reports on application network usage and performance throughout the enterprise, reports on performance of cloud applications and allows customer IT administrators to manage application SLAs.	
Requirement	Description
M11.2.4 Application discovery and network usage reporting	The Cisco platform enables the discovery of application protocols transiting a network interface for both incoming and outgoing traffic. A solution based on Cisco Network Based Application Recognition version 2 (NBAR2) provides stateful deep packet inspection (DPI) for granular, application-level traffic inspection, and it provides the ability to identify over 1000 application signatures. NBAR is also capable of defining up to 120 customized application profiles based on ports, URL or even payload values. NBAR is implemented on the Cisco ASR 1000 Series Aggregation Services Routers (ASR 1000), Cisco Integrated Service Routers Generation 2 (ISR G2) and ISR 4000 Series, and the Cisco Cloud Services Router (CRS1000v). In order to address the evolving nature of applications, as part of the service delivery, the partner will update on a regular basis the network devices with NBAR2's application signature protocol packs, which may be applied while the router is in-service. Additionally, NBAR2 metrics are exported using industry standard open export formats NetFlow Version 9 and IP Flow Information Export (IPFIX). By accessing the partner's cloud customer web portal, customer IT administrators gain visibility into applications running in their networks and their network usage, top talkers, top sites. The partner must present evidence of how this requirement is delivered to their customers using their cloud based service delivery platform.

M11.2.5 Optional application network usage alerting	As a service option, the partner may provide the capability to generate an alarm on the occurrence of a flow condition. If provided, the partner must present evidence of how this requirement is delivered to their customers using their cloud based service delivery platform.
M11.2.6 Optional application URL hit count reporting	As another service option, the partner may provide subscribers with the capability to get information based on which websites end users are visiting. Using Cisco NBAR2's capability to analyze the HTTP traffic streams and observe the URLs that are being accessed, the information is exported out via NetFlow using the IPFIX standard. If provided, the customer IT administrator would, by accessing the partner's cloud customer web portal, get an understanding of which websites end users are accessing and application trends over time. This therefore also provides insight into any suspicious sites that may need to be blocked. If provided, the partner must present evidence of how this requirement is delivered to their customers using their cloud based service delivery platform.
M11.2.7 Transactional and media application performance reporting	The solution must provide visibility into transactional application performance and media application performance metrics. By accessing the partner's cloud customer web portal, IT administrators will have visibility on application response time (ART) metrics and media application performance metrics such as latency and jitter. The partner must present evidence of how this requirement is delivered to their customers using their cloud based service delivery platform.
M11.2.8 Optional transactional and media application performance Alerting	As a service option, the partner may offer the capability to generate an alarm on the occurrence of a performance metric condition. If this option is provided, the partner must present evidence of how this requirement is delivered to their customers using their cloud based service delivery platform.
Media Performance Troubleshooting (Optional)	
In addition to Media Application Performance alert using threshold (application a media performance alerting), the partner may optionally offer a media performance troubleshooting service.	
M11.2.9 Optional media performance troubleshooting	The media performance troubleshooting service is based on the Cisco router Mediatrace capability to support their customer in performing fault isolation. If provided, the partner must present evidence of understanding the Mediatrace capability and how this service is delivered to their customers.
Application Quality of Service and Bandwidth Control	
With this service option, customer IT administrators can from the partner customer web portal define application policies for media applications and business critical applications which need guaranteed performance. Policies include performance objective in terms of bandwidth, delay, jitter, and packet loss.	
Requirement	Description
M11.2.10 Granular application control policies	The solution must provide centralized application based policy enforcement. Using the application classification provided by NBAR2's DPI technology within Cisco routers, this service allows customers to reprioritize critical applications or enforce application bandwidth use for individual applications or groups of applications using Cisco's industry-leading Quality of Service (QoS) capabilities. By accessing the partner's cloud customer web portal, IT administrators can centrally define application Quality of Service policies and produce reports that detail application bandwidth usage and performance on a per class of service basis. The central service delivery platform automatically updates the application QoS policies on Cisco CPE routers. The partner must present evidence of how this requirement is delivered to their customers.

Application Optimization and Acceleration (Optional)	
For locations with bandwidth-restricted connectivity, the partner's WAN Optimization service option accelerates response time, improving the delivered of Intelligent WAN. It is built on Cisco WAAS technology which includes a combination of features such as redundancy elimination, TCP acceleration and application acceleration mechanisms. WAN Optimization is applied consistent with the Application Quality of Service and Bandwidth Control policies, ensuring the performance enhancements serve the most critical applications first.	
Requirement	Description
M11.2.11 Transport level flow acceleration	The partner provides transport level flow acceleration using the following Cisco WAAS mechanisms: • Transport flow optimization (TFO): TFO improves application packet flow under unfavorable WAN conditions such as packet loss and small initial windows while helping ensure fairness. • Data redundancy elimination (DRE): DRE is an advanced form of network compression that uses a bidirectional database to store previously seen TCP traffic and replace redundant patterns with very small signatures. DRE can provide up to 100:1 compression depending on the data being examined. • Adaptive persistent session-based compression: This type of compression can provide up to an additional 5:1 compression. The partner must present evidence of how this requirement is delivered to their customers.
M11.2.12 Application acceleration	The partner provides application acceleration using the following Cisco WAAS capabilities: • Protocol acceleration: Application-specific latency is reduced through a variety of application-layer techniques such as read -ahead, operation prediction, connection reuse, message multiplexing, pipelining, and parallelization, resulting in LAN-like performance despite deployment over a WAN. • Application optimizers: Protocol-specific acceleration is available for Microsoft Windows file sharing (Common Internet File System [CIFS]); Microsoft Exchange (Messaging API [MAPI] and MAPI over SSL); encrypted MAPI [EMAPI], HTTP, and HTTPS applications such as Oracle, SAP, and Microsoft SharePoint and Outlook Web Access (OWA); Microsoft Windows print services; UNIX Network File System (NFS); and Citrix ICA. These features improve end user application response times, significantly improving employee productivity. • Content prepositioning: Centralized policy-based file distribution and prepositioning can be used to push files to edge Cisco WAAS devices, accelerating software patch distribution and file access for all users. • Print Application Optimization (Print AO): Increasingly, many customers are consolidating print servers at the head-end or aggregation point. For high-latency WAN branch offices, Cisco Print Application Optimization AO can drastically improve the response time. The partner must present evidence of how this requirement is delivered to their customers.

M11.2.13 Optional caching with Akamai Connect	The partner can offer a significant performance benefit to customers in branches where upgrading WAN bandwidth is prohibitively expensive, or where partner is responding to an RFP for lower priced internet circuits. Typical use cases in retail, financial services, education, oil & gas, and education involve very small WAN links with a high demand for bandwidth. The partner provides this service option using Akamai connect software running on Cisco WAAS product. The software works in any WAN configuration, and it acts as a single sided optimizer to cache HTTP traffic in the absence of a WAAS head-end. Cisco recommends but does not require deploying both technologies, Akamai Connect and symmetrical WAAS optimization, together. The HTTP object caching added by Akamai Connect can provide up to 100% WAN offload after the first pass. Akamai Connect complements Cisco WAAS byte level caching and de-duplication software, and adds the following features and benefits: • Transparent caching: Offload http traffic from the corporate intranet or the Internet by caching http objects near the user. Cache commonly used internet or intranet sites, software updates like Apple IOS updates • Akamai Connected Cache: Cache content from internet sites accelerated by Akamai – up to 30% of all internet traffic – which would not be cacheable with other caching technologies. • Preposition HTTP sites: Utilize off-peak hours to preposition URLs at the customer site. Use cases include employee training, digital signage, curriculum, point of sale catalogs, software updates (roadmap) and websites. • Cache content with dynamic URLs such as YouTube: Offloading of YouTube traffic can be a substantial improvement in WAN congestion. Additionally, customer business use of YouTube has increased substantially and the ability to deliver this content to sites with small WAN pipes in HD very quickly has resonated across many verticals. The partner must present evidence of how this requirement is delivered to their customers.
Service Delivery Platform High Availability (Optional)	
In case high availability is proposed as a service option, the partner must have service delivery platforms deployed in two separate data centers.	
Requirement	Description
M11.2.14 NetFlow / IPFIX duplicated exporter	With this service option, each router is configured to duplicate NetFlow / IPFIX data to a second data collection server.
M11.2.15 Service delivery platform high availability	The partner must explain the architecture and mechanisms used to redirect customer web portal access requests from a primary to a backup data center and real-time data replication between data centers.
Service Security: Customer Premises Equipment (CPE)	
The partner must demonstrate 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.	
Requirement	Description
M11.2.16 The Provider must leverage Secure Connectivity over all underlay transport at the branch and hub locations.	Secure connectivity protects the corporate communications and offloads user traffic directly to the Internet. Strong IPsec encryption, zone-based firewalls, and strict access controls are used to protect the WAN over the public Internet. Routing remote-site users directly to the Internet improves public cloud application performance while reducing traffic over the WAN.
M11.2.17 Disk encryption for data at rest must be deployed for all headend and remote WAVEs, using FIPS 140-2 level 2 compliant 256-bit AES disk encryption with automatic and centralized key management	Disk encryption can be enabled selectively or globally with disk encryption keys managed by the Cisco WAAS Central Manager to ensure that data written to the Cisco WAVE disks is completely unusable should a system be compromised. This helps ensure the compliance with Payment Card Industry (PCI) regulation along with other federal and industry-related compliance initiatives.
M11.2.18 Provider should offer complete stateful firewall inspection and network virus scanning for	The partner should demonstrate how the solution will integrate seamlessly and transparently into network security, visibility, and control functions. It must not break

all direct Internet access traffic	security practices of tunneling through and opening application ports in firewalls.

M11.3 Service-Level Management Requirements (Operate)

Service-Level Agreement (SLA) Components

This section describes the SLAs 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 SLAs may also be presented as evidence of meeting these requirements.

Requirement	Description
M11.3.1 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.
M11.3.2 Mean Time to Restore Service (MTRS)	If there is a disruption to the performance or availability of resources allocated to a customer, the partner must provide an expectation of restoration time. The specifics may vary according to customer agreements. MTRS, also known as Mean Time to Restore (MTTR), measures the total elapsed time from the start of a service outage to the time the service is restored. 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
M11.3.3 Service availability	The uptime for the service described per customer rather than overall network availability. Provide evidence of which service availability elements are covered by the SLA components agreed with customer and how different Operating-Level Agreement (OLA) components are measured and managed.

Customer Web Portal

The following section describes the online capabilities 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 portal from the customer viewpoint, including a real-time view of connectivity and status. Security mechanisms should include password protection or two-factor authentication, used to restrict access to the portal to authorized individuals.

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.

Requirement	Description
M11.3.4 Provide a secure web portal to communicate current status and performance	Provide a secure web portal to present an operational view for multiple audiences; designed to give a view of the network status, including current availability, reliability, and security for managed devices.
M11.3.5 Data retention	Application performance data is stored in the partner's cloud for historic analysis purposes. Data must be retained for period of time established with the customer.

M11.3.6 Summary-level dashboards to communicate key performance criteria	The IWAN dashboard must include: • Real-time status map • Path Control monitoring report • Usage report • Top servers • Top applications • Path Control or PfR policy violations • Top client to server communication • Application bandwidth usage • Application response / transaction time • Connection quality (response time, delay, % retransmissions)

Reporting

The following section describes the reports that are to be made available to the customer via the portal. Example reports must be provided or a view of customer web portal with ability to select reports listed.

Requirement	Description
M11.3.7 Performance analysis reports	Historical performance analysis of the service would typically be available over a number of sample periods (daily, weekly, monthly), and the report would include data to allow the customer to understand how the overall service is performing. Example performance metrics are utilization of Wide-Area Network (WAN) links, quantity of traffic generated by a particular application, and how each application is performing over the WAN.
M11.3.8 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.
M11.3.9 Device Inventory reports	Reports of devices under management for the customer; provide data that is relevant to the customer regarding inventory of equipment used in delivering the service.
M11.3.10 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.
M11.3.11 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.
M11.3.12 Application optimization reports	Provide application oriented details to the customer on: • Top optimized applications being used • General optimization statistics (e.g., WAN bandwidth savings) • Traffic volumes per application and per device

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.

Requirement	Description
M11.3.13 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)

Click here to return to Table of Contents

Cisco Powered Cloud Services

C1 Infrastructure as a Service (IaaS)

Introduced: April 2010
Last updated: May 2017

Overview

Cloud Infrastructure as a Service (IaaS) provides physical IT server resources - computing, memory, and storage - on demand to the Service Providers' customers from the cloud. Rather than purchasing servers, software, data center space, and network equipment, customers are able to consume those resources as a fully managed service. Service Providers often bill such services on a utility basis, based on the actual amount of resources consumed or resources reserved during a defined duration. This section describes the architecture, solution, and service offering requirements that must be met by a partner offering IaaS needed to obtain Cisco Powered accreditation.

The architectural foundation of Cisco Powered Infrastructure as a Service can be implemented using the Virtual Multiservice Data Center (VMDC) solution, with or without Cisco Application Centric Infrastructure (ACI).

VMDC is an end-to-end architecture based on Cisco technology that defines how to create and manage flexible and dynamic pools of virtualized resources which can be shared efficiently and securely among multiple customers. The VMDC architecture consists of infrastructure layers as well as management, orchestration, and assurance components. The orchestration solution creates a service portal that reduces resource provisioning efforts and improves time to deliver services to the subscribing customers. The assurance solution provides monitoring and troubleshooting capabilities that are used for delivering end-to-end Service-Level Agreements (SLAs).

Refer to VMDC Design and Implementation Guidelines.

Multiple releases of VMDC are available for deployment. Any of these releases can be used as the infrastructure basis for an IaaS offering.

Cisco Application Centric Infrastructure technology enables you to integrate virtual and physical workloads in an easy-to-use and highly programmable, multi-hypervisors fabric that is excellent for any multi-service or cloud datacenter. The Cisco ACI fabric consists of discrete components that operate as routers and switches but is provisioned, configured, and managed as a single entity.

Refer to the Intercloud Data Center Application Centric Infrastructure 1.0, Implementation Guide.

Note: The IaaS designation does not inherently give a partner access to purchase or deliver restricted data center products. The partner must meet applicable ATP requirements to purchase and deliver restricted data center products.

C1.1 Prerequisites

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

Requirement	Description
C1.1.1 Meet all CMSP partner requirements in Cisco Channel Program Audit and Policies document	See CMSP partner requirements in Cisco Channel Program Audit and Policies document.
C1.1.2 Submit at least two customer references for the service	CMSP partners are required to have a minimum of two customer references, from existing contractual relationships, for each Cisco Powered service. One customer may serve as reference to multiple designations. A customer with multiple sites does not qualify as a second reference however. The intent is to ensure that the partner has proven and repeatable service practices. The partner must submit at least two customer references for the service at the time of the audit, or must provide evidence of the ability to deliver the service to an end customer. In the event that no customer references are available at the time of the audit, two customer references must be provided upon recertification. Refer to Customer Reference Validation template.

C1.1.3 Provide the following documents unique to the service: • Service-Level Agreement • Marketing Service Description • Technical Service Description • Architectural 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 partner 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 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. The Technical Service Description provides documentation on how capacity is managed on the IaaS system. This may be either an externally or internally published document. 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.
C1.1.4 Employ at least one CCNP Data Center certified individual	The Cisco CCNP Data Center certification is a job-role-focused training and certification program using the following technologies: Cisco Nexus® Switches (1000, 5000, 6000, 7000, and 9000 Series), Cisco UCS® B-Series and C-Series Blade Servers, Cisco UCS Manager, Cisco Data Center Network Manager, Cisco Virtual Network Management Center, and Cisco MDS Series Multilayer Switches. A Cisco CCIE certification, of any technology specialization, supersedes and fulfills the certification requirements for this service. For information, visit: Cisco Certifications.
C1.1.5 Audit representation	If the partner has contracted Cisco Services or a third-party cloud builder to design or build the Infrastructure as a Service platform, providing some or all of the requirements, at the partner's discretion, the third party may participate in the audit and provide evidence on how the requirements they have provided are fulfilled. If the partner has contracted for Cisco Services to operate the Infrastructure as a Service platform, providing some or all of the requirements, at the partner's discretion, Cisco Services may participate in the audit and provide evidence on how the requirements have been fulfilled.

C1.2 Partner System/Solution Requirements (Build)

The following section describes the basic functions of a cloud Infrastructure as a Service solution. Design details for each section are covered in depth in the VMDC documentation.

The partner 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.

Requirements	Description
C1.2.1 Data Center WAN Edge design	Data Center WAN Edge routers provide networking capability for services such as Internet, L3VPN, and L2VPN services. The partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural diagrams.
C1.2.2 Data Center Core design	The Data Center Core design provides a high-speed switching backplane for all flows going in and out of the data center. In smaller designs the core and Aggregation Layers may be collapsed. The partner must provide evidence of how the core design ensures resilient Layer 3 routing with no single points of failure and rapid convergence around link failure. An Application Centric Infrastructure (ACI) fabric may be implemented using a spine and leaf model to address this requirement. The partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural diagrams.

C1.2.3 Aggregation Layer	The Aggregation Layer provides the Layer 3 and Layer 2 boundaries for the data center infrastructure, linking the Layer 2 broadcast domains to the Layer 3 routed domain. It is also often used as the insertion point for network-based services such as firewalling. The partner must explain how they achieve resiliency in the event of link, interface, or switch failure. An Application Centric Infrastructure (ACI) fabric may be implemented using a spine and leaf model to address this requirement. The partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural or topology diagrams.
C1.2.4 Services Layer	Network-based services may be multi-tenant, multi-context capable, and provide per-customer security control. Alternatively, they could be per-customer, discrete, and virtualized. The Services Layer is designed together with the DC Core and Aggregation Layers to provide a high scalability. When multi-tenanted, a resilient framework is also required. The Services Layer can be based on the Cisco VMDC architecture or the Cisco Application Centric Infrastructure. The partner must provide evidence that all of the following functions are delivered on a Cisco platform: • Firewall • Intrusion Prevention System (IPS) • Encryption / VPN And the partner must be able to provide the following functions: • Load balancing The partner must explain how resiliency is achieved in this layer using a document such as an architectural diagram.
C1.2.5 Access Layer	The Access Layer provides connectivity for compute nodes within the data center. Virtualization of the physical servers creates a virtual Access Layer. This allows the function of the logical Layer 2 Access Layer to span multiple physical devices. The partner must explain the architectural approach taken for the Access Layer, types of switches used, and the benefits that this approach provides to the customer. The partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural or topology diagrams.
Virtualization Requirements	
Virtualization is the abstraction of network, compute, and storage resources. This functionality is critical in enabling the dynamic, on-demand characteristics of IT resources delivered from the cloud. It is enabled through the capabilities of Cisco as well as our key technology partners. The Service Provider partner must provide evidence that their services incorporates the key aspects described here and utilizes Cisco technology partner solutions that have been tested as part of the architecture.	
Requirement	Description
C1.2.6 Network virtualization	Segmenting a common network into separate virtual networks, providing logical separation of data-plane and some control-plane functionality in order to achieve customer traffic separation is required. There can be several forms of network virtualization: • Virtual LANs (VLANs): Separate L2 LAN broadcast domains. • VX LAN: Separate L2 LAN broadcast domains. • Virtual Routing Forwarding (VRFs): Separate L3 routing domains. • Virtual Private Networks (VPNs): Virtual point-to-point connection across a shared network. • Virtual appliances: Network services, such as firewalls, load balancers, and routers, can be delivered using physical or virtualized appliances • Secure Domain Routers (SDRs): Creating separate logical routers, isolated from each other in terms of their resources, performance, and availability • Virtual Device Contexts (VDCs): Logical separation of processes that enables the collapsing of multiple logical networks into a single physical infrastructure The partner must explain how virtualization is used within their service design to

	allow segmentation of a device into separate logical entities and to isolate/separate the user/tenant traffic within individual network domains. Additionally, evidence must be provided how this requirement is delivered on a Cisco platform or platforms, such as architectural or topology diagrams.
C1.2.7 Server virtualization	Hardware assisted virtualization is used to simulate a complete hardware environment, or Virtual Machine, in which an unmodified "guest" operating system executes in complete isolation. Multiple virtual compute environments can be activated and executed on a single hardware platform. The partner may offer shared or dedicated resources. Additionally, bare metal servers may be offered in addition to Virtual Machine based services. The partner must provide evidence of how server virtualization is used in their service design. The partner must present evidence of how this requirement is delivered on a Cisco UCS platform, such as architectural diagrams.
C1.2.8 Storage virtualization	Storage virtualization allows data location independence by abstracting the physical location. Storage area networks (SANs) can also be virtualized into zones and Virtual SANs (VSANs) if based on FC or FCoE. VLANs and other Ethernet-based virtualization may be used for iSCSI and NFS-based connectivity. The partner must present evidence of how the virtualization system provides the customer a logical space for data storage and then handles the process of mapping it to the actual physical location, allowing the physical data to be stored without the customer needing to be aware of its actual location. The partner must present evidence of how external storage is connected via a Cisco platform, such as architectural diagrams.
C1.2.9 Unified fabric	A unified fabric consolidates the different types of traffic within the data center onto a single, multi-purpose, high-performance, high-availability network that greatly simplifies the network infrastructure. To achieve this, a unified fabric must be intelligent enough to identify the different types of traffic and handle them appropriately. The Cisco Unified Computing System (Cisco UCS) is the next-generation data center platform that unites network, compute, storage, and virtualization resources in an integrated system. The partner must present evidence of how this requirement is delivered on a Cisco UCS platform, such as architectural or topology diagrams.

Cloud Management Framework Requirements

Cloud management is a complex task that requires the administration of real and virtual resources as well as control of the people and processes that enable the data center to function. The following section defines a framework that includes the key management functions and processes required regardless of the architectural design, including the service orchestration capabilities required to deliver the service. Service orchestration includes a consistent technology architecture, a structured approach to data collection and processing as well as automation wherever possible to minimize human intervention and possible error. This enables a portal-based configuration model in which the customer can pick from a limited number of customized service options.

The purpose of service orchestration is to hide the underlying complexities required to deliver a service by providing an abstracted set of resources described to the end customer in easy to understand language and that has visibility into all of the resources required to set up the requested service such that the customer has clear visibility of whether a requested service creation or amendment can be supported.

Requirement	Description
C1.2.10 Infrastructure services	The management framework must incorporate these key functions to manage the infrastructure: • Virtual server: Memory, CPU, storage, and allocated capacity management • Network Virtualization: VLAN, VXLAN, VRF, SVI, virtual context, virtual address, virtual firewalls, load balancers, VPN, QoS, and/or ACL filtering • Storage: Multi-pathing, storage classification and tiers, storage volume management, and workload mobility

	Recommended functions that may be part of the management framework: • Site Selection: Intra and inter-site workload mobility, global address management (IP and DNS), bursting, failover, disaster recovery management • Virtual Machine Migration: Migration from physical to virtual, and virtual to physical (coordinated provisioning with server migration tools) • APIs: For driving notification, approval billing, chargeback, utilization, IP address management, accounting, SLA management, identity, and general automation The partner must present evidence of how this requirement is delivered on Cisco platform via architectural diagrams or an equivalent.
C1.2.11 Service orchestration	The service orchestration layer must have intelligence to ensure that no configuration actions take place if one of the components within the service being requested through the portal is unavailable (out of logical pools, node down, over capacity thresholds, etc.). The orchestration layer must provide the following functions: • Provide a view of all the services pools available across multiple pods and across multiple data centers • APIs that would provide access to information to other management tools The partner must explain the service orchestration layer that they have put in place and how it can ensure that service requests are only accepted if the underlying resources are available.

Cloud Services Requirements	
This section describes the service capabilities used by the partner to deliver cloud Infrastructure as a Service. The service is built around the Virtual Multiservice Data Center (VMDC) or Cisco Application Centric Infrastructure (ACI). The partner must provide evidence how their service offerings use these capabilities to deliver differentiated services and must allow the customer flexibility to self-provision and manage server capacity based on some or all of the characteristics listed.	
Requirement	Description
C1.2.12 Virtual machine sizing	Service profiles based on different compute, storage, and memory capacity. These can be pre-configured for the customer, such as small, medium, and large VMs or could allow for individual resource size selection. Service profiles can be made available for the customers to select themselves via a web portal as needed.
C1.2.13 Storage	The service profiles can be differentiated based on the types of storage capabilities provided, like RAID protection levels, disk types and speeds, and data protection capabilities.
C1.2.14 Service offer tiers	Service bundles can offer differentiated support where different service profiles can have different layers or tiers of VMs and potentially different levels of redundancy and load balancing.
C1.2.15 Quality of Service (QoS)	The partner must provide evidence of how the features of their solution that ensure Quality of Service can be maintained for the IT resources being managed; examples include: • Classification of traffic • Ability to prioritize resources allocated to different resources • Ability to allocate resources such as allocating bandwidth according to priorities set • Load balancing of traffic across servers
C1.2.16 Service reliability	The partner 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. Service must include all of these features: • Physical layer redundancy within network components • Connectivity via load sharing, dual paths, or similar features • Multi-tenancy, providing multiple customers a secure and isolated environment

C1.3 Customer Requirements

Not applicable

C1.4 Service-Level Management Requirements (Operate)

Service-Level Agreement Components

This section describes the SLAs that the partner must contract for with their customer as part of the service. These are normally available as part of the service description. Existing customer contract that include the relevant SLAs may also be presented as evidence of meeting these requirements.

Requirement	Description
C1.4.1 Mean Time to Notify (MTTN)	If the customer experiences any resource or performance-affecting event the partner must notify the customer of the issue. The specific guarantees 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.
C1.4.2 Mean Time to Restore Service (MTRS)	If there is a disruption to the performance or availability of resources allocated to a customer, the partner must provide an expectation of restoration time. The specifics 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
C1.4.3 Service availability	Provide evidence of which service availability elements are covered by the SLA components agreed with customer and how different Operating-Level Agreement (OLA) components are measured and managed: • Infrastructure SLA • Network SLA (the network operated by the partner that is used to provide connectivity from the Internet or VPN, and the data center itself): A third party could provide network connectivity. Appropriate documentation must be provided to demonstrate how the Underpinning Contracts (UCs) are measured and managed between partner and third party. • Seamless SLA (end-to-end service experience): Where elements of the end-to-end service are provided by a third party, appropriate documentation must be provided to demonstrate how the Underpinning Contracts (UCs) are measured and managed between partner and the third party.

Customer Web Portal

The following section describes the online capabilities 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 portal from the customer viewpoint, including a real-time view of connectivity and status. Security mechanisms should include password protection or two-factor authentication, used to restrict access to the portal to authorized individuals.

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.

Requirement	Description
C1.4.4 Status and performance	Partner must provide an operational view for each customer, designed to give a view of the service status, including current availability and performance.

C1.4.5 Self-provisioning	Depending on business needs/objective, this function can be provided by the partner on behalf of the customer. If the customer is performing this function, the partner must provide the ability for the customer to be able to view and manage their virtual resources via a customer portal including: • Memory • Processing power (number of processors) • Storage • Network The management process of adjusting/changing VM resources must be provided such that the time to enable new servers or to change attributes is measured in hours or days. If the partner is managing the creation/changes to server resources, the partner must provide evidence of the process used to do so. The partner must explain how these requests are measured, tracked, and managed.
C1.4.6 Service overview	The partner's customer portal typically provides the following capabilities: • Customer contacts allow to communicate with the partner regarding service changes/ordering, accounting and billing, managing the list of authorized contacts • Assignment of network resources and security options such as IP pools, VLANs, and security policies • Assignment of Virtual Machines with standard and customized builds (OS, IP addressing, CPU, memory, cloning) • Assignment of storage service class, storage allocation, and utilization • Accounting and SLA management The customer portal could either be a partner owned/branded or a third-party white-labeled solution. If the partner does not provide a customer portal, the partner must explain as to how above capabilities are provided to customers.

External Reporting

The following section describes the reports that are to be made available to the customer via the customer portal. Example reports must be provided or a view of customer web portal with ability to select reports listed.

If 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 portal is considered an industry standard and allows partners to differentiate themselves from other providers via a captivating user experience.

Requirement	Description
C1.4.7 Performance analysis reports	Historical performance analysis of the service would typically be available over a number of sample periods (daily, weekly, monthly), and the report would include data to allow the customer to understand how the overall service is performing.
C1.4.8 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.
C1.4.9 Resource inventory reports	Reports of resources under management for the customer provide data that is relevant to the customer for managing their IaaS subscription and understanding what resources are available for their use and have been used historically.
C1.4.10 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.

Internal Performance Reporting	
The following section describes reports that are to be internally created and reviewed. May be proven by providing an example of reports or demonstration of reporting tool with ability to select reports listed.	
Requirement	Description
C1.4.11 Customer-related reports/internal performance metrics	Reports on metrics used to measure trends of service performance, including: • SLA violations • Aggregate resource utilization Performance against internal targets (typically more stringent than those agreed with the customer).
C1.4.12 Capacity management	Report on performance and capacity of the IaaS environment over the reporting period. This report speaks to the ability of the environment to sustain normal on-boarding of new customers. Metrics shall include: • I/O consumption and headroom • Memory consumption and headroom • CPU consumption and headroom • Storage consumption and headroom • Bandwidth consumption and headroom at relevant points in the environment • Number of additional virtual machines and storage that can be provisioned with current capacity or other capacity planning metrics at the partner's discretion

Click here to return to Table of Contents

C2 UC as a Service Based on HCS (HCS)

Introduced: September 2011
Last updated: November 2017

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 partner the opportunity to create subscription-based "as a service" offers utilizing hosted and managed models.

The partner 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 in two different hardware deployment models:

1. Productized Architectural Solution - that contains specific hardware and software designs, components and software versioning
2. Cisco Powered, CMSP compliant IaaS data center with UC on UCS requirements and restrictions.

Refer to Cisco Hosted Collaboration Solution for more information.

C2.1 Prerequisites

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

Requirement	Description
C2.1.1 Meet all CMSP partner requirements in Cisco Channel Program Audit and Policies document	See CMSP partner requirements in Cisco Channel Program Audit and Policies document.
C2.1.2 Have 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 partner must present evidence that the A2Q review was completed successfully with no open issues, within the prior three months of the audit. Information on the A2Q process can be found here: HCS A2Q Process. If partner has a valid approved phase 3 A2Q within the last three years, they are not required to submit an A2Q for CMSP annual renewal.
C2.1.3 Submit at least two customer references for the service	CMSP partners are required to have a minimum of two customer references (existing contractual relationships) for each Cisco Powered service to validate service offering requirements. One customer may serve as reference to multiple designations. A customer with multiple sites does not qualify as a second reference. The intent is to ensure that the partner has proven and repeatable service practices. The partner must submit at least two customer references for the service at the time of the audit, or must present evidence to the ability to deliver the service to an end customer. In the event that no customer references are available at the time of the audit, two customer references must be provided upon recertification. Refer to Customer Reference Validation template.
C2.1.4 Have a commercial agreement in place with Cisco	HCS requires a contractual commitment between partner and Cisco that outlines the licensing agreements and any volume commitment. The partner must provide evidence of this agreement.

C2.1.5 Employ at least one CCNP Collaboration certified individual and at least one CCNP Data Center certified individual on staff where the HCS service originates	As part of the partner's Collaboration Architecture Specialization, the CCNP validates the ability to plan, implement, verify, and troubleshoot local and wide-area enterprise networks. Additionally, they have the skills and expertise to work collaboratively with specialists on advanced security, voice, and video solutions. The Cisco CCNP Data Center certification is a job-role-focused training and certification program using the following technologies: Cisco Nexus® Switches (1000, 5000, 6000, 7000, and 9000 Series), Cisco UCS® B-Series and C-Series Blade Servers, Cisco UCS Manager, Cisco Data Center Network Manager, Cisco Virtual Network Management Center, and Cisco MDS Series Multilayer Switches. 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.
C2.1.6 Maintain Master Unified Communications, Master Collaboration, or Advanced Collaboration Architecture Specialization in country where HCS service originates	The partner must maintain one of the following: Master Unified Communications Specialization, Master Collaboration Specialization, or Advanced Collaboration Architecture Specialization in the country where the UCaaS service originates.
C2.1.7 Audit representation	If the partner has contracted Cisco Services or a third-party cloud builder to design or build an UCaaS platform, providing some or all of the requirements, at the partner's discretion, the third party may participate in the audit and provide evidence on how the requirements they have provided are fulfilled. If the partner has contracted for Cisco Services to operate the UC as a Service Based on HCS platform, providing some or all of the requirements, at the partner's discretion, Cisco Services may participate in the audit and provide evidence on how the requirements have been fulfilled.

C2.2 Partner System/Solution Requirements (Build)

Service Capabilities

The HCS Data Center (DC) is built around the Cisco Unified Compute System (Cisco UCS), Nexus 1000V virtual switches, Multilayer Director Switch (MDS) storage switches, SAN and NAS storage arrays, Nexus 7000 and Nexus 5000 Aggregation (switching and routing), and Nexus 5000 Access (switching) layers connecting into Adaptive Security Appliance (ASA) and Aggregation Services Routers (ASR) WAN routers. Partners are allowed to leverage Cisco Application Centric Infrastructure (ACI) if they meet the HCS DC Flexibility Guidelines.

The following section describes the key requirements needed within the data center infrastructure to conform to HCS requirements. The partner must explain the infrastructure that has been deployed to support each function.

Requirement	Description
C2.2.0 Data Center Aggregation Layer	The DC Aggregation Layer is characterized by a high degree of high-bandwidth port density capacity, and thus, optimized for traffic distribution and link fan-out capabilities to Access Layer switches. Functionally, the nodes in the Aggregation Layer typically serve as the L2/L3 boundary. Multiple Aggregation Layers can connect to the WAN router (Data Center Perimeter), providing for increased density and east-west traffic within the DC. The partner must provide evidence that the data center Aggregation Layer is based on Cisco devices. If deployed utilizing the Productized Architectural Solution, must meet the compatible Cisco Nexus hardware and the minimum NX-OS version that have been validated by Cisco as part of HCS. Refer to Cisco HCS Release Information for more information.

C2.2.1 Data Center Interconnect	Data Center Interconnect (DCI) transparently extends LAN and SAN connectivity and provide accelerated, highly secure data replication, server clustering, and workload mobility between geographically dispersed data centers. ***This is an optional deployment configuration that partners may choose to implement.*** If implemented based upon EoMPLS or EoVPLS, the partner must provide evidence that the DCI is based on Cisco Aggregation Services Routers (ASR) WAN router with the minimum IOS XR version, that has been validated by Cisco as part of HCS. LAN extension functionality is supported by either: • Point-to-point interconnection using Ethernet over Multiprotocol Label Switching (EoMPLS) natively (over an optical or MPLS enabled core) and over a Layer 3 IP core (EoMPLSoGRE) • Point-to-multipoint interconnections using virtual private LAN services (VPLS) natively (over an optical or MPLS enabled core) If implemented based upon OTV (Overlay Transport Virtualization), the partner must provide evidence that the DCI is based on Cisco Nexus 7000 devices. LAN extension functionality is supported by the following: Control Plane Considerations: • Multicast Enabled Transport Infrastructure • Unicast-Only Transport Infrastructure (Adjacency-Server Mode) • Data Plane: Unicast Traffic • Data Plane: Multicast Traffic • Multicast Enabled Transport Infrastructure • Unicast-Only Transport Infrastructure (Adjacency-Server Mode) • Data Plane: Broadcast Traffic Refer to Cisco HCS Release Information for more information.
C2.2.2 Data Center Aggregation Services Layer	The Aggregation Services Layer comprises network and security services such as firewalls, server load balancers, SSL offload, intrusion prevention, network analysis, etc. A distinct difference arises between the conventional DC Services Layer and cloud DC Services Layer in that the solution set for the latter must support application of L4 - L7 services at a per-tenant level, through logical abstraction of the physical resources. The partner must provide evidence that the minimum data center aggregation services are based on the following Cisco devices. If deployed utilizing the Productized Architectural Solution, must meet the minimum IOS XR/ASA OS version that have been validated by Cisco as part of HCS: • Cisco ASA 5500-X Series Next-Generation Firewall, • Cisco ASA 5500-X Series IPsec and SSL VPN Remote Access, or • Cisco ASR 1000 Series IPsec and SSL VPN Remote Access
C2.2.3 Data Center Access Layer	The Access Layer of the network provides connectivity for server farm end nodes residing in the data center and is primarily deployed in Layer 2 mode. Design of the Access Layer is tightly coupled to decisions on server density, form factor, and server virtualization that can result in higher interface count requirements. Traditional data center Access Layer designs are strongly influenced by the need to locate switches in a way that most conveniently provides cabling connectivity for racks full of server resources. The most commonly used traditional approaches for data center server farm connectivity are end-of-row, top-of-rack, and integrated switching. Each design approach has pros and cons, and many enterprises use multiple access models in the same data center facility as dictated by server hardware and application requirements. The partner must provide evidence that the data center Access Layer is based on Cisco devices. If deployed utilizing the Productized Architectural Solution, must meet the compatible Cisco Nexus hardware and minimum NX-OS version that have been

	validated by Cisco as part of HCS. Refer to Cisco HCS Release Information for more information.
C2.2.4 Virtual Access Layer	The Virtual Access Layer is a logical layer inside the server fabric providing connectivity with virtualized server hardware, hypervisor and VMs with additional functionality of policy management (separation, ACL, etc.), mobility, and service assurance capability. Cisco Nexus 1000V series switches provide a comprehensive and extensible architectural platform for virtual machine (VM) and cloud networking. The switches are designed to accelerate server virtualization and multitenant cloud deployments in a secure and operationally transparent manner while providing policy-based virtual machine connectivity, mobile VM security, enhanced QoS, and network policy. The partner must provide evidence that VMware vSphere Enterprise Plus as well as the Cisco Nexus 1000v switch is configured. Cisco Nexus 1000V installation can be verified using the Cisco Nexus 1000v Installer Application. A vNetwork Standard Switch is not a supported configuration because administrators must manually maintain consistency of the vSwitch configuration across all ESXi hosts to ensure that they can perform operations such as vMotion. The only exception to this is if the partner has deployed all UCS C-series Rack Mount servers without connection to the Cisco UCS 6x00 Series Fabric Interconnects. If the partner uses an alternative distributed virtual software switch, then the partner must provide evidence of the ability to manage the virtual switch across all VMs in a homogeneous manner and control traffic congestion in the fabric interconnect environment.
C2.2.5 Unified Computing System	The Cisco Unified Computing System (Cisco UCS) is a next-generation data center platform that unites computing, networking, storage access, and virtualization resources. The system integrates a low-latency, lossless 10 Gigabit Ethernet unified network fabric with enterprise-class, x86-architecture servers. The system is an integrated, scalable, multi-chassis platform in which all resources participate in a unified management domain. The Cisco UCS 6x00 Series Fabric Interconnects provides the management and communication backbone for the Cisco UCS B-Series Blade Servers and 5100 Series Blade Server Chassis. All chassis, and therefore all blades, attached to the Cisco UCS 6x00 Series Fabric Interconnects become part of a single, highly available management domain. In addition, by supporting unified fabric, the Cisco UCS 6x00 Series provides both the LAN and SAN connectivity for all blades within its domain and integrates with Cisco UCS Central Software (optional) and Cisco UCS Director (also optional). The partner must provide evidence that the data center design is based on these products or later products and that the version of Cisco UCS Manager being utilized is in compliance with the version of VMware vSphere (vCenter and ESXi) along with UC application compatibility and the version of the Cisco Nexus 1000v that is also being utilized. References: • Cisco UCS Interoperability Information • Cisco HCS Release Information • Cisco Nexus 1000V Switch for VMware vSphere • Unified Communications VMware Requirements • Unified Communications Virtualization Supported Applications • UCSM Managed UCS Server Compatibility • VMware Compatibility Guide
C2.2.6 UCS Servers	Cisco HCS exclusively uses Cisco Unified Computing System (Cisco UCS) B-series and C-series servers and within the following support models: UC on UCS Tested Reference Configuration (TRC) - TRCs are required for all Cisco

	UCS C-Series Rack-Mount Standalone Server deployments with UC applications. Some TRCs are available as packaged collaboration solutions like Cisco Business Edition 6000 or Cisco Business Edition 7000. Cisco UCS B-series TRCs are supported but not mandatory. UC on UCS Specs-based - Any Cisco UCS B-series that satisfies the UC Virtualization Supported Hardware specifications. Specs-based Cisco UCS C-Series Rack-Mount Standalone Servers are not supported within HCS. Third-party Servers are not supported within HCS. The partner must provide evidence that the data center design is based on these products or later products and must meet the UC application version interoperability requirements for the following: • Must be supported by Cisco UCS Manager, Drivers, and Server firmware - reference: Cisco Unified Computing System Technical References • Must be supported by Cisco Nexus 1000v - reference: Cisco Nexus 1000V Switch for VMware vSphere • Must be supported by VMware (vCenter and ESXi) - reference: VMware Compatibility Guide • http://www.vmware.com/resources/compatibility/search.php References: • Cisco UCS Interoperability Information • Cisco HCS Release Information • Cisco Nexus 1000V Switch for VMware vSphere • Unified Communications VMware Requirements • Unified Communications Virtualization Supported Applications • UCSM Managed UCS Server Compatibility • VMware Compatibility Guide
C2.2.7 Storage Array Switch interoperability	The partner must provide evidence that the Storage Array Switch is compliant with the version of Cisco UCS Manager being utilized as well as the version of VMware vSphere (vCenter and ESXi) that is also being utilized. References: • Cisco UCS Interoperability Information • Cisco HCS Release Information
C2.2.8 Storage Array	The partner must provide evidence that the Storage Array is compliant with the version of Cisco UCS Manager being utilized as well as the version of VMware vSphere (vCenter and ESXi) that is also being utilized. References: • Cisco UCS Interoperability Information • Cisco HCS Release Information • Cisco UC Virtualization Storage System Design Requirement A VMware Virtual SAN (VSAN), software-defined shared storage using the local DAS within the C-Series server for virtual machines, is not a supported deployment model and should not be implemented.
Partner VoIP Infrastructure	
The following section describes the key requirements needed within the Voice Over IP (VoIP) infrastructure to conform to HCS requirements. The partner 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 partner must explain how the necessary function is achieved and show that Cisco and partner have agreements in place that indicate the partner has taken responsibility for the performance of the particular aspect of the solution.	

C2.2.9 IP Demarcation Layer	The partner must have an IP Demarcation Layer. Validated options include Cisco Unified Border Element (Enterprise Edition) to perform as the Session Border Controller (SBC) in HCS. The 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. Under HCS DC Flexibility guide, partners can deploy a 3rd party Session Border Controller as well. References: Cisco HCS Flexibility Guide
C2.2.10 Signaling Aggregation Layer	The Aggregation Layer provides connection to the partner 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 (CUBE Session Management Edition [SME]), 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 partner must explain the architectural approach they have adopted for the Aggregation Layer and which products have been deployed to provide this function.
C2.2.11 Security	The service design must include a firewall to separate the customer premises-based components and UC applications instances in the data center. The firewall must be deployed in a redundant mode from the partner's cloud. Additionally, there must be a firewall between the UC applications and management domain with 1:1 NAT functionality. This function must be met with a Cisco platform.
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 partner 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.	
C2.2.12 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 partner must explain the architectural approach adopted for the service management layer and which products have been deployed to provide this function.

C2.2.13 Fulfillment Integration layer	The partner must use Cisco Hosted Collaboration Mediation - Fulfillment (HCM-F). HCM-F provides solution-level utilities such as Platform Manager (upgrades), Service Inventory (billing mediation), License Manager, and Infrastructure Platform Automation (VM provisioning automation).
C2.2.14 Unified Communications application monitoring	For versions prior to 10.0: The partner must use Cisco Unified Operations Manager, which monitors UC applications and devices for fault management. For version 10.0 and later: The partner may use Cisco Prime Collaboration for Assurance, which monitors UC applications and devices for fault management.
C2.2.15 Call quality and performance monitoring	For versions prior to 10.0: The partner must use Cisco Unified Service Monitor, which provides and evaluates quality-of-voice metrics associated with active calls in a monitored network. For version 10.0 and later: The partner may use Cisco Prime Collaboration for Assurance, which provides and evaluates quality-of-voice metrics and performance associated with active calls in a monitored network.
C2.2.16 Unified Communications provisioning	Cisco UC Domain Manager (CUCDM) provisions and activates UC services for subscribers. For HCS Release 9.2 or later, an alternate 3rd party Domain Manager may be deployed, provided the partner presents evidence of ability to provision and activate UC subscribers with the alternate Domain Manager via the API Gateway of HCM-F.
C2.2.17 Data Center infrastructure monitoring	The monitoring of the status of the data center infrastructure to maintain service quality, the following components are mandatory: Cisco UCS Manager VMware vCenter The following components are optional but recommended: • Data Center Network Manager (DCNM) • Adaptive Security Device Manager (ASDM) • Cisco Virtual Network Management Center (VNMC) • Cisco Prime Network Services Controller (formally VNMC) The partner must provide evidence that they monitor network infrastructure to assure service quality. The partner must also show evidence of how Cisco UCS Manager is being utilized for monitoring of the UCS infrastructure as well as how VMware vSphere (vCenter and ESXi) monitoring is being accomplished. *Note: If the data center compute platform is based on the Cisco UCS C-Series rack-mount server, there are no fabric extenders and interconnects requirements therefore Cisco UCS Manager is not required*. *In this case, the Cisco Integrated Management Controller (CIMC) is the management service for the C-Series servers. CIMC runs within each server. The partner can use a web-based GUI or SSH-based CLI to access, configure, administer, and monitor the server in regards to faults, alarms, and server status.*

Collaboration Service Features	
The following section describes the collaboration software features required to be offered on customer request. The partner 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.	
C2.2.18 IP communications service core functions	The foundation of the service is IP-PBX call control functionality for VoIP and video telephony, using Cisco Unified Communications Manager 9.1 or later. The partner 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
C2.2.19 Voice and integrated messaging	The partner must present evidence of support for the key features of Cisco Unity Connection 9.1 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 partner 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.
C2.2.20 Presence and Instant Messaging	The partner must provide evidence that Presence and Instant Messaging (IM) capabilities are available to customers. The partner 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 partner 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)

C2.2.21 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 partner 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
C2.2.22 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 partner 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
C2.2.23 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 partner 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
C2.2.24 Internet access to services	If a partner 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 partner must deploy at least one pair of Cisco Expressway (C and E) per customer and add more Expressway clusters to meet the scaling needs. • CUBE-ENT: The Cisco Unified Border Element enables remote access over the Internet for IP Phones like 79xx, 78xx, 89xx and 99xx series. The partner can deploy CUBE-ENT at customer premises and/or deploy at the data center.

C2.3 Customer Requirements

Customer VoIP Infrastructure

Each customer is supported with the customer's unique instance of the required applications.

The partner 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
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 partner 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 partner's SIP network. The partner 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 partner 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)

Service-Level Agreement (SLA) Components

This section describes the SLAs 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 SLAs may also be presented as evidence of meeting these requirements.

Requirement	Description
C2.4.1 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.
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 partner 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 partner, or the customers may be given access to do this themselves. If the customer carries out these changes, the partner must present evidence of how access is provided. If changes are the responsibility of the partner, 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 partner or of the customer. If the customer carries out these changes, the partner must provide evidence of how access is provided. If changes are the responsibility of the partner, 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 partner must also be able to demonstrate that event logs can be stored and made accessible.

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.

Requirement	Description
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 partner 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.

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.

Requirement	Description
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.

Requirement	Description
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

Click here to return to Table of Contents

C3 Contact Center as a Service Based on HCS (HCS_CC)

Introduced: October 2010
Last updated: November 2017

Overview

Cisco Powered Contact Center as a Service Based on HCS (HCS_CC) is designed for companies with up to 12,000 concurrent knowledge workers or agents per Cisco Contact Center instance. This solution delivers the advanced capabilities of Cisco Unified Contact Center Enterprise and Cisco Customer Voice Portal with all the benefits of cloud computing.

Note: Contact Center as a Service Based on HCS is not supported with a Hosted Collaboration Solution (Micro Node) deployment.

C3.1 Prerequisites

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

Requirement	Description
C3.1.1 Meet all CMSP partner requirements in Cisco Channel Program Audit and Policies document	See CMSP partner requirements in Cisco Channel Program Audit and Policies document.
C3.1.2 Submit at least two customer references for the service	CMSP partners are required to have a minimum of two customer references, from existing contractual relationships, for each Cisco Powered service. One customer may serve as reference to multiple designations. A customer with multiple sites does not qualify as a second reference however. The intent is to ensure that the partner has proven and repeatable service practices. The partner must submit at least two customer references for the service at the time of the audit, or must provide evidence of the ability to deliver the service to an end customer. In the event that no customer references are available at the time of the audit, two customer references must be provided upon recertification. Refer to Customer Reference Validation template.
C3.1.3 Meet UC as a Service Based on HCS (HCS) requirements	See UC as a Service Based on HCS (Cisco Powered Cloud Services, section C2) for requirements. UC as a Service Based on HCS and Contact Center as a Service Based on HCS may be audited at the same time.
C3.1.4 Have a commercial agreement in place with Cisco	Contact Center as a Service Based on HCS requires a contractual commitment between the partner and Cisco that outlines the Contact Center as a Service Based on HCS licensing agreements. The partner must provide evidence of this agreement.
C3.1.5 Have deployment that adheres to one of the four reference architectures	Reference architectures can be found in the Install and Upgrade Guides document. Any deviation from the reference architecture models must be disclosed at the time of audit or renewal.
C3.1.6 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. 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.
C3.1.7 Employ at least one UCCE ATP or Trained Personnel on staff	Unified Contact Center Enterprise 9.0 and later requires that the partner must: Hold the UCCE ATP certification. Or have personnel that have completed the UCCE Deployment Engineer/TAC Support (DE/TS) and Customer Voice Portal Developer training. See Authorized Technology Partner. for more information.

C3.1.8 Audit representation	If the partner has contracted Cisco Services or a third-party cloud builder to design or build a Contact Center as a Service Based on HCS platform, providing some or all of the requirements, at the partner's discretion, the third party may participate in the audit and provide evidence on how the requirements they have provided are fulfilled. If the partner has contracted for Cisco Services to operate the Contact Center as a Service Based on HCS platform, providing some or all of the requirements, at the partner's discretion, Cisco Services may participate in the audit and provide evidence on how the requirements have been fulfilled.

C3.2 Partner System/Solution Requirements (Build)

Service Capabilities

The following section describes the basic functions of a Contact Center as a Service Based on HCS (HCS for CC) offering.

The partner must provide evidence of the Contact Center as a Service Based on HCS capability 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.

Requirement	Description
C3.2.1 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.
C3.2.2 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 partner must demonstrate of how Customer Voice Portal is supported.
C3.2.3 Deployment type	Unified Contact Center Administration deployment type selection, must be one of the following: • HCS-CC 500 Agents • HCS-CC 1000 Agents • HCS-CC 4000 Agents (includes Small Contact Center) • HCS-CC 12000 Agents Partner must provide evidence that all deployment rules and capacity info have passed validation (using the Unified CC Administration deployment page).
C3.2.4 Agent IP phone support	Partner 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.
C3.2.5 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 partner must provide evidence of how ACD is supported.
C3.2.6 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 partner must provide evidence of how agents are supported, such as architectural or topology diagrams.
C3.2.7 Remote Silent Monitoring	Remote Silent Monitoring enables a caller to dial into and listen to an agent conversation. The partner must provide evidence of how Remote Silent Monitoring is supported, if included as part of the partner's offering.

C3.2.8 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 partner must provide evidence of how Intelligent Call Routing is supported.
C3.2.9 In-bound call routing	For SIP Trunks are being aggregated into a Session Border Controller (SBC). The partner 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 partner must deploy either Cisco TDM-IP Gateway or CUBE-E for every all customer inbound calls.
C3.2.10 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. The partner must demonstrate the use Cisco Unified Customer Voice Portal (CVP).
C3.2.11 Multi-channel support	The partner must show the support for Email Integration Manager and Web Integration Manager (EIM/WIM), The partner must provide evidence of support for these applications, if included as part of the partners offering.
C3.2.12 Customer Relationship Manager integration	If Customer Relationship Manager (CRM) is offered, CRM integration is only supported through the Cisco CTI server. The partner must provide evidence of CRM integration if offered.
C3.2.13 Outbound dialing	The partner 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 partner can order additional transferable outbound dialer licenses. The partner must provide evidence of support for outbound dialing, if included as part of the partner's offering.
C3.2.14 Cisco MediaSense	Cisco MediaSense allows partners to efficiently gather and cost-effectively analyze business intelligence from the contact center's thousands of customer conversations each day. For versions 10.0 and later. Cisco MediaSense provides network-based multimedia capture, streaming, and recording. The partner must provide evidence of MediaSense support, if included as part of the partner's offering.

Infrastructure

The following section describes the requirements for a service which 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.

Requirement	Description
C3.2.15 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.

C3.2.16 Quality of service (QoS) assurance for remote operators	The partner 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.
C3.2.17 Antimalware protection for servers	There are many servers that may be used in support of the delivery of this managed service. The partner must provide evidence that processes are 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 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.

Requirement	Description
C3.2.18 Reporting platform	Partner 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 partner can deploy one of the following: • Cisco Unified Intelligence Center • Exony VIM • Third party reporting solution The partner must provide evidence of the reporting solution used.
C3.2.19 Contact Center Application monitoring	For version 10.0 and later: the partner must use Cisco Prime Collaboration for Assurance, which monitors Contact Center applications and devices for fault management.
C3.2.20 Contact Center Call Quality and Performance monitoring	For version 10.0 and later: the partner must use Cisco Prime Collaboration for Assurance, which provides and evaluates quality of the Contact Center service and performance associated with agents in a monitored network.
C3.2.21 Contact Center Domain Manager	Contact Center Domain Manager is an extensible web portal that allows for multi-level administration of the contact center. The partner must support Contact Center Domain Manager.
C3.2.22 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.

C3.3 Customer Requirements

The partner 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.

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

C3.4 Service-Level Management Requirements

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.

Requirement	Description
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 partner must offer an SLA that ensures proper call handling.
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.	
Requirement	Description
C3.4.3 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

Click here to return to Table of Contents

C4 Video and TelePresence as a Service (TPaaS)

Introduced: September 2011
Last updated: November 2016

Overview

Cisco Powered Video and TelePresence as a Service is a video conferencing offer based on the Cisco Meeting Server (CMS) delivered from the partner's cloud to end users. Video and TelePresence as a Service enables customers to use the cloud for multipoint calling and interoperability capabilities. Video and TelePresence as a Service is designed to support pervasive and reservation-less services.

Note: The Video and TelePresence as a Service designation does not inherently give a partner access to purchase or deliver restricted Cisco TelePresence products. The partner must meet applicable ATP requirements to purchase and deliver restricted Cisco TelePresence products.

C4.1 Prerequisites

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

Requirement	Description
C4.1.1 Meet all CMSP Master or Advanced partner requirements in Cisco Channel Program Audit and Policies document	See the CMSP partner requirements in Cisco Channel Program Audit and Policies document.
C4.1.2 Submit at least two customer references for the service	CMSP partners are required to have a minimum of two customer references (existing contractual relationships) for each Cisco Powered service to validate service offering requirements. One customer may serve as reference to multiple designations. A customer with multiple sites does not qualify as a second reference. The intent is to ensure that the partner has proven and repeatable service practices. The partner must submit at least two customer references for the service at the time of the audit, or must demonstrate the ability to deliver the service to an end customer. In the event that no customer references are available at the time of the audit, two customer references must be provided upon recertification. Refer to Customer Reference Validation template.
C4.1.3 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. 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.
C4.1.4 Manage all Cisco TelePresence and video components related to the delivery of the Video and TelePresence as a Service	The partner must support the management functions for all equipment delivered as part of the Video and TelePresence as a Service offering. This includes but is not limited to moves, adds, changes, and deletions (MACDs), configuration changes, performance monitoring, issue troubleshooting, and corrective actions to resolve issues. All Cisco TelePresence room components can be managed, for example, via Simple Network Management Protocol (SNMP), web interfaces, and Command Line Interface (CLI).
C4.1.5 Actively use and have the ability to demonstrate the Video and Telepresence as a Service solution internally within the partner	Leverage first-hand experience to provide an understanding of the solution's benefits and the technical implications of adding this service to an integrated IP network. Based on this, the partner must use TelePresence internal to their organization. This can be based on any of the Cisco TelePresence Video products in the portfolio. The partner must be able to demonstrate the Video and TelePresence as a Service offering to a customer on the partner's network.

C4.1.6 When applicable, provide evidence of the ability to deliver immersive Cisco Telepresence traffic over a Quality of Service (QoS) network that meets the stringent requirements.	To ensure a quality end-to-end experience, the immersive Cisco TelePresence sites must be connected via a QoS-enabled network service. The partner must have contractual arrangements in place with providers of this service if they do not own the WAN infrastructure used to deliver the service. The QoS-enabled network must be configured to ensure the following targets for Cisco TelePresence traffic are met: • Latency: < 150ms • Video Jitter: < 50ms • Loss: < 0.05% The partner must provide evidence of end-to-end QoS configuration or contractual arrangements and support that partner delivered WAN services are configured for QoS related to TPaaS delivery.
C4.1.7 Meet third-party contracting relationship requirements (if applicable)	Partners who have achieved two or more Cisco Powered managed or cloud services using in-house capabilities may subcontract portions of their Video and TelePresence as a Service solution so long as the subcontracted party is Cisco Remote Managed Service (RMS) or another CMSP partner or Cisco partner with a Cisco TelePresence Video ATP.
C4.1.8 Employ at least one trained/certified individual on staff	The partner must have an individual(s) on staff that has taken and passed the following Cisco Certification exams: • Collab150 – Cisco Meeting App Foundation • Collab350 – Cisco Meeting Server Advanced
C4.1.9 Audit representation	If the partner contracted Cisco Services or a third-party cloud builder to design or build a Video and TelePresence as a Service platform (TPaaS), providing some or all of the Video and TelePresence as a Service audit requirement. At the partner's discretion, Cisco Services or the cloud builder may participate in the audit and provide evidence on how the requirements have been fulfilled. If the partner contracted with Cisco Service to operate the Video and TelePresence as a Service, providing some or all of the Video and TelePresence as a Service audit requirement. At the partner's discretion, Cisco Services may participate in the audit and provide evidence on how the requirements have been fulfilled.

C4.2 Partner System/Solution Requirements

Service Capabilities

The following section describes the basic functions of the Video and TelePresence as a Service solution based on the Cisco Meeting Server (CMS).

The partner must be able to provide evidence of the service capabilities, and explain the key benefits of the service to enhance the way a customer can run their business.

Requirement	Description
C4.2.1 Support multipoint video service in a multi-tenant cloud-based or dedicated cloud-based configuration	Multipoint capabilities must be delivered using CMS on Cisco supported hardware to support HD video calling. The service must include the following features: • HD videoconferencing • Reservation-less (always available, always on) • PIN security • Active presence • Audio only dial in • Content sharing
C4.2.2 Internet access to the Video and TelePresence as a Service	Cisco Firewall Traversal is supported using an appropriate Cisco Edge solution (E.g., VCS, Expressway). This is to allow users to connect to the service via the Internet.
C4.2.3 Interoperability/integration for video calling	CMS supports interoperability/integration for video calling in a dedicated or multi-tenant cloud-based configuration. The following endpoint types must be supported by the service: • Cisco SIP-based endpoints • All standards-based endpoints

C4.2.4 Security best practices implemented for the overall video bridging service	The partner must provide evidence that a security design for the service that ensures at least: • Signaling encryption • Media encryption • Access to management tools is restricted to authorized personnel The partner must describe their security procedures for the overall service, explain how it is designed to ensure the integrity of the customer environment, and justify the benefits of the Cisco solution to the customer.
C4.2.5 Service provisioning	The service must provide the following functions: • Creation and assignment of virtual meeting rooms • Creation and assignment of named users
C4.2.6 Subscription based licensing	This solution will be purchased from Cisco in an as-a-service based subscription model only. Both the Shared VMR and the Named User licenses have to be purchased from Cisco for every equivalent customer license sold.

Design Considerations

The following section describes the two methods in which the Video and TelePresence as a Service is delivered. The partner can choose to deliver shared VMR or Named Users or both the methods described below.

Requirement	Description
C4.2.7 Shared Virtual Meeting Room (VMR)	A Shared VMR is defined as a cloud-based shared conference bridge. The Shared VMR is intended as a shared resource to be leveraged by multiple employees within the customer and is intended to complement the Named Users. The Shared VMR must be reservation-less, with a PIN.
C4.2.8 Named User (enterprise wide)	Named Users are defined as cloud-based conference participants with at least one personal VMR. It is anticipated that most if not all video-enabled employees in a given enterprise would attain a named user license.

C4.3 Service-Level Management Requirements

Service-Level Agreement (SLA) Components

This section describes the SLAs 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 SLAs may also be presented as evidence of meeting these requirements. C4.3.1 through C4.3.11 are optional.

Requirement	Description
C4.3.1 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.
C4.3.2 Mean Time to Restore Service (MTRS)	If there is a disruption to the performance or availability of resources allocated to a customer, the partner must provide an expectation of restoration time. May vary according to customer agreements. MTRS, also known as Mean Time to Restore (MTTR), measures the total elapsed time from the start of a service outage to the time the service is restored. 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

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. These requirements may be proven by a demonstration of portal from customer viewpoint, including a real-time view of connectivity and status. Security mechanisms, such as password protection, may be used to restrict access to the online 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.

Requirement	Description
C4.3.5 Communicate 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: • Real-time status map • Monitoring report • Usage report

External Reporting

The following section describes the reports that are to be made available to the customer via the customer web portal. Report documents or a demonstration of the reporting within the web portal must be provided.

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 the partners to differentiate themselves from other partners.

Requirement	Description
C4.3.6 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.
C4.3.7 Service Availability reports	Summary views of reports on the overall service availability, e.g., by site or equipment.
C4.3.8 Device Inventory reports	The partner must provide reports of devices under management for the customer, supplying data regarding inventory of equipment or WAN services used in delivering the service.
C4.3.9 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.
C4.3.10 Exception reports	The partner must provide the ability for customers to self-select parameters on individual devices and determine thresholds for the raising of exceptions and associated reporting.
C4.3.11 Call Detail reports	The partner must provide reports on the TelePresence calls that are made. This must include: • Call Manager status and performance (Hosted only) • Call statistics (e.g., duration, failed attempts)

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.	
Requirement	Description
C4.3.12 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) • UC and TP endpoint peripheral failures • Detailed POS reporting to Cisco in order to support Cisco sales compensation plan

Click here to return to Table of Contents

C5 Desktop as a Service (DaaS)

Introduced: June 2013
Last Updated: November 2016

Overview

Desktop as a Service (DaaS) provides dedicated and shared desktop resources on demand to the customer, delivered from the partner's cloud. Rather than purchasing servers, software, data center space, or network equipment, clients are able to consume those resources as a fully managed service. Partners typically bill such services based on the number of desktops or number of session users in either a reserved or consumed model.

The architectural foundation of Cisco Powered Desktop as a Service can be implemented using the Virtual Multiservice Data Center (VMDC) solution, with or without Cisco Application Centric Infrastructure (ACI).

VMDC is an end-to-end architecture based on Cisco technology that defines how to create and manage flexible and dynamic pools of virtualized resources which can be shared efficiently and securely among multiple customers. The VMDC architecture consists of infrastructure layers as well as management, orchestration, and assurance components. The orchestration solution creates a service portal that reduces resource provisioning and improves time to market for IaaS-based services. The assurance solution provides monitoring and troubleshooting capabilities that are used for delivering end-to-end Service-Level Agreements (SLAs).

Refer to VMDC Design and Implementation Guidelines.

Multiple releases of VMDC are available for deployment. Any of these releases can be used as the infrastructure basis for an IaaS offering.

Cisco Application Centric Infrastructure technology enables you to integrate virtual and physical workloads in an easy-to-use and highly programmable, multi-hypervisors fabric that is excellent for any multi-service or cloud datacenter. The Cisco ACI fabric consists of discrete components that operate as routers and switches but is provisioned, configured, and managed as a single entity.

Refer to the Intercloud Data Center Application Centric Infrastructure 1.0, Implementation Guide.

Note: The IaaS designation does not inherently give a partner access to purchase or deliver restricted data center products. The partner must meet applicable ATP requirements to purchase and deliver restricted data center products.

C5.1 Prerequisites

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

Requirement	Description
C5.1.1 Meet all CMSP partner requirements in Cisco Channel Program Audit and Policies document	See CMSP partner requirements in Cisco Channel Program Audit and Policies document.
C5.1.2 Submit at least two customer references for the service	CMSP partners are required to have a minimum of two customer references (existing contractual relationships) for each Cisco Powered service to validate service offering requirements. One customer may serve as reference to multiple designations. A customer with multiple sites does not qualify as a second reference. The intent is to ensure that the partner has proven and repeatable service practices. The partner must submit at least two customer references for the service at the time of the audit, or must demonstrate the ability to deliver the service to an end customer. In the event that no customer references are available at the time of the audit, two customer references must be provided upon recertification. Refer to Customer Reference Validation template.

C5.1.3 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. 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.
C5.1.4 Employ at least one CCNP Data Center certified individual on staff	The Cisco CCNP Data Center certification is a job-role-focused training and certification program using the following technologies: Cisco Nexus Switches (1000, 5000, 6000, 7000, and 9000 Series), Cisco UCS B-Series and C-Series Blade Servers, Cisco UCS Manager, Cisco Data Center Network Manager, Cisco Virtual Network Management Center, and Cisco MDS Series Multilayer Switches. A Cisco CCIE certification, of any technology specialization, supersedes and fulfills the certification requirements for this service.
C5.1.5 Audit representation	If the partner has contracted Cisco Services or a third-party cloud builder to design or build a DaaS platform, providing some or all of the Desktop as a Service requirement. At the partner's discretion, Cisco Services or the cloud builder must participate in the audit and provide evidence on how the requirements have been fulfilled. If the partner has contracted Cisco Services to operate the Desktop as a Service platform, providing some or all of the Desktop as a Service requirement. At the partner's discretion, Cisco Services must participate in the audit and provide evidence on how the requirements have been fulfilled.

C5.2 Partner System/Solution Requirements (Build)

Service Capabilities

The following section describes the basic functions of the Desktop as a Service (DaaS) solution.

The partner 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 on the Cisco Nexus series of products or the Cisco Catalyst switch range.

Requirements	Description
C5.2.1 Data Center WAN Edge design	Data Center WAN Edge routers provide networking capability for services such as Internet, L3VPN, and L2VPN services. ASR9K/1K are examples of devices acting as Data Center WAN Edge routers. The partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural or topology diagrams.
C5.2.2 Data Center Core design	The Data Center Core design provides a high-speed switching backplane for all flows going in and out of the data center. In smaller designs the core and Aggregation Layers may be collapsed. The partner must provide evidence of how the core design ensures resilient Layer 3 routing with no single points of failure and rapid convergence around link failure. An Application Centric Infrastructure (ACI) fabric may be implemented using a spine and leaf model to address this requirement. The partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural diagrams.
C5.2.3 Aggregation Layer	Provides the Layer 3 and Layer 2 boundary for the data center infrastructure, linking the Layer 2 broadcast domains to the Layer 3 routed domain. It is also often used as the insertion point for network-based services such as firewall. The partner must explain how they achieve resiliency in the event of link, interface, or switch failure. An Application Centric Infrastructure (ACI) fabric may be implemented using a spine and leaf model to address this requirement.

	The partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural or topology diagrams.
C5.2.4 Services Layer	Network-based services may be multi-tenant, multi-context capable, and provide per-customer security control. Alternatively, they could be per-customer, discrete, and virtualized. The Services Layer is designed together with the DC Core and Aggregation Layers to provide a high scalability. When multi-tenanted, a resilient framework is also required. The Services Layer can be based on the Cisco VMDC architecture or the Cisco Application Centric Infrastructure. The partner must provide evidence that all of the following functions are delivered on a Cisco platform: • Firewall • Intrusion Prevention System (IPS) • Encryption / VPN And the partner must be able to provide the following functions: • Load balancing The partner must explain how resiliency is achieved in this layer using a document such as an architectural diagram.
C5.2.5 Access Layer	Provides connectivity for server farm end nodes residing in the data center. Virtualization of the physical servers creates a virtual Access Layer. This allows the function of the logical Layer 2 Access Layer to span multiple physical devices. The partner must explain the architectural approach taken for the Access Layer, types of switches used, and the benefits that this approach provides to the customer. The partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural or topology diagrams.

Virtualization Requirements

Virtualization is the abstraction of network, compute, and storage resources. This functionality is critical in enabling the dynamic, on-demand characteristics of IT resources delivered from the cloud. It is enabled through the capabilities of Cisco as well as our key technology partners. The Service Provider partner must provide evidence that their services incorporates the key aspects described here and utilizes Cisco technology partner solutions that have been tested as part of the architecture.

Requirement	Description
C5.2.6 Network virtualization	Segmenting a common network into separate virtual networks, providing logical separation of data-plane and some control-plane functionality in order to achieve customer traffic separation is required. There can be several forms of network virtualization: • Virtual LANs (VLANs): Separate L2 LAN broadcast domains • Virtual Routing Forwarding (VRFs): Separate L3 routing domains • Virtual Private Networks (VPNs): Creating virtual circuits in a shared network. This can be done via physical appliance or virtualized using the Cisco Cloud Services Router 1000v (CSR1KV) or the virtualized Cisco Adaptive Security Appliance (ASAv). Commonly deployed VPN technologies include MPLS and IPsec • Virtual network edge services: Network services can be delivered using physical or virtualized appliances. • Virtual contexts: Used on firewalls, load balancers, and other application networking platforms. • Virtual Extensible LANs (VXLANs): Achieved using Cisco Nexus 9000 Series switches in fabric mode when used in combination with the Cisco Application Policy Infrastructure Controller (APIC) The partner must explain how network virtualization is used in their service design to isolate/separate the customer traffic within individual network domains. The partner must present evidence of how this requirement is delivered on a Cisco

	platform, such as architectural diagrams.
C5.2.7 Desktop virtualization	Hardware assisted virtualization is used to simulate a complete hardware environment, or virtual machine (VM), in which an unmodified "guest" desktop or single user operating system executes in complete isolation. The partner must provide evidence of how server virtualization is used in their service design to provide improved capabilities for load balancing and flexibility in deployment and management of server resources for the customer. This must be based on a hypervisor solution that has been certified to operate on the Cisco UCS platform.
C5.2.8 Shared desktop virtualization	Remote Desktop Services, formerly Terminal Services, is a server role in Windows Server that provides technologies that enable users to access session-based desktops, or applications in the data center from both within a corporate network and from the Internet. Remote Desktop Services enables a rich-fidelity desktop or application experience, and helps to securely connect remote users from managed or unmanaged devices.
C5.2.9 Server virtualization	Hardware assisted virtualization is used to simulate a complete hardware environment, or Virtual Machine, in which an unmodified "guest" operating system executes in complete isolation. Multiple virtual compute environments can be activated and executed on a single hardware platform. The partner must provide evidence how server virtualization is used in their service design. The partner must present evidence of how this requirement is delivered on a Cisco UCS platform, such as architectural diagrams.
C5.2.10 Storage virtualization	Storage virtualization allows data location independence by abstracting the physical location. Storage area networks (SANs) can also be virtualized into zones and Virtual SANs (VSANs) if based on FC or FCoE. VLANs and other Ethernet-based virtualization may be used for iSCSI and NFS-based connectivity. The partner must present evidence of how the virtualization system provides the customer a logical space for data storage and then handles the process of mapping it to the actual physical location, allowing the physical data to be stored without the customer needing to be aware of its actual location. The partner must present evidence of how external storage is connect via a Cisco platform, such as architectural diagrams.
C5.2.11 Single image management	Image management across multiple virtual device specifications can cause maintenance of a number of copies and versions that only differ by the virtual HW spec they are applied to. Customers want to see how they can use a single image template, also known as a “Golden Image,” and apply it against a variety of virtual device specifications varying by CPU, RAM, or HD size.
C5.2.12 Unified Fabric	A unified fabric consolidates the different types of traffic within the data center onto a single, multi-purpose, high-performance, high-availability network that greatly simplifies the network infrastructure. To achieve this, a unified fabric must be intelligent enough to identify the different types of traffic and handle them appropriately. The Cisco Unified Computing System (Cisco UCS) is the next-generation data center platform that unites network, compute, storage, and virtualization resources in an integrated system. The partner must present evidence of how this requirement is delivered on a Cisco UCS platform, such as architectural or topology diagrams.

Cloud Management Framework Requirements	
Cloud management is a complex task that requires the administration of real and virtual resources as well as control of the people and processes that enable the data center to function. The following section defines a framework that includes the key management functions and processes required regardless of the architectural design, including the service orchestration capabilities required to deliver the service. Service orchestration includes consistent technology architecture, a structured approach to data collection and processing as well as automation wherever possible to minimize human intervention. This enables a portal-based configuration model in which the customer can pick from a limited number of customized service options. The purpose of service orchestration is to hide the underlying complexities required to deliver a service by providing an abstracted set of resources described to the end customer in easy to understand language and that has visibility into all of the resources required to set up the requested service such that the customer has clear visibility of whether a requested service creation or amendment can be supported.	
Requirement	Description
C5.2.13 Infrastructure services	The management framework must incorporate these key functions to manage the infrastructure: • Virtual server: Memory, CPU, capacity management, and storage allocation • Network Virtualization: VLAN, VXLAN, VRF, SVI, virtual context, virtual address, virtual firewalls, load balancers, VPN, QoS, ACL filtering • Storage: Multi-pathing, storage classification and tiers, storage volume management, and workload mobility Recommended functions that may be offered as part of the service: • Site Selection: Intra and inter-site workload mobility, global address management (IP and DNS), bursting, failover, disaster recovery management • Virtual Machine Migration: Migration from physical to virtual, and virtual to physical (coordinated provisioning with server migration tools) • APIs: For driving notification, approval billing, chargeback, utilization, IP address management, accounting, SLA management, identity, and general automation The partner must present evidence of how this requirement is delivered on Cisco UCS via architectural diagrams or an equivalent.
C5.2.14 Service orchestration	The service orchestration layer must have intelligence to ensure that no configuration actions take place if one of the components within the service being requested through the portal is unavailable (out of logical pools, node down, over capacity thresholds, etc.). The orchestration layer must provide the following functions: • Provide a view of all the services pools available across multiple pods and across multiple data centers • APIs that would provide access to information to other management tools The partner must explain the service orchestration layer that they have put in place and how it can ensure that service requests are only accepted if the underlying resources are available.
C5.2.15 Business service management	The business service management layer includes the key functions required to support the service desk. These functions can be provided manually, element based or fully automated: • Service catalog • Service-level management • Billing • Event management • Configuration management • Problem management The partner must explain the service management functions that are in place to support the key functionality required to deliver and manage customer service.

Cloud Services Requirements	
This section describes the service capabilities used by the partner to deliver cloud Desktop as a Service. The service is built around the Virtual Multiservice Data Center (VMDC) or Cisco Application Centric Infrastructure (ACI). The partner must provide evidence how their service offerings use these capabilities to deliver differentiated services and must allow the customer flexibility to self-provision and manage server capacity based on some or all of the characteristics listed.	
Requirement	Description
C5.2.16 Role Separation	A key distinction of cloud services is role separation and isolation of key functions between Service Provider, IT administrator, and end user. The partner must provide evidence how the solution achieves role separation without requiring AD-Trust or other shared credentials between end customer and Service Provider so that customer does not have access to any Service Provider information and vice versa.
C5.2.17 Virtual desktop sizing	Service profiles based on different compute, storage, and memory capacity. These can be pre-configured for the customer, such as office user, standard user, and power user desktops or could allow for individual resource size selection. Service profiles can be made available for the customers to select themselves via a web portal as needed.
C5.2.18 Security	A key concern of potential customers of a DaaS service is security. The partner must be able to explain the security benefits of the Cisco architecture to address the functions below: • Traffic separation across the WAN using VPN at L2 or L3 • Mapping of that traffic onto a dedicated Virtualized LAN (VLAN) infrastructure in the data center The following functions are optional to enhance the service offering: • Encryption or VPN functionality dedicated to the customer • Firewall and optionally IPS functionality dedicated to the customer
C5.2.19 Service reliability	The partner 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. Service must include all of these features: • Physical layer redundancy within network components • Connectivity via load sharing, dual paths, or similar features • Multi-tenancy, providing multiple customers a secure and isolated environment
C5.2.20 Client Network Isolation	The partner must provide evidence of how the customer can maintain full network isolation and control of their network services such as DHCP and DNS without concern for collision or restriction with the Service Provider network and network services.
C5.2.21 Resilient architecture	A key component of DaaS is service resiliency. The partner must provide evidence that the solution is designed with no single point of failure such as non-HA management components or a single database. Where impact to one customer might affect all customers on the platform.
C5.2.22 Rolling Software Updates	Customers want software updates to be scheduled at their convenience and not due to a Service Provider schedule requirement. The partner must provide evidence how software updates can be delivered at the customer's schedule requirement.

C5.3 Customer Requirements

Not applicable

C5.4 Service-Level Management Requirements (Operate)

Service-Level Agreement (SLA) Components

This section describes the SLAs 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 SLAs may also be presented as evidence of meeting these requirements.

Requirement	Description
C5.4.1 Mean Time to Notify (MTTN)	If the customer experiences any resource or performance-affecting event the partner must notify the customer of the issue. The specific guarantees 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.
C5.4.2 Mean Time to Restore Service (MTRS)	If there is a disruption to the performance or availability of resources allocated to a customer, the partner must provide an expectation of restoration time. The specifics may vary according to customer agreements. MTRS, also known as Mean Time to Restore (MTTR), measures the total elapsed time from the start of a service outage to the time the service is restored. • P1: 4 hours • P2: 24 hours • P3: 2 business days • P4: 5 business days
C5.4.3 Service availability	Provide evidence of which service availability elements are covered by the SLA components agreed with customer and how different Operating-Level Agreement (OLA) components are measured and managed: • Infrastructure SLA • Network SLA (the network operated by the partner that is used to provide connectivity from the Internet or VPN, and the data center itself): A third party could provide network connectivity. Appropriate documentation must be provided to demonstrate how the Underpinning Contracts (UCs) are measured and managed between partner and third party. • Seamless SLA (end-to-end service experience): Where elements of the end-to-end service are provided by a third party, appropriate documentation must be provided to demonstrate how the Underpinning Contracts (UCs) are measured and managed between partner and the third party
Partner / 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 Desktop as a Service subscription. These requirements may be proven by a demonstration of portal from customer viewpoint, including a real-time view of connectivity and status. Security mechanisms, such as password protection, may be used to restrict access to the online 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.	
Requirement	Description
C5.4.4 Partner administration portal	The partner must demonstrate the ability to set up and manage desktops pools. The partner must be able configure the following attributes: • Type of desktops or sessions • Base template • Number of desktops or sessions to create • Users that will be mapped to the pool
C5.4.5 Customer administration portal	The customer administration portal must provide the following management capabilities: • Importing virtual desktop images from an external resource • Updating and propagating template changes • Provisioning and updating pools • Mapping users to pools • Accessing desktops or sessions as part of providing support to end users The portal for the customer administrator role must also provide reporting capabilities including a summary of the environment and desktop or session performance and usage.

C5.4.6 Customer End User portal	The customer end user portal must provide the following capabilities: • Link to desktop or session access • Thin client download if applicable • Ability for end user to perform desktop lifecycle functions as well as remotely disconnected sessions • Educational material on how use the service and access support when required

External Reporting

The following section describes the reports that are to be made available to the customer administrative contacts via the 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 portal is considered an industry standard and allows partners to differentiate themselves from other providers via a captivating user experience.

Requirement	Description
C5.4.8 Performance analysis reports	Historical performance analysis of the service would typically be available over a number of sample periods (daily, weekly, monthly), and the report would include data to allow the customer to understand how the overall service is performing.
C5.4.9 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.
C5.4.10 Resource inventory reports	Reports of resources under management for the customer provide data that is relevant to the customer for managing their IaaS subscription and understanding what resources are available for their use and have been used historically.
C5.4.11 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.

Click here to return to Table of Contents

C6 Disaster Recovery as a Service (DRaaS)

Introduced: December 2013
Updated: November 2016

Overview

Disaster Recovery as a Service (DRaaS) allows partners to provide a managed, multi-tenant, cloud-based recovery environment for mission-critical production workloads that reside in a customer-controlled environment, such as an on-premises data center. DRaaS allows these customer environments that are typically managed and owned by the customer to be continually replicated to a cloud provider data center and recovered as full application environments, including compute, storage, and network services, in the event of a disaster.

This section describes architecture, solution, and service offering requirements that must be met by a partner offering DRaaS so as to obtain Cisco Powered accreditation.

Cisco Powered DRaaS environments may be layered on top of the same VMDC architectural foundation, with or without Cisco Application Centric Infrastructure (ACI), used to deliver IaaS services or deployed on a stand-alone infrastructure specifically designed for DRaaS. Refer to the VMDC Design and Implementation Guidelines for details. Multiple releases of VMDC are available for deployment. Any of these releases may be used to comply with the requirements for the DRaaS listed below.

Cisco Application Centric Infrastructure (ACI) technology enables you to integrate virtual and physical workloads in an easy-to-use and highly programmable, multi-hypervisors fabric that is excellent for any multi-service or cloud datacenter. The Cisco ACI fabric consists of discrete components that operate as routers and switches but is provisioned, configured, and managed as a single entity.

Refer to the Intercloud Data Center Application Centric Infrastructure 1.0, Implementation Guide.

DRaaS provides recovery of the customer's data center services in a virtualized, multi-tenant with minimal data loss and a rapid recovery time backed by an explicit provider service-level agreement (SLA) for recovery time objective. Suppliers typically bill on the number of protected servers or VMs, the storage space required for replication, and the compute resources that will be made available upon customer declaration or test.

C6.1 Prerequisites

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

Prerequisites

Requirement	Description
C6.1.1 Meet all CMSP partner requirements in Cisco Channel Program Audit and Policies document	See CMSP partner requirements in Cisco Channel Program Audit and Policies document.
C6.1.2 Submit at least two customer references for the service	CMSP partners are required to have a minimum of two customer references, from existing contractual relationships, for each Cisco Powered service. One customer may serve as reference to multiple designations. A customer with multiple sites does not qualify as a second reference however. The intent is to ensure that the partner has proven and repeatable service practices. The partner must submit at least two customer references for the service at the time of the audit, or must provide evidence of the ability to deliver the service to an end customer. In the event that no customer references are available at the time of the audit, two customer references must be provided upon recertification. Refer to Customer Reference Validation template.
C6.1.3 Provide the following documents unique to the service: • Service-Level Agreement (SLA) • Marketing Service Description (MSD) • Technical Service Description (covering the capacity utilization policy) • Architectural 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 partner must provide an actual SLA with an existing customer or SLAs for multiple customers. The Marketing Service Description 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.

	The Technical Service Description provides documentation on how capacity is managed on the IaaS system. This may be either an externally or internally published document. 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.
C6.1.4 Employ at least one CCNP Data Center certified individual on individual	The Cisco CCNP Data Center certification is a job-role-focused training and certification program using the following technologies: Cisco Nexus® Switches (1000, 5000, 6000, 7000, and 9000 Series), Cisco UCS® B-Series and C-Series Blade Servers, Cisco UCS Manager, Cisco Data Center Network Manager, Cisco Virtual Network Management Center, and Cisco MDS Series Multilayer Switches. A Cisco CCIE certification, of any technology specialization, supersedes and fulfills the certification requirements for this service. For information, visit: Cisco Certifications.
C6.1.5 Audit representation	If the partner has contracted Cisco Services or a third-party cloud builder to design or build the Disaster Recovery as a Service platform, providing some or all of the requirements, at the partner's discretion, the third party may participate in the audit and provide evidence on how the requirements they have provided are fulfilled. If the partner has contracted for Cisco Services to operate the Disaster Recovery as a Service platform, providing some or all of the requirements. At the partner's discretion, Cisco Services may participate in the audit and provide evidence on how the requirements have been fulfilled.

C6.2 Partner System/Solution Requirements (Build)

Service Capabilities

The following section describes the basic functions of a Disaster Recovery as a Service (DRaaS) solution. Design details for each section are covered in depth in the VMDC and VSA documentation along with the DRaaS documentation.

The partner 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.

Requirements	Description
C6.2.1 Data Center WAN edge design	Data Center WAN Edge routers provide networking capability for services such as Internet, L3VPN, and L2VPN services. The partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural or topology diagrams.
C6.2.2 Data Center Core design	The Data Center Core design provides a high-speed switching backplane for all flows going in and out of the data center. In smaller designs the core and Aggregation Layers may be collapsed. The partner must provide evidence of how the core design ensures resilient Layer 3 routing with no single points of failure and rapid convergence around link failure. An Application Centric Infrastructure (ACI) fabric may be implemented using a spine and leaf model to address this requirement. The partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural diagrams.
C6.2.3 Aggregation Layer	Provides the Layer 3 and Layer 2 boundary for the data center infrastructure, linking the Layer 2 broadcast domains to the Layer 3 routed domain. It is also often used as the insertion point for network-based services such as firewall. The partner must explain how they achieve resiliency in the event of link, interface, or switch failure. An Application Centric Infrastructure (ACI) fabric may be implemented using a spine and leaf model to address this requirement.

	The partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural or topology diagrams.
C6.2.4 Services Layer	Network-based services may be multi-tenant, multi-context capable, and provide per-customer security control. Alternatively, they could be per-customer, discrete, and virtualized. The Services Layer is designed together with the DC Core and Aggregation Layers to provide a high scalability. When multi-tenanted, a resilient framework is also required. The Services Layer can be based on the Cisco VMDC architecture or the Cisco Application Centric Infrastructure. The partner must provide evidence that all of the following functions are delivered on a Cisco platform: • Firewall • Intrusion Prevention System (IPS) • Encryption / VPN And the partner must be able to provide the following functions: • Load balancing The partner must explain how resiliency is achieved in this layer using a document such as an architectural diagram.
C6.2.5 Access Layer	Provides connectivity for compute nodes within the data center. Virtualization of the physical servers creates a virtual Access Layer. This allows the function of the logical Layer 2 Access Layer to span multiple physical devices. The partner must explain the architectural approach taken for the Access Layer, types of switches used, and the benefits that this approach provides to the customer. The partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural or topology diagrams.

Virtualization Requirements

Virtualization is the abstraction of network, compute, and storage resources. This functionality is critical in enabling the dynamic, on-demand characteristics of IT resources delivered from the cloud. It is enabled through the capabilities of Cisco as well as our key technology partners. The Service Provider partner must provide evidence that their services incorporates the key aspects described here and utilizes Cisco technology partner solutions that have been tested as part of the architecture.

Requirement	Description
C6.2.6 Network virtualization	Segmenting a common network into separate virtual networks, providing logical separation of data-plane and some control-plane functionality in order to achieve customer traffic separation is required. There can be several forms of network virtualization: • Virtual LANs (VLANs): Separate L2 LAN broadcast domains • Virtual Routing Forwarding (VRFs): Separate L3 routing domains • Virtual Private Networks (VPNs): Creating virtual circuits in a shared network. This can be done via physical appliance or virtualized using the Cisco Cloud Services Router 1000v (CSR1KV) or the virtualized Cisco Adaptive Security Appliance (ASAv). Commonly deployed VPN technologies include MPLS and IPsec • Virtual network edge services: Network services can be delivered using physical or virtualized appliances. • Virtual contexts: Used on firewalls, load balancers, and other application networking platforms. • Virtual Extensible LANs (VXLANs): Achieved using Cisco Nexus 9000 Series switches in fabric mode when used in combination with the Cisco Application Policy Infrastructure Controller (APIC) The partner must explain how network virtualization is used in their service design to isolate/separate the customer traffic within individual network domains. The partner must present evidence of how this requirement is delivered on a Cisco

	platform, such as architectural diagrams.

C6.2.7 Server virtualization	Hardware assisted virtualization is used to simulate a complete hardware environment, or Virtual Machine, in which an unmodified "guest" operating system executes in complete isolation. Multiple virtual compute environments can be activated and executed on a single hardware platform. The partner must provide evidence how server virtualization is used in their service design. The partner may also offer dedicated or bare metal servers in addition to their Virtual Machine based services. The partner must present evidence of how this requirement is delivered on a Cisco UCS platform, such as architectural diagrams.
C6.2.8 Storage virtualization	Storage virtualization allows data location independence by abstracting the physical location. Storage area networks (SANs) can also be virtualized into zones and Virtual SANs (VSANs) if based on FC or FCoE. VLANs and other Ethernet-based virtualization may be used for iSCSI and NFS-based connectivity. The partner must present evidence of how the virtualization system provides the customer a logical space for data storage and then handles the process of mapping it to the actual physical location, allowing the physical data to be stored without the customer needing to be aware of its actual location. The partner must present evidence of how external storage is connect via a Cisco platform, such as architectural diagrams.
C6.2.9 Unified fabric	A unified fabric consolidates the different types of traffic within the data center onto a single, multi-purpose, high-performance, high-availability network that greatly simplifies the network infrastructure. To achieve this, a unified fabric must be intelligent enough to identify the different types of traffic and handle them appropriately. The Cisco Unified Computing System (Cisco UCS) is the next-generation data center platform that unites network, compute, storage, and virtualization resources in an integrated system. The partner must present evidence of how this requirement is delivered on a Cisco UCS platform, such as architectural or topology diagrams.
Disaster Recovery Management Framework Requirements	
Delivering DRaaS requires the provider abstract the complexity of the solution.	
Requirement	Description
C6.2.10 Service catalog	The provider must have well-defined offerings for Disaster Recovery as a Service in a service catalog with established pricing. This may be proven by showing an ordering or quoting tool that has standard pricing that relates to service components such as protected servers, recovery environment size, storage, bandwidth, and other relevant components.

C6.2.11 Customer qualification and onboarding management	The partner must present evidence of the following elements of the customer experience: • Technical marketing materials explaining the service offering, SLA, provider process and customer/provider responsibilities intended for the customer's technical decision maker • A process for qualifying the customer's environment for support in the recovery environment; this may be an automated or semi-automated tool or a manual environment survey provided to the customer for completion • A quote for the environment generated from the service catalog or other appropriate tools • Customer onboarding documentation such as a welcome kit or other materials customer receives at time of onboarding (recommended) These may be proven by showing the customer-facing technical collateral, quotes, and any tools used by the sales engineering organization to qualify customers for service eligibility.
C6.2.12 Runbook automation	The partner must have a solution to automate the runbook tasks that will need to be performed in the event of a disaster to ensure the partner's staff is able to handle multiple customer failovers simultaneously. The runbook automation solution must address the following: • Boot order and priority of recovery VMs and multi-tier applications • Association and/or remapping of VLANs and IP addresses to recovery VMs • Validation of successful VM boot up These capabilities should be provided on a per-tenant basis. The partner must explain the runbook automation solution that they have put in place and how it can ensure that tasks are automated at time of declaration.
Disaster Recovery Service Requirements	
This section describes the service features and capabilities the DRaaS solution must provide. A solution overview may be found in the Design Zone.	
Requirement	Description
C6.2.13 Ability to replicate protected VMs or physical servers	The service must be able to provide asynchronous replication of data and system volumes for virtual and/or physical environments, as defined in the offering definition. Support for heterogeneous storage environments is required unless the service is explicitly positioned for an identified storage vendor.
6.2.14 Recovery configurations	The ability to capture recovery configurations for protected VMs or physical servers is required.
C6.2.15 Support for recovery of Windows and Linux VMs or physical servers	The service must support for replication and recovery of both Microsoft Windows and Linux VMs or physical servers. If physical servers are supported, both Microsoft Windows and Linux must be supported for recovery.
C6.2.16 Compression and encryption services offload	Compression and encryption of the replication traffic must not be performed by the customer's production workloads and should be performed via a dedicated physical or virtual appliance such as a Cisco ISR or CSR providing compression, WAN optimization, and encryption. These capabilities may be provided by the disaster recover platform itself, but they cannot be provided on stand-alone, physical or virtual, non-Cisco network appliance. The partner must present evidence, such as a topology diagram, of how this requirement is delivered from the DRaaS software or a Cisco platform.
C6.2.17 Continuous Data Protection	The service must provide near continuous data protection with retention of numerous recovery points per hour and a retention journal of at least twenty-four (24) hours of recovery points. Data replication frequency should be attuned to customer business requirements, but multiple replications per hour are required. The partner must present evidence showing replication frequency configuration and recovery point journaling.

C6.2.18 Consistency groups	The solution must allow for write-order consistency across multiple volumes on one physical or virtual machine, such as log and database volumes. The solution should provide crash-consistent recovery points at 15-minute intervals or application-consistent recovery points at 30-minute intervals or less. The partner must present evidence showing how consistency is accomplished between multiple volumes on the same physical or virtual machine.
C6.2.19 Secure container context	All replication and normal operations between tenant and partner service delivery VMs shall occur in a securely isolated network environment. The partner must present evidence showing how data replication is isolated between tenants.
C6.2.20 Differential failback	The solution should allow failback replication to the customer of only blocks changed since failover.
C6.2.21 Sandbox testing	The service must allow the partner and customer to conduct disaster recovery test exercises within a testing sandbox, without breaking replication or failing over production traffic. The partner must be able to load the customer recovery environment, including booting VMs and attaching them to recovery VLANs, and allow the customer access to validate functionality of the application layer testing via remote access protocol and/or VPN. A completed sandbox testing report would serve as evidence of this requirement.
C6.2.22 Security	Security is a key concern of potential DRaaS customers. The partner needs to be able to explain the benefits of the Cisco architecture to address these concerns, by supporting all of the following: • Isolation of tenant DRaaS service delivery components such as replication targets into tenant network containers • Isolation of shared provider DRaaS management infrastructure (runbook, automation servers, etc.) from tenant environments • Encryption of replication data flows from customer premises to tenant network container • Traffic separation across the WAN • Mapping of that traffic onto a dedicated virtualized LAN infrastructure in the data center • Encryption or VPN functionality dedicated to the customer • Firewalling functionality dedicated to the customer The partner must present evidence of how this requirement is delivered on a Cisco platform or from within the DRaaS software platform itself such as architectural or topology diagrams.
C6.2.23 Service reliability	The partner must provide evidence and explain the main features of their solution that are used to deliver a reliable infrastructure for the service, as well as offering different levels of service availability according to customer needs. Service must include all of these features: • Physical layer redundancy within switches • Connectivity via load sharing, dual paths, or similar features • Routing or switching around node failures • Multi-tenancy: the ability to support multiple customers in a secure and isolated configuration The partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural or topology diagrams.
C6.2.24 Support for partial failover/failback scenarios with Layer 2 network extension	The partner must provide customer the ability to fail over only an identified portion of the protected servers with the ability for servers in the same subnets and/or VLANs to span both the production and recovery environment. This capability would typically be provided via the use of OTV services on the Cisco Cloud Services Router (CSR) or Advanced Services Router (ASR) in conjunction with Location Identity Separation Protocol (LISP) on a supported virtual or physical router.

	The partner must present evidence of how this requirement is delivered via the DRaaS software platform or on a Cisco platform such as architectural or topology diagrams.

C6.3 Process Management Requirements

Not applicable

C6.4 Service-Level Management Requirements (Operate)

Service-Level Agreement (SLA) Components

This section describes the SLAs 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 SLAs may also be presented as evidence of meeting these requirements.

Requirement	Description
C6.4.1 Mean Time to Respond (MTTR)	If the customer experiences any resource or performance-affecting event the partner must notify the customer of the issue. The specific guarantees 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.
C1.4.2 Mean Time to Restore Service (MTRS)	If there is a disruption to the performance or availability of resources allocated to a customer, the partner must provide an expectation of restoration time. The specifics may vary according to customer agreements. MTRS, also known as Mean Time to Restore (MTTR), measures the total elapsed time from the start of a service outage to the time the service is restored. 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
C6.4.3 Recovery Time Objective (RTO)	When and if the customer declares a disaster through whatever process the partner defines such as phone-based declaration or trouble ticket submission, the partner must provide a contractually agreed upon time line for the recovery of the customer's environment. The RTO SLA measures the total elapsed time from the time the customer completes the final step in the declaration process to the time that the partner presents the recovered environment to the customer with restored virtual machines and any required network services. For managed DRaaS offers, RTO SLAs must provide a recovery time of 4 hours or less for up to 50 servers.

C6.4.4 Service availability	Provide evidence of which service availability elements are covered by the SLA components agreed with customer and how different Operating-Level Agreement (OLA) components are measured and managed: • Infrastructure SLA • Network SLA (the network operated by the partner that is used to provide connectivity from the Internet or VPN, and the data center itself): A third party could provide network connectivity. Appropriate documentation must be provided to demonstrate how the Underpinning Contracts (UCs) are measured and managed between partner and third party. • Seamless SLA (end-to-end service experience): Where elements of the end-to-end service are provided by a third party, appropriate documentation must be provided to demonstrate how the Underpinning Contracts (UCs) are measured and managed between partner and the third party

Customer Web Portal

The following section describes the online capabilities 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 portal from the customer viewpoint, including a real-time view of connectivity and status. Security mechanisms should include password protection or two-factor authentication, used to restrict access to the portal to authorized individuals.

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.

Requirement	Description
C6.4.5 Customer web portal	Provides an operational view for multiple audiences; designed to provide view of the network status, including current availability, reliability, and security for managed devices and infrastructure involved in service delivery of DRaaS services. The partner's customer web portal typically provides the following capabilities: • Customer authentication with ordering, accounting, billing, management of their services • Expert-level authorization for customization of firewall rules either via direct configuration editing or via viewing current policy and providing a ticket with change requests • Ability to view protected servers or VMs and associated volumes or drives • Ability to view current achievable recovery point objective (RPO) for protected servers or VMs • Ability to view current achievable application-consistent RPO. Platform must be able to identify any drift from committed RPO. • Ability to identify replication failures that have occurred The customer web portal could either be a partner owned/branded or a third-party white-labeled solution. If the partner does not provide an online web portal, the partner must explain how above capabilities are provided to customer.

External Reporting

The following section describes the reports that are to be made available to the customer via the 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 portal is considered an industry standard and allows partners to differentiate themselves from other providers via a captivating user experience.

Requirement	Description
C6.4.6 Protected resources	Report details the servers or VMs protected by the service, including machine name and/or source IP, protected volumes, and any other pertinent information
C6.4.7 Recovery network configuration	Report details the configuration of the virtual and/or physical network that will be available to customer at time of declaration. This includes mapping of servers to VLANs, inter-VLAN routing and firewalling, routing configuration of the environment, and configuration of edge firewall and VPN policies.

C6.4.8 Disaster Recovery exercise results	Report based on the findings of the most recent disaster recovery exercise conducted between the partner and customer. This report should include a list of VMs booted in the DRaaS cloud and the results of whether the VMs were able to establish connectivity to required resources and whether the customer was able to validate the application layers running on each recovery VM (such as conducting a transaction using the recovery environment).
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.	
Requirement	Description
C6.4.9 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)
C6.4.10 Capacity management	Report on performance and capacity of the DRaaS environment in steady state over the reporting period. This report speaks to the ability of the environment to sustain normal loading as customers replicate to the environment, conduct exercises under normal (non-extreme) conditions and as the Service Provider on-boards new customers. This report should consider factors that may degrade performance of the environment under normal conditions or result in recovery point objective drift. Metrics shall include: • I/O consumption and headroom • Memory consumption and headroom • CPU consumption and headroom • Bandwidth consumption and headroom at relevant points in the environment • Number of additional tenants or protected servers that can be on boarded with current capacity or other capacity planning metrics at the partner's discretion
C6.4.11 Disaster recovery capacity management	Report used by the partner to manage the actuarial oversubscription risk the partner is exposed to in the event of disaster declaration by multiple customers due to a regional event, such as a natural disaster. This report should be designed to manage risk and oversubscription in accordance with the partner's business rules and would typically include comparison of the attributes below against the spare capacity identified in the capacity management reports above: • Notional vRAM and vCPU commitments in aggregate for all protected servers and largest 2 customers if any single customers represent more than 10% of the total environment • Notional bandwidth commitments in aggregate for all recovery environments and largest 2 customers if any customers represent more than 10% of the environment I/O forecast for recovery environment

Click here to return to Table of Contents

C7 Cloud Cell Architecture for SAP HANA (SAP HANA)

Introduced: May 2014
Updated: November 2016

Overview

The Cisco Powered Cloud Cell Architecture for SAP HANA offer is based on the Cisco HANA Reference Architecture to enable Service Providers to offer SAP HANA in an "as-a-Service" model from a cloud-based platform. The architecture is based on Cisco Integrated Infrastructure (CII) standards and covers a cell based design for SAP HANA, management and orchestration, a scalable network design and security and isolation.

C7.1 Prerequisites

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

Requirement	Description
C7.1.1 Meet all CMSP partner requirements in Cisco Channel Program Audit and Policies document	See CMSP partner requirements in Cisco Channel Program Audit and Policies document.
C7.1.2 Submit at least two customer references for the service	CMSP partners are required to have a minimum of two customer references (existing contractual relationships) for each Cisco Powered service to validate service offering requirements. One customer may serve as reference to multiple designations. A customer with multiple sites does not qualify as a second reference. The intent is to ensure that the partner has proven and repeatable service practices. The partner must submit at least two customer references for the service at the time of the audit, or must provide evidence of the ability to deliver the service to an end customer. In the event that no customer references are available at the time of the audit, two customer references must be provided upon recertification. Refer to Customer Reference Validation Template.
C7.1.3 Provide the following documents unique to the service: • Service-Level Agreement (SLA) • Marketing Service Description (MSD) • Technical Service Description (covering the capacity utilization policy) • Architectural 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 partner must provide an actual SLA with an existing customer or SLAs for multiple customers. The Marketing Service Description 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. The Technical Service Description provides documentation on how capacity is managed on the IaaS system. This may be either an externally or internally published document. 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.
C7.1.4 Employ at least one CCNP Data Center certified individual	The Cisco CCNP Data Center certification is a job-role-focused training and certification program using the following technologies: Cisco Nexus® Switches (1000, 5000, 6000, 7000, and 9000 Series), Cisco UCS® B-Series and C-Series Blade Servers, Cisco UCS Manager, Cisco Data Center Network Manager, Cisco Virtual Network Management Center, and Cisco MDS Series Multilayer Switches. A Cisco CCIE certification, of any technology specialization, supersedes and fulfills the certification requirements for this service. For information, visit: Cisco Certifications.

C7.1.5 Audit representation	If the partner has contracted Cisco Services or a third-party cloud builder to design or build the Infrastructure as a Service platform, providing some or all of the requirements, at the partner's discretion, the third party may participate in the audit and provide evidence on how the requirements they have provided are fulfilled. If the partner has contracted for Cisco Services to operate the Infrastructure as a Service platform, providing some or all of the requirements, at the partner's discretion, Cisco Services may participate in the audit and provide evidence on how the requirements have been fulfilled.

C7.2 Partner System/Solution Requirements (Build)

Network POD

The following section describes the basic functions of the Cloud Cell Architecture for SAP HANA (SAP HANA) solution.

The partner 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.

Requirements	Description
C7.2.1 Data Center WAN Edge design	Data Center WAN Edge routers provide networking capability for services such as Internet, L3VPN, and L2VPN services. The partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural diagrams.
C7.2.2 Data center core design	The Data Center Core design provides a high-speed switching backplane for all flows going in and out of the data center. In smaller designs the core and Aggregation Layers may be collapsed. The partner must provide evidence of how the core design ensures resilient Layer 3 routing with no single points of failure and rapid convergence around link failure. An Application Centric Infrastructure (ACI) fabric may be implemented using a spine and leaf model to address this requirement. The partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural diagrams.
C7.2.3 Aggregation Layer	Provides the Layer 3 and Layer 2 boundary for the data center infrastructure, linking the Layer 2 broadcast domains to the Layer 3 routed domain. It is also often used as the insertion point for network-based services such as firewall. The partner must explain how they achieve resiliency in the event of link, interface, or switch failure. An Application Centric Infrastructure (ACI) fabric may be implemented using a spine and leaf model to address this requirement. The partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural or topology diagrams.
C7.2.4 Services Layer	Network-based services may be multi-tenant, multi-context capable, and provide per-customer security control. Alternatively, they could be per-customer, discrete, and virtualized. The Services Layer is designed together with the DC Core and Aggregation Layers to provide a high scalability. When multi-tenanted, a resilient framework is also required. The Services Layer can be based on the Cisco VMDC architecture or the Cisco Application Centric Infrastructure. The partner must provide evidence that all of the following functions are delivered on a Cisco platform: • Firewall • Intrusion Prevention System (IPS) • Encryption / VPN And the partner must be able to provide the following functions: • Load balancing

	The partner must explain how resiliency is achieved in this layer using a document such as an architectural diagram.
C7.2.5 Access Layer	Provides connectivity for compute nodes within the data center. Virtualization of the physical servers creates a virtual Access Layer. This allows the function of the logical Layer 2 Access Layer to span multiple physical devices. The partner must explain the architectural approach taken for the Access Layer, types of switches used, and the benefits that this approach provides to the customer. The partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural or topology diagrams.
Compute POD	
The following section describes the Unified Computing system capabilities that bring together the network, compute, storage, and virtualization resources into an integrated system. It relies on the concept of a unified fabric that consolidates different types of traffic onto a single network and optimizes the virtualized environment to provide management and scale capabilities.	
Requirement	Description
C7.2.6 Cisco Unified Computing System (UCS)	The Cisco Unified Computing System (Cisco UCS) is the next-generation data center platform that unites network, compute, and virtualization resources in a seamless system. The Cisco Powered Cloud Cell Architecture for SAP HANA must consist of: • UCS Blade Server Chassis/Server Blades or Rack Mount Servers • Configuration must conform to the SAP Product Availability Matrix (PAM) OR • Configuration must satisfy the requirements for SAP's Tailored Data Center Integration (TDI) The UCS configuration must be a certified configuration by SAP, used for delivering an SAP HANA cloud service. The compute nodes used for HANA production workloads must be dedicated for that purpose. However, other compute nodes in the architecture can be used to deliver applications. The number of chassis' and blades will be determined by the size of the deployment. The partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural or topology diagrams. Along with the SAP documentation that the Cisco platform is certified. The SAP PAM document should be the current version available. Refer to the Certified and Supported SAP HANA Hardware Directory
C7.2.7 Fabric Interconnect	Unified fabric consolidates the different types of traffic within the data center onto a single, general-purpose, high-performance, high-availability network that greatly simplifies the network infrastructure. The Cisco Powered Cloud Cell Architecture for SAP HANA must consist of: UCS Fabric Interconnect: Configuration must conform to the SAP Product Availability Matrix (PAM) The partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural or topology diagrams. Along with the SAP documentation that the Cisco platform is certified. The SAP PAM document should be the current version available. Refer to the Certified and Supported SAP HANA Hardware Directory

C7.2.8 Compute POD switching	Fabric-Interconnects and Nexus switches are utilized for high speed, low latency communication between HANA nodes, server fail-over and connection to the persistency layer (storage). Configuration must conform to the SAP Product Availability Matrix (PAM) The partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural or topology diagrams. Along with the SAP documentation that the Cisco platform is certified. The SAP PAM document should be the current version available. Refer to the Certified and Supported SAP HANA Hardware Directory
Management POD	
The following section describes the Unified Computing system capabilities that bring together the network, compute, storage, and virtualization resources into an integrated system. It relies on the concept of a unified fabric that consolidates different types of traffic onto a single network and optimizes the virtualized environment to provide management and scale capabilities.	
Requirement	Description
C7.2.9 Management servers	The management POD platform must be based on Cisco Unified Computing Systems (UCS) chassis/blade servers or rack-mount servers, providing Virtual Machines (VMs) outside of the HANA cloud cell. The partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural or topology diagrams.
C7.2.10 Management POD switching	The management POD switching layer must be provided on Cisco Nexus switches. The partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural or topology diagrams.
C7.2.11 Element management	The element management platform must be able to provide the following functions: • End-to-end automation • Unified policy-driven provisioning • Model-based automation – no need for scripting • Ongoing lifecycle management UCS Director is the recommended platform for element management.
C7.2.12 Orchestration layer supporting the Service Catalog	It is recommended that the partner provide an Orchestration Layer platform to extend cloud management platforms beyond self-service delivery of virtual machines and infrastructure resources, while increasing the use of cloud-based solutions to enhance business agility and effectiveness. Orchestration Layer platform should support the following: • Web-based service catalog • End customer and provider portal • Policy-based controls • Role-based access control • Lifecycle management and tracking Cisco Prime Service Catalog (bundled with Cisco Process Orchestrator) is the recommended platform.
Virtualization Requirements	
Virtualization is the abstraction of network, compute, and storage resources. The partner must provide evidence that their service incorporates the key aspects described here and utilizes Cisco partner solutions that have been tested as part of the architecture.	

Requirement	Description
C7.2.10 Network Virtualization	Segmenting a common network into separate virtual networks, providing logical separation of data-plane and some control-plane functionality in order to achieve customer traffic separation is required. There can be several forms of network virtualization: • Virtual LANs (VLANs): Separate L2 LAN broadcast domains • Virtual Routing Forwarding (VRFs): Separate L3 routing domains • Virtual Private Networks (VPNs): Creating virtual circuits in a shared network. This can be done via physical appliance or virtualized using the Cisco Cloud Services Router 1000v (CSR1KV) or the virtualized Cisco Adaptive Security Appliance (ASAv). Commonly deployed VPN technologies include MPLS and IPsec • Virtual network edge services: Network services can be delivered using physical or virtualized appliances. • Virtual contexts: Used on firewalls, load balancers, and other application networking platforms. • Virtual Extensible LANs (VXLANs): Achieved using Cisco Nexus 9000 Series switches in fabric mode when used in combination with the Cisco Application Policy Infrastructure Controller (APIC). The partner must explain how network virtualization is used in their service design to isolate/separate the customer traffic within individual network domains. The partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural diagrams.
C7.2.11 Server virtualization	Hardware assisted virtualization is used to simulate a complete hardware environment, or Virtual Machine, in which an unmodified "guest" operating system executes in complete isolation. Multiple virtual compute environments can be activated and executed on a single hardware platform. The partner must provide evidence how server virtualization is used in their service design. The partner may also offer dedicated or bare metal servers in addition to their Virtual Machine based services. The partner must present evidence of how this requirement is delivered on a Cisco UCS platform, such as architectural diagrams.
C7.2.12 Storage virtualization	Storage virtualization allows data location independence by abstracting the physical location. Storage area networks (SANs) can also be virtualized into zones and Virtual SANs (VSANs) if based on FC or FCoE. VLANs and other Ethernet-based virtualization may be used for iSCSI and NFS-based connectivity. The partner must present evidence of how the virtualization system provides the customer a logical space for data storage and then handles the process of mapping it to the actual physical location, allowing the physical data to be stored without the customer needing to be aware of its actual location. The partner must present evidence of how external storage is connect via a Cisco platform, such as architectural diagrams.
Cloud Services Requirements	
This section describes the service capabilities used by the partner to deliver Cloud Cell Architecture for SAP HANA (SAP HANA). The partner must provide evidence how their service offerings use these capabilities to deliver differentiated services and allow the customer flexibility to self-provision and manage server capacity based on some or all of the characteristics listed.	

Requirement	Description
C7.2.13 Service reliability	The partner 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. Service must include all of these features: • Physical layer redundancy within network components • Connectivity via load sharing, dual paths, or similar features • Multi-tenancy, providing multiple customers a secure and isolated environment

C7.3 Customer Requirements

Not applicable

C7.4 Service-Level Management Requirements (Operate)

Service-Level Agreement (SLA) Components

This section describes the SLAs that the partner must contract for with their customer as part of the service. These are normally available as part of the service description. Existing customer contract that include the relevant SLAs may also be presented as evidence of meeting these requirements.

Requirement	Description
C7.4.1 Service availability	Calculated on a monthly basis excluding planned maintenance windows, technical availability of the individual SP systems, measured by a logon check with the network boundaries of the SAP HANA Enterprise cloud, thus excluding WAN and application availability and any planned downtimes. Minimum Service Availability SLA requirements: • 99.5% for all PROD systems • 95% for QAS and DEV systems Monthly maintenance window is defined as 4 hours per month.
C7.4.2 Data backup and replication	Minimum data protection SLA requirements: • Local backup retention period: 1 month for production, 14 days for non-production, or per customer defined requirements • 100% of application data backed up • 100% of application data replicated to an alternate data center • Recovery point objective (RPO): 48 hours • Recovery time objective (RTO): 48 hours
C7.4.3 Incident Reaction Time (IRT)	The amount of time between SAP Support Level 1 is notified of the incident and the first action taken by SAP support person to repair the incident. Minimum IRT SLA requirements: • Priority 1 (Very High): 1 hour (7*24h) • Priority 2 (High): 2 hours (7*24h)

External Reporting

The following section describes the reports that are to be made available to the customer. Example reports must be provided.

Requirement	Description
C7.4.4 Performance analysis reports	Historical performance analysis of the service would typically be available over a number of sample periods (daily, weekly, monthly), and the report would include data to allow the customer to understand how the overall service is performing.
C7.4.5 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.
C7.4.6 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.
Internal Performance Reporting	
The following section describes reports that are to be internally created and reviewed. May be proven by providing an example of reports or demonstration of reporting tool with ability to select reports listed.	
Requirement	Description
C7.4.7 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)

Click here to return to Table of Contents

C8 Hybrid Cloud

Introduced: July 2015
Last updated: May 2017

Overview

Cisco Powered Hybrid Cloud defines a Service Provider offer focusing on the end customers' applications and management thereof more so than the underlying IT resources – computing, memory, and storage. Cisco based software defined data center environments have unique characteristics and capabilities which other clouds do not, specifically around policy based controls and visibility. However third-party, hyperscale public cloud providers as well as unmanaged, private cloud environments will be used for some end customer needs, and the Service Provider can provide application level management of resources in these environments and value-added services too.

Hybrid Cloud is based on the Cisco Application Centric Infrastructure (ACI) design for one or more cloud service environments and one or more tenancy models, which allows application requirements to define the network. This architecture simplifies, optimizes, and accelerates the entire application deployment life cycle.

Combined with Cisco CloudCenter, the CMSP partner is able to more securely deploy and manage applications in private cloud and public cloud environments, with customer, Service Provider, and third-party management options.

This architecture will utilize virtualization, application centric infrastructure, application orchestration and management via Cisco CloudCenter, and likely third-party cloud services to deliver Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) offers supporting hybrid IT.

Note: The Cisco Powered Hybrid Cloud designation does not inherently give a partner access to purchase or deliver restricted data center products. The partner must meet applicable ATP requirements to purchase and deliver restricted data center products.

C8.1 Prerequisites

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

Requirement	Description
C8.1.1 Meet all CMSP partner requirements in Cisco Channel Program Audit and Policies document	See CMSP partner requirements in Cisco Channel Program Audit and Policies document.
C8.1.2 Submit at least two customer references for the service	CMSP partners are required to have a minimum of two customer references, from existing contractual relationships, for each Cisco Powered service. One customer may serve as reference to multiple designations. A customer with multiple sites does not qualify as a second reference however. The intent is to ensure that the partner has proven and repeatable service practices. The partner must submit at least two customer references for the service at the time of the audit, or must provide evidence of the ability to deliver the service to an end customer. In the event that no customer references are available at the time of the audit, two customer references must be provided upon recertification. Refer to Customer Reference Validation template.
C8.1.3 Provide the following documents unique to the service: • Service-Level Agreement • Marketing Service Description • Technical Service Description • Network/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 partner 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 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.
C8.1.4 Employ at least one CCNP Data Center certified individual on staff	The Cisco CCNP Data Center certification is a job-role-focused training and certification program using the following technologies: Cisco Nexus® Switches (1000, 5000, 6000, 7000, and 9000 Series), Cisco UCS® B-Series and C-Series Blade Servers, Cisco UCS Manager, Cisco Data Center Network Manager, Cisco Virtual Network Management Center, and Cisco

	MDS Series Multilayer Switches. A Cisco CCIE certification, of any technology specialization, supersedes and fulfills the certification requirements for this service. Refer to Cisco Certifications for more information.
C8.1.5 Audit representation	If the partner has contracted Cisco Services or a third-party cloud builder to design or build the Hybrid Cloud, providing some or all of the requirements, at the partner's discretion, the third party may participate in the audit and provide evidence on how the requirements they have provided are fulfilled. If the partner has contracted for Cisco Services to operate the Hybrid Cloud, providing some or all of the requirements, at the partner's discretion, Cisco Services may participate in the audit and provide evidence on how the requirements have been fulfilled.

C8.2 Partner System / Solution Requirements (Build)

Service Provider Cloud Capabilities

The following section describes the basic functions of the Service Provider's cloud infrastructure service as a foundation to Hybrid Cloud.

The partner 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.

Requirements	Description
C8.2.1 Application Centric Infrastructure (ACI) Fabric Architecture	The data center network design must conform to the Cisco Application Centric Infrastructure (ACI) Fabric Architecture. The ACI fabric includes Cisco Nexus 9000 Series switches with the Application Policy Infrastructure Controller (APIC) to run in the leaf/spine ACI fabric mode. These switches form a "fat-tree" network by connecting each leaf node to each spine node; all other devices connect to the leaf nodes. The APIC manages the ACI fabric.
C8.2.2 Application Policy Infrastructure Controller (APIC)	The minimum configuration for the APIC is a cluster of three replicated hosts. The APIC is responsible for fabric activation, switch firmware management, network policy configuration, and instantiation.
C8.2.3 Data Center WAN Edge design	Data Center WAN Edge routers provide networking capability for services such as Internet, L3VPN, and L2VPN services. Edge routers are connected to leaf nodes in the ACI architecture. The partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural or topology diagrams.
C8.2.4 Cisco Unified Computing System	The Cisco Unified Computing System (Cisco UCS) is the next-generation data center platform that unites network, compute, and virtualization resources in a seamless system. The partner must present evidence of how this requirement is delivered on a Cisco UCS platform.
C8.2.5 Services Layer	Network-based services may be multi-tenant, multi-context capable, and provide per-customer security control. Alternatively, they could be per-customer, discrete, and virtualized. When multi-tenanted, a resilient framework is also required. The Services Layer can be based on the Cisco VMDC architecture or the Cisco Application Centric Infrastructure. The partner must provide evidence that all of the following functions are delivered on a Cisco platform: • Firewall • Intrusion Prevention System (IPS) • Encryption / VPN

	And the partner must be able to provide the following functions: • Load balancing The partner must explain how resiliency is achieved in this layer using a document such as an architectural diagram.

Virtualization Requirements	
Virtualization is the abstraction of network, compute, and storage resources. This functionality is critical in enabling the dynamic, on-demand characteristics of IT resources delivered from the cloud. It is enabled through the capabilities of Cisco as well as our key technology partners. The Service Provider partner must provide evidence that their services incorporates the key aspects described here and utilizes Cisco technology partner solutions that have been tested as part of the architecture.	
Requirement	Description
C8.2.6 Network Virtualization	Segmenting a common network into separate virtual networks, providing logical separation of data-plane and some control-plane functionality in order to achieve customer traffic separation is required. There can be several forms of network virtualization: • Virtual LANs (VLANs): Separate L2 LAN broadcast domains. • VX LAN: Separate L2 LAN broadcast domains. • Virtual Routing Forwarding (VRFs): Separate L3 routing domains. • Virtual Private Networks (VPNs): Virtual point-to-point connection across a shared network. • Virtual appliances: Network services, such as firewalls, load balancers, and routers, can be delivered using physical or virtualized appliances • Secure Domain Routers (SDRs): Creating separate logical routers, isolated from each other in terms of their resources, performance, and availability • Virtual Device Contexts (VDCs): Logical separation of processes that enables the collapsing of multiple logical networks into a single physical infrastructure The partner must explain how virtualization is used within their service design to allow segmentation of a device into separate logical entities and to isolate/separate the user/tenant traffic within individual network domains. Additionally, evidence must be provided how this requirement is delivered on a Cisco platform or platforms, such as architectural or topology diagrams.
C8.2.7 Server virtualization	Hardware assisted virtualization is used to simulate a complete hardware environment, or Virtual Machine (VM), in which an unmodified "guest" operating system executes in complete isolation. Multiple virtual compute environments can be activated and executed on a single hardware platform. The partner must provide evidence how server virtualization is implemented in their service design using a hypervisor such as Microsoft Hyper-V, VMware vSphere, or KVM. The partner has the option of deploying services utilizing dedicated or bare metal servers, in which server virtualization is not required. The partner must present evidence of how are delivered on Cisco UCS, such as architectural or topology diagrams.
C8.2.8 Storage virtualization	Storage virtualization allows storage location independence by abstracting the physical location of the data. Storage area networks (SANs) can also be virtualized into zones and Virtual SANs (VSANs) if based on FC or FCoE. VLANs and other Ethernet-based virtualization may be used for iSCSI and NFS-based connectivity. The partner must present evidence of how the virtualization system provides the user a logical space for data storage and then handles the process of mapping it to the actual physical location, allowing the physical data to be stored remotely without the user needing to be aware of its actual location. The partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural or topology diagrams.

Cloud Infrastructure Services Requirements	
This section describes the service capabilities of the Service Provider's cloud infrastructure service as a foundation to Hybrid Cloud. The partner must provide evidence how their service offerings use these capabilities to deliver differentiated services and must allow the customer flexibility to self-provision and manage server capacity based on some or all of the characteristics listed.	
Requirement	Description
C8.2.9 Virtual machine sizing	Service profiles based on different compute, storage, and memory capacity. These can be pre-configured for the customer, such as small, medium, and large VMs or could allow for individual resource size selection. Service profiles can be made available for the customers to select themselves via a web portal as needed.
C8.2.10 Storage	The service profiles can be differentiated based on the types of storage capabilities provided, like RAID levels, disk types and speeds, backups, and snapshot capabilities.
C8.2.11 Service offer tiers	Service bundles can offer differentiated support where different service profiles can have different layers or tiers of VMs and potentially different levels of redundancy and load balancing.
C8.2.12 Quality of Service (QoS)	The partner must provide evidence of how the features of their solution that ensure Quality of Service can be maintained for the IT resources being managed; examples include: • Classification of traffic • Ability to prioritize resources allocated to different resources • Ability to allocate resources such as allocating bandwidth according to priorities set • Load balancing of traffic across servers
Cloud Management Framework Requirements	
Cloud management is a complex task that requires the management of real and virtual resources as well as management of the people and processes that enable the data center to function. The following section defines a framework that includes the key management functions and processes required regardless of the architectural design, including the Service Orchestration capabilities required to deliver the service. Service Orchestration includes consistent technology architecture, a structured approach to data collection and processing as well as automation wherever possible to minimize human intervention. This enables a portal-based configuration model in which the subscriber can pick from a limited number of customized service options.	
Requirement	Description
C8.2.13 Infrastructure services	The management framework must incorporate these key functions to manage the infrastructure: • Virtual machines: Memory, CPU, capacity management, and storage allocation • Network virtualization: virtual network interface cards, IP addresses • Storage: Multi-pathing, storage classification and tiers, and storage volume management Recommended functions that may be offered as part of the service: • Site Selection: Intra- and inter-site workload mobility, global address management (IP and DNS), burst, failover, proximity • Virtual network management: VLAN, VRF, SVI, virtual context, virtual address, virtual firewalls, load balancers, VPN, QoS, ACL filtering • Data migration: VM migrations from physical to private cloud and/or public cloud, application data replication • APIs: Notifications, approval billing, chargeback, utilization, IP address management, accounting, SLA management, and cloud identity tools • Data protection: backup (onsite, offsite), disaster recovery The partner must present evidence of how these requirements are delivered via a demonstration.
C8.2.14 Cloud application management	The partner must implement Cisco CloudCenter to facilitate deployment and management of cloud workloads. An IT Services Managed (ITSM) may or may not be used as the user interface.

	Evidence for this requirement would include a MSD for application-centric cloud services and a demonstration of the user experience.
C8.2.15 Multi cloud support	Multi cloud support allows partners to provide workload secure workload deployment and management across multiple cloud environments. The partner must utilize Cisco CloudCenter to facilitate secure deployment and management of applications between two distinct cloud deployment models with at least one of these being the provider managed infrastructure described above. Example cloud deployment models are private, virtual private, and public clouds. Evidence for this requirement would include a MSD for multi cloud services, supporting multiple cloud deployment models in addition to a topology diagram showing the connectivity between two or more physically separated cloud environments.

C8.3 Customer Requirements

Not applicable

C8.4 Service-Level Management Requirements (Operate)

Service-Level Agreement (SLA) Components

This section describes the SLAs 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 SLAs may also be presented as evidence of meeting these requirements.

Requirement	Description
C8.4.1 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.
C8.4.2 Mean Time to Restore Service (MTRS)	If there is a disruption to the performance or availability of resources allocated to a customer, the partner must provide an expectation of restoration time. May vary according to customer agreements. MTRS, also known as Mean Time to Restore (MTTR), measures the total elapsed time from the start of a service outage to the time the service is restored. 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
C8.4.3 Service Availability	Provide evidence of which service availability elements are covered by the SLA components agreed with customer and how different Operating-Level Agreement (OLA) components are measured and managed: • Infrastructure SLA • Network SLA (the network operated by the partner that is used to provide connectivity from the Internet or VPN, and the data center itself): A third party could provide network connectivity. Appropriate documentation must be provided to demonstrate how the Underpinning Contracts (UCs) are measured and managed between partner and third party.

	Seamless SLA (end-to-end service experience): Where elements of the end-to-end service are provided by a third party, appropriate documentation must be provided to demonstrate how the Underpinning Contracts (UCs) are measured and managed between partner and the third party.

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.

The portal can be provided using Cisco Prime Services Catalog, Windows Azure Pack Tenant Portal (WAP), or a third-party portal product. A demonstration of portal from customer viewpoint must be provided as evidence of the following requirements; including real-time views of connectivity and status.

Requirement	Description
C8.4.4 Status and performance	Partner must provide an operational view for each customer, designed to give a view of the service status, including current availability and performance.
C8.4.5 Self-provisioning of virtual machines	Depending on business needs/objective, this function can be provided by the partner on behalf of the customer. If the customer is performing this function, the partner must provide the ability for the customer to be able to view and manage their virtual resources via a customer portal including: • Memory • Processing power (number of processors) • Storage • Network The management process of adjusting/changing VM resources must be provided such that the time to enable new servers or to change attributes is measured in hours or days. If the partner is managing the creation/changes to VM resources, the partner must provide evidence of the process used to do so. The partner must explain how these requests are measured, tracked, and managed.
C8.4.6 Service overview	The partner's customer portal typically provides the following capabilities: • Customer contacts allow to communicate with the partner regarding service changes/ordering, accounting and billing, managing the list of authorized contacts • Assignment of network resources and security options such as IP pools, VLANs, and security policies • Assignment of Virtual Machines with standard and customized builds (OS, IP addressing, CPU, memory, cloning) • Assignment of storage service class, storage allocation, and utilization • Accounting and SLA management The customer portal could either be a partner owned/branded or a third-party white-labeled solution. If the partner does not provide a customer portal, the partner must explain as to how above capabilities are provided to customers.

External Reporting

The following section describes the reports that are to be made available to the customer via customer portal, at the time that this is supported from the Cisco ACI Fabric architecture.

Example reports must be provided or a view of customer web portal with ability to select reports listed.

Requirement	Description
C8.4.7 Performance analysis reports	Historical performance analysis of the service would typically be available over a number of sample periods (daily, weekly, monthly), and the report would include data to allow the customer to understand how the overall service is performing.

C8.4.8 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.
C8.4.9 Resource inventory reports	Reports of resources under management for the customer provide data that is relevant to the customer for managing their IaaS subscription and understanding what resources are available for their use and have been used historically.
C8.4.10 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.
Internal Performance Reporting	
The following section describes reports that are to be internally created and reviewed. May be proven by providing an example of reports or demonstration of reporting tool with ability to select reports listed.	
Requirement	Description
C8.4.11 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)

Click here to return to Table of Contents

C9 Cisco Spark SP

Introduced: May 2017
Last Updated: November 2017

Overview

Cisco Powered Cisco Spark SP addresses the full spectrum of enterprise collaboration requirements across messaging, meetings, and calling delivering a rich yet simple, secure and unified end-user experience.

Cisco Spark SP partners recognize the strategic advantage and resulting differentiation of providing customers an end-to-end collaboration solution based on both cloud delivered and Service Provider hosted functions. They provide the applications, platform operations, management and support, network access, licenses and end points as a unified solution, bundled together in a service wrapper and SLAs that only a SP partner can offer. This differentiates their business-critical services from over-the-top, unmanaged, point solutions while delivering exceptional end user experiences to a vast number of endpoint devices. An all-in Cisco collaboration solution helps SPs increase the ARPU while delivering the best collaboration experience in the industry.

Cisco Spark SP partners share Cisco's vision of utilizing the cloud, allowing very rapid releases of new features and an ever-enhancing user experience. They share Cisco's vision to bring rich collaboration productivity tools and the best meeting experience into every interaction, every meeting room, desktop and pocket. Enabling both 1:1 and team-based interactions, Cisco Spark SP partners deliver a unified collaboration experience including enterprise-grade UC through HCS to the rich features sets of Cisco Spark including team-based persistent messaging, collaborative whiteboarding, and rich audio and web conferencing. As the foundation for communications-enabled business automation, the Cisco Spark platform allows partners to be the innovator through a rich set of API's and business application integrations.

Note: The Cisco Powered Spark SP service designation does not inherently give a partner access to purchase or deliver restricted data center products. The partner must meet applicable ATP requirements in order to purchase such restricted products.

C9.1 Prerequisites

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

Requirement	Description
C9.1.1 Meet all CMSP partner requirements in Cisco Channel Program Audit and Policies document	See CMSP partner requirements in Cisco Channel Program Audit and Policies document.
C9.1.2 Submit at least two customer references for the service	CMSP partners are required to have a minimum of two customer references (existing contractual relationships) for each Cisco Powered service to validate service offering requirements. One customer may serve as reference to multiple designations. A customer with multiple sites does not qualify as a second reference. The intent is to ensure that the partner has proven and repeatable service practices. The partner must submit at least two customer references for the service at the time of the audit, or must present evidence to the ability to deliver the service to an end customer. In the event that no customer references are available at the time of the audit, two customer references must be provided upon recertification. Refer to Customer Reference Validation template.
C9.1.3 Provide the following documents unique to the service: • Service-Level Agreement • Marketing Service Description • Technical Service Description • Architectural 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 partner 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 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. The Technical Service Description (TSD) provides documentation on how capacity is managed related to the delivery of this service. This may be either an externally or internally published document.

	The architectural diagram(s) must show how the service is delivered and through what network connections and devices communications traffic will flow.
C9.1.4 Have a commercial agreement in place with Cisco	Spark SP requires a contractual commitment between the partner and Cisco which outlines the business and licensing relationship between the parties. The primary document covers the partner reselling Cisco products and services, generally called the Cisco Reseller Agreement. The rest depend on the specific product/features to be resold and can include the Cisco Spark Flex Plan Addendum, the Cisco HCS Addendum and the Cisco ELA 2.0 Terms and Conditions. The partner must provide evidence of these agreements.
C9.1.5 Be enrolled in Cisco's Software-as-a-Service Subscription Resale Partner Program	The partner must be accepted in the Software-as-a-Service Subscription Resale Partner Program, specifically the Resale with Lifecycle Management track. This program can be enrolled and approved at within Cisco's Partner Program Enrollment (PPE) tool. Refer to http://www.cisco.com/go/saassubscriptions for more information, including the program Terms and Conditions.
C9.1.6 Have a Customer Success practice	Customer Success is the function within a Service Provider organization responsible for managing the relationship between the partner and its customers. The goal of customer success is to maximizing the value the customer generates from utilizing the Service Provider's solutions, while enabling the Service Provider to derive high return from the customer value. Partner must provide evidence of inclusion in the Cisco Lifecycle Adoption program or a Customer Success practice discreet from reactive customer support. For the latter, such evidence includes dedicated staffing details, processes related to the practice, and metrics of performance.
C9.1.7 Employ at least one CCNP Collaboration certified individual	As part of the partner's Collaboration Architecture Specialization, the CCNP Collaboration validates the ability to plan, implement, verify, and troubleshoot local and wide-area enterprise networks. Additionally, they have the skills and expertise to work collaboratively with specialists on advanced security, voice, and video solutions. A Cisco CCIE certification, of any technology specialization, supersedes and fulfills the certification requirements for this service. Refer to Cisco Certifications for more information.
C9.1.8 Audit representation	If the partner has contracted Cisco Services or a third-party cloud builder to design or build the Spark SP platform, providing some or all of the requirements, at the partner's discretion, the third party may participate in the audit and provide evidence on how the requirements they have provided are fulfilled. If the partner has contracted for Cisco Services to operate the Spark SP platform, providing some or all of the requirements, at the partner's discretion, Cisco Services may participate in the audit and provide evidence on how the requirements have been fulfilled.

C9.2 Partner System/Solution Requirements (Build)

Service Capabilities

Cisco Powered Cisco Spark SP requires the Service Provider partner to offer a suite of collaboration services, including calling, messaging, meeting, and conferencing, each of which being video enabled.

Several other services are highly recommended for profitability and differentiation, but are considered optional.

The partner must provide evidence of each productized offering through the documentation referenced in C9.1.3.

Requirement	Description
C9.2.1 Call control from UC as a Service based on HCS	Call control capabilities are delivered from the Service Provider partner's owned and operated infrastructure. UC as a Service based on HCS (HCS) must be built and audited per section C2 of this document.

C9.2.2 Cisco Spark messaging	Cisco Spark messaging provides always-on messaging, delivered from the Cisco Cloud. The partner is responsible for enabling users with the right messaging bundles and/or providing customers' administrators access to the management portal to provision and entitle their users.
C9.2.3 Cisco WebEx	Cisco WebEx is the industry's premier video conferencing service. Conferences can be securely joined nearly any browser and a multitude of devices. At a minimum, the partner must offer Cisco WebEx Meeting Center, but may opt to provide additional services around Cisco WebEx Event Center, Cisco WebEx Training Center, and/or Cisco WebEx Support Center. Cisco WebEx is delivered from the Cisco Cloud. The partner is responsible for enabling users with the right meeting bundles and/or providing customers' administrators access to the management portal to provision and entitle their users.
C9.2.4 Cisco WebEx Cloud Connected Audio	The partner must implement the Cisco WebEx Cloud Connected Audio Service Provider (CCA-SP) architecture whereby the partner peers with the Cisco and provides the transport and access (phone numbers) while Cisco provides audio bridging from the Cisco Cloud.
C9.2.5 Soft client	Today's work environments typically involve workers accessing corporate resources and services from various locations. Cisco provides several software clients that allow the partner to enable customers to access voice and video services while away from their corporate desktop device. The partner must support at least one of these two options: • Cisco Spark client: persistent messaging, meetings and audio/video calling • Cisco Jabber: instant messaging and audio/video calling
C9.2.6 Cisco Spark Board (optional)	Cisco Spark Board allows enterprise users to wirelessly present, white board, and participate in video/audio conferencing at the touch of a finger. Partners can differentiate their collaboration offering by providing enablement and management services for Cisco Spark Board.
C9.2.7 Cisco Spark Room (optional)	Enabling room conferencing and collaboration for small and large audiences, Cisco Spark Room Kits integrate with smart panel displays and offer sophisticated camera technology with speaker-tracking capabilities. Partners can differentiate their collaboration offering by providing enablement and management services for Cisco Spark Board.
C9.2.8 Hybrid Media Services (optional)	Hybrid Media Services integrate non-Cisco Spark applications, such as HCS calling platform, enterprise calendaring, and Microsoft Active Directory, with Cisco Spark to provide a more cohesive user experience to end users. Additionally, Service Provider managed infrastructure can be used to keep media, such as video or attachments, off of the public network and on the managed enterprise and or Service Provider network. Partners can establish a practice around providing Hybrid Media Services to offer optimized and managed services to their customers, offering greater profitability and differentiation.
C9.2.9 Spark care (optional)	Cisco Spark care is a digital customer support solution for help desks and small teams. It enables connected digital experiences by supporting customer care teams that want to deliver contextual, continuous, and capability-rich journeys to external or internal customers. Cisco Spark care can quickly be embedded on your website to offer chat and callback services. Cisco Spark care includes a customer care agent workspace and integrated reporting with customer feedback to improve help desk productivity and effectiveness. Partners can establish services around Cisco Spark care to increase their profitability and differentiation.

C9.3 Customer Requirements

Customer Collaboration Environment

In the case of premises based applications, each customer is supported with a unique instance of the required applications.

The partner must be able to explain the design solution for a typical customer, products deployed and benefits of the Cisco Spark SP 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
C9.3.1 Customer premises layer	This layer connects customer endpoints (video endpoints, phones, mobile devices, local gateways, etc.) to the IP network. Customer premises are deployed with Survivable Remote Site Telephony (SRST) CPE, switch and end devices only. If using HCS for call control, the partner must present evidence that the design of the customer premises solution incorporates SRST, and the partner must demonstrate they can articulate the benefits of using a Cisco based solution.
C9.3.2 Customer migration plan	The partner must present evidence of their capability to build a clear migration plan that allows the customer to move over to the new service while interoperating with existing services. 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.

C9.4 Service-Level Management Requirements (Operate)

Service-Level Agreement (SLA) Components

This section describes the SLAs 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 SLAs may also be presented as evidence of meeting these requirements.

Requirement	Description
C9.4.1 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 is notified. Notification can be delivered by any method of communication agreed with the customer.
C9.4.2 Mean Time to Restore Service (MTRS)	If there is a disruption to the performance or availability of resources allocated to a customer, the partner 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
C9.4.3 Existing user changes	Changing a user profile may be the responsibility of the partner, or the customers may be given access to do this themselves. If the customer carries out these changes, the partner must present evidence of how

	access is provided. If changes are the responsibility of the partner, a published service description or an example of existing customer documentation must be provided showing what agreement is in place for how quickly user changes will be implemented.
C9.4.4 User addition to service	The addition of new users may be the responsibility of the partner or of the customer. If the customer carries out these changes, the partner must provide evidence of how access is provided. If changes are the responsibility of the partner, a published service description or an example of 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. This 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 partner must also be able to demonstrate that audit logs can be stored and made accessible.	
Requirement	Description
C9.4.5 Role-based service 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 Spark SP resources. The partner must demonstrate the provided portal and how various user roles are implemented.
C9.4.6 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.
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 a customer web portal with the 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.	
Requirement	Description
C9.4.7 Service availability reports	Provide a summary view of service availability which may allow for details down to specific sites and/or equipment.
C9.4.8 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.
C9.4.9 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.	
Requirement	Description
C9.4.10 Customer-related reports with internal performance metrics	Generate 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

Click here to return to Table of Contents

Cisco Powered Cloud Managed DNA Services

Cisco provides a portfolio of cloud-based, managed services solutions to Service Providers, allowing them to deliver business services in a dynamic, on-demand, and automated manner. In contrast with traditional managed services, cloud managed services utilize cloud infrastructure, network functions virtualization (NFV) and software defined networking (SDN) technologies, enabling Service Providers to offer automated and secure services including managed WAN, managed CPE, managed security, and other business services to their end customers.

Cisco Powered Cloud Managed DNA Services is defined as a category of managed services that have following key attributes:

- Based on Cisco Digital Network Architecture (DNA);
- The services are delivered and managed from the Service Providers' or Cisco's data centers;
- The services are delivered by Cisco physical network functions / appliances and/or Cisco virtual network functions (VNFs);
- The services are orchestrated by Cisco orchestration software or services such as Cisco network orchestration or Cisco security orchestration software hosted by Service Providers or Cisco;
- Cisco customer premise equipment (CPE), such as an Integrated Services Router (ISR) or Cisco Enterprise Network Compute System (ENCS), if CPE is required for a particular service;
- Cisco Network Function Virtualization Infrastructure (NFVI), whether in data centers, POPs, and/or customer premises, may be used to deploy the orchestration software platform or virtualized network functions (VNFs) required for the services.

This section describes the detailed requirements for each Cisco Powered Cloud Managed DNA Service.

D1 Cloud Managed SD-WAN

Introduced: February 2017
Last updated: November 2017

Overview

Cisco software defined wide area networking (SD-WAN) technologies, including Cisco Intelligent WAN (IWAN), Cisco Meraki cloud managed SD-WAN, and Cisco SD-WAN (Viptela), provide Service Providers with solutions to deliver automated, hybrid WAN services to business customers. Service Providers can deploy Cisco-based managed SD-WAN services in a traditional per-tenant and on-premise manner. Section M11 of this document defines the requirements for Cisco Powered Managed IWAN, aligning to the delivery of this service as a traditional CPE managed service offer. This section defines the requirements of the Cisco Powered Cloud Managed SD-WAN designation to support the cloud based, multitenant managed service offer.

The Cisco Powered Cloud Managed SD-WAN service is a suite of managed SD-WAN solutions delivered and managed from the Service Provider's cloud by using Cisco cloud orchestration solutions or using Cisco Meraki solution, delivered from the Cisco Cloud. The end customers are consuming a set of SD-WAN services such as hybrid WAN, performance routing, load balancing, application visibility and control from a Service Provider similar to traditional managed IWAN as defined in M11. The differences in the cloud managed SD-WAN services versus traditional managed IWAN services is that Service Providers are able to deliver SD-WAN at a higher scale, with more efficiency, and in a more automated fashion by utilizing Cisco cloud service orchestration or Cisco Meraki cloud managed networking service. The end customers will gain additional self-service capabilities for configuring, monitoring, and reporting via a cloud based service portal.

Cisco Powered Cloud Managed SD-WAN can be delivered by using one of several solutions from Cisco, including deploying Cisco Virtual Managed Services (VMS) Platform with the IWAN service and CPE orchestration packages or deploying Cisco Network Services Orchestrator (NSO) with an IWAN function pack. The IWAN function pack can be either delivered by Cisco as a part of the solution, or be developed by a Service Provider for its own unique IWAN service offering.

Cisco Powered Cloud Managed SD-WAN can also be offered by a partner by using Cisco Meraki cloud managed SD-WAN solution or Cisco SD-WAN (Viptela).

Regardless of which Cisco solution is deployed, Cisco Powered Cloud Managed SD-WAN services must use a Cisco CPE such as an ISR G2 series, ISR 4000 series, CSR 1000V series, ENCS 5400 series with ISRv, Meraki MX or vMX. vEdge or ISR4000 series with vEdge software. When additional virtualized network functions (VNFs) are used to deliver value-added services such as Wide Area Application Services (WAAS) or security, these VNFs can be deployed on Cisco NFV infrastructure (NFVI) or Cisco virtualized CPE such as the ENCS 5400 series.

Note: The Cisco Powered Cloud Managed SD-WAN Service designation does not inherently give a partner access to purchase or deliver restricted data center products. The partner must meet applicable ATP requirements in order to purchase such restricted products.

D1.1 Prerequisites

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

Requirement	Description
D1.1.1 Meet all CMSP partner requirements in Cisco Cloud and Managed Services Program Audit and Policies document	See CMSP partner requirements in Cisco Channel Program Audit and Policies document.
D1.1.2 Submit at least two customer references for the service	CMSP partners are required to have a minimum of two customer references, from existing contractual relationships, for each Cisco Powered service. One customer may serve as reference to multiple designations. A customer with multiple sites does not qualify as a second reference however. The intent is to ensure that the partner has proven and repeatable service practices. The partner must submit at least two customer references for the service at the time of the audit, or must provide evidence of the ability to deliver the service to an end customer. In the event that no customer references are available at the time of the audit, two customer references must be provided upon recertification. Refer to Customer Reference Validation template.
D1.1.3 Provide the following documents unique to the service: • Service-Level Agreement • Marketing Service Description • 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 partner must provide an actual SLA with an existing customer or SLAs for multiple customers. The Marketing Service Description 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. The architectural diagram(s) must show how NFVI, CPEs, service orchestration, service portal and service assurance are deployed and how the service is delivered over the provider's network.
D1.1.4 Maintain at least one CCNP Service Provider certified individual and at least one Certified Meraki Networking Associate (CMNA) on staff when offering Meraki SD-WAN.	The Cisco Certified Network Professional Service Provider (CCNP Service Provider) certification is for Service Provider network engineers, systems engineers, and network specialists who are responsible for delivering a scalable carrier-grade infrastructure capable of rapid expansion to support ongoing introduction of new managed services and other customer requirements. A Cisco CCIE certification, of any technology specialization, supersedes and fulfills the certification requirements for this service. Certified Meraki Networking Associate (CMNA) certification validates the necessary technical capabilities needed to manage Cisco Meraki devices and services. For information, visit Cisco Certifications and Cisco Meraki CMNA certification.
D1.1.5 Audit representation	If the partner has contracted Cisco Services or a third party to design, build, and/or operate a Cloud Managed SD-WAN service, at the partner's discretion, Cisco Services or the third party must participate in the audit and provide evidence on how the requirements have been fulfilled.

D1.2 Service Design (Build)

Service Capabilities

Cisco Cloud Managed SD-WAN enables partners to offer hybrid WAN using MPLS, Internet, mobile network, intelligent path control using performance routing (PfR) or policy based routing, application visibility and application optimization based on application aware quality of service (QoS) and traffic management, and secure VPN overlay with encryption.

A partner has several options to deliver SD-WAN services, either by using Cisco IWAN technology with Cisco network service orchestration and Cisco CPE, Meraki cloud managed SD-WAN with Meraki MX as CPE, or Cisco SD-WAN based on Viptela and Cisco CPE.

This section structures the service design requirements into three sub-sections: Cisco IWAN technology based cloud managed SD-WAN, Cisco Meraki cloud managed SD-WAN, and Cisco SD-WAN based on Viptela.

A partner has an option to consume Cisco Cloud Managed SD-WAN as a service that is operated and managed by Cisco and deliver SD-WAN service to its end customers. In that case, the following cloud orchestration requirements in this section are satisfied.

Requirements	Description
D1.2.1	This sub-section describes the requirements (D1.2.1.1 – D1.2.1.9) for Cisco Powered Cloud Managed SD-WAN based on Cisco IWAN technology.
D1.2.1.1 Manage the Path Control or Performance Routing Master Controller	For all IWAN deployments, the partner must host the Path Control or Performance Routing Master Controller in their cloud environment or manage as a dedicated platform at the customer premise. Cisco Performance Routing (PfR) consists of border routers (BRs) that connect to the dynamic multipoint virtual private network (DMVPN) for each carrier network and a master controller (MC) application process that enforces policy. The MC defines the IWAN domain and the hub MC is the platform singled out in this requirement.
D1.2.1.2 Manage the WAAS Central Manager	For WAN Optimization subscribers, the partner must host virtual WAAS Central Manager in their cloud environment or WAAS Central Manager on a dedicated WAVE appliance with an option for a redundant configuration. Central Manager provides the following functionality: • Manages central configuration, provisioning, monitoring, fault management, logging, and reporting for up to 2500 WAVEs within a Cisco WAAS topology • Comprehensive statistics: Comprehensive logs, reports, graphs, and statistics for Cisco WAVE device functions help IT administrators to optimize system performance and troubleshooting Monitoring, reporting, and alerts: The option for a redundant configuration would provide active/standby deployment with automatic failover, replication of Central Manager database and encryption keys.
D1.2.1.3 SD-WAN service capability requirements	Cloud Managed SD-WAN must deliver the same service capabilities as defined Cisco Powered Managed IWAN M11.2.1 to M11.2.18 in section M11. The mandatory and optional Managed IWAN requirements apply to Cloud Managed SD-WAN.
D1.2.1.4 Cloud orchestration software	The Cisco cloud orchestration is a core capability Cloud Managed SD-WAN service. A Service Provider deploys the cloud orchestration software in its data center to orchestrate the service capabilities defined in D.1.2.13. It provides service management, configuration, service chain creation, device management, zero-touch deployment of CPE, monitoring and report of IWAN network and application performance. Partner must deploy one of the following cloud orchestration software platforms to meet the cloud orchestration requirement for the designation: • Cisco Virtual Managed Services (VMS): When using Cisco VMS to deliver Cloud Managed SD-WAN services, the partner must use Cisco VMS System Platform software which is responsible for service orchestration and control, VMS device management software for CPE management and zero touch provision and applicable IWAN service function packs. • Cisco Network Services Orchestrator (NSO): Instead of deploying the entire VMS software package, a partner has option to use Cisco Network Orchestrator (NSO) with NSO IWAN function packs to orchestrate the IWAN service. NSO and function packs are used to manage CPE, configure and monitor services. The IWAN function packs could be standard Cisco IWAN function packs developed by Cisco, or customized IWAN function packs developed by Cisco services or by partner or 3rd party, as long as the function packs support the service capabilities as defined in D1.2.1.3 at a minimum. The partner must provide an architecture design, proof of software license, and a demonstration of the Cisco cloud orchestration software as evidence.
D1.2.1.5 Service portal	Cloud Managed SD-WAN shall provide a service management interface or portal for service administrators and end customers to order, manage, monitor and change the services. The service interface must have secure access control based on role

	and must support multi-tenancy capabilities. The partner has an option to deploy Cisco VMS Service Interface as a portal when the VMS platform is chosen as a service orchestration solution. The partner also has the option to use an internally developed portal or 3rd party portal on top of Cisco NSO orchestration layer to manage the service. The partner must demonstrate the Service Portal as evidence for this requirement.
D1.2.1.6 Network Function Virtualization Infrastructure (NFVI) (optional)	Network Function Virtualization Infrastructure consists of virtual infrastructure management (VIM) such as OpenStack, KVM hypervisor or a thin layer of virtualization OS on CPE, computing, storage and network infrastructure. Cisco service orchestration software and virtualized network functions (VNFs) such as WAAS, virtual firewall shall be deployed on NFVI. It is recommended to deploy Cisco service orchestration software and Cisco VNFs on Cisco validated NFVI for best performance. The partner can use service architecture design to demonstrate that Cisco NFVI is used to deploy the services. The partner also has the option to use a 3rd party NFVI that is supported by Cisco orchestration software and Cisco VNFs.
D1.2.1.7 SDN and Virtual Switches (optional)	SDN and virtual switches provide network virtualization function on a server platform. These technologies support service chaining of multiple VNFs over a high-performance data path with multi-tenant capabilities. When a Cloud Managed SD-WAN service uses multiple VNFs to create a service chain, the partner must present the evidence e.g. service architecture design that Cisco certified SDN and virtual switches are deployed in NFV infrastructure. The examples include Cisco Virtual Topology System (VTS) and OVS.
Customer Premise Equipment Requirements	
Cisco Cloud Managed SD-WAN requires CPE for service delivery, and the customer premise equipment orchestration client is required for zero touch deployment. The partner must provide evidence that the following CPE requirements are met to deliver the service.	
Requirement	Description
D1.2.1.8 Cisco customer premise equipment and/or virtual customer premise equipment	To ensure end-to-end service delivery and automation, Cisco Cloud Managed SD-WAN Service requires Cisco CPE and/or virtualized CPE (vCPE). The partner must offer Cloud Managed SD-WAN based on following Cisco CPE and/or virtual CPE: • ISR G2 and ISR 4000 series • ASR 1000 series • ENCS 5400 series with ISRv • CSR1000v series The partner must provide evidence such as service description and network architecture diagrams to demonstrate that Cisco CPE/vCPE are used to deliver the service.

D1.2.1.9 Maintain appropriate licenses on Cisco router platforms	The partner must offer Intelligent WAN services based on one or more of the following appropriately licensed Cisco technologies: • AX license on ISR G2 and ISR 4000 series • AX licenses for ISRs enable both Application Visibility and Control (AVC), PfR Path Control, zone based firewall (ZBFW) and WAAS capabilities at the most economical price point. With the correct initial hardware configuration, they enable upsell of the subscriber to the WAN Optimization service level without a truck roll. • AX or AVC license on a ASR 1000 series router. Because the ASR 1000 does not support WAAS running directly on the router, the AX license for the ASR 1000 offers a discount for the purchase of WAAS physical or virtual appliances to be used in association with the ASR 1000. • Premium license for CSR 1000V • WAN Essential at a minimum on ENCS5400 series platform
Requirements	Description
D1.2.2	This sub-section describes the requirements for Cisco Powered Cloud Managed SD-WAN using Cisco Meraki cloud managed SD-WAN solution.
D1.2.2.1 Hybrid WAN Design	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. The partner must present evidence of how this requirement is delivered to their customers such as an architectural diagram, or via the Meraki dashboard.
D1.2.2.2 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. The Partner must present evidence that AutoVPN is implemented by demonstrating the configuration via the Meraki dashboard.
D1.2.2.3 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 configure 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. The partner must present evidence of how this requirement is delivered to their customers.

D1.2.2.4 Application visibility and reporting (optional)	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. This is an optional service that a partner can offer as part of a managed SD-WAN offer. When doing so, a partner must present evidence via a service description and the Meraki dashboard.
Customer Premise Equipment Requirements	
Meraki based Cloud Managed SD-WAN must meet the following CPE requirements	
Requirement	Description
D1.2.2.5 Cisco customer premise equipment and/or virtual customer premise equipment	Meraki based Cisco Cloud Managed SD-WAN Service requires Cisco CPE and/or virtualized CPE (vCPE). The partner must offer Cloud Managed SD-WAN based on following Cisco CPE and/or virtual CPE: • Meraki MX family, or • Meraki virtual MX (vMX) The partner must provide evidence via the Meraki dashboard.
D1.2.2.6 Maintain appropriate licenses of Meraki SD-WAN	As a minimum requirement, Meraki Enterprise license is required for MX product family for Meraki cloud managed SD-WAN. Meraki Security licenses are optional. Partner must provide evidence that valid licenses are in place for the SD-WAN service using the Meraki dashboard.
Requirements	Description
D1.2.3	This sub-section describes the requirements for Cisco Powered Cloud Managed SD-WAN using Cisco SD-WAN cloud managed SD-WAN solution based on Viptela.
D1.2.3.1 Manage the Cisco vSmart Controller policy engine	For all deployments, the partner must host the Cisco vSmart Controller in the Service Provider datacenter or Service Provider managed public cloud environment. Cisco vSmart Controllers establish secure SSL connections to all other components in the network, and run an Overlay Management Protocol (OMP) to exchange routing, security and policy information. The centralized policy engine in vSmart provides policy constructs to manipulate routing information, access control, segmentation, extranets and service chaining.
D1.2.3.2 Cisco vBond Orchestrator software	Cloud orchestration is a core capability Cloud Managed SD-WAN service. A Service Provider deploys vBond Orchestrator software in its cloud to orchestrate service capabilities. The vBond orchestrator facilitates the initial bring-up by performing initial authentication and authorization of all elements into the network. vBond provides the information on how each of the components connects to other components. The partner must provide an architecture design and a demonstration of the Cisco vBond Orchestration software as evidence.
D1.2.3.3 Service portal	Cloud Managed SD-WAN shall provide a service management interface or portal for service administrators and end customers to order, manage, monitor and change the services. The service interface must have secure access control based on role and must support multi-tenancy capabilities. The partner has an option to deploy Cisco vManage as a portal. The partner also has the option to use an internally developed portal or 3rd party portal on top of the Cisco vBond Orchestration layer to manage the service. The partner must demonstrate the Service Portal as evidence for this requirement.
D1.2.3.4 Application Aware Routing	Application Aware Routing maximizes the value of multiple network paths (like dual MPLS access or dual Service Providers or MPLS + Internet) by allowing the steering of traffic based on SLA requirements of the application. For example, if you have two sites with dual connectivity to MPLS and Internet, data plane modules (located at customer sites) can steer traffic over either the MPLS or Internet transport based on end-to-end latency or drops. They do this by maintaining real-time characteristics of loss, latency and, jitter and then apply policies on the

	centralized controller. Critical traffic is always steered to the most reliable link. The partner must present evidence of how this requirement is delivered to their customers.
D1.2.3.5 Application visibility and reporting (optional)	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 management dashboard. This is an optional service that a partner can offer as part of a managed SD-WAN offer. When doing so, a partner must present evidence via a service description and the management dashboard.

Customer Premise Equipment Requirements

Viptela based Cloud Managed SD-WAN must meet the following CPE requirements

Requirement	Description
D1.2.3.6 Cisco customer premise equipment and/or virtual customer premise equipment	Viptela based Cisco Cloud Managed SD-WAN Service requires Cisco CPE and/or virtualized CPE (vCPE). The partner must offer Cloud Managed SD-WAN based on following Cisco CPE and/or vCPE: • Cisco ISR or ISRv • Cisco vEdge • ISR4000 with vEdge software The partner must provide evidence such as service description and network architecture diagrams to demonstrate that Cisco CPE/vCPE are used to deliver the service.

D1.3 Customer Requirements

Not applicable

D1.4 Service-Level Management Requirements (Operate)

Service-Level Agreement (SLA) Components

This section describes the SLAs that the partner must contract for as part of the service. These are normally available as part of the Marketing Service Description. Existing customer contracts that include the relevant SLAs may also be presented as evidence of meeting these requirements.

If a partner uses Cisco managed SD-WAN as a service, Cisco Meraki service, or Cisco SD-WAN based on Viptela to deliver SD-WAN services to end customers, the partner still owns the responsibility to provide the evidence how the following SLA requirements in this section are met by working with Cisco.

Requirement	Description
D1.4.1 Mean Time to Notify (MTTN)	If the customer experiences any resource or performance-affecting event the partner must notify the customer of the issue. This may vary according to specific customer agreements. MTTN measures the average time taken to notify a customer of an issue. The measurement encompasses the time that an alarm is generated to the time the customer notified, which can be by any method of communication agreed upon with the customer.

D1.4.2 Mean Time to Restore Service (MTRS)	If there is a disruption to the performance or availability of resources allocated to a customer, the partner must provide an expectation of restoration time. This may vary according to specific customer agreements. MTRS measures the total elapsed time from the start of a service outage to the time the service is restored. This is also known as Mean Time to Restore/Repair (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
D1.4.3 Service Availability	Provide evidence of which service availability elements are covered by the SLA components, agreed upon with the customer, and how different Operating-Level Agreement (OLA) components are measured and managed: • Platform SLA: Infrastructure, orchestration and Service Interface level SLAs; • Network SLA (the network operated by the partner that is used to provide connectivity from the Internet or VPN, and the data center itself): a third party could provide network connectivity. Appropriate documentation must be provided to demonstrate how the Underpinning Contracts (UCs) are measured and managed between partner and third party. • End-to-End Service SLA: Where elements of the end-to-end service are provided by a third party, appropriate documentation must be provided to demonstrate how the Underpinning Contracts (UCs) are measured and managed between partner and the third party.

Customer Service Portal

The following section describes the online capabilities 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 the customer viewpoint, including a real-time view of connectivity and status. Security mechanisms should include password protection or two-factor authentication, used to restrict access to the portal to authorized individuals.

Whether the partner choses to deploy Cisco VMS portal or use an internally developed customer portal or 3rd party customer portal, the partner must provide the portal demonstration as evidence to meet the following requirements.

If a partner chooses to consume a service that is operated and managed by Cisco to deliver SD-WAN service to its end customers, or use Cisco Meraki to deliver the SD-WAN service, the following customer web portal requirements in this section are satisfied.

Requirement	Description
D1.4.4 Customer web portal requirements	Provide a secure customer web portal that meets the equivalent customer portal requirements defined in Cisco Managed IWAN M11.3.4 – M11.3.13, section M11.
D1.4.5 Secure multi-tenant capability	Provide secure multi-tenant portal to customers based on customer identity and roles. Ensure secure separation of each customer's data related to the service.

Click here to return to Table of Contents

D2 Cloud Managed Security

Introduced: May 2014
Updated: May 2017

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 partner to obtain Cisco Powered accreditation.

Cloud Managed Security allows the provider to leverage hosted SaaS 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 (TTM) for security services.

Cloud Managed Security is based on Cisco security technologies and provides a partner the opportunity to create subscription-based "as a service" offers utilizing hosted and managed models. The partner 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.

D2.1 Prerequisites

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

Requirement	Description
D2.1.1 Meet all CMSP partner requirements in Cisco Channel Program Audit and Policies document	See CMSP partner requirements in Cisco Channel Program Audit and Policies document.
D2.1.2 Submit at least two customer references for the service	CMSP partners are required to have a minimum of two customer references, from existing contractual relationships, for each Cisco Powered service. One customer may serve as reference to multiple designations. A customer with multiple sites does not qualify as a second reference however. The intent is to ensure that the partner has proven and repeatable service practices. The partner must submit at least two customer references for the service at the time of the audit, or must provide evidence of the ability to deliver the service to an end customer. In the event that no customer references are available at the time of the audit, two customer references must be provided upon recertification. Refer to Customer Reference Validation template.
D2.1.3 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 partner must provide an actual SLA with an existing customer or SLAs for multiple customers. The Marketing Service Description 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. The architectural diagram(s) must show how the compute, storage, and networking components are connected along with how a customer will gain access to services via network connectivity.
D2.1.4 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 CCNP Security professional demonstrates the skills required to secure and manage network infrastructures to protect productivity, mitigate threats, and reduce costs. The curriculum emphasizes Cisco Secure Access solution (TrustSec / ISE), network perimeter security solution based on Cisco Adaptive Security Appliance (ASA) or IOS routers, secure VPN connectivity, Intrusion Prevention Systems (IPS), Web and Email Security Solution as well as techniques to optimize these technologies in a single, integrated network security solution. A Cisco CCIE certification, of any technology specialization, supersedes and fulfills the certification requirements for this service.
D2.1.5 Audit representation	If the partner has contracted Cisco Services or a third-party cloud builder to design

	or build the Cloud Managed Security platform, providing some or all of the requirements, at the partner's discretion, the third party may participate in the audit and provide evidence on how the requirements they have provided are fulfilled. If the partner has contracted for Cisco Services to operate the Cloud Managed Security platform, providing some or all of the requirements, at the partner's discretion, Cisco Services may participate in the audit and provide evidence on how the requirements have been fulfilled.
D2.1.6 Point of sale (POS) reporting	Partners must provide monthly detailed Point of Sale (POS) and customer usage data, including the end customer name, must be provided to Cisco to support the Cisco sales compensation plan. Partners must enroll into the Cloud Compensation Program via the Partner Program Enrollment (PPE) tool after completing the audit process.
D2.1.7 Dedicated Security Operations Center (SOC)	Partner must document the existence of a Security Operations Center (SOC) for incident prevention, detection, and response capabilities. The partner must provide documentation of security event detection, escalation, and remediation processes consistent with their SLA.
D2.1.8 Cloud Orchestration Software	Policy deployment and service orchestration are core capabilities of Cloud Managed Security Services. A Service Provider deploys the cloud orchestration software in its data center 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 Meraki dashboard, Cisco Network Services Orchestrator (NSO), Cisco Defense Orchestrator (CDO), Cisco Firepower Management Console (FMC), and Service Provider or third-party software.

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 partner can deliver using a Cisco based virtualized Cloud Infrastructure.

Requirement	Description
D2.2.1 Must offer at least two security services	The Cloud Managed Security services are aimed at partners offering a range of security capabilities to protect their customer from a variety of security threats. The partner must deliver a minimum of two of the following services: • Firewall as a Service • Next Generation Firewall as a Service • AMP for Network • VPN as a Service • Web Security as a Service • Email Security as a Service • Cisco Cloud Web Security • Cisco Umbrella • Cisco Cloud Email Security • AMP for Endpoints Services must be delivered using any of the following: • Cisco security appliances (e.g. ASA, Firepower, ESA, WSA, or Meraki MX) • Cisco virtual security appliances (e.g. CSR1000v, ASAv, ESAv, WSAv, NGFWv) • Cisco hosted SaaS platforms

D2.2.2 Firewall as a Service Capabilities

The following section describes the basic functions of the Firewall as a Service offering. The partner 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.

If the partner has already achieved Master Security Specialization, the following requirements are waived: D2.2.2.1–D2.2.2.12.

Requirement	Description
D2.2.2.1 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.
D2.2.2.2 Optional support for De-Militarized Zones (DMZs)	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.
D2.2.2.3 Optional support for Private Zones	This security service option is only applicable when Service Provider is delivering IaaS, PaaS, or SaaS. The compute, platform or application services will be delivered from virtual machine provisioned in the private zone.

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 partner 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 partner will need to show that they will have the required expertise to implement these features when demanded by the market.

Requirement	Description
D2.2.2.4 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 corporate zone.
D2.2.2.5 Optional support for user based policy authentication	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.
D2.2.2.6 Optional support for layer 2 (transparent) firewall support	Layer 2 firewall support is a security service option that provides the ability to insert firewall transparently into existing configured cloud environment and restrict traffic across the firewall to specific devices using LAN bridging. Users can allow selected devices from a subnet to traverse the firewall while denying access to other devices on the same subnet.
D2.2.2.7 Optional support for stateful inspection	Stateful inspection of encrypted traffic may be used when customers need to protect

of encrypted traffic	public Internet servers on a DMZ. The firewall first allows encrypted traffic through to the DMZ based on standard rules. The traffic is then unencrypted within the DMZ, and a second pass through a firewall can now inspect the contents of the packets to ensure conformance to policies. After being passed, the traffic can then be re-encrypted and passed on to its destination.

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 partner 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 partner will need to show that they will have the required expertise to implement these features when demanded by the mark.

Requirement	Description
D2.2.2.8 Optional Instant Messenger (IM) blocking	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.
D2.2.2.9 Optional Peer-to-peer control	Peer-to-peer control individually blocks access to BitTorrent, Gnutella, KaZaA, and eDonkey file-sharing networks.
D2.2.2.10 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.
D2.2.2.11 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.
D2.2.2.12 Optional Java blocking	With the proliferation of Java applets available on the Internet, protecting networks from malicious applets has become a key issue for network managers. The Java blocking feature can be configured to filter or completely deny access to Java applets that are not embedded in archives or compressed in files.

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 partner must exhibit an understanding of the capabilities and ensure they are activated.

Requirement	Description
D2.2.2.13 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.
D2.2.2.14 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.
D2.2.2.15 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

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. If the partner has already achieved Master Security Specialization, the following requirements can be waived: D2.2.2.16–D2.2.2.17.	
Requirement	Description
D2.2.2.16 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.
D2.2.2.17 Configuration backup	Storage of configurations of all virtual devices used in the firewall service with ability to provide restoration.
Secure Encrypted VPN 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 partner 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. If the partner has already achieved Master Security Specialization, the following requirements can be waived: D2.2.2.18–D2.2.2.26.	
Site to Site VPN(Optional)	
Requirement	Description
D2.2.2.18 Support for internet site-to-site VPN.	The partner 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 partner hosted security cloud infrastructure. The partner must present evidence of how this is delivered using a Cisco platform such as architectural or topology diagrams.
D2.2.2.19 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 partner must provide evidence that they support one or more of these protocols. The partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural or topology diagrams.
Remote Access VPN (Optional)	
D2.2.2.20 Internet remote access VPN	The partner must offer a remote access VPN termination service from its cloud infrastructure to protect end customer mobile users. The partner must present evidence of how this is delivered using a Cisco platform, such as architectural or topology diagrams.
D2.2.2.21 Remote access IP VPN technologies	The partner must support at least one of the following remote access VPN deployment solution: • Remote access IPsec-based VPN • Remote access SSL-based VPN The partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural or topology diagrams.
D2.2.2.22 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 partner must present evidence of how this requirement is delivered on a Cisco platform, such as architectural or topology diagrams.
D2.2.2.23 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 partner, 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 partner site, a RADIUS server can store all AAA and configuration information, or the information can be split across two servers. For this component, the partner 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 partner 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.	
Requirement	Description
D2.2.2.24 Optional dual VPN gateway support with stateless failover	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.
D2.2.2.25 Optional dual VPN gateway support with stateful failover	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.
D2.2.2.26 Configuration backup	Storage of configurations of all virtual devices used in the firewall service with ability to provide restoration. The partner must present evidence of how this requirement is delivered, such as a screen shot from the configuration backup system.
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, ENCS, or Meraki CPE. Example best practices documents are available at: Cisco Guide to Harden IOS Devices and Meraki MX Security Appliances. 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 if using a Cisco IOS platform. If the partner has already achieved Master Security Specialization, the following requirements can be waived: D2.2.2.27 –D2.2.2.29.	
Requirements for Cisco IOS Devices	Description
D2.2.2.27 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.
D2.2.2.28 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.
D2.2.2.29 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.

D2.2.3 Email Security as a Service Capabilities	
The following section describes the basic functions of Email Security as a service offering. The partner 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 Cloud Email Security or Cisco Email Security Appliance (physical or virtual). If the partner has already achieved Master Security Specialization, the following requirements can be waived: D2.2.3.1 –D2.2.3.10.	
Requirement (Inbound Email Security)	Description
D2.2.3.1 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 partner 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 Email Security, the partner 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.
D2.2.3.2 Anti-virus	The scale and complexity of recent virus attacks highlight the importance of a vigorous, secure messaging platform. The partner must explain how the service can combat this threat by using Cisco Email Security to detect incoming infected messages and filter SMTP traffic for optimal detection rates and security.
D2.2.3.3 Inbound email content filtering	Businesses may have specific policies about emails entering their company. The partner 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.
D2.2.3.4 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, anti-virus, message and content filters. The partner must explain how using their service incoming or outgoing messages can be placed them quarantines.
D2.2.3.5 Optional enhanced email security with Advanced Malware Protection	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 partner 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 partner 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 (Outbound Email Security-Optional)	Description
D2.2.3.6 Anti-virus	Businesses may have specific policies to avoid sending email corrupted with viruses outside their company. The partner must explain how the service can deliver this capability by: Using Cisco Email Security to detect outgoing infected messages and filter SMTP traffic for optimal detection rates and security.
D2.2.3.7 Outbound content filtering	Businesses may have specific policies about emails exiting their company. The partner 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.
D2.2.3.8 Data Loss Prevention	Businesses must prevent the malicious or unintentional distribution of sensitive and proprietary information over the Internet. The partner must also be able to explain how protect customer's information and intellectual property and enforce compliancy using Cisco Email Security 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 partner'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.	
Requirement	Description
D2.2.3.9 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 partner should be able to explain to explain high availability capability based on either Cisco Email Security clustering capability for active-active or traffic redirection to a standby virtual appliance fore active passive.
D2.2.3.10 Configuration backup	Storage of configurations of all virtual devices used in the email security service with ability to provide restoration.
D2.2.4 Web Security as a Service Capabilities	
The following section describes the basic functions of Web Security as a Service offering. The partner 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 via Cisco Umbrella, the Service Provider cloud, or via their corporate sites. If the partner has already achieved Master Security Specialization, the following requirements can be waived: D2.2.4.1-D2.2.4.11.	
Requirement (Real time threat protection services)	Description
D2.2.4.1 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 partner 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 Virtual Web Security appliance
D2.2.4.2 Malware scanning	The partner 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	Description
D2.2.4.3 URL filtering	The partner must explain how the solution provides user access control based on the web server category of a particular HTTP or HTTPS requests.
D2.2.4.4 Application Visibility and Control	The partner must explain how the solution provides industry-leading visibility and protection from web use violations.
D2.2.4.5 Optional Software as a Service (SaaS) access policy control	The partner 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.
D2.2.4.6 Transparent user authentication	The partner 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 user name mapping.
Advanced Malware Protection (optional)	Description
D2.2.4.7 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 partner 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.

Advanced policy control services (Optional)	Description
D2.2.4.8 Granular access control	The partner must explain how the solution provides differentiated security policies to individual users or group of users.
D2.2.4.9 Remote access (mobile) user	The partner 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.	
Requirement	Description
D2.2.4.10 Optional high availability	Active-active or active-passive high availability for the web security function allows the partner to continue service delivery during a planned or unplanned outage. The partner 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.
D2.2.4.11 Configuration backup	The partner 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.
D2.2.5 Next Generation Firewall as a Service Capabilities	
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 partner 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. If the partner has already achieved Master Security Specialization, the following requirements can be waived: D2.2.5.1–D2.2.5.9.	
Requirement	Description
D2.2.5.1 Support for standard firewall capabilities	Partner must support standard firewall capabilities, such as network-address translation (NAT) and stateful protocol inspection as specific in section D2.2.2.4 to D2.2.2.7 of this document.
Application Visibility and Control Support	
The following section describes key features of the NGFW that provides advanced visibility, detection and control for the service.	
Requirement	Description
D2.2.5.2 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. Partner implements network discovery policies to monitor traffic and collect host, application, and non-authoritative user data. By accessing the partner'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. Partner must present evidence how these features are delivered to their customers using their cloud based service delivery platform.
D2.2.5.3 Optional advanced visibility	The partner 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.

D2.2.5.4 Application access control	Provide centralized Application based policy enforcement including the following functions:
	• Block, Allow, rate limit Traffic based on 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

D2.2.5.5 SSL inspection	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.
Next Generation Intrusion Prevention System (NGIPS) (Optional)	
The following section describes the functions of NGIPS service options. The partner 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.	
Requirement	Description
D2.2.5.6 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 partner must provide evidence of the intrusion detection and prevention capability, and provide evidence of procedures to implement customer policies.
D2.2.5.7 Implementation and profiling service	To enable an effective intrusion detection and prevention solution, partner 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. Partner 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. Partner uses correlation policies to generate events and trigger responses (such as alerts or external remediation) to specific types of connections or traffic profile changes.
D2.2.5.8 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: partner creates event-focused rules and actions to block suspicious traffic and trigger inspections and remediation for a targeted system in customer's environment The partner 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.
D2.2.5.9 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 partner 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.
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. Partner 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.	
D2.2.5.10 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	
D2.2.5.11 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.
D2.2.5.12 Configuration backup	The partner 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.

D2.2.6 Advanced Malware Protection (AMP) Service for Endpoints	
The following section describes the functions of Advanced Malware Protection for Endpoints service option for Next Generation Firewall as a Service. Partner must provide evidence of the Advanced Malware Protection for Endpoints 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) on an endpoint.	
D2.2.6.1 Endpoint-based AMP	Endpoint-based Advanced Malware Protection solution continuously inspects endpoints for threats 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 • 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 • AV Detection – Malware and anti-virus 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. 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	
D2.2.6.2 Configuration backup	The partner 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.

D2.3 Service-Level Management Requirements

Service-Level Agreement (SLA) Components

This section describes the SLAs that the partner 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.

Requirement	Description
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 24 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.
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 partner must also be able to show that event logs can be stored and made accessible via the portal.

Requirement	Description
D2.3.6 Secure web portal	A secure, customer web portal is used to communicate 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 period of time established with the customer.
D2.3.8 Summary-level dashboard to communicate key performance criteria, including: Real-time status map 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 partners to differentiate themselves from other partners.

Requirement	Description
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.
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.	
Requirement	Description
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 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 provision of example reports or a demonstration of the reporting tool with ability to select reports listed. For non–service affecting incidents, partner must provide evidence of a process to investigate reported problems as necessary in order to prevent them from affecting service to the customer.	
Requirement	Description
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

Click here to return to Table of Contents

D3 Cloud Managed Access

Introduced: November 2017

Overview

An access network connects the users and devices to the core enterprise network and wide area network for communication and accessing business applications. It is a critical layer of enterprise networking that delivers high performance and secure, wired or wireless connectivity to the associated devices. The access layer of the network consists of switches and 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.

The Cisco Powered Cloud Managed Access service is defined as managed local area network (LAN) service or managed wireless LAN (WLAN) service that is delivered from the cloud and managed by the service provider by using Cisco Meraki cloud managed network solution. The end customers are consuming a set of access network services such as managed LAN, managed WLAN and other value-added services, such as presence analytics service and proximity marketing services. The differences in the Cloud Managed Access services versus traditional managed access network services are that service provider partner is able to deliver the services and/or service management from the cloud with support of multi-tenancy and automation, aimed at delivering more efficiently at scale and providing a compelling user experience. The end customer's IT administrators are able to utilize status and reporting capabilities over the Internet and use self-service capabilities as defined by the service provider partner.

Cisco Powered Cloud Managed Access refers to the managed services that use Cisco Meraki cloud managed WLAN and LAN services. The partners are required to have managed service practices, and the partners are responsible for managed access network services definition, SLA management and proactive monitoring.

D3.1 Prerequisites

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

Requirement	Description
D3.1.1 Meet all CMSP partner requirements in Cisco Cloud and Managed Services Program Audit and Policies document	See CMSP partner requirements in Cisco Channel Program Audit and Policies document.
D3.1.2 Submit at least two customer references for the service	CMSP partners are required to have a minimum of two customer references, from existing contractual relationships, for each Cisco Powered service. One customer may serve as reference to multiple designations. A customer with multiple sites does not qualify as a second reference however. The intent is to ensure that the partner has proven and repeatable service practices. The partner must submit at least two customer references for the service at the time of the audit, or must provide evidence of the ability to deliver the service to an end customer. Refer to Customer Reference Validation template.
D3.1.3 Provide the following documents unique to the service: • Service-Level Agreement • Service Description • Service Architecture Description • User Guide	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. The Service Description 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 service definition must be a published document. The Service Architecture description is a technical document that describes how the partners service monitoring tool and backend operation systems are integrated with Cisco Meraki cloud management portal and/or CPEs. The User Guide is a document that must show how to access the cloud service portal for self-service, including service activation, on-boarding, configuration and monitoring procedures.
D3.1.4 Have a Customer Success practice	Customer Success is the function within a Service Provider organization responsible for managing the relationship between the partner and its customers. The goal of

	customer success is to maximizing the value the customer generates from utilizing the Service Provider's solutions, while enabling the Service Provider to derive high return from the customer value. Partner must provide evidence of acceptance in the Cisco Lifecycle Adoption program or of a Customer Success practice discreet from reactive customer support. For the latter, such evidence includes dedicated staffing details, processes related to the practice, and metrics of performance.
D3.1.5 Maintain at least one Certified Meraki Networking Operator (CMNO) on staff when offering Meraki based cloud managed access services.	Certified Meraki Networking Operator (CMNO) is a certification and training program which validates the necessary technical proficiency to configure and troubleshoot manage Cisco Meraki devices and services. At least one member of the partner's operations staff is required to go through a formal CMNO class. Partner must provide evidence of a CMNO certificate. For information, visit Cisco Meraki CMNO certification.
D3.1.6 Audit representation	If the partner has contracted Cisco Services or a third party to design, build, and/or operate a Cloud Managed Access Networks service, at the partner's discretion, Cisco Services or the third party must participate in the audit and provide evidence on how the requirements have been fulfilled.

D3.2 Service Design (Build)

Service Capabilities

Cisco Meraki cloud managed network solution enables partners 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.

While utilizing the Cisco Meraki cloud managed network solution, a partner must demonstrate managed service practice as defined in this section in order to obtain the Cisco Powered designation. Resell alone of Cisco Meraki cloud managed network services are not sufficient to meet the designation requirements.

This section details the service design requirements of the Cisco Powered Managed Access designation.

Requirements	Description
D3.2.1 Must use Cisco Meraki cloud managed network solution	The partner must offer managed WLAN or managed LAN services using Cisco Meraki cloud managed solution, including Meraki CPE equipment as stated in CPE requirements section D3.2.6 - D3.2.7.
D3.2.2 Cloud based service portal and application programing interface	The partner must provide access to a web services portal and application programing interfaces (APIs) for integration with other services. If the partner does not provide direct access to the Meraki dashboard and/or Meraki APIs, the partner must provide their own web interface and APIs, based on the Meraki APIs. The partner shall provide an end customer demonstration of the web services portal and a user guide related to APIs as evidence of meeting this requirement.
D3.2.3 Service activation	The partner must be responsible for service activation of the end customers, including initial account setup, customer vetting, and onboarding. The partner must demonstrate the evidence such as service activation procedure document.
D3.2.4 Initial configuration and deployment	The partner must be responsible for initial configuration of the service and CPE such that Meraki device will automatically connect to the Meraki cloud for service delivery. The deployment of the devices can be either done by the partner or by end customers via self-service. An installation and setup document related to the service must be provided as evidence of meeting the requirement.
D3.2.5 Must offer at least one managed access network service	A partner must deliver a minimum of one of the following services: • Cloud Managed Wireless LAN (WLAN) service • Cloud Managed LAN service
D3.2.5.1 WLAN management service (required for cloud managed WLAN)	The partner 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 partner can make some or all of these management capabilities available for end customer self-service via Meraki dashboard. The partner must demonstrate these management capabilities in the service portal as evidence of meeting this requirement. Additionally, these capabilities should be reflected in the Market Service Description document.
D3.2.5.2 WLAN analytics and reporting (required for cloud managed WLAN)	The partner must offer WLAN analytics to end customers via the service portal. The basic analytics including location analytics and client analytics: • 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 end customer service portal can be used to demonstrate evidence of meeting this requirement.
D3.2.5.3 LAN service management capability (required for cloud managed LAN)	The part must offer the following management capabilities to end customers including • LAN device management • Switch ports management • VLAN management • Access control policy management • Switch stacking management The partner can make some or all of these management capabilities available for end customer self-service via Meraki dashboard. The partner must demonstrate these management capabilities in the service portal as evidence of meeting this requirement. Additionally, these capabilities should be reflected in the Market Service Description document.
D3.2.5.4 LAN analytics and reporting (required for cloud managed LAN)	The partner must provide analytics and reporting capabilities related to network topology, network usage report at switch, port level. • Network level usage • Top device by usage • Top clients by usage • Top application by usage • Port level stats: including top usage, clients and applications on the port The service portal can be used to provide evidence of meeting this requirement.
D3.2.6 Proactive monitoring of managed WLAN service or managed LAN service	The partner must offer proactive monitoring as part of cloud managed WLAN service or managed LAN service. The access point or switch device and service availability is proactively monitored from the partner operation center rather than waiting for end customer to notify the service status change. The partner must provide evidence such as an operations procedure document or demonstration of the partners network management systems where the status of end customer devices can be viewed.

Customer Premise Equipment Requirements	
The Cisco Power Cloud Managed Access service requires CPE for service delivery. The partner must provide evidence that the following CPE requirements are met.	
Requirement	Description
D3.2.6 Managed WLAN CPE (required for cloud managed WLAN service)	The partner must offer cloud managed WLAN services using Cisco Meraki MR series products and MX series products with WiFi capability. The evidence can be demonstrated via the Meraki dashboard.
D3.2.7 Managed LAN CPE (required for cloud managed LAN)	The partner must offer cloud managed LAN services using Cisco Meraki MS product family. The evidence can be demonstrated via the Meraki dashboard.
D3.2.9 Maintain valid software license on CPE	The partner must ensure a valid software license is on CPE devices used for service delivery. Failure to properly manage the software license expiration could result is a service outage for the end customer. The evidence can be demonstrated via the Meraki dashboard license management panel or a CPE license management report to show those organizations/CPEs license approaching expiry date (e.g. 3 months). A process around license expiration management with the end customer is also required.

D3.3 Customer Requirements

Not applicable

D3.4 Service-Level Management Requirements (Operate)

Service-Level Agreement (SLA) Components

This section describes the SLAs that the partner must contract for as part of the service. These are normally available as part of the Marketing Service Description. Existing customer contracts that include the relevant SLAs may also be presented as evidence of meeting these requirements.

When a partner uses Cisco Meraki solution to deliver managed LAN and managed WLAN services to end customers, the partner still owns the responsibility to provide the evidence how the following SLA requirements in this section are met by working with Cisco.

Requirement	Description
D3.4.1 Mean Time to Notify (MTTN)	If the customer experiences any resource or performance-affecting event the partner must notify the customer of the issue. This may vary according to specific customer agreements. MTTN measures the average time taken to notify a customer of an issue. The measurement encompasses the time that an alarm is generated to the time the customer notified, which can be by any method of communication agreed upon with the customer.
D3.4.2 Mean Time to Restore Service (MTRS)	If there is a disruption to the performance or availability of resources allocated to a customer, the partner must provide an expectation of restoration time. This may vary according to specific customer agreements. MTRS measures the total elapsed time from the start of a service outage to the time the service is restored. This is also known as Mean Time to Restore/Repair (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 daysP4: 5 business days
D3.4.3 Service availability	Provide evidence that service availability elements are covered by a SLA, agreed upon with the customer, and how different Operating-Level Agreement (OLA) components are measured and managed: • Service SLA that include service portal availability and CPE availability.

	• Network SLA, meaning the network operated by the partner that is used to provide connectivity to deliver the service or access the management portal when such a service is bundled with transport service. Appropriate documentation must be provided to demonstrate how the Underpinning Contracts (UCs) are measured and managed between partner and third party. • End-to-End Service SLA where elements of the end-to-end service are provided by a third party, availability of CPE, availability of service portal. The appropriate documentation must be provided to demonstrate how the Underpinning Contracts are measured and managed between partner and the third party.

Click here to return to Table of Contents

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 and phone numbers are listed on the Cisco website, at www.cisco.com/go/offices.