Service Description for
Cisco Unified Communications as a Service (UCaaS), Powered by Cisco UCM Cloud for Partners

This document (this "**Service Description**") describes the Service features, components, and terms of the managed services ("**Services**") Partner will purchase from Cisco for one or more end customers to support Cisco's Unified Communications Manager Cloud ("**UCM Cloud**"). The specific quantity and type of the Services purchased by Partner will be documented in a written Ordering Document between the parties. Appendix A to this Service Description sets forth the applicable terms and conditions governing the Services.

This Service Description, along with the relevant Ordering Document(s), is incorporated into the agreement between Partner and Cisco governing Partner's provision of the Cisco services to end customers (the "**Agreement**").

Service Summary

- This Service Description is meant to be read in conjunction with the Cisco UCM Cloud Service Description, which describes the terms and conditions applicable to the UCM Cloud and is available at: https://www.cisco.com/c/en/us/solutions/collateral/collaboration/unified-communications-manager-cloud/salestool-c96-742547.html. In order to purchase the Services, Partner must also purchase a UCM Cloud subscription, and the Services purchased by Partner for an end customer will be co-terminous with the term of the end customer's UCM Cloud subscription.
- The Services consist of the monitoring, management, and troubleshooting of the core UCM Cloud applications specific to the customer configuration, along with Cisco voice gateways and if applicable, certain third party integrations and/or applications used in connection with the UCM Cloud and identified in the Ordering Document for the relevant end customer (for purposes of this Service Description, the "**Managed Components**"), along with other optional services to support an end customer's use of UCM Cloud. The Services are provided based upon practices recommended by the Information Technology Infrastructure Library (ITIL).
- Unless otherwise expressly provided, all Services will be delivered remotely from Cisco's global Network Operations Centers (NOCs) global delivery model, and all Services will be provided 24x7x365, except where noted.
- If specified in the applicable Ordering Document, this Service Description will be deemed to incorporate by reference one or more of the following Supplements for Cisco Managed Services: Contact Center Collaboration, Video Collaboration, and/or Voice Collaboration.

Summary Table: The following tables summarize the Services components and the optional Services components available.

Select Services Components	Optional Service Components**
Service Transition – Planning and Support*	Customer-Facing Services Manager
Service Transition – Managed Component Activation*	Service Request Fulfillment
Portal	Service Fulfillment Portal
Service Asset Inventory Management	Management of Third Party Managed Components
Backup and Restoral Services	Smart Bonding for CMS
Event Management	
Incident Management	
Change Management	
Problem Management	
Services Manager	
Dashboards and On-demand Reporting	
Dial Plan Support	
Cisco Emergency Responder Support	

*as required based upon Service components **subject to additional charges

Service Components

Below is a description of the standard services included as part of the Services, to the extent applicable based on the service components ordered in the relevant Ordering Document. As noted below, some service components may not be applicable for a particular end customer.

Service Transition- Planning and Support (*applicable only to the extent agreed and described in an Ordering Document*)	
Summary: If applicable, Cisco and Partner will work together to provide details on the scope of the Services, including identifying the Managed Components as listed in the applicable Ordering Document, and to define the requirements and plan for establishing connectivity between Cisco and the Managed Components. See Section 2.3 of Appendix A (*Managed Services Terms*) for more information.	
Cisco Responsibilities • Host and lead a kick-off meeting via phone or web conference • Define the high-level scope of work required to transition the in-scope Devices to be managed as a Managed Component, including assessing changes required to Customer's platform, network, and processes in order to Activate the Managed Components • Define the required inventory information and topology requirements necessary to Activate the Managed Components • Identify a single point of contact (SPOC) to engage with Customer during the Service Transition • Perform any other tasks designated as Cisco's responsibility in the Transition Plan by the date specified in the Transition Plan	**Partner Responsibilities** • Unless otherwise agreed in writing, provide the reasonably requested inventory and topology information by the dates provided in the Transition Plan • Review and approve Transition Plan, including Activation date(s) • Identify a SPOC to engage with Cisco throughout the Service Transition period • Perform tasks specified as Partner's responsibility, and ensure performance by end customer of tasks specified as end customer's responsibility, in the Transition Plan by the date specified in the Transition Plan
Output: Transition Plan	

Service Transition – Managed Component Activation (*applicable only to the extent agreed and described in an Ordering Document*)	
Summary: If applicable, with Partner's assistance, Cisco will connect the Managed Components to Cisco NOCs, perform tests to confirm that the Managed Components are ready for remote monitoring, management, and troubleshooting and Activate the Managed Components onto the Cisco Managed Services Platform (CMSP).	
Cisco Responsibilities • Provide a VPN endpoint (hardware or software) to Partner with instructions how to install and configure the endpoint • Design, implement, and test bidirectional management capabilities • Provide Partner with general guidance on stabilization activities required to allow Activation • Activate and/or remove Managed Components, per the applicable Ordering Document(s) and Partner guidance • Implement CMSP and conduct tests to confirm that the Managed Components are Activated and ready for management • Provide notification to Partner that Activation is complete • Provide a draft of Runbook to Partner	**Partner Responsibilities** • Install and configure VPN endpoint at end customer location(s) according to its documentation • Unless Cisco is performing installation services, perform any required hardware or software installations, configuration changes and other stabilization activities required to enable connectivity and communication between the Managed Components and CMSP • Assist Cisco in establishing and validating bidirectional management capabilities between the Managed Components and CMSP • If desired, review and monitor Cisco's ready for use testing and results • Review and approve Partner-specific and end customer-specific elements in the Runbook
Outputs: Draft Runbook, initial Managed Component inventory, Change Request, if needed	

Portal
Summary: Cisco will make available a Portal allowing the Partner secure access to view their dashboard, pull on-demand reports, and requests (e.g., MACDs, etc.). For security reasons, the Portal is accessible only via the VPN tunnel to Cisco and is not accessible via the public internet. Cisco will provide Partner with the ability to create and administer accounts for its authorized users. Requests submitted by Partner are deemed to be authorized by Partner.

Service Asset Inventory Management
Summary: Cisco will collect and maintain inventory information about the Managed Components and the associated environment (excluding Cisco's UCM Cloud assets). Cisco will make this information available via the Portal or upon written request.
Output: Managed Component list and environment details

Backup and Restoral Services	
Summary: If supported by the Managed Components, Cisco will perform a backup of the configuration settings of the Managed Components (but not the content on the Managed Component) and restore this data as necessary to maintain the Services or in response to a Service Request.	
Cisco Responsibilities • Provide backup storage requirements • Perform, verify, and document in CMSP that the backup is performed based upon the applicable schedule • Alert Partner if the backup does not run as scheduled or if Cisco become aware of a backup error or failure • As a part of Incident or Change Management, restore to the last known good configuration and settings file from the backup to the applicable Managed Components	**Partner Responsibilities** • Provide local storage for the backup files • Ensure backup files meet requirements for retention • Ensure Cisco has 24x7x365 access to the backup files should a restore be required • Maintain the backup files • Provide all the necessary credentials (as defined in the onboarding guide) to enable Cisco to perform the backups • Perform any tasks specified in the CAB process • Provide means for Cisco to access and make changes to the relevant applications and hardware • Facilitate change record disposition post-activation • Identify any dependencies for out of scope hardware, software, and services • Communicate and secure maintenance window from end customer • Perform any tasks specified in the Change Advisory Board (CAB) process • Facilitate change record disposition post-activation • Identify any dependencies for out of scope hardware, software, and services • Perform backup of Managed Components that cannot be backed up by Cisco (e.g., Third Party Managed Components)
Output: Backup of settings of Managed Components, which will be stored by Partner	

Event Management
Summary: Cisco will monitor the Managed Components for the occurrence of Events.
Cisco Responsibilities • Create and implement Event Management policies (e.g., Event thresholds) • Monitor the Managed Components for Events by monitoring syslog, SNMP trap messages, Key Performance Indicators (KPIs), and/or Threshold Crossing Alerts (TCAs) from Managed Components • Help identify meaningful Events by creating filtering and correlation rules • Implement Event correlation, timing, and filtering through Event Management policies when an Event occurs
Outputs: Threshold Crossing Alert settings; filtering and correlation rules

Incident Management	
Summary: Cisco will help identify, troubleshoot, and restore normal operational functionality of the Managed Components if an Incident is detected or reported by Partner.	
Cisco Responsibilities • Create Incident tickets from detected or reported Incidents • Manage Incidents by classifying, prioritizing, troubleshooting, and restoring operation of the Managed Components, or providing recommendations to resolve the Incident • Assign and reassess Incident priorities in accordance with the process defined in Appendix B of this Service Description • Notify relevant parties about Incidents, keeping the parties updated through Incident closure • Provide Incident Reports pertaining to the Managed Components • Make recommendation to resolve Incident if the cause is out of scope our out of Cisco's control	**Partner Responsibilities** • Provide details about support contracts and other documentation/authorization required to facilitate Incident resolution • Contact Cisco if Partner believes an Incident is in-progress or has occurred, per Runbook • If Cisco cannot perform the changes or if the changes are out of scope, perform Cisco or third-party recommended changes to Managed Components or third-party hardware, software, or services
Outputs: Incident Ticket, Change Request to resolve Incident; Recommendation to resolve Incident	

Change Management	
Summary: Cisco will manage the deployment of technical changes to the Managed Components (e.g., configuration changes) in end customer's environment. Change types supported by Change Management are Emergency Changes, Normal Changes, Custom Changes, Standard Changes, and Informational Changes.	
Cisco Responsibilities • Manage the lifecycle of Change Management Requests (e.g., planning, testing, backout, etc.), resulting from an Incident, Problem, Service Request, or as otherwise mutually agreed in writing • Coordinate and perform changes to Managed Components, using commercially reasonable efforts to minimize any adverse impacts of those changes to end customer's environment • Validate and prioritize Change Requests based on urgency, including notifications from Cisco's Product Security Information Response Team (PSIRTs), when applicable • Provide personnel who will attend up to two hours of CAB meetings per week • Identify and recommend changes to the Managed Components • Provide notifications of change request start and completion for end customer-impacting changes • Follow the Change Management Process as described in the Runbook • Perform pre- and post-change Health Checks	**Partner Responsibilities** • Notify Cisco of and review with Cisco any Informational Changes or other updates or changes planned in end customer's environment that may impact the Services • Submit Requests for Change (RFCs) as Service Requests, Informational Changes, or Incidents via approved method • Review, implement, and execute Cisco-initiated Change Requests in accordance with Cisco's instructions as described in the Change Request • Follow the Change Management Process as described in the Runbook • Consult with Cisco on scheduling, communicating, and executing of changes • Invite Cisco to CAB meetings and facilitate communication between Cisco and the CAB • Determine and mitigate any impacts to monitored-only or out-of-scope devices as a result of any changes to the Managed Components • Promptly review and approve changes based on urgency of request • Perform, and assist Cisco in the performance of, all tasks agreed in writing via CAB process
Output: Recommendations for Change; Change Request; Change Plan; Change Record	

Problem Management	
Summary: Cisco will analyze Incidents post-restoration to identify a Root Cause for P1 or similar, recurring P2 Incidents (as defined in Appendix B). Cisco will proactively perform activities aimed at identifying and resolving Problems before Incidents occur. Proactive activities include the following: trend analysis, health checks, and platform tuning.	
Cisco Responsibilities • Create Problem record, and analyze Events (e.g., threshold violations) and Incidents to assist in identifying trends or errors from criteria above • Perform predictive analytics to help determine source of Problem • Analyze Cisco PSIRT High and Critical notifications, Cisco security vulnerabilities, Known Error databases, and field notices against Problem records • Define remediation of PSIRT notifications • Provide actionable recommendations to Partner to resolve the Problem and reduce or eliminate Incidents resulting from that Problem • Implement Changes to resolve problems according to Change Management • Maintain Problem Records to determine if the action taken resolved the Problem	**Partner Responsibilities** • If applicable, coordinate with third-party suppliers to address situations where out of scope devices or monitored-only components are the cause of a Problem • Implement Cisco-recommended changes • Approve PSIRT remediation recommendations • If applicable, coordinate with third party suppliers to address situations or incompatibilities where a Third-Party Managed Component or third-party Device is the cause of a Problem • Implement Cisco or third-party recommended changes if outside the scope of the Service or outside of Cisco's control • Determine and mitigate any impacts to the monitored-only or out-of-scope devices as a result of any upgrades required for new releases of applications or the core UCM Cloud or other changes to the Managed Components
Outputs: Change Request; Change Record; Problem Record; recommendations to resolve Incident or Problem	

Services Manager	
Summary: To support high quality service and confirm that service delivery processes are in place, Cisco will provide a designated Service Delivery Manager as a part of the Services. This individual will provide support directly to the Partner across all their associated end customers. The Service Delivery Manager will not interact directly with any end customers.	
Cisco Responsibilities • Provide a single point of contact and advocate with Cisco, working to help customers achieve business outcomes • Monitor and manage service delivery to ensure alignment with contract obligations • Discuss alignment of Services with changing business needs • Drive resolution of commercial issues, contract renewals, and growth opportunities. • Maintain Runbook to ensure operational procedures are documented and current	**Partner Responsibilities** • Provide a key point of contact for Cisco for escalations, commercial issues, and contract renewals discussions • Provide a representative to attend and agree to perform any Partner actions discussed during Cisco engagements • Evaluate and approve Cisco-recommended actions and provide updates regarding past actions
Outputs: Recommendations, meeting agenda, draft Change Request, performance reports	

Dashboards and On-demand Reporting
Summary: Cisco will make available to the Partner technology and business dashboards and on-demand reports as outlined in the Reporting Guide. Cisco will make available the following reports, which list may be updated from time to time: SLA and KPI Reporting, Availability Reporting, Adoption & Usage Based Reporting, Incident Management Report, Problem Management Report, Change Management Report, and Capacity Management Report.
Outputs: Dashboards; Reports

Dial Plan Support
Summary: Cisco will support the dial plan configured as part of UCM Cloud as described in the Cisco UCM Cloud Service Description.

Cisco Emergency Responder Support
Summary: Cisco will support the Cisco Emergency Responder (CER) feature configured as part of UCM Cloud as described in the Cisco UCM Cloud Service Description.

Optional Service Components

One or more of the following may be purchased via an Ordering Document as optional Service components in addition to the purchase of the Services:

Customer-Facing Services Manager	
Summary: To support high quality service and confirm that service delivery processes are in place, Cisco will provide a designated Services Manager who will act as a SPOC for the end customer as a part of the Services.	
Cisco Responsibilities • Assign a delivery manager (and backup, as needed) as single point of contact for day to day operations of the Services • Provide agenda and host monthly operations meetings to review and discuss reports, service level performance, historical and trending operational and performance data, and operational risks • Provide agenda and host quarterly business reviews focused on service adoption, features consumption, new capabilities that are available since the previous meeting • Perform any tasks mutually agreed in writing as a result of meeting • Maintain Runbook to so that operational procedures are documented and current with existing practice	**Partner/End Customer Responsibilities** • Provide a SPOC for Cisco for day to day receipt and operations of the Services • Evaluate and approve Cisco-recommended actions and provide updates regarding past actions • Provide a representative to attend and perform any tasks mutually agreed to in writing as a result of meeting • Evaluate and approve recommended actions and provide updates regarding past actions
Outputs: Recommendations, meeting agenda, draft Change Request, performance reports	

Service Request Fulfillment	
Summary: Cisco will implement Service Requests as described in the Service Catalog, consuming Partner's Service Request Units (SRUs) according to the cost in SRUs as provided in the Service Catalog. Service Request types not in the service catalog will be separately scoped and quoted before proceeding.	
Cisco Responsibilities • Provide the Portal for Partner to make, and for Cisco to categorize, approve, prioritize, and manage, Service Requests • Manage submitted Service Requests through validation, completion, and closure • Fulfill approved Service Requests • Handle Urgent Service Requests as a priority during Standard Business Hours on an as-available basis and per the Service Catalog	**Partner Responsibilities** • Create Service Requests • Provide acknowledgement, if requested, when each Service Request is completed • Provide a list of users authorized to submit Service Requests • Perform any physical or onsite changes to Managed Components reasonably required by Cisco to help fulfill Service Requests • Provide reasonably requested additional details pertaining to Service Requests • Prioritize Service Requests
Outputs: Service Request reporting, Service Request catalog	

Service Fulfillment Portal	
Summary: Cisco will implement a web-based cloud services brokerage platform. The Service Fulfillment Portal provides three optional functions: a business catalog, custom workflows, and orchestration.	
Cisco Responsibilities • Provide Partner with access to the Service Fulfillment Portal • Configure orchestration workflows according to agreed listings • Configure Partner's business catalog according to mutually agreed listings • Manage the Service Requests according to workflows through to final fulfillment of such Service Requests • Provide notifications in accordance with the applicable Service Request orchestration workflow • Enable Service Reporting for Partner service fulfillment cycle and service inventory • Provide reporting on Service Requests	**Partner Responsibilities** • Provide a list of users authorized to access the Service Fulfillment Portal and their respective roles • Provide service details for entries in the Service Catalog design • Provide details for customization of Service orchestration workflows • Provide future roadmap and assist in the implementation of Service Fulfillment Portal business catalog changes • Provide SPOC with respect to the management and oversight of Customer's responsibilities with respect to the Service Fulfillment Portal • Follow Change Management Process for Change Requests with respect to Service Fulfillment Portal business catalog and service orchestration workflow
Outputs: Access to Service Fulfillment Portal, Service Request reporting	

Management of Third Party Managed Components	
Summary: Cisco will manage Third Party Managed Components identified in an Ordering Document, pursuant to a valid Letter of Agency (LOA) and as described in this Service Description. Cisco will oversee the interactions with, and management of, the relevant suppliers that provide certain third-party products and/or services to an end customer, to the extent that Third Party Managed Components are listed in the applicable Ordering Document(s).	
Cisco Responsibilities • Manage Third Party Managed Components as provided in the Ordering Documents or as mutually agreed in writing	**Partner Responsibilities** • Provide Cisco and the applicable third party supplier with a valid LOA as described in Appendix A • Maintain valid support contract with the relevant third party supplier • Identify Third Party Managed Components and the associated third-party suppliers • Manage all security incidents, notifications, and/or alerts and notify Cisco of any such security incidents, notifications, and/or alerts with respect to Third Party Managed Components • If Change Management is not part of the scope of services, manage and perform any Changes to the Third-Party Managed Components
Output: Customer communications, as required	

Smart Bonding for CMS	
Summary: Cisco will provide CMSP integration points to allow Partner's IT Service Management (ITSM) system to communicate with the CMSP to facilitate the exchange of tickets, status updates, workflow processes, and with other related information. Unless otherwise agreed in writing, Smart Bonding is limited to a single integration from Cisco's CMSP and Partner's ITSM.	
Cisco Responsibilities • Provide ITSM integration interface between the CMSP and Partner's ITSM to facilitate the bidirectional exchange of Change Management, Incident Management, and Service Request Management workflow, Incident ticketing, and status updates • Provide Partner an Application Programming Interface (API) specification and documentation to enable integration of Partner's ITSM with the CMSP • Notify Partner of any material changes to Cisco's API interface	**Partner Responsibilities** • Customize and configure Partner's ITSM system to interoperate with CMSP API interface • Provide a SPOC for Smart Bonding operations • Follow requirements contained in documentation to enable the integration • Notify Cisco when any material changes are made to the relevant ticketing systems • Contact Cisco if Partner believes Smart Bonding ticketing data or information is incorrect
Outputs: Integration and API specification	

Appendix A: General Terms and Conditions

1. Services Terms

1.1 **Scope of Additional Services.** Unless the Services are expressly provided for above, all other Cisco services are out of scope for this Service Description. Therefore, in addition to any Service Requests in the Service Catalog, Cisco will work with Partner to accommodate custom Service Requests or custom Services ("**Custom Services**"). The scope and associated charges for any Custom Services will be agreed in writing between Cisco and Customer before Cisco proceeds.

1.2 **Managed Components.**

(a) As part of Service Transition, Cisco will identify which devices, hardware, or equipment on an end customer's network will be Activated as Managed Components and will identify any limitations of the Services with respect to the Managed Components and/or any monitored-only components, if applicable. For example, certain Third-Party Managed Components may only be monitored for availability (sometimes called "up/down") with limited additional Services provided.
(b) Cisco will not provide Services for any Managed Components that are unauthorized (e.g., grey market) or EoX (e.g., End of Life, End of Support, etc.) unless expressly provided in the applicable Ordering Document(s).
(c) If not documented in the Ordering Documents, management of Third-Party Managed Components or any EoX Managed Components is limited to Event Management, creation and closure of an Incident ticket, and standard reporting based on available data.
(d) Any management of devices (i.e. not Managed Components identified in an Ordering Document) by Cisco will be on a reasonable-efforts basis without warranty of any kind.
(e) Partner or the relevant end customer must maintain a valid Cisco license, support, and maintenance, agreement for all Managed Components. Cisco reserves the right to charge Partner the equivalent support and maintenance fee for those Managed Components that are not covered or reduce the services (e.g., updates, submit requests for hardware replacement, etc.) for those Managed Components that do not have a valid Cisco license, support, and maintenance agreement.

1.3 **Reporting.** Cisco will provide, or make available via the Portal, the reports listed in the Reporting Guide provided by Cisco. Cisco reserves the right to add, change, or remove reports in its reasonable discretion. Partner is responsible for reviewing, analyzing, and, if needed, discussing with Cisco the information contained in the reports. Partner will notify Cisco within a reasonable timeframe if Partner believes there is an inaccuracy in any report.

1.4 **Cisco Managed Services Platform (CMSP).** The CMSP will be the system of record for the Services. The CMSP uses cloud-based components to process Managed Component data to provide the Services. These components are hosted in a secure data center with at least one redundant system. Cisco will be responsible for maintenance of CMSP and CMSP Tools with reasonable access and on-site assistance provided by Partner.

1.5 **Cisco Recommendations and Changes.** If Partner fails to implement any reasonably requested Cisco recommendations or requirements, or fails to allow Cisco to make reasonably recommended Changes with respect to the Managed Components or the Services, Cisco shall have no responsibility for any resulting delays, failure(s), or increased security risks with respect to the performance of the Services. In addition, if Partner's failure to implement Cisco's reasonable recommendations or its unreasonable refusal to allow Cisco to make Changes causes Cisco to incur more costs or effort to provide the Services, Cisco may charge additional charges to address such items until the recommendations are implemented.

1.6 **Training and Policies**. Cisco personnel required to access any Partner or end customer site(s), Managed Components, or other Partner or end customer systems will remotely participate in any reasonable Partner-requested training (up to a maximum of 6 hours per year) without additional Charges. In addition, Cisco will materially comply with any reasonable written security policies applicable to the Services provided that: (a) the policies are in writing and provided to Cisco reasonably in advance of the requested compliance date; (b) Cisco has sufficient control to implement the polices; and (c) the policies do not conflict with Cisco's policies, amend or conflict with the Agreement or this Service Description, change the allocation of risk or liability between the parties, increase the scope of Services, or cause Cisco to incur increased risks or costs to comply with such policies.

1.7 **General Partner Responsibilities.** Cisco's provision of the Services is dependent on Partner's compliance with its responsibilities, and Partner's ensuring any end customer's compliance with its responsibilities, as listed in this Service Description or reasonably requested by Cisco. If Partner or the end customer fails to perform its responsibilities or if an exclusion (listed in Section 1.8 below) applies, Cisco will be excused from performing the Services (including achieving any Service Levels) to the extent, and for the duration that Partner or the end customer fails to meet its responsibilities. In addition, Cisco reserves the right to charge Partner for expenses, costs or time incurred, caused by Partner's or end customer's failure to perform its responsibilities. In addition to Partner's and end customer's responsibilities listed above, Partner will also be responsible, and will ensure that end customer will be responsible, for the following:

(a) Promptly supply Cisco with reasonably requested and necessary technical data (e.g., network diagrams, host names, IP addresses, SNMP strings, and passwords) and other similar information to allow Cisco to provide the Services.
(b) Provide prompt, reasonable cooperation and assistance to Cisco in performance of the Services (e.g., making Changes to Managed Components or CMSP Tools that cannot be done remotely, locally running tests or diagnostics on Managed Components, updating configurations or VPN settings, etc.).
(c) Maintain the locations and environmental conditions, including power, HVAC, connectivity, space (physical and rack space), security, raised floors, fire containment, connectivity, reliable out of band access, and other requirements necessary for the proper operation of the Managed Components, Third Party Managed Components, monitored-only components, and other infrastructure and applications, all as they relate to the Services.
(d) Back-up and protection of its own data against loss, damage, theft or destruction.
(e) Provide Cisco and Cisco personnel prompt physical and remote (logical) access to the Managed Components, Cisco equipment, and Partner or end customer's other infrastructure, as reasonably required for Cisco to perform all elements of the Services (e.g., opening ports, changing firewall settings, providing change windows, etc.). This responsibility includes obtaining any needed internal or third party approvals or licenses.
(f) Manage all third-party products and/or services that are not in the scope of Services, including enforcing any third-party supplier contract terms and any applicable service level agreements.
(g) Notify Cisco in advance of any updates or changes planned in Partner's or end customer's environment. Failure to notify Cisco of such updates or changes may result in Partner being charged for additional Service Request Units.
(h) Identify any dependencies for out-of-scope hardware, software and/or services.
(i) Where applicable (e.g., for end customer-held or Partner-held licenses for Third Party Managed Components or other third party software, products, or services), provide a Letter of Agency (LOA) to any applicable third party vendor and Cisco authorizing Cisco and its contractors to act as end customer's agent with respect to the management of any applicable Third Party Managed Components or other software, products, or services.
(j) Provide and maintain connectivity (including, without limitation, any required local circuits, cross connects, and hardware) to Cisco's NOC, including providing reasonably required permissions. The minimum speed is 10Mbps per connection for both download and upload (symmetric circuit).

1.8 **Exclusions**

Products and services that are not described in this Service Description are not part of the Services, including, but not limited to, the following examples:

- Any and all network connectivity, including, without limitation, PSTN or MPLS circuits and cross connections
- Services or software to resolve any Incidents or Problems resulting from a third-party product or causes beyond Cisco's control unless specified otherwise in the applicable Ordering Document(s)
- Software or hardware upgrades unless expressly referenced in this Service Description, Supplement(s) to this Service Description, or the applicable Ordering Document(s)
- Change Management or implementation with respect to equipment not managed by Cisco
- Unless provided for in an Ordering Document, providing Services onsite or in any language other than English
- Troubleshooting Incidents that predate Service Activation

2 Commercial Terms.

2.1 **Pricing Summary**. The charges for the Services ("**Charges**") and payment terms will be detailed in the applicable Ordering Document. The Charges listed in the Ordering Document reflect a charge per Knowledge Worker and per Common Area Device (each, a **"Subscriber"**) per month. For the avoidance of doubt, any increases in the number of Knowledge Workers and/or Common Area Devices on the UCM Cloud will also result in increased Charges for the Services based on the total number of Knowledge Workers and Common Area Devices authorized to access the UCM Cloud. All Charges paid are non-refundable.

2.2 **Invoicing.**

(a) If Customer has prepaid for the Services, Cisco will invoice Partner on or after the effective date described in the applicable Ordering Document (the "Effective Date").
(b) If no invoicing terms are provided in the Ordering Documents, the Charges will be pro-rated for the number of years (and/or any portion of a year) of the term and paid annually in advance.
(c) If the Ordering Documents provide for invoicing upon Activation, Cisco will begin invoicing on the deemed Activation date or the original Activation date provided in the Transition Plan, whichever occurs first. Cisco will delay invoicing on a day-for-day basis if Cisco is the primary cause of the delay in Activation.

(d) Cisco's rights to invoice for the charges for the Services and Partner's obligation to pay will not be affected by (i) any delays caused by Partner or end customer (or anyone acting on behalf of Partner or end customer), (ii) Partner's or end customer's failure to perform or delay in performing its obligations under this Service Description or the UCM Cloud Service Description, or (iii) Partner's failure to issue a purchase order

2.3 **Activation.** The Activation date will be provided in the Transition Plan. If no date is provided in the Transition Plan, the Managed Components will be deemed Activated on the date of actual Activation by Cisco or ninety (90) days from the effective date of the Ordering Document, whichever happens first.

2.4 **Additional Devices Added as Managed Components**. To the extent that Customer makes any change to the number of Managed Components from the number of Managed Components quoted/priced in the applicable Ordering Document, the monthly Charges for the Services will be adjusted accordingly. If Customer wishes to add new Devices as Managed Components and there is no true-up, audit, rate card, or similar provision in the Ordering Document, the parties will follow Cisco's standard change request process.

2.5 **Service Request Units (SRUs) and Related Charges**. Partner's applicable Ordering Document(s) will list the aggregate number of SRUs purchased. If Partner uses all of its available SRUs, then Partner may purchase additional SRUs. SRUs are not refundable and must be used during the term listed in the applicable Ordering Document or they expire. Cisco will invoice Partner for any Service Requests that are fulfilled by Cisco during the applicable billing month. For the avoidance of doubt, Service Request Units may not be used to offset the additional monthly Charges associated with such an increase in the total number of Managed Components.

2.6 **Minimum Term and Minimum Charges Commitment**. The Ordering Documents will contain any minimum term or minimum Charges commitment associated with the Services.

2.7 **Term, Termination, and Renewal.**

(a) **Term**. The term of the Services will be provided in the Ordering Documents. Unless provided in the Ordering Documents, the Term will begin upon the Effective Date of the Ordering Document and will be co-terminous with the end customer's term for UCM Cloud.
(b) **Termination**. Where an Ordering Document contains a minimum commitment or contract value, if Customer terminates the Services for convenience, Cisco will invoice the remainder of contract value or minimum commitment due under the Ordering Document. If the Ordering Document does not contain a minimum commitment, Customer may not terminate the Services for convenience, even if the Agreement allows it, unless expressly provided in the Ordering Document. Rights to terminate for material breach are provided in the Agreement.
(c) **Renewal**. The Service will automatically renew for additional one-year terms at the same price to the extent that Partner's order for UCM Cloud also renews, unless Cisco notifies Partner in writing at least ninety (90) days in advance of, or Partner notifies Cisco in writing at least forty-five (45) days in advance of, the expiration of the then-current term that it does not want to renew the Services.

3 Legal Terms.

3.1 **Definitions.** Capitalized terms not defined in this Service Description will have the meanings given in the Glossary of Terms for the Service Description for Cisco Managed Services (available at www.cisco.com/go/servicedescriptions) (**"Glossary of Terms"**). In the event of any conflict in definitions defined in the body of this Service Description and the corresponding definition in the Glossary of Terms, the definition in the body of this Service Description will prevail.

3.2 **Related Documents**. This document should be read in conjunction with the following documents: (1) Glossary of Terms; (2) any Service Level Agreement referencing this Service Description; (3) any Supplement(s); (4) the methodology and associated terminology used in determining the priority level of an Incident, which is included in Appendix B of this Service Description; and (5) any Ordering Document(s).

3.3 **Order of Preference.** If there is a conflict between this Service Description, any Supplement(s), an Ordering Document, the Agreement, the following priority will apply (from highest to lowest): (a) any Ordering Document, as applicable; (b) this Service Description; (c) any Supplement(s); and (d) the Agreement.

3.4 **Compliance with Laws.** Cisco will comply with applicable laws, rules and regulations, including, but not limited to, all applicable export control laws and regulations. Partner will comply, and Partner will ensure that Customer will agree to comply, with all applicable laws, rules, and regulations related to the receipt and use of the Services and will obtain all approvals and licenses required by any third parties related to the Managed Components, Partner's or end customer's locations, systems, software, and network as are reasonably necessary for Cisco to provide the Services.

3.5 **License.** Cisco grants to Partner and to Partner's end customer a limited, non-transferable, non-sublicensable, internal use, license to use the executable version of Portal, any CMSP Tools, and any software provided by Cisco as part of the Services (either installed on Partner's or end customer's premises or available via software as a service) only to the extent and duration reasonably required to receive the Services. There are no warranties associated with these items outside of their use as part of the Services. Upon expiration or termination of the Services, the license to the Portal, any CMSP Tools, and any software will automatically terminate. If applicable, Partner will return all Cisco-owned hardware and software licensed for the receipt of the Services (e.g., CMSP Tools). Except to the extent caused by Cisco, Partner will be responsible for any loss, theft or damage to the CMSP Tools until they are returned.

3.6 **Security and Data Privacy Program.** Each party will, and Partner will ensure that end customer will agree to, maintain a reasonable information security and data privacy program with appropriate technical, administrative, and physical safeguards designed to prevent any (i) unauthorized access, use, distribution, or deletion of Partner's or end customer's data and (ii) compromise of the Managed Components or CMSP Tools. More information on Cisco's security and privacy policy can be found here: http://www.cisco.com/c/en/us/about/trust-transparency-center/data-protection.html. If the parties do not have a mutual data protection agreement in place (or equivalent privacy and data protection terms), the following Mutual Data Protection Agreement is incorporated into this Service Description: https://trustportal.cisco.com/c/dam/r/ctp/docs/dataprotection/cisco-master-data-protection-agreement.pdf.

3.7 **Cooperation.** To the extent reasonably requested by the other party and permitted by Applicable Law, each party will provide reasonable assistance to, and communicate and cooperate with, the other party, as well as to any subcontractor or supplier that provides services to such other party in connection with the Services. Each party will use commercially reasonable efforts to procure all such cooperation from its own subcontractors and suppliers.

3.8 **Confidential Information.** The Runbook, Charges, Portal, CMSP Tools, and Service Level performance information are Confidential Information (as defined in the Agreement). This information may not be used for any purpose other than in connection with Partner's and end customer's use of the relevant Services provided by Cisco.

3.9 **Telemetry Data.** Cisco may collect data on Partner's and end customer's usage of the Services in order to maintain, improve, market, or promote the Services. In addition, Cisco may use anonymized and aggregated data on Partner's and end customer's use of the Services, Managed Component performance (Cisco products only), and network performance ("**Telemetry Data**") to create or improve its products and services. Cisco will comply at all times with applicable law related to Cisco's collection and use of the data above and will use reasonable physical, technical, and procedural means to protect the Telemetry Data that contains Personal Data in accordance with the Cisco Online Privacy Statement, which is made available at http://www.cisco.com/c/en/us/about/legal/privacy-full.html or such other site(s) as Cisco may publicly communicate from time to time.

3.10 **Subcontractors.** Cisco may use subcontractors to provide services to Partner and end customer on its behalf for the purposes of providing the Services. Cisco will remain responsible for its subcontractors' compliance with the obligations under this Service Description and the Agreement as if performed by Cisco. References to Cisco in this Service Description shall include its subcontractors, as applicable.

4. **Service Levels.** The Service Level Agreement for Cisco UCaaS powered by UCM Cloud is hereby incorporated by reference into this Service Description.

Appendix B: Priority Levels

This Appendix describes the methodology used in determining the priority level of an Incident. Cisco classifies Incidents according to "Impact" and "Urgency" and then defines the Priority of the Incident by applying the Impact and Urgency terms to the chart below.

Impact An Incident is classified according to the breadth of its impact on end customer's business (the size, scope, and complexity of the Incident).	**Urgency** The Urgency of an Incident is classified according to its impact on the Services or ability for end customer to receive the Services and the financial impact to end customer's business.
There are four impact levels: • Widespread: Entire Service is affected (more than three quarters of individuals, locations or Managed Components) • Large: Multiple locations are affected (between one-half and three-quarters of individuals, locations, or Managed Components) • Localized: A single location and/or multiple users are affected (between one-quarter and one-half of individuals, locations, or Managed Components) • Individualized: A single user is affected (less than one-quarter of individuals, locations, or Managed Components)	There are four urgency levels • Critical: Primary function is stopped with no redundancy or backup. There may be a significant, immediate financial impact to end customer's business. • Major: Primary function is severely degraded and supported by backup or redundant system. There is a probable significant financial impact to end customer's business. • Minor: Non-critical function is stopped or severely degraded. There is a possible financial impact to end customer's business. • Low/Notice: Non-critical business function is degraded. There is no impact. Partner or end customer perceives the issue as low.

Priority Definitions

Priority defines the level of effort that will be expended by Cisco and Partner to resolve the Incident. The Priority level is determined by applying the Impact and Urgency definitions to the chart below.

IMPACT					
URGENCY		Widespread	Large	Localized	Individualized
	Critical	P1	P1	P2	P2
	Major	P1	P2	P2	P3
	Minor	P2	P3	P3	P3
	Low/Notice	P4	P4	P4	P4

Notes:

- Cisco will adjust the case priority in accordance with updated Priority of Impact or Incident resolution.
- Customer requests to escalate Incidents to a higher priority than their classification may incur additional Charges
- The case may be left open for a prescribed period while operational stability is being assessed.

Cisco Incident Management priorities are defined as follows:

- P1: Cisco and Partner will commit any necessary resources 24x7 to resolve the situation.
- P2: Cisco and Partner will commit full-time resources during Standard Business Hours to resolve the situation.
- P3: Cisco and Partner are willing to commit resources during Standard Business Hours to restore service to satisfactory levels.
- P4: Cisco and Partner are willing to commit resources during Standard Business Hours to provide information or assistance.