Service Description for Cisco UCM Cloud Enterprise Service

This document ("**Service Description**") describes the Service features, components, and terms of the managed services ("**Services**") Cisco will provide to Customer to support Customer's use of Cisco's Unified Communications Manager Cloud ("**UCM Cloud**"). The specific quantity and type of the Services purchased by the Customer will be documented in a written Service Service Order between the parties. This Service Description should be read in conjunction with the document entitled "How Cisco Provides Services", which is incorporated by reference.

1. Service Summary

- The Services consist of the monitoring, management, and troubleshooting of the core UCM Cloud applications, certain in-scope third party integrations and/or applications used in connection with the UCM Cloud. As an optional Services element, Cisco will remotely monitor and manage customer premise Devices and applications. All the items above are known as "**Managed Elements**" as specified in a Service Order.
- 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 monitored 24x7x365, except where noted.
- The Services are provided based on Information Technology Infrastructure Library (ITIL) practices.
- This Service Description is to be read in conjunction with the Cisco UCM Cloud Offer Description or Enterprise License (as applicable) ("**UCM Cloud Agreement**"), which describes the terms and conditions applicable to the UCM Cloud. In order to purchase the Services, Customer must also purchase an appropriate UCM Cloud subscription.
- Base Service Transition Services are provided if and as part of the UCM Cloud Agreement. If Customer wishes to receive additional migration, installation, or similar services, it will be subject to a separate written engagement.

Summary Table: The following tables summarize the Included Services components, optional Services components which can be ordered at no extra charge ("Optional, Included Services"), and optional Services components which Cisco may offer subject to additional terms and Charges ("Optional Services").

Included Services	Optional, Included Services	Optional Services
1. Proactive 3rd party SIP Integration Monitoring	7. Service Request Fulfillment	12. IaaS for Commercial
2. Incident Management	8. Simple Moves, Adds, Changes or Deletes **(MACDs)**- 5% MACD of knowledge worker users	13. Smart Bonding for CMS
3. Problem Management	9. Standard Dial Plan Implementation	14. Service Transition of Managed Elements
4. Change Management	10. Self-Service Onboarding for UCM Cloud - (excludes 3rd-party PBXs and 3rd-party integrations)	15. Management of On-Premises Managed Elements
5. Service Delivery Management	11. Hosted PSTN vCUBE (SIP PSTN Integration)	
6. Security Certificate Management		

Included Services.

1. Proactive Monitoring

Summary: Cisco will monitor Customer's Network connectivity, covering Internet Control Message Protocol (ICMP) connectivity monitoring and notification of failed reachability to a single designated Customer IP address.
Cisco will also monitor compatible third-party Session Initiation Protocol (SIP) integrations as part of the Service.

Accompanying Tasks
• Cisco will notify Customer if a persistent reachability failure is detected for [ICMP?] connectivity or SIP integrations; and • Customer will be responsible for remediating any Customer Network issues (unless the underlying network is also optionally being managed by Cisco).
Output: Customer notification; Incident Ticket (if UCM Cloud is impacted)

2. Incident Management

Summary: If an Incident is detected or reported on behalf of Customer, Cisco will work to identify, troubleshoot, and restore normal operational functionality of UCM Cloud or the applicable in scope Managed Elements. Cisco may provide restoration through a temporary workaround. Incident Management includes the support and resolution of Incidents related to UCM Cloud application configurations that are either proactively detected by Cisco or reported by Customer. Cisco will deploy fixes to the configuration to restore previously working UCM Cloud feature/capabilities. An Incident is considered resolved once the Managed Element resumes standard operation or Cisco provides a restoration recommendation to Customer.

Accompanying Tasks

• The parties will each designate single points of contact for all Incidents;
• Incident classification- Cisco will create an Incident ticket, classify (or reclassify) the Incident according to Appendix B, and work towards resolution of the Incident;
• Incident Status- Cisco will notify Customer of the Incident and provide updates;
• The parties will work to verify the Incident, its source and the cause;
• The parties will promptly review and approve proposed Changes to resolve an Incident;
• If the cause of an Incident is out of scope or out of Cisco's control, Cisco will notify Customer with recommendations to help resolve the Incident;
• Customer may be required to perform the portions of the Changes if Cisco either cannot (or does not have permission to) perform the Changes, or the Changes are out of scope (e.g. a Change required to out of scope software);
• Customer will provide an appropriately staffed and qualified end-user service desk for Customer's UCM Cloud end users. Customer's service desk will be responsible for the following:
  ○ Review and initial triage of Incidents;
  ○ Communication, interaction, and Incident ownership with Customer's UCM Cloud end users, regardless if the issue is escalated to other Customer tiers or organizations;

- General UCM Cloud service information, including explaining how to use the service, devices, soft clients, new feature introduction, and the support of functionality that has not been previously accepted as working;
- Filtering non-technical problems from technical problems; and
- Configuring new features or business requirements into the application configuration.

- If Customer purchases the optional Management of Third Party and On-premises Components, Cisco will request replacement Managed Elements on Customer's behalf and will help coordinate the delivery of the replacement Managed Elements to Customer.

Outputs: Incident Ticket, Change Request for Incident restoration; RMA documentation, Recommendation for Incident restoration

3. Problem Management

Summary: Cisco will work to identify the root cause of P1 and recurring P2 Incidents. Cisco will create and maintain a Problem record, analyze the Problem using the root cause information, analytics, known error databases, and other tools, work to resolve or reduce the severity of the Problem, help prevent the further occurrence of their underlying Incidents, and perform trend analysis and health checks.

Accompanying Tasks
• Cisco will review Cisco PSIRT High and Critical notifications, Cisco security vulnerabilities, Known Error databases, and field notices against Customer Problem records; • Cisco will provide actionable recommendations to Customer to help resolve the Problem and help prevent further Incidents resulting from that Problem; • The parties will implement Changes to resolve Problems via Change Management; and • Customer will manage and address third-party suppliers and causes of Problems which are out of Cisco's scope or control.
Output: Change Request; Change Record; Problem Record; Root cause analysis; recommendations to resolve Incident or Problem

4. Change Management

Summary: As a part of the other Service components in this Service Description, Cisco will manage the lifecycle (i.e. planning, testing, backout or rollback, Customer notification, and post-change checks) of the deployment of technical changes to UCM Cloud and "in scope" Managed Elements. Change types supported by Change Management are Emergency Changes, Normal Changes, Custom Changes, Standard Changes, and Informational Changes.

Accompanying Tasks
• The parties will review, validate, approve, and prioritize Change Requests based on urgency; • The parties will perform the tasks specified in the Change Request and follow the change management process as described in the Runbook; • If Cisco is unable to perform all elements of the Change remotely, Customer will assist Cisco in performing the Changes (with Cisco guidance); and

• Customer will review and mitigate any impacts to out of scope Devices as a result of any Changes to the Managed Elements.
Output: Change Request; Change Plan; Change Record

5. Service Delivery Management

Summary: To support Cisco's provision of the Services and to confirm that service delivery processes are in place, Cisco will, in addition to the Service Delivery Management activities as specified below, provide a primary point of contact (and backup, as needed) to the Customer in respect of the Services.

Accompanying Tasks
• Cisco will provide an agenda and host monthly operational meetings to discuss items such as Incident tickets and reports, SLA performance, suggested Changes, etc.); • Cisco will also provide an agenda and host quarterly relationship meetings to discuss items such as Problems, Services improvement recommendations, and Services alignment to Customer's strategy and priorities; • Cisco will update the Runbook in response to material changes in the Services and mutually agreed changes; • Customer will assign complementary single points of contact for Services receipt and coordination; and • Each party will perform assigned tasks resulting from meetings, as mutually agreed in writing.
Output: Recommendations, meeting agenda, draft Change Request, performance reports.

6. Security Certificate Management

Summary: Cisco will manage the deployment and lifecycle of security certificates (e.g. authenticate devices and applications) for UCM Cloud. Note, the minimum expiry for certificates is 365 days.

Accompanying Tasks
• Cisco will generate Certificate Signing Requests (CSR) and coordinate signatures; • If Cisco owns the certificate, it will sign the requests; • If Customer owns the certificate, Customer will sign the request; and • Cisco will deploy signed certificates to UCM Cloud via Change Management
Outputs: CSR

Included, Optional Services.

7. Service Request Fulfillment

Summary: Cisco will implement fully qualified Service Requests and Move Add Change Delete (MACDs) requests from Customer. Service Requests and MACDs are categorized as Simple (a low complexity Change with a defined process), Standard (a Change with defined process), Normal (a non-emergency Change that requires review), and Emergency (a Change in response to an Incident). MACDs are listed in a Service Catalog provided by Customer. Cisco will separately scope and quote Service Request types not in the Service Catalog and get approval from Customer before proceeding.

Accompanying Tasks
• Cisco will, through the Portal, allow Customer to view the Service Catalog and request, categorize, approve, prioritize, check status of, and obtain reports on, Service Requests; • Customer will provide authorized requestors that may submit Service Requests on the Portal; • Cisco will manage submitted Service Requests through their lifecycle-e.g., receipt, validation, approval, qualification completion, closure, notifications, and updating documentation in conjunction with Change Management process; • Customer will submit requested information to qualify a Service Request. Failure to submit all needed information may result in delay. • If requested by Cisco, Customer will acknowledge when the Service Request has been completed; and • Cisco will handle prioritized Service Requests via the Service Catalog.
Output: Service Request reporting and Change Request

8. Move, Add Change, Delete (MACDs)- Up to 5% of Contracted Knowledge Worker per month

Summary: As a part of Service Request Fulfillment, Cisco will implement MACDs equaling up to 5% of the Contracted Knowledge Worker count per month. Supported MACD request types supported are outlined in the UCM Cloud Enterprise Cloud Service MACD Service Catalog. MACDs in excess of 5% of the Contracted Knowledge Worker count per month will be subject to additional Charges.

Accompanying Tasks
• This service requires the adoption of the standard dial plan implementation and configuration; • The parties will execute fully qualified MACD Service Requests from Customer using Service Request Fulfillment and Change Management.
Outputs: UCM Cloud Enterprise Cloud Service MACD Service Catalog; Service Requests

9. Standard dial plan Implementation

Summary: UCM Cloud is delivered with an available baseline dialing configuration. Cisco will implement the standard configuration including a PSTN dial plan. This initial configuration will have a fixed structure and naming convention that help facilitate the onboarding of future Devices and future self-service capabilities.

Accompanying Tasks
• Cisco will provide Customer with an information template for Customer to onboard users on to UCM Cloud with a standard configuration; • Cisco will perform basic tests to confirm that the standard configuration is working; • Customer is responsible for feature testing and testing that each end user's configuration is operational; • Customer is responsible for testing and supporting integrations and associated compatibility issues.
Outputs: Standard Configuration

10. Configuration Support and Self-Service Onboarding

Summary: Cisco will support standard or Customer configurations as part of UCM Cloud. For Cisco's default configuration only, Cisco will help enable the use of Cisco's Self-Service Onboarding capabilities within UCM Cloud via the use of Cisco tools.

Accompanying Tasks
• Cisco will test whether Customer is able to onboard an end user using Cisco's standard configuration and the parties will, if applicable, troubleshoot and resolve errors arising from the test's failure; • Customer will be responsible for onboarding its remaining end users and for any configuration or feature testing;
Outputs: Successful end user onboarding test.

11. Hosted PSTN vCUBE (SIP PSTN Integration)

Summary: Cisco will support the integration of a compatible third-party PSTN cloud provider through the deployment of a virtual Cisco Unified Border Element (vCUBE).

Accompanying Tasks
• Cicso will deploy vCUBE to allow SIP PSTN integration and proactively monitor and manage vCUBE as a Managed Element; • Cisco will maintain vCUBE software version that is compatible with the current UCM Cloud version; and • Customer will be responsible for all other elements of its deployment, use and maintenance of its PTSN (e.g. configuration, testing, support, capacity management, etc.).
Outputs: Hosted PSTN vCUBE infrastructure

Optional Services

12. Infrastructure as a Service (IaaS) for Commercial

Summary: Customer may order infrastructure capacity that is hosted and managed by Cisco and on which Customer may deploy Cisco applications or Cisco-approved third-party applications ("Applications") for use in conjunction with the Customers use of UCM Cloud. The specific capacity purchased by Customer will be documented in an Service Order between the parties.

IaaS Components
• Infrastructure capacity is purchased strictly in blocks of 1vCPU, 4GB memory, and 100GB storage and no excess capacity, high-availability or redundancy is provided unless purchased; • Cisco will make available an Application Service Catalog ("Catalog") that will list the capacity requirements for each supported Application. • Customer will determine what capacity is required for its needs

- The Services may only be used by Customer to host Applications to support its provisioning of Cisco UCM Cloud. Customer may not use the infrastructure IaaS for any purpose not expressly described in this Service Description (e.g., general hosting or storage);
- Applications are not included in the Services and will not be managed by Cisco as part of the Services. Customer must procure and maintain all required licenses for, and perform any required installation, configuration, integration activation, and upgrades with respect to, Applications hosted via the Services.
- The Services will not enable Internet access for any Applications.

Availability: The IaaS is available from the Geographies and Locations listed in the table below. The initial Geography and Location for a particular end customer's infrastructure will be indicated in Customer's Service Service Order.

Geographic Location(s)

North America	San Jose, CA
	Dallas, TX
EMEA	Amsterdam, Netherlands
	London, England
APJ	Tokyo, Japan
	Singapore

Cisco Responsibilities	**Customer Responsibilities**
• Conduct all provisioning for the CPU, memory, and storage specified in the order. • Connect the VM to the relevant end customer network • Maintain infrastructure layer: physical and environmental controls. • Maintain HW and VM layers. This includes all patches or upgrades needed to remediate any material security issues. • Maintain version compatibility between VMWare and UCM Cloud CSR • Support VM failover if there is a hardware failure • Planning and communicating the maintenance windows required to maintain the infrastructure Install the OS provided by the Customer	• Provide and maintain all operating system and Application licensing, interoperability, configuration, security and management • Ensure the compatibility of any Application(s) with the UCM Cloud • Determine the capacity requirements for all Applications • Perform Application and OS release management, including compatibility with the UCM Cloud. This includes patches or upgrades needed to remediate any security issue. • Installation of anti-virus and intrusion protection software • Ensure Application IP Address space is taken from Customer-provided block Provide requirements and software for Cisco to perform the initial OS install, as needed

Outputs: Hosted and managed virtual machine(s)

13. Smart Bonding for CMS

Summary: Cisco will provide CMSP integration points to allow Customer's IT Service Management (ITSM) system to communicate with the CMSP to facilitate the exchange of Incident tickets, status updates, workflow processes, and similar information. The extent and type of the Integration will be provided in the Service Service Order or mutually agreed in writing.

Accompanying Tasks
• If not provided in Service Service Order, the parties will agree in writing an integration plan, data exchange types (e.g., one or bi-directional, which data categories, etc.) and a test plan; • Cisco will provide an ITSM integration interface (e.g., APIs), specifications and documentation to allow the integration between the CMSP and Customer's ITSM; • Unless otherwise provided in writing, Customer will configure and maintain Customer's ITSM system in order to interoperate with CMSP API interface. Cisco will provide reasonable troubleshooting support for the integration; • If changes to the CMSP require the update to the integration, Cisco will notify Customer, provide updated APIs and documentation, and assist Customer in testing and troubleshooting Customer's updated integration; and • Smart Bonding is limited to a single integration between Cisco's CMSP and Customer's ITSM.
Output: Integration and API specifications and documentation; test plan

14. Service Transition and Activation

Summary: If Customer wishes Cisco to manage additional (optional) Devices outside of the hosted UCM Cloud application, Cisco and Customer will define the plan for establishing connectivity between Cisco and the Devices (e.g. Customer's voice gateway). The parties will also connect the additional "in scope" Customer premise Devices to the Cisco Managed Services Platform (CMSP), through a VPN endpoint provided by Cisco. Cisco will then perform tests to confirm that the additional "in scope" Devices are ready for remote management as Managed Elements ("**Activation**," "**Activate,"** etc.).

Accompanying Tasks
• Cisco will define the scope of work required to transition the additional Devices to be Activated as a Managed Elements, including required inventory information and topology requirements, assessing stabilization activities required to the Devices and Network; • Customer will promptly provide Cisco with remote access and control to the Managed Elements and will provide Cisco with reasonably requested inventory and topology information; • The parties will review and approve a Services Activation Plan, including Activation date(s); • Each party will perform any other tasks designated as its responsibility in the Services Activation Plan (e.g., Customer stabilization activities, sharing port requirements, etc.) by the date specified in the Services Activation Plan; • Customer will install and configure a VPN endpoint (with Cisco assistance) using Cisco-provided instructions; and • Cisco will Activate the Managed Elements, per the applicable Service Service Order(s).
Output: Services Activation Plan, Draft Runbook, initial Managed Element inventory, and Change Request, if needed

15. Management of Customer-premise Managed Elements

Summary: Cisco will manage the Manage Elements as described in this Service Description and identified in the Service Order. For example, Cisco may provide Incident Management and Change Management, but not Problem Management for a Customer premises Managed Element..

Accompanying Tasks
• If the Managed Element are provided by a third party, provide Cisco and the applicable third-party supplier with a valid Letter of Agency (LOA) • For third party Third Party Managed Elements, Customer will manage all security incidents, notifications, and/or alerts and notify Cisco of any such security incidents, notifications • If Change Management is not part of the scope of services, manage and perform any Changes to the Third-Party Managed Elements
Outputs: Customer Provided LOA

Appendix A: General Terms and Conditions

1. Services Terms

1.1 Scope of Services. Products and services that are not described in this Service Description are not part of the Services. For clarity, the following are not included in the Services unless Customer purchases them separately or they are requested via an applicable MACD or Service Request:

a) Installation Migration, implementation, configuration of UCM Cloud (except standard dialing and onboarding configurations described above);
b) Software or hardware upgrades or updates to the Managed Elements unless in response to an Incident or Problem;
c) Troubleshooting Incidents that predate Service Activation;
d) Configuration of voice, video, and "Instant Messaging and Presence" (IM&P) services outside of Cisco's standard configuration;
e) Implementing an end user to the Cisco self-care portal;
f) Product or service usability, "how-to" guidance, and questions or training for end users;
g) Initial configuration, new feature introduction, and the support of functionality that has not been previously accepted as operating with specifications; and/or
h) Customization of standard configurations.

1.2 Non-Standard Configurations. The Services are primarily designed for a standard configuration. If Customer uses its own configuration or customizes Cisco's standard configuration after initial implementation, some Services components may not be available (e.g. MACDs, Change Management, Problem Management, etc.), or may be limited. If Customer uses a custom configuration, Cisco will provide the Services "as is" without any warranties or Service Levels of any kind. If Customer wishes Cisco to create and/or to have a fully supported custom configuration, it will be subject to separate mutually agreed terms and charges.

1.3 Managed Elements.

1.3.1 As part of Service Transition, Cisco will describe any limitations of the Services with respect to the Managed Elements, if applicable. For example, certain Third-Party Managed Elements may only be monitored for availability. If needed, the parties will execute a Change Request to reflect the updated scope of Services.

1.3.2 Cisco will not provide Services for any Managed Elements that are either unauthorized (e.g. no valid license) or past their applicable "Last Day of Support" (as specified by Cisco), unless expressly provided in the Service Service Order(s).

1.3.3 Customer must maintain a valid Cisco license and support and maintenance agreement for all Managed Elements. For Third-Party Managed Elements, Customer must maintain an appropriate support and maintenance agreement, covering the Third-Party Managed Elements.

1.3.4 Customer must use the Managed Elements according to their applicable licenses and documentation.

1.3.5 Customer will provide and maintain sufficient connectivity to use UCM Cloud and to connect to Cisco's NOC.

1.4 Reporting. Cisco will provide, or make available via the Portal, the reports listed in the reporting documentation for Cisco Managed Services. Cisco reserves the right to add, change, or remove Reports at its reasonable discretion. Customer may review any reports with Cisco as a part of Service Delivery Management. Customer should notify Cisco within a reasonable timeframe if Customer believes a report is inaccurate. UCM Cloud may also contain additional reports, see the Offer Description for UCM Cloud for additional information.

1.5 Portal. Cisco will provide a web-based Portal that provides Customer at least the following core functionality:

a) Review of Reports and information related to the Services;

b) Ability to submit and monitor Incident tickets; and

c) Ability to submit and monitor Service Requests and MACDs

In addition, UCM Cloud may have additional Web-based capabilities (e.g. onboarding). Please see the UCM Cloud Service Description for additional details. Requests submitted by Customer's requestors are deemed to be authorized by Customer.

1.6 Cisco Managed Services Platform (CMSP). The CMSP will be the system of record for the Services. The CMSP uses cloud-based services to process Managed Element data and provide the Services. These components are hosted in a secure data center with at least one redundant system. See How Cisco Provides Services for additional details. Cisco is responsible for maintenance of the CMSP.

1.7 Cisco Recommendations and Changes. Cisco's provision of the Services is dependent on Customer's compliance with its responsibilities as listed in this Service Description and those responsibilities described in How Cisco Provides Services. In addition, if Customer'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 (e.g., significantly increased number of Incidents), Cisco may charge additional charges to address such items until the recommendations are implemented.

1.8 Governance. In addition to Service Delivery Management, Cisco and Customer will implement a governance function with the following goals: discuss alignment of the services to Customer's business needs and this Service Description, identify opportunities to improve the Services (e.g., increase quality or reliability), resolve disputes, highlight new Cisco technologies, any Services renewals or extensions, identify market and technology trends

related to the Services and similar matters. Cisco will provide an agenda and host remote quarterly governance meetings to discuss the above items.

1.9 Third Party Products. While certain third-party products and services may integrate with UCM Cloud and the Services, Cisco does not provide support or guarantee ongoing integration support for products and services that are not provided by Cisco.

1.10 Policies. Cisco will materially comply with Customer's 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.

1.11 Resale. If a Cisco authorized reseller, distributor or systems integrator authorized by Cisco to resell the Services ("Reseller") purchases the Services for Resale to an End User, then in addition to the Resale-specific terms contained in How Cisco Provides Services, the provisions of this Services Description will apply as between Cisco and Reseller, all references to "Customer" will be deemed to refer to Reseller, and Cisco will deliver the Services to Reseller's designated End User. Reseller will be responsible for obtaining appropriate agreements with Reseller's designated End User reflecting (i) the provisions of this Service Description, (ii) the terms applicable to UCM Cloud and (iii) an obligation to perform responsibilities as required by this Service Description. Where Reseller elects to perform some or all of the Customer's responsibilities on End User's behalf, the parties will reasonably cooperate to provide the Services to Reseller's End User.

2 Commercial Terms

2.1 Pricing Summary. The charges for the Services ("Charges") and payment terms will be detailed in the Service Service Order or Agreement and are based on the Charges for UCM Cloud (e.g. an increase in the number of subscribers to UCM Cloud will result in an increase in the Charges for the Services). The Charges will also include Service Requests or MACDs fulfilled in excess of the amounts contained in the Service Description and Service Service Order.

2.2 Minimum Commitment. The Service Order will specify the minimum term and minimum Charges for the Services. Cisco's rights to invoice for the charges for the Services and Customer's obligation to pay will not be affected by (i) any delays caused by Customer (or anyone acting on behalf of Customer), (ii) Customer's failure to perform or delay in performing its obligations under this Service Description or the UCM Cloud Service Description, or (iii) Customer's purchase Service Order requirements.

2.3 MACDs and Service Requests

2.3.1 MACDs. If Customer wishes to have more than 5% allotted for MACDs, Customer may subscribe to a larger number for an additional fee. Any MACDs not consumed within the monthly period will expire and not roll over to the next month. Expedited and Complex MACD requests are excluded from this entitlement and incur

a fee as outlined in the Service Catalog. Any bulk MACD requests (10 or more of the same action) should be submitted as a single bulk request and will be separately priced.

2.3.2 If a Service Request or MACD exceed Customer's allotment, Customer will pay for the overage at the rates provided in the Service Catalog. Cisco will track the number of MACD and Service Requests fulfilled, remaining requests or SRU's available, and provide this information in its Reports.

2.4 Service Activation. If the Service Order doesn't provide a specific Service Activation date, the Service Activation date will be the same as the activation date of UCM Cloud. [

2.5 Term. The Service Orders will provide the term. If it does not, the term will be the same as the term of UCM Cloud and will be co-terminus with that subscription.

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). There are four impact levels.	**Urgency:** The Urgency of an Incident is classified according to its impact on the Services or ability for end ccustomer to receive the Services and the financial impact to end ccustomer's business. There are four urgency levels.
Widespread: Entire Service or multiple regions are affected **Large:** Multiple locations are affected **Localized:** A single location and/or multiple users are affected **Individualized:** A single or few users (e.g. less than 10) are affected	**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. 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.

Priority Definitions

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

IMPACT					
		Widespread	Large	Localized	Individualized
URGENCY	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 Iimpact 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 Customer will commit any necessary resources 24x7 to resolve the situation.
- P2: Cisco and Customer will commit full-time resources during Standard Business Hours to resolve the situation.
- P3-4: Cisco and Customer are willing to commit resources during Standard Business Hours to restore service to satisfactory levels or provide requested information

Appendix C: Service Level Agreement

1. **Purpose and Scope**. This Service Level Agreement ("SLA") describes Cisco's performance targets for the Technology Services, as described on Attachment A ("**Service Levels**") and the Service Credits Cisco will provide Customer if Cisco fails to meet the Service Levels ("**Service Credit**").

2. **Cisco Managed Services.** This SLA only applies to **Cisco UCM Cloud Enterprise Service**, may be found at the following location: https://www.cisco.com/c/en/us/about/legal/service-descriptions.html, or this SLA will be attached to the agreement to which they apply.

3. **Service Level and Service Credits**. Cisco will perform the Services so that the Service Level Performance will, in each Measurement Period, meet or exceed the Service Levels. Customer will be entitled to claim Service Credits for Cisco's failure to achieve the Service Levels (subject to this SLA).

4. **Performance Measurement**. Unless otherwise agreed in writing by the Parties, Cisco will use its standard processes and tools for measuring its performance and determining whether the Service Levels were achieved.

5. **Performance Reports.** Cisco will issue reports under this SLA as described below:

5.1. The first Measurement Period starts 90 days after the Service Activation date. Where additional Managed Elements are added after the Service Activation Date, the first Measurement Period for those new Managed Elements will be the next Measurement Period (e.g., if a Measurement period is June 1- June 30, and a Managed Element is added on June 14th, that new Managed Element will be a part of the July Measurement Period).

5.2. Cisco will provide to Customer a report on the Service Level Performance for the relevant Measurement Period within thirty days of the end of each Measurement Period ("**Performance Report**").

5.3. Customer will review the Performance Reports and promptly (within 30 days) notify Cisco in writing of any errors or if it disputes the Performance Report. If Customer fails to notify Cisco of a dispute in that time, the Performance Report will be considered final.

5.4. If Customer does dispute the Performance Report, the parties will discuss the matter in good faith.

6. **Term and Termination**. This SLA will start on the on its effective date and will automatically terminate with the termination or expiration of the Service Term.

7. **Entitlement and Application of Service Credits**.

7.1. Customer will not be entitled to any Service Credits unless Customer submits to Cisco a timely written claim for Service Credits. Once the request is validated and Service Credit is issued, Customer may use that Service Request be applied to a particular Cisco Managed Services invoice.

7.2. If a single Incident results in Cisco missing more than one Service Level, Customer may claim one Service Level miss and Service Credit of its choosing.

8. **Service Credit Limits**

8.1. The maximum and aggregate Service Credit amount will be five percent (5%) of the Monthly Service Charges paid by Customer for the Services for the relevant Measurement Period.

8.2. Customer may not transfer, sell, or assign any Service Credits.

8.3. If the Service Term ends and Customer has Service Credits, those Service Credits will first automatically be applied to any outstanding invoices or amounts due. After that, a Service Credit for any Cisco Product or Service will be issue within 60 days of the end of the Services Term.

9. **Exclusive Remedy.** Service Credits are Customer's sole and exclusive remedy against Cisco, for Cisco's failure to meet the Service Levels. Any Service Credits paid by Cisco under this SLA will count toward the limitation of Cisco's liability under the Agreement.

10. **Customer Responsibilities.** Customer will make available to Cisco a single point of contact to work with Cisco and respond to any Cisco requests to verify Service Level performance.

11. **Reseller Credit**. If Customer is an Authorized Reseller, Customer will be responsible for passing any Service Credits to the End Customer.

12. **Exceptions**. Any failure by Cisco to meet the Service Level and/or KPI will be excused to the extent caused by:

a) A material act or omission of Customer in breach of the terms and conditions of Agreement or Service Description, including, any Supplement or Exhibit;

b) Customer's failure to perform its responsibilities in the Service Description (including the referenced How Cisco Provides Services), the Agreement, the Service Service Order, or as mutually agreed in writing.;

c) Any mutually agreed schedule of activities that causes service levels to fall outside of measured and defined Service Level obligations set forth in this SLA (e.g., maintenance windows);

d) Any delays or faults caused by Customer, third party equipment, software, services, support, or vendors not under the control of Cisco (e.g., Carrier cycle time);

e) Any events outside of Cisco's reasonable control;

f) Any Cisco or third-party hardware dispatch and replacement, which may be covered under a separate agreement;

g) failure by Customer to provide a required response necessary for Cisco to meet the Service Levels;

h) any conditions existing prior to Cisco management of the Managed Elements, including any incident, problem, error or other event subject to an open support ticket from a legacy or other third-party service provider; and/or

i) Changes to the Managed Elements that were not approved by Cisco.

Attachment C-1: Service Level

Service Level Target	The Availability Percentage will be **99.995%** or greater for each Measurement Period (as defined below).
Measurement Period	One calendar month
Service Level Calculation and Related Definitions	"**Availability Percentage**" will be calculated as follows, converted to a percentage: **Total Service Time – Total Qualifying Outage Time** **Total Service Time** "**Total Service Time**" equals the average number of Knowledge Workers connected to the System in a Measurement Period, multiplied by the total number of minutes in a Measurement Period (calculated by multiplying 60 (minutes) by 24 (hours) by the number of calendar days in the Measurement Period). Cisco will determine the average number of Knowledge Workers for the relevant Measurement Period based on the information included in the Management Information (MI) report provided to Customer. **"Qualifying Outage"** means an outage for the ability to place or receive calls that is directly attributable to a failure of the System to deliver the Core Services; not a result of customer or Customer fault, and not due to any failure of the System to interoperate with any customer premise Components that are not under the direct monitoring and management of Cisco. For avoidance of doubt, an outage impacted by a customer premise voice gateway that is not under Cisco service's monitoring and management, or a misconfiguration of the application caused by the Customer or customer would be excluded as a qualifying outage. **"Total Qualifying Outage Time"** equals the aggregate sum of the downtime attributable to all Qualifying Outages during the Measurement Period. The downtime for each Qualifying Outage will be calculated by multiplying (a) the total number of Knowledge Workers directly impacted by the Qualifying Outage by (b) the number of minutes of the Qualifying Outage. For the purposes of calculating Total Qualifying Outage Time, each Qualifying Outage will (i) commence upon the earlier of (a) Cisco's detecting the outage or (b) Cisco's logging an Incident ticket upon Customer's notice to Cisco of the outage with sufficient information for Cisco to confirm the outage; and (ii) end when the Core Services are fully restored. The duration of a Qualifying Outage will be rounded upward or downward to the nearest

<table>
<tr><td></td><td>minute.

“System” means the collective Cisco-provided components located in the Cisco’s data canters and used by Cisco to provide the Services to Customer. The following will not be included in the calculation of Total Qualifying Outage Time: (a) outages during scheduled maintenance windows and (b) emergency Operational Changes approved by Customer in advance.</td></tr>
<tr><td>Service Credit</td><td>Subject to the terms of this SLA, Cisco will pay Customer Service Credits will be calculated in accordance with the table below:
<table>
<tr><th>If the Availability Percentage achieved in the Measurement Period is:</th><th>then Customer may claim Service Credits in an amount equal to the corresponding percentage of Customer’s Monthly Service Charges for the Measurement Period:</th></tr>
<tr><td><99.995% and ≥ 99.97%</td><td>1%</td></tr>
<tr><td><99.97% and ≥ 99.95%</td><td>2%</td></tr>
<tr><td><99.95%</td><td>3%</td></tr>
</table></td></tr>
</table>

Appendix D: Supported MACDs

The Table below describes MACD service requests supported:

Add a User (Entitlement Package)	Add a Line	Add a Subscriber Device
Add a Voicemail	Add Extension Mobility (EM)	Add Single Number Reach (SNR)
Add Speed Dials	Add Pickup Group	Add Group Intercom
Add Peer to Peer Intercom	Add a Call Handler	Add Hunt Group
Configuring and administering existing UC Attendant Console	Time of Day Routing calls (ToD)	Softphone (IP Communicator or Jabber)
Modify Subscriber First Name/ Last	Name Modify Line	Modify Softkey Template
Modify Class of Service (COS)	Modify Phone Button Template	Modify Call Coverage
Modify SNR	Modify Call Handler	Modify Hunt Group
Modify Pickup Group	Modify Locale for a Device	Modify User Password / Pin
Modify Speed Dials	Modify Auto Attendant Greeting	Reset Single Phone
Move a User	Move a Phone	Delete User
Delete Device	Delete Speed Dials	Delete Line
Delete Voicemail	Delete Call Handler	Delete Hunt Group
Delete Pickup Group	Delete SNR	Delete EM
Delete Intercom	Translation Patterns (single line)	