SERVICE DESCRIPTION FOR INFRASTRUCTURE AS A SERVICE FOR CISCO UCM CLOUD APPLICATIONS

This document (this "Service Description") describes the Cisco Unified Communications Manager Cloud Infrastructure as a Service ("Services") that the Customer/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 the Services purchased by the Customer will be documented in a written order- e.g., Statement of Work, quote, Service Order, or online order- ("Order") between the parties. 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. To purchase the Services, Partner must also maintain a valid UCM Cloud subscription, and the Services purchased will be co-terminus with the term of the same Customer's UCM Cloud subscription.

Service Summary

Customer may order infrastructure capacity that is hosted and managed by Cisco and on which Customer may deploy Cisco applications or supported third-party applications ("Applications") for use in conjunction with the Customers use of UCM Cloud. Customer may order the Services via a paper or electronic document (e.g., Service Order, Statement of Work, quote, or online order submission) signed or accepted by Cisco that details the Services purchased by Customer, such as pricing, capacity, service term, payment terms, and other commercial terms (an "Order").

- Capacity is provided in predefined "blocks" of hypervisor, CPU, memory, and storage.
- Cisco will provide an online portal to enable the Customer to deploy supported Applications and will be responsible for infrastructure health, ongoing maintenance, and the Service's compatibility with Cisco UCM Cloud (not the Applications).
- Cisco will provide Customer with a Service Catalog to select and configure Customer provided operating systems and other attributes.
- Unless otherwise expressly provided, all Services will be provided remotely from Cisco's global data centers, and all Services will be monitored 24x7x365, except where noted.
- Cisco will provide the Services to meet high availability requirements (see Availability below for additional information).

Cisco will provide technical support for Incidents impacting the operational availability of the hardware platform, portal, and its supporting infrastructure Services as provided in Customer's applicable underlying UCM Cloud support subscription (e.g., Standard Service, Solution Support, UCM Cloud Enterprise Service, etc.).

1. Infrastructure

- Cisco will make available the capacity based on the Customer order (i.e., CPU, memory, storage) and provide instructions to provision the Services.
- Cisco will maintain infrastructure (e.g., HVAC, power, etc.), including installing new patches or firmware for Infrastructure and hypervisors to help maintain performance and remediate security risks to the Services.
- Cisco will maintain compatibility between the Services infrastructure and UCM Cloud (not the Applications).
- Cisco will support virtual machine failover if there is a hardware failure.
- Cisco to provide a datastore with install media for all available Applications.
- Customer is responsible for providing needed operating systems.
- Cisco will plan and communicate maintenance windows with reasonable advanced notice required to maintain the

infrastructure.

2. Portal and Service Catalog

Cisco will provide and maintain an online portal with a service catalog to configure the Services so that Customer may deploy supported Applications.

3. Capacity

- Cisco will provide the capacity as provided in the Order.
- Capacity is sold in pre-defined "blocks" of CPU, memory, and storage and no substitutions or mix/match is permitted.
- Each block provides 1vCPU, 4GB memory and 125GB of storage.
- This capacity above is listed as a single quantity unit in the Order.
- Customer will be responsible for determining and adhering to capacity requirements for each Application.
- If needed, Customer must purchase additional capacity as needed- Cisco will not oversubscribe capacity.

4. Provisioning

Customer will be responsible for the following:

- Providing, maintaining, monitoring, and troubleshooting all Operating System and Application licensing, installation, interoperability with the Services, configuration, and management;
- Implementing and maintaining any compatibility between the Operating System, Application(s) and UCM Cloud;
- Performing timely Application and operating system maintenance (e.g., install patches) and release management to remediate security risks, including remediating any Critical (Score: 10) Common Vulnerability Scoring Standard (CVSS) within 48 hours and any High (Score: 7-9.9) CVSS vulnerabilities within 10 days.
- Customer is responsible for any Security Incident Monitoring and Response activities associated with the deployed Operating Systems and application services.
- Determining the capacity requirements for all Applications;
- Performing security scans to identify and remediate any security vulnerabilities or incidents with the Applications and associated data;
- Deployment, operation, and monitoring of any required Application or data backups. For avoidance of doubt, Cisco does not perform virtual machine level backups of IaaS virtual machines;
- Installing and maintaining appropriate security and intrusion protection software for the applicable operating system and Applications;
- Using the IP address from Cisco provided blocks of the Services; and
- Updating UCM Cloud SSL certificates if required

5. Availability

- Cisco will provide the Services to meet high availability for the location(s) selected. However, Customer is responsible for ordering the Services for the locations and the corresponding configuration to enable geo-redundancy or high availability across locations.
- Customer may access the Services from the current locations listed in the table below with data centers located in the same country. These location(s) will be provided in the Order.
- Infrastructure blocks may not be shared across locations.

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

6. General Terms and Limitations

- Unless the Services are expressly provided for above, all other Cisco services are out of scope for this Service Description.
- Each instance of the Services may only be used by Customer to host Applications for use with Cisco UCM Cloud for its internal use (or for a named end user if Customer is an authorized reseller).
- The Services may not be used for general computing or for any purpose not expressly described in this Service Description.
- The Services will not enable Internet access for any Applications, Internet access will be via the Customer network.
- Customer is responsible for safeguarding the customer data, including sensitive and/or PII data, the customer may store and/or generate in the Services, operating system, and applications. See the UCM Cloud terms for Cisco's privacy and security obligations for UCM Cloud.
- Customer is responsible for Identifying and resolving any dependencies for out-of-scope hardware, software and/or services.
- Cisco reserves the right to conduct periodic vulnerability scans on all hosted Applications and the Services. If Cisco identifies a vulnerability or evidence of a security incident that is determined to be a risk to the UCM Cloud and/or the Services Cisco may temporarily disconnect the Application or Services. Cisco will make reasonable attempts to notify Customer before it performs this action.
- Use of the Portal and any ancillary software or services is according to the EULA in the UCM Cloud agreement. Upon expiration or termination of the Services, the license to the Portal will automatically terminate.

Attachment A- Service Level Objectives (SLO)

1. **Purpose and Scope**. This SLO describes:

1.1 The parties' responsibilities and sets Cisco's performance targets (Service Levels) for the Services
1.2 Actions Cisco will take if there is an unexcused failure to meet the Service Levels provided below.

2. **SLO Scope**. This SLO only applies to the Infrastructure as a Service ("Services") and not to UCM Cloud.

3. **Service Level Objectives (SLO).** If Cisco fails to meet the Service Levels provided below, it will review the reasons it failed meet the Services Levels and will use commercially reasonable efforts to remediate the cause of the failure. However, other than the obligation above, there will be no financial or legal penalty if Cisco fails to meet the SLOs.

4. **Service Levels**

Infrastructure Availability	
"**Availability**" is the availability of the infrastructure to host Applications, converted to a percentage: **Calculation**: (Number of minutes in the month – Outage Time) / Number of minutes in the month. "**Outage Time**" shall commence upon the earlier of: (1) Cisco's detecting the outage and logging an Incident ticket or (2) Cisco's logging an Incident ticket upon Customer's notice to Cisco of the outage, which notice contains sufficient information to confirm that the outage is occurring in the Services. The Outage Time ends when the System is returned to a usable level of service. The duration of Outage time shall be rounded to the nearest minute. Cisco will log an Incident ticket promptly following notification from Customer or its own detection of an outage.	
SERVICE LEVEL	**Infrastructure Availability**: 99.99%
MEASUREMENT PERIOD: Monthly (one calendar month)	

5. **Exceptions.** Any failure by Cisco to achieve the Service Levels will be excused if caused by:

   a. A material act or omission by Customer in breach of the terms and conditions of the Agreement or the Service Description
   b. Any mutually agreed schedule of activities that causes service levels to fall outside of measured and defined Service Level obligations set forth in this SLO;
   c. Any delays or faults caused by Customer
   d. Periods of maintenance where updates, patches, etc. are installed and configured (i.e., Maintenance Windows);
   e. A Force Majeure event;
   f. Failure to implement Cisco's recommendations necessary to remediate Incidents;
   g. Failure by Customer to provide a required response necessary for Cisco to meet the Service Levels; or
   h. Errors or security vulnerabilities in the Applications that cause the Service Level to be missed.