Offer Description

IMPORTANT: READ CAREFULLY

Context Service Offer Description

The Cisco Universal Cloud Agreement ("**Agreement**") and the terms in this Offer Description govern your use of the Cisco Context Service ("**Cloud Service**"). A current copy of the Agreement is located at: http://www.cisco.com/c/en/us/about/legal/cloud-and-software.html. All capitalized terms not otherwise defined herein shall have the same meaning as provided for in the Agreement. In the event of a conflict with the Agreement, this Offer Description shall control.

Overview of the Cloud Service

The Cloud Service is a Cisco operated, cloud-based, semi-structured data storage service that interoperates with release 11.5 and higher of Cisco's Contact Center Express and Contact Center Enterprise solutions. You may use the Cloud Service to integrate a wide variety of contextual data from the interactions that Your customers have with Your business – whether via voice, chat, social media, email or web – to provide Your agents with the information that they need to deliver a personalized service experience to Your customers.

Cloud Service Entitlement

The Cloud Service is provided to You with the purchase of Cisco Software Support Service for Cisco Contact Center Express or Cisco Contact Center Enterprise release 11.5 and above ("**SWSS**"). You may activate and use the Cloud Service if (i) Your billing address is located in any country other than those listed in the Geographic Availability Restrictions section, below, and (ii) You have an active SWSS subscription for one or more of the following Cisco Contact Center products:

- Unified CCX agent licenses – all types
- Unified CCE agent licenses – all types
- Unified CVP port licenses
- Packaged CCE agent licenses
- HCS-Contact Center agent licenses

Cloud Service Support

Support for the Cloud Service is the same support that you receive under your SWSS service contract. The SWSS Service Description is available on the Cisco Services Descriptions page at the following address: http://www.cisco.com/c/dam/en_us/about/doing_business/docs/cisco-software-support-service.pdf

Security Features

Cisco cannot see any information that You have identified as Personally Identifiable Information (PII) or encrypted and You also define how data is classified. The security model is detailed in this white paper https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cloudCollaboration/context-service/cisco-context-service-security-white-paper.pdf.

Third Party Application Integration

Cisco provides a developer kit on Cisco DEVNET (https://developer.cisco.com/) that You may, subject to the DEVNET terms and conditions, use to integrate the Cloud Service with third party applications.

Data Center Locations

Cisco operates the Cloud Service exclusively in data centers that are located in the United States.

Cloud Service Activation

Activation Overview

To activate the Service, You will need a current email address and a password. The Cisco reseller from which you purchased SWSS will create your Cloud Service entitlement. You will then use that email and password to connect Your Cisco Contact Center Express or Contact Center Enterprise solutions with Cloud Service. Cisco strongly recommends that you change your password once you have logged into the Cloud Service administrator portal.

Customer Responsibilities

General Information and Reasonable Assistance.

You shall supply Cisco with all reasonably requested and reasonably necessary, accurate, complete, and up-to-date information that Cisco requires to supply the Cloud Service to You, such as information concerning Your hardware and software environment, networking information, and similar information. You will work with Cisco in a timely manner to aid in Cisco's provision of the Cloud Service to You by assisting with any third-party cooperation, documents or approvals required for provision of Cisco's Cloud Service. You understand that if You delay providing the information or cooperation or approvals required to enable the service, Cisco may delay the provision of its Cloud Service to You.

Issue Triage & Resolution.

You will provide a technical resource to capture and provide details of reported issues, aid in replication and triaging issues as reasonably requested by Cisco, aid in testing fixes of issues, and determining if any issues are related to Your hardware, software, applications, or other sources.

Data Protection

You control the access to Your data and must maintain appropriate security against unauthorized access, use or deletion of Your data. You must establish and maintain appropriate security policies within Your infrastructure, as well as any operating systems or applications, to secure the connection with the Cloud Service.

- You are responsible for any catastrophic security events that result from any unauthorized configuration of the Cloud Service components by Your personnel. These include, but are not limited to, configuring the Cloud Service components in a manner not prescribed in the Documentation, creating an open relay, changing the network configuration set by Cisco, shutting down Cisco's infrastructure, etc.
- You are solely responsible for managing and controlling access to Your administrator credentials that You use to access the Cloud Service. You shall immediately modify your credentials if You think or have reason to know that a third-party has access to your credentials. You shall also take measures to maintain the security of Your credentials and ensure that only individuals that are duly authorized by You have access to the Cloud Service. You shall ensure that credentials are used only by the person to whom they were assigned. Cisco shall not be liable if a third-party gains unauthorized access to your Credentials. You shall indemnify and hold Cisco harmless in respect of any damage Cisco may incur as a result from such unauthorized access.

Cloud Service Operations

Support and Escalation Guidelines

Support and escalation is provided as set forth in the associated Service Description for SWSS.

Maintenance and Updates

- From time to time, Cisco performs scheduled maintenance, to update the servers and software that are used to provide the Service. Cisco will make all notifications for such scheduled maintenance solely via https://status.ciscospark.com/. Notwithstanding the foregoing, You acknowledge that Cisco may need to perform emergency maintenance without providing advance notice.
- Cisco reserves the right to modify and update the features and functionality of the Cloud Service. These updates shall include any subsequent release or version of the Cloud Service containing functional enhancements, extensions, error corrections or fixes which are generally made available free of charge to eligible customers as defined above. Updates shall not include any release, option or future product which Cisco licenses separately or which is not included under the applicable level of support.
- Cisco provides notice of any material modification or update via http://www.cisco.com/go/contextservice. Cisco will use reasonable efforts to ensure that any modifications or updates do not materially degrade the performance of the Cloud Service or Your use of the Cloud Service.
- Cisco will use reasonable efforts to implement modifications or updates in a manner that minimizes the impact on Your use of the Cloud Service.
- Cisco must occasionally schedule maintenance windows, which Cisco tries to minimize so that the Cloud Service achieves the Uptime Objective. Cisco endeavors to provide You with notice of any suspension of the Cloud Service ("**Service Suspension**") seven (7) days in advance, post updates on progress during suspension of service, and to post updates regarding resumption of Cloud Service following any such suspension. Cisco currently posts such information publicly, but shall have no liability for the manner in which we may do so or if we fail to do so.

Service Objective for Uptime and Unscheduled Availability

Cisco operates the Cloud Service in a manner that seeks to achieve an uptime of 99.9% ("**Uptime Objective**").

You acknowledge that Your access to and use of the Cloud Service may be suspended for the duration of unanticipated or unscheduled downtime, including as a result of catastrophic events, external denial of service, or operational incidents. Cisco endeavors to minimize and eliminate incidents under its control to achieve its Uptime Objective.

Service Objective for Disaster Recovery

Cisco backs up the Production Mode data stored in the Cloud Service and provides disaster recovery operations to protect the data that is stored within the Cloud Service. Under a disaster scenario, Cisco endeavors to restore data to a period no more than 24 hours before the incident occurred ("**Recovery Point Objective**"), as part of its disaster recovery practice.

Limitations and Disclaimers

Cisco makes the Cloud Service available on an "AS IS" and "AS AVAILABLE" basis.

Service Objectives described in this Offer Description are used solely by Cisco to monitor the performance of the Cloud Service. Cisco shall not be liable whatsoever if Cisco fails to meet its Service Objectives.

Record Retention Limits

The Cloud Service provides data tiers and operational modes that You may configure to customize the Cloud Service.

- A "**data tier**" is a collection of settings associated with record limits, and record online retention, record offline retention, backup, and other data governance attributes. Cisco offers a single standard tier ("**Standard Tier**"), however custom tiers may be negotiated.
- There are three operational modes – production, lab, and trial, as described below. Production mode is intended for normal business operations, and lab mode for experimentation. If You are a Cisco Spark Care customer then you also have access to a trial mode.

The Standard Tier

Cisco does not support offline storage for any of the modes of the Standard Tier. All data is stored exclusively in Cisco data centers. The Standard Tier includes the following modes:

Production Mode

- No imposed record limits outside organizational maximums.
- Data is held online for 18 months. Records older than 18 months may be deleted on rolling monthly cycle
- Data is backed up with a 24-hour Recovery Point Objective for disaster recovery.

Lab Mode

- Limit of 50,000 records after which new records will not be able to be added. The customer can delete old records and then add new.
- Data is held online for 90 days. Records older than 90 days are disposed on a rolling monthly cycle.
- Cisco does not backup the data.

Trial Mode (for Cisco Spark Care customers only)

- Limit of 50,000 records, after which new records will not be able to be added. The customer can delete old records and add new records during the trial period.
- Cisco retains data during the 90-day trial period. Within the 90-day trial, customers who purchase Cisco Spark Care can transition their records to production to retain them.
- Cisco does not back up the data.

Geographic Availability Restrictions

In addition to any restrictions under Section 16 of the Agreement, the Cloud Service is not available to Cisco customers located in the Russian Federation or the People's Republic of China.