Service Description: Cisco Managed Services for Collaboration: Unified Communications and Unified Contact Center

Technology Addendum to Cisco Managed Services for Enterprise Common Service Description

This document referred to as a Technology Addendum describes the Cisco Managed Services for Collaboration: Unified Communications (UC) and Unified Contact Center (UCC).

Related Documents: This document should be read in conjunction with the Cisco Managed Services for Enterprise Common Service Description posted at www.cisco.com/go/servicedescriptions.

Direct Sale from Cisco

If you have purchased these Services directly from Cisco, this document is incorporated into your Master Services Agreement (MSA), Advanced Services Agreement (ASA), or equivalent services agreement executed between you and Cisco. If not already covered in your MSA or equivalent services agreement, this document should be read in conjunction with the Related Documents identified above. In the event of a conflict between this Service Description and your MSA or equivalent services agreement, this Service Description shall govern.

Sale via Cisco Authorized Reseller

If you have purchased the Service through a Cisco Authorized Reseller, this document is for informational purposes only; it is not a contract between you and Cisco. The contract, if any, governing the provision of this Service is the one between you and your Cisco Authorized Reseller. Your Cisco Authorized Reseller should provide this document to you.

The Service

This Technology Addendum is designed to be read in conjunction with the Cisco Managed Services Common Service Description that provides a baseline understanding of and sets expectations about the Cisco Managed Services, hereinafter referred to as the Service, provided by Cisco. In addition to the activities and deliverables outlined in the Common Services Description, this Technology Addendum outlines the unique activities and deliverables for the Customer's UC and UCC devices and infrastructure that are being managed by Cisco. Both service descriptions should be read in combination to fully understand the scope of the Service being purchased.

The Service described herein, and other optional services are intended to supplement a current support agreement for Cisco products, and only available where all the Managed Components in a Customer's network and Cisco Unified Communications Solution are supported through a minimum of core services such as Cisco's SMARTnet, Software Application Services, Essential and Essential Onsite, as applicable. Cisco will provide the Service described below as selected and detailed on the purchase order for which Cisco has been paid the appropriate fee.

Cisco shall provide a Quote setting out the extent of the Service and the term for which Cisco will provide the Service. Cisco will receive a purchase order that references the Quote agreed between the parties and that, additionally, acknowledges and agrees to the terms contained therein. Cisco only provides support for Managed Components, unless specifically noted. For any device, component or solution element not specifically designated as a Managed Component, Cisco shall have no responsibilities whatsoever.

This Technology Addendum describes the services capabilities, supported devices, elective changes, and reports delivered.

Two managed service packages are available:
- Standard Managed Services
- Comprehensive Managed Services

These service packages are described in detail in the Common Service Description. In addition to these two service packages, the Customer can also purchase Optional Services as needed to augment the selected package. The table below outlines the specific activities and deliverables provided under the Unified Communications and Unified Contact Center offer as well as the Optional Services available for the Service.

Activities / Deliverables	Standard Services	Comprehensive Services	Optional Services
Remote Monitoring	X	X	
Quality of Service Ticketing	X	X	
Backups	X	X	
Standard Reports	X	X	
Advanced Reports		X	
Defined Changes			X
Custom Changes			X
Dedicated Reporting Server			X
Business Continuity			X
IP-SLA Monitoring			X
Phone Problem Reporting			X
Non-Cisco Contact Center Application Support			X

1   Subscriber Definitions

- **Essential Subscriber** – Subscriber that uses an analog or fax end points or entry-level Cisco IP phone. Entitles the subscriber for support of voice only services. Analogous to an Essential licensed user.

- **Social Subscriber** – Subscriber that uses Instant Messaging (IM) and Presence functions only (no voice/video service). Entitles the subscriber for IM and Presence support.

- **Enhanced Subscriber** – Subscriber that has voice, IM, Presence and standard voice and video features and mid/high endpoints that are used as device as anonymous/share Pubic space (e.g. Extension Mobility endpoints). Entitles the subscriber for support of voice, IM and point-to-point video entitlement. Analogous to an Enhanced or Enhanced Plus licensed user.

- **Standard Subscriber** – Subscriber that has voice, voice mail, advanced voice features, point-to-point video and mobility features. Entitled for support of up to 10 end points such as a hard

phone, soft phone, wireless, and/or smart phone client. Analogous to a CUWL Standard licensed user.

- **Professional Subscriber** – Subscriber that has voice, voice mail, advanced voice features, mobility, point-to-point video and contact center entitlement. Entitled to have up to 10 end points supported. Analogous to a CUWL Professional licensed user.

- **Executive Subscriber** – Professional Subscriber profile plus Live Desk support**.**

- **CC Inbound Agent** – Agent performing inbound call center activities.

- **CC Inbound/Outbound Agent** – Agent performing inbound and outbound call center activities.

- **CC Multi Channel Agent** – Agent using social tools like chat, email, video, etc for call center activities.

- **ICME Agent** – Agent connecting to a standalone Intelligent Contact Management Enterprise (ICME) deployment.

- **Sites** – A site is a physical location that Subscribers included in the service reside.

- **Nodes** – Combination of a managed application, Operating System, Virtual Machine and compute. Count is analogous to an application under management.

- **Cisco Unified Border Element (CUBE)** – Device that runs the Cisco Unified Border Element feature set.

- **IPT or Large/Modular Analog Gateway** – Device that runs the Unified Communications Gateway and/or SRT feature set. Or VG350 or analog service module.

- **Analog Gateway** – Device that connects non-IP phones to a Unified Communication solution such as a VG224 or VG248.

- **CME/CUC** – Device that runs the Communications Manager Express or Cisco Unified Connect Express feature set.

2   Standard Package Features

2.1 UC and UCC Remote Monitoring Capabilities

The Service provides real-time monitoring on key UC and UCC components and proactively declares incident events for:
- System and/or application availability

- System and/or application performance

- Hardware environmentals

- Operating system availability

- Syslog and traps

2.2 Quality of Service Ticketing

Voice Quality of Service (QoS) monitoring and ticketing is an important element of the UC & UCC offer. The capability provides monitoring of QoS metrics like jitter, latency and packet loss as indicated within a Mean Opinion Score (MOS).

The Service delivery platform analyzes Unified Communication Manager call processing metrics—ranking individual QoS attributes and providing a corresponding mean opinion score (MOS) for each call—providing staff with an estimation of the call quality as it may have been perceived by the telephone user. The quality analysis engine is tunable within the Cloud and Managed Services

Platform (CMSP) to map directly to the level of call quality that a support organization wishes to establish as the benchmark. Benchmarks, or threshold criteria, is configured to match the level of monitoring mutually agreed by the Customer and Cisco.

2.3 UC and UCC Backups

Backup activities include monitoring the state of the backup service/process within applications such as Cisco Unified Communications Manager. The Service does not include the verification of the content or completion of a backup, but simply the status of the backup process. See the Technology Addendum for Cisco Managed Services for Enterprise Networks service description for information about backup services for IOS and CatOS devices.

2.4 UC and UCC Standard Reports

The CMSP constantly gathers device level information from the Managed Components covered within the Service. This information is compiled and made available via reports available on the Portal. Device level reports available include:

- **Bandwidth Utilization** – Bandwidth usage per day across monitored devices
- **Graph Export** – Downloadable reports of performance metrics
- **Hardware Inventory Report** – List of hardware components under management
- **Key Performance Indicators** – Performance metrics and resource utilization
- **System Infrastructure Report** – IOS image per managed device
- **Top Active Devices** – Devices that caused the most incidents
- **Registered Phone Count Report** – Record of registered phones at the time that the report is generated
- **Voice Service Levels** – Voice service levels per device pool. Cisco measures MOS to determine call quality.
- **Cisco Version Report** – Cisco IOS/CatOS version information
- **System Uptime** – Device uptime metrics
- **Syslog** – Logs from the syslog system log module

3 Comprehensive Package Features

3.1 UC and UCC Advanced Reports

Advanced Reports provide a detailed look at the Service and the Managed Components covered by the Service. Specific reports include:

- **System Hardware Report** – Identifies each hardware component under management and provides the following information: host name, IP address, device model, serial #, site name, contract expiration date.
- **System Infrastructure Report** – Identifies IOS image and flash/RAM per managed device and consists of the following information: site name, host name, device model, modules, IOS version, IOS subset, IOS image name, Flash (size), RAM.
- **System Application Report** – Identifies OS releases and fixes per MCS and equivalent server under management. The report contains the following: site name, device name, device model, model #, device manufacturer, OS type, OS version, application version, hot fixes.

- **Registered phone count report** – Identifies registered phones at the time that the report is generated. The report contains the following: CUCM host name, CUCM IP address, CUCM cluster site location, device type, device registered ID (MAC address), device description, calling search space, partition, device IP address, status (registered or not registered); creates summary report xx phones registered; creates a historical trend report month by month.

- **Inventory Report** – Lists all active Customer managed devices, by site name, device type/model, device name, managed Customer IP address (if NAT), last good backup (IOS/CAT OS) and config archive exceptions. The report consist of the following: site name, site location, device type, device name, IP address (Natted), IP Address (not Natted), SNMP community string, activation date (optional) and date of last backup.

- **Global Ticket Report** – Identifies the devices in the system that have been impacted by an Incident or Problem and the extent of AutoCase activity. The device names indicate the location in production environments. The end user selects the system and time frame, and generates a report via the Portal.

- **Service Experience Report** – Identifies top ten sites that have experienced the most tickets and indicates the causes. The report consists of: site name, site location, # of Change tickets, # of Incident tickets, device type, device name, and major cause.

- **Application Server Report** – Identifies the following key server statistics: Utilization of CPU, memory, disk space, network and Service status of all monitored services on Cisco UC & UCC servers. The end user selects the server time frame and generates a report via the Portal.

- **Voice Service Level Summary Report** – Provides Cisco Unified Communications Manager cluster-based report representing: MOS, latency, jitter, packet loss, disconnect cause summary, call type report and inbound/outbound call report.

- **Operations Report** – Provides monthly ticket activity, detail by user, suppression, created by, notification and response times.

4 Service Options

4.1 Customer Requested Change Management

Customers purchase a block of support hours that can be used for Defined Changes and Custom Scoped Elective Changes that a Customer has purchased as part of the Service. The Customer must have a sufficient balance of support hours on account to cover the requested change. Additional support hours may be purchased if required.

4.1.1 Defined Changes

Defined Changes are categorized into Small, Medium, and Large activities. A Defined Change is a requested change by the Customer that is pre-approved and does not cause a risk to the environment. Defined Changes are not the result of Cisco Incident Management and/or Problem Management processes. The Customer identifies the needed type of change and submits a Defined Change Request via the Portal.

4.1.1.1 Defined Changes – Unified Communications

Defined Changes Type 1:

- Phone administration (single phone):
    - Adding a new phone

- Adding a new user
- Configure/Change/Delete Lines
- Configure speed dials
- Configure XML services (e.g. Extension Mobility) NOTE: If service is provided
- Agent Association with skillset/queues
- Dial plan administration
  - Time of day routing of calls (THIS DOES NOT INCLUDE DESIGN)
  - Configuring line and hunt groups
  - Configuring and administering UC Attendant Console
- MeetingPlace/MeetingPlace Express
  - Managing user accounts and groups

Note: Customer may submit up to 12 type 1 MACDs per business day. More than 12 per customer per business day will be negotiated.

Defined Changes Type 2:

- Configuring and administering Auto-Attendant (options, recordings, prompts)
- IP Communicator setup (includes call-manager config and personal computer walkthrough)
- CUCM: Add or update user directory entries – per 20 entries
- CUCM: Configuration of BV Endpoint, simple – per change
- CUCM: Reboot a single CUCM node
- CUCM, UC, UCCX, CER, Presence: Install SW feature COP file – Additional nodes

Defined Changes Type 4:

- Cisco Unity
  - Unity Call Handler changes
- Gateway Administration
  - Allocate Directory Numbers (DN) to trunks for analog ports (1 trunk)
- Cisco Communications Manager
  - CUCM: Configuration of call routing or feature
  - Reboot multiple CUCM nodes and verify database sync
  - Configure Disaster Recovery per cluster
  - CUCM, UC, UCCX, CER, Presence: Install SW feature COP file – First node
  - Upgrade phone firmware (up to 100 endpoints)
- Other
  - CUCM, UC, UCCX, CER, Presence: Install SW feature COP file – First node

Defined Changes – Type 8:

- License uploads/audits
- Private Line Ring Down (PLAR)
- Upgrade phone firmware (up to 1000 endpoints)

4.1.1.2   Defined Changes – Unified Contact Center

Defined Changes – Type 2:

- Computer Telephony Integration (CTI)
    - Port and route point integration updates
- Routing script adjustments
    - Perform changes to routing scripts in support of call routing applications
- Administration script adjustments
    - Perform changes in support of administrative applications
- Configuration Manager Changes
    - Perform updates to Configuration Manager
- Port Administration
    - Modifications
    - Turn up/down
- Wave File, Text to Speech (TTS) and access services router (ASR) Administration
    - Changes to, prompts, vocabulary, administration, tuning and basic call transfer
    - File additions, modifications and deletions
- Email Administration
    - Administration of application
- Ingress Gateway Administration
    - Service changes for new application deployments, call service additions and dial peers
    - Administer changes to the ingress gateway
- Gatekeeper Administration
    - Changes to gatekeeper configuration
- Outbound campaign modifications
    - Administer the system configuration
    - Changes to dialer lists, modes and scripts
- CVP self-service applications in Audium/Design Studio
    - Application changes and enhancements
- Session Initiation Protocol (SIP) Proxy Server
    - Configuration and Table changes
- CVP Operations Console and Reporting server and Database
    - Application changes and enhancements
    - File additions, modifications and deletions

Defined Changes Type 4

- Computer Telephony Integration (CTI)
    - Scripting updates
- Provisioning applications and interfaces

- Provisioning of integration elements between applications
- License Administration
  - Administer modifications to licenses, including additions and deletions
- Outbound campaign modifications
  - Administer outbound campaign application
- CVP self-service applications in Audium/Design Studio
  - File additions, modifications and deletions

4.1.2 Elective Custom Scoped Changes

Custom Scoped Elective Changes are Customer requested changes that fall outside Incident and Problem (Standard) changes for restoring service. Custom Scoped Elective changes require a mutually agreed upon statement of work (SOW) that describes the scope of changes to be executed. See Cisco Managed Services for Enterprise Common Service Description for more details of Custom Scoped Elective Change support.

4.1.2.1 UC and UCC Custom Scoped Elective Changes

Examples of UC and UCC Custom Scoped Elective Change activities are listed below. This list is not intended to be a complete list but rather to show the type of changes Cloud and Management Services for Collaboration: UC and UCC can perform:

- Dial plan administration
  - Minor dial-plan updates and corrections
- Cisco Media Convergence Server (MCS) and Unified Compute System (UCS) administration
  - Operating system patches (does not include patch evaluation/testing and subject to the Managed Service approval)
- Cisco application software administration
  - Apply Cisco-recommended minor software updates and patches
  - Apply Cisco-recommended (minor, same code train) software updates security-related purposes
  - IOS same-train software upgrades
- Capacity Planning – Supplemental activities of Optimization services from Cisco Advanced Services
  - Evaluation of Network performance and current resource utilization
  - Determining impacts and required modifications to support new applications and services
- Creation of custom reports
  - Consultation
  - Definition
  - Configuration

- Creation of custom dashboards
  - Consultation
  - Definition
  - Configuration
- SIP Proxy Server
  - Upgrades, additions, modifications and deletions
- Feature Upgrades
  - Communications Manager, Unity Connection, Router IOS, etc. major upgrades

4.1.2.1.1   Discovery Audit

For Customers with existing Cisco equipment, a discovery audit may be required in order to turn-up service if the details of how a UC or UCC solution is deployed are unknown or unconfirmed. The discovery audit service will be Custom Scoped and conducted by Managed Service Team using Cisco-supplied processes and tools.

If the Customer so elects, Cisco can perform this audit as a Custom Scoped Elective Change Service. The audit process will use Cisco-supplied macros to identify peripherals, routing clients, dialed numbers, dialed number map, call types, services, routes, peripheral targets, labels, device targets, skill groups, skill group members, agents, person and agent person map.

The audit, where applicable, will provide the following documentation:

- Architecture diagrams (to include Trunk and Port counts per peripheral)
- Network diagrams (to include IP addressing for visible and private Networks)
- Design Docs
- Network implementation plan
- As-built documentation
- Customer change control process
- Mapping of DNIS to call types, variables and scripts
- Population points of all variables

4.1.2.1.2   Synthetic Transactions

The Synthetic Transactions function is a Custom Scoped service in which the Cisco service delivery platform provides the advanced capability to run both OnDemand call tests and scheduled AutoTests. This function allows support personnel to easily test call processing throughout the Network from a centralized support site or any other location. All synthetic call tests are an optional service component and are available for additional fees.

- The OnDemand call test function, conducted from within Entity Manager, generates a call to a specific entered number. The OnDemand test is run without preparation, reservation or advance notice. The number may be an internal or external destination. Following execution, a call trace log is presented that states the success or failure of the call. A verbose call trace, providing detail on each call step, can also be accessed.

- When the test is complete, the CMSP systematically obtains the Unified Communication Manager call detail record (CDR) for the call and presents it for analysis.
- The AutoTest capability runs under the control of the Portal event analysis engine. The test is run at routine intervals to select destinations established in the Portal configuration. Destinations may be established to test service to a specific location, or to destinations for the purpose of testing a prescribed path. For instance, if a retail location in a store chain opens at 9:00 a.m., the CMSP can be configured to generate an AutoTest call to the store at 6:00 a.m. If the test call is not completed successful, an incident ticket is generated explaining the condition and the appropriate support staff notified so that corrective action can be taken before the store opens for business. Customer-assisted configuration for the supporting call processing aspects may be required.

Within the service delivery platform Entity Manager, support personnel can view a log of AutoTest results, including their pass or fail status. From the log, personnel can also access the case that has been generated for failed calls to get additional detail, view the call trace, or view the CDR that culminated from the test call.

4.2 Dedicated Reporting Server

The dedicated reporting server option supports extended offline storage of management and performance data gathered through normal operation. Data is regularly moved from the primary service delivery platform system to the dedicated report server. Customer can access this data for reporting or data mining. This option is for organizations that need to store call detail records for an extended period of time, or for those that wish to examine historic system performance data.

4.3 Business Continuity

The Service business continuity option optimizes support for geographically-dispersed service delivery platforms. It enables redundant management applications to provide backup capability in the event of data center failures. Cisco Unified Communications Microsoft Windows servers systematically confirms on a programmable, routine basis that vital configuration files are synchronized between primary and secondary systems, to address redundancy in the event the primary system fails.

4.4 IP-SLA Monitoring

This option provides access to analyze IP SLA statistics, for a consistent, scheduled approach to voice management. These statistics are monitored and recorded within the IP SLA section of the service delivery platform.

The Service team utilizes IP SLA, in conjunction with MOS scoring, to enhance monitoring of converged voice networks. IP SLA monitoring is based on regularly-scheduled testing, while individual phone calls are random and less frequent.

To provide additional insight, Cisco employs in-depth IP SLA analysis. The test requires the use of two routers, configured as a source and a responder, running IP SLA, a feature within Cisco IOS.

Each minute, the source router generates 100 packets at a rate of 50 per second, which are tagged with the voice class of service. This method ensures that the test packets follow the same path as voice packets, with a small size that does not impact network performance.

As the packets leave the initiator, they are tagged with a date/time stamp. The packets are also date/time stamped when arriving at the responder. These same packets are then marked in the same

fashion when leaving the responder, and once again when arriving back at the initiator. Test data is analyzed to determine jitter, latency and packet loss.

4.5 IP Phone Problem Reporting

The XML Integration enables users who are experiencing an incident with voice services to use the dynamic capabilities of Cisco IP telephone menus to report the problem to support personnel. When an incident report is submitted from a phone, the Service automatically opens a case that includes the available Unified Communication Manager detail reported for the event. Support personnel analyze the issue, take the appropriate actions, and work the case through to completion using the Service's Incident Management capabilities. Case data is archived to form a centralized repository on the time, type, and frequency of incidents, as well as the stations impacted.

Subscription services include:
- Cisco IP Telephone XML integration application
- XML code maintenance support

Activation services include:
- Provide XML code and configuration guidelines for installation of application on Cisco Communications Manager
- Testing

4.6 Non-Cisco Contact Center Application Support

As part of this optional service component, Cisco will provide the following activities:
- Cisco will provide monitoring of the compute infrastructure upon which the non-Cisco Unified Contact Center solution elements reside. Monitoring details will consist of information provided in the Unified Communications and Data Center Monitor Details for the compute systems.
- Cisco will provide monitoring of non-Cisco applications services when provided such details by the non-Cisco application provider. Monitoring will consist of service failure, notification and ticket creation.
- Cisco will manage incident tickets for the non-Cisco application and compute system either initiated by automated monitoring or user. Management will consist of responding to and coordinating incidents until service is restored.
- Cisco will execute Standard changes to remediate Incidents. These changes will be consumed from the Elective Service Hour pool.
- Cisco will execute application elective changes and administrative MACD's as part of Elective Service Hours. Elective changes will be scoped at the time of request.

Troubleshooting Incidents or third party Managed Components may be dependent on collaboration with non-Cisco organizations.

Cisco requires applicable Letters of Agency in order to coordinate on Customer's behalf for the management of non-Cisco components.

As part of its role in providing support for non-Cisco Managed Components, Cisco will:
- Engage Customer non-Cisco parties as necessary to maintain service and resolve issues, including escalation to
- Customer for non-Cisco non-responsiveness.

- Provide and coordinate requisition and fulfillment activities for Managed Component replacement with non-Cisco vendors as needed
- Triage and escalate problems to appropriate support staff or non-Cisco party suppliers for resolution subject to Customer entitlements and established Letter of Agency between Customer and Cisco.

Cisco Responsibilities
- Activate monitoring of non-Cisco application and compute within Managed Service platforms.
- Monitor compute system upon which the non-Cisco application is running.
- Monitor non-Cisco application service(s).
- Provide electronic notification to customer of Incident management tickets.
- Act as single point of contact for Incident management tickets.
- Manage Incidents generated by monitoring or application user.
- Restore service to non-Cisco application by coordinating the application provider resources.
- Manage hardware RMA's with non-Cisco application provider.
- Interface and open tickets with Cisco TAC if the non-Cisco application is supported by Cisco TAC, rather than the application provider.

Customer Responsibilities
- Provide to Cisco Managed Services a point of contact to interface with the non-Cisco application provider.
- Maintain in good standing non-Cisco hardware and software maintenance contracts for application under Cisco Managed Services.
- Provide Letter of Agency to Cisco for the purpose of interfacing with the non-Cisco application provider.
- Coordinate backups and restores of defined applications as required.
- Ensure testing of all application updates and upgrades has been completed prior to Cisco executing the updates or upgrades.