



## Service Description: Cisco Remote Management Services

This document describes the following Cisco Remote Management Services:

- Cisco Unified Communications Remote Management Services
- Cisco Unified Contact Center Remote Management Services
- Cisco Foundation Technologies Remote Management Services
- Cisco Application Delivery Remote Management Services
- Cisco Wireless Remote Management Services

This Service Description is designed to provide a baseline understanding of and set expectations about the activities and deliverables that make up the Service. Please read this document carefully as it contains important information regarding the Services you have purchased from us.

**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. 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 these Services 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 the contract to you. You can obtain a copy of this and other Cisco service descriptions at [www.Cisco.com/go/servicedescriptions/](http://www.Cisco.com/go/servicedescriptions/).

This Service Description has 6 appendices below:

- Cisco Unified Communications Remote Management Services
- Cisco Unified Contact Center Remote Management Services
- Cisco Foundation Technologies Remote Management Services
- Cisco Application Delivery Remote Management Services
- Cisco Wireless Remote Management Services
- Glossary of Terms

Cisco Remote Management Services are intended to supplement a current support agreement for Cisco products, and only available where all Managed Components in a Customer's Network are supported through a minimum of core services such as Cisco SMARTnet and Cisco Software Application Services or Cisco's Unified Communications Essential Operate Service, as applicable. Cisco shall provide Cisco Remote Management Services described below as selected and detailed on the purchase order for which Cisco has been paid the appropriate fee. The Service consists of 2 service components:

1. Management Services
2. Elective Change Services

Cisco shall provide a Quote for Services (Quote) setting out the extent of the Services and duration that Cisco shall provide such Services. Cisco shall 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 of Managed Components.

### 1 Management Services

With Management Services, Cisco provides Monitoring, Incident Resolution, Reactive Problem Management, service level management and Standard Changes to resolve all Incidents

#### 1.1 Cisco Management Application Platform

Monitoring is a service component that provides monitoring for all Managed Components in your solution. The Service may require the installation of the Management Application Platform (MAP) on your Network in order to provide monitoring coverage.

The MAP is configured with Customer-specific installation and monitoring data prior to being placed into service. Once installed, the MAP will discover the components under management as indicated via the Service Activation Kit (see 1.3.2) and build the inventory report.

The MAP is a suite of management applications that may be deployed in a redundant configuration and consists of all management software and hardware required for service delivery. The MAP is deployed in a single configuration instance or multiple instance configurations depending on the number, type, and location of the managed devices. The MAP or portions thereof may exist on the Customer Premise and/or at Cisco. The MAP configuration is determined by Cisco during the Transition Management phase.

The implementation of Monitoring Services may include some or all of the following activities:

- Installation of operating system and supporting applications on the MAP. This may possibly be accomplished remotely.
- Installation and testing of monitoring application. This may possibly be accomplished remotely.
- Shipment of servers, appliances and/or devices to the designated Customer location
- Installation assistance to Customer for the servers, appliances and/or devices.
- Establishment of connectivity between the Customer site and Cisco.
- Establishment of remote monitoring and management of the Customer's Network devices and applications from Cisco.

The Management Application Platform is an integral part of the Service and is installed for the duration of Services. During the Service term, the Customer is granted a nonexclusive and nontransferable license to use the hardware and the software resident thereon solely on the Management Application Platform supplied. The Customer must return any and all associated Management Application Platform materials (devices if applicable along with documentation) and connectivity devices to Cisco immediately upon expiration or termination of Services.

## 1.2 Management Connectivity

Management Connectivity establishes bi-directional communication between the Customer Premises and Cisco for Management Data to be securely and consistently transmitted between Managed Components and Cisco. Management Connectivity consists of two areas: primary connectivity and overall security.

Management Connectivity requires access to specific ports and protocols; such requirements will be reviewed with Customer during the Transition Management process.

### 1.2.1 Primary Management Connectivity

Primary Management Connectivity will be provided by Cisco. At Cisco's discretion, one of two options will be selected based on the type of Service.

- A dedicated circuit between Cisco ROS Point of Presence and the Customer-designated handoff. The handoff will be at the Customer data center or other supported Network termination point.
- A virtual connection via a Virtual Private Network (VPN) between Cisco ROS Point of Presence and Customer Network.

Each option may include a Cisco-provided Termination Device located on the Customer Premises. The size of the connection

between the Cisco POP and Customer handoff will depend on the type of Service and number of Managed Components.

Redundant and/or additional circuits are an available option, but fees to cover any additional circuits are to be paid by the Customer.

### 1.2.2 Termination Device

Cisco will ship a termination device for installation at the Customer site. The termination device terminates the Management Connection. The termination device is a Managed Component supplied by Cisco and resides at the Customer Premises. The termination device must have Network access to Managed Components.

Unless otherwise agreed upon, title to all termination devices shall remain in Cisco possession. Customer must return the Termination Device to Cisco immediately upon expiration or termination of Services

Cisco, or its subcontractors, shall be allowed access to the Customer Premises (location occupied by Customer or Customer's end user) to the extent reasonably determined by Cisco for the inspection or emergency maintenance of Cisco-supplied Termination Device. Failure to allow timely access may invalidate Cisco SLAs and SLOs and delay restoration of Services.

## 1.3 Transition Management

Transition Management is a phased process approach in which Cisco prepares Customer infrastructure for the Management Services. The Customer must place an order with Cisco and attach Cisco Service Description to initiate the Transition Management process. The Transition Management process concludes at the negotiated Start Date of monitoring provided by Services.

### 1.3.1 Kickoff Meeting

Cisco will assign a Project Coordinator to act as a single point of contact during the Transition Management phase. Thirty (30) days from once a valid Purchase Order is received and processed by Cisco, the Project Coordinator will contact the Customer to schedule the kickoff meeting. The kickoff meeting is typically accomplished via a conference call with the executed contract detail and may include a Cisco partner. The kickoff meeting will indicate the initiation of the kickoff phase. The kickoff phase, as well as all remaining phases within Transition Management, is typically facilitated by the Project Coordinator in collaboration with Cisco Engineers assigned to the Customer account.

This Transition Management phase includes the following activities:

- Coordinating, scheduling, and executing the Kickoff meeting

- Reviewing roles and responsibilities of Cisco personnel, Customer contacts, and Partner contacts (if applicable)
- Providing Customer with escalation documentation for Service Desk
- Reviewing the support model
- Reviewing Services purchased, as indicated on the Purchase Order
- Aligning Cisco and Customer on all major activities, risks and milestones during the Transition Management phase
- Reviewing and completing the Service Activation Kit (SAK)

### 1.3.2 Service Activation Kit

Reviewing the SAK components and key information is critical to success for Transition Management. It is the Customer's responsibility to fill out all relevant data fields in the SAK, which include all necessary Network details and Managed Component details that are required for activating Services.

The Project Coordinator will develop a project plan for subsequent steps with distribution to project contacts.

### 1.3.3 Management Application Platform Configuration

Once the Management Application Platform is installed, Cisco executes a discovery process for Managed Components per Purchase Order. The Project Coordinator will communicate any discrepancies between discovered devices and devices on the Purchase Order. Any requested additions beyond the Managed Components defined on the Purchase Order will be subject to incremental Service fees and additional Transition Management intervals.

Cisco inputs Managed Component information into Management Application Platform database and sets-up system consoles and dashboards (per Purchase Order). All Managed Components are organized into defined device groupings. Service, support and escalation processes are configured in the Service Management Application Platform. This completes the implementation of the Monitoring Services.

### 1.3.4 Remote Training Session

The Project Coordinator schedules remote training sessions. The sessions are conducted using a conference bridge and collaborative software.

The objectives of the training sessions are:

- Using the Management Application Platform
- Present service documentation
- Review
  - Support services to be delivered
  - Processes for obtaining service
  - Service escalation process

- Change control policies
- Submit change requests
- Standard reports
- Explain the recurring operational meetings
- Review the Customer Acceptance timing

## 1.4 Customer Acceptance

Cisco will work with the Customer to validate that Transition Management phase is complete.

Once an agreed Customer acceptance date has been received and agreed by Cisco, the service transitions from Transition Management to Service Delivery phase. All exceptions to the Service Delivery phase will be documented within the Transition Management material.

## 1.5 Software Updates for the Management Application Platform

The Service includes routine software updates for the Management Application Platform. The Customer shall receive an email notification from Cisco which identifies the modifications included in the next release. Cisco will schedule a maintenance window using the calendar on the Management Application Platform. A reminder ticket will automatically be opened at the beginning of the change window. The ticket will be updated and closed by Cisco upon completion of the update.

## 1.6 Incident Monitoring

The Incident Monitoring process monitors Managed Components 24x365, using the Management Application Platform to raise awareness of specific events that have the potential to cause adverse impact to business operations.

The Service:

- Monitors Managed Components
- Detects Incidents or that a service-impacting performance threshold has been exceeded
- Captures Incident and correlation data, enriches the data with relevant device information and creates an Incident ticket
- Sends automated e-notification(s) as defined in the SAK to:
  - Customer contacts
  - Partner contacts (if desired)

## 1.7 Incident Notification

The Incident Notification informs the Customer that an Incident has been recorded. Cisco utilizes four communication mediums to notify Customers:

- Electronic mail
- Pager or cellular phone

- Telephone
- Web portal

Cisco's primary means for incident notification is electronic mail.

## 1.8 Management Portal

Cisco provides reports on Tickets as well as performance for Managed Components. Reports are available on the Cisco Management Portal ("the Portal"), which provides Customers and Partners a Web-based method for accessing information about their Network and relationship with Cisco.

Customers receive end-user licenses to access the Portal. Instructions to access and navigate the Portal are provided in the remote or Video on Demand ("VoD") training sessions as well as in the Portal User Guide. The Portal User Guide is available on the Portal.

## 1.9 Reports

The Service shall provide device-level performance, availability and inventory reports. End-users generate reports using the reporting capabilities and tools accessible via the Portal on the Management Application Platform. See the Appendices A-E for more detail about the reports available for each service.

## 2 Managing & Resolving Incidents

### 2.1 Incident Management

The monitoring and incident notification work together with Incident Resolution processes to form the Incident Management service component. Incident Management restores Normal Service Operation within a reasonable time to contain the adverse impact on business operations, service quality and availability.

Cisco will:

- Utilize Incident remediation procedures to collect any additional data required to diagnose and match to Known Errors in our Knowledge Base
- Work to restore services within agreed service levels, initiating Change Management as needed for restoration
- Coordinate the dispatch of support personnel to the Customer Premises to perform necessary onsite repairs as per the end-Customer maintenance and support contracts. This requires a signed Letter of Agency by the Customer.
- Remotely assist onsite personnel as needed to facilitate service restoration.
- Remotely facilitate hardware replacement and software updates determined to be required by Cisco.

### 2.2 Incident Prioritization

Cisco classifies and prioritizes incidents according to impact and urgency.

#### 2.2.1 Impact Definitions

An Incident is classified according to its impact on the business (the size, scope, and complexity of the Incident).

Impact is a measure of the business criticality of an Incident or Problem, often equal to the extent to which an Incident leads to degradation of a Service running on the Network. Cisco shall work with Customer to specify impact for each Managed Component during Transition Management. There are four impact levels:

- Widespread: Entire Network is affected (more than three quarters of individuals, sites or devices)
- Large: Multiple sites are affected (between one-half and three-quarters of individuals, sites or devices)
- Localized: Single site and/or multiple users are affected (between one-quarter and one-half of individuals, sites or devices)
- Individualized: A single user is affected (less than one-quarter of individuals, sites or devices)

#### 2.2.2 Urgency Definition

Urgency defines the criticality of the Incident or Problem to the Customer's business. Cisco shall work with the Customer to understand and set the proper urgency level.

Cisco Incident and Problem urgency levels are defined as follows:

- Critical – Primary business function is stopped with no redundancy or backup. There may be an immediate financial impact to the Customer's business. The Customer determines the issue as critical.
- High – Primary business function is severely degraded or supported by backup or redundant system. There is a probable significant financial impact to the Customer's business. The Customer perceives the issue as high.
- Medium – Non-critical business function is stopped or severely degraded. There is a possible financial impact to the Customer's business. The Customer perceives the issue as medium.
- Low - Non-critical business function is degraded. There is little or no financial impact. The Customer perceives the issue as low.

#### 2.2.3 Priority Definitions

Priority defines the level of effort that will be expended by Cisco and the Customer to resolve the Incident.

Cisco Incident Management priorities are defined as follows:

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

		IMPACT			
		Widespread	Large	Localized	Individualized
URGENCY	Critical	P1	P1	P2	P2
	High	P1	P2	P2	P3
	Medium	P2	P3	P3	P3
	Low	P4	P4	P4	P4

Cisco will downgrade the case priority in accordance with reduced severity of impact or Incident resolution. The case may be left open for a prescribed period while operational stability is being assessed.

Incident Ticket shall be closed by Cisco or Customer upon validation of issue remediation and the systems return to operational stability.

Complete Ticket detail resides in a Knowledge Base which is used to support Incident Management and Problem Management processes.

### 2.3 Incident Escalation

Incidents are escalated according to a defined process. At any point in the Incident Management process, the Customer may request escalation via Cisco duty manager to address concerns about the processing of the Incident. If service restoration requires activities by a third party, Cisco will initiate and manage the process.

The Customer is notified that the Incident has been resolved and provided the opportunity to verify that services have been restored satisfactorily. Following Incident resolution and Customer notification, the Incident shall be closed by Cisco or Customer. Reports regarding Incident Management are available on the Portal.

### 2.4 Translation Support

The Service is delivered in English language. For Customers who require support in another language other than English,

Cisco provides telephone translation support. When a Customer calls Cisco, the Cisco Engineer determines the language spoken, places the Customer on hold, and conferences the translator into the call.

### 2.5 Metrics

The following Incident metrics are gathered:

- Time to Notify (TTN)
- Time to Restore (TTR)

### 2.6 Reactive Problem Management

Reactive Problem Management describes the Problem Management processes that primarily support Incident Management. These processes are initiated when an Incident cannot be matched to a Known Error. A Problem is declared for the purpose of tracking the activities that lead to identifying a root cause and a resolution to the Incident's underlying error. The process concludes when a Known Error, including its root cause and resolution, has been identified and recorded in the Known Error database. The Known Error will then be used to resolve and close all associated open and future Incidents. Reactive problem management has two major sub-processes: primary control process and error control process.

#### 2.6.1 Primary Control Process

The primary output of the problem control process is the identification of a root cause for the Problem. The process steps start with analyzing available data, identifying and recording Problems, and classifying Problems according to impact, urgency, and status.

The rest of Problem control involves troubleshooting and diagnosing Problems to identify root causes and potential workarounds.

#### 2.6.2 Error Control Process

Error control takes over Problem control when a root cause of a problem has been identified. First, a Known Error is identified and recorded based on the root cause of the Problem.

Next, the Error is assessed to determine potential resolutions, which can include both temporary workarounds as well as permanent fixes. If a permanent fix is possible and cost-justifiable, a recommendation will be made to the Customer to correct the error by initiating a change via Change Management.

The final step and major output of Error control is to document the resolutions in the Known Error database so that the remediation procedure can be used by Incident Management.

### 2.7 Change, Release and Configuration Management

Change, Release, and Configuration Management are a tightly integrated set of processes due to the interdependence of their process activities. The evaluation of a proposed change is strongly dependent on accurate configuration data. Approved Changes are executed via the Release Management process,

which is also strongly dependent on accurate configuration data for design and testing activities. Configuration Management activities must be invoked whenever Changes are released to keep configuration data accurate.

## 2.8 Change Management

The purpose of Change Management is to ensure that changes to Managed Components are evaluated, coordinated, and communicated to all impacted parties to minimize negative impacts of the Change to Management Services.

Changes fall into 2 categories: Standard Change and Elective Change. Elective Changes are always requested by Customers by submitting a Change Request. For more information about Elective Changes, please see **Section 3.0**.

### 2.8.1 Standard Changes

A Standard Change is a Cisco recommended change that is often as a result of Incident Management and Problem Management processes or Cisco Field Notice. Cisco Engineer will submit a Standard Change Request to start Change Management process. Standard Changes are included in Management Services.

Incidents will result in the creation of a Ticket which will initiate Change Management when Cisco deems it is required to resolve the Incident.

Problems, much like Incidents, will result in the creation of a Ticket. However, Cisco changes initiated as a result of a Problem will also be documented as Known Error and added to Knowledge Base for future use.

### 2.8.2 Applying Patches

Application of a Patch is at the discretion of Cisco. Patches will be evaluated to ensure the stability of the current environment is maintained.

Patches to remediate an Incident or Problem are handled as a Standard Change. Patches that are Customer-requested for the purpose of obtaining additional features or functions are considered discretionary and must be handled as an Elective Change.

As part of Patch process, Cisco will:

- Review Cisco Field Notices to determine impact and urgency to the Customer system and existing software levels.
- Remotely apply service pack updates to Managed Components operating system, system software and applications.
- Remotely apply Patch to Managed Components operating system, system software and applications
- Perform remote software levels audit to determine the current releases/patched based on Cisco leading practices. This is a quarterly audit.

- Provide a Change Management Report that identifies work ticket and number of hours spent on ticket.

## 2.9 Coordinating and Planning

Cisco provides an application on the Portal for submitting Standard and Elective Change Requests to Cisco. Cisco will utilize the Portal's Scheduled Outage capability as applicable to include suppression of events during a change window. Approved changes will be coordinated, planned and monitored via the Management Application Platform. This will allow coordination of activities to determine how to schedule activities to minimize negative impact.

Once a Standard or Elective Change has been released and the configuration data has been updated, the Change will be evaluated to determine the level of success in meeting the goals of the Change. This evaluation is used to improve Change Management for future Changes. The Engineer will confirm that all relevant stakeholders, including the Customer, have been notified that the Change is complete. Once evaluation and notification have been completed, the Change is closed.

## 2.10 Release Management

Release Management is focused on the actual implementation of approved Changes.

Rollout planning includes planning the details involved in executing the Change into the production environment. This includes setting the detailed timetable including securing a Customer change window if necessary, identifying and communicating to all stakeholders that need to be notified, and coordinating with Customer change procedures.

Execution is the act of introducing the Change into the production environment. Once the Change has been executed, Configuration Management is initiated to record the changes to all impacted Configuration Items.

## 2.11 Configuration Management

Cisco shall maintain an inventory of the Managed Components. This inventory detail includes certain configuration data and the levels of service applied to each Managed Component.

### 2.11.1 Cisco Series Routers and Switches

Cisco shall perform back-up process for Cisco Series Routers and Switches with Cisco IOS. This includes definition and execution of service restoration process for Managed Components.

### 2.11.2 Cisco Unified Communications Applications

Cisco shall provide leading best practice recommendations to Customer in support of their back-up of Cisco Unified Communications servers. This includes providing scheduling recommendations for performing back-ups.

Cisco shall monitor the availability for the back-up service executable (.exe) on Cisco Unified Communications servers under management.

### 3 Elective Change Services

An Elective Change is requested by the Customer and is often the result of changes in the Customer Network, business processes, or the business. Elective Changes are not the result of Cisco Incident Management and Problem Management processes. The Customer identifies the requirement and submits Elective Change Requests on the Portal.

Elective Changes are scheduled services that the Customer must request in advance of service delivery. Elective Change service delivery response time is defined in the **Service Level Management** section of this agreement.

The available Cisco Elective Change Services are itemized in the **Appendices**. Cisco may elect to offer additional services within its areas of competency in response to a Customer's request for service.

Customers purchase a block of hours that are used for executing Elective Changes. The amount of hours purchased may vary by contract. The Customer must have a sufficient balance of hours on account to cover their requested Change based on time estimations provided by Cisco at the time the change is requested.

Elective Change hours are debited from the Customer's block of hour account balance as delivered, per the following:

- All Elective Change Requests will require a minimum of 0.5 hour charge. Billing will be charged in 0.5 hour increments thereafter.
- Cisco's priority handling of urgent Elective Change Requests is on an as-available basis. Cisco will use commercially reasonable efforts to respond to such requests. If priority handling request is accepted it will be charged as a minimum 2-hour charge. Billing will then be charged in 0.5 hour increments thereafter.
- Customer Elective Change Requests where requested time of service delivery is outside of Normal Business Hours will be billed at a rate of 1.2 times the standard rate if the time is accepted by Cisco. Elective Change Requests to be delivered on Cisco-observed holidays will be billed at 2 times the rate if the change time is accepted by Cisco.
- All Elective Change hours must be used within the duration of an annual contract period. If a multiple year contract is purchased then the hours allocated to each year should be used completely by the end of the year. In the event that the Customer has hours left over at the end of the year and the Customer has purchased or is purchasing additional year(s) of service then and only then may the previous years' unused hours be carried over. Hours from the subsequent year may not be borrowed against and used in the current year. In the event that elective hours are carried over into the

next year, the monthly allocation in the next year is recalculated by adding the carried over hours to the contracted hours of the next year and dividing the sum by 12.

- In a single month, Customers can submit Elective Changes that add up to no more than 50% over the monthly allocation of hours. For example, if Customer purchases a block of Elective hours for 10 hours per month for a total of 120 hours per year, the Customer may use their 10 hour monthly allocation plus 50% more resulting in a maximum of 15 hours for the month. The entire 15 hours is then debited against the Customer's entire hourly allocation for the year. If the Customer requires more hours for a particular month then additional hours may be purchased. .
- During the Change process, the Customer is required to have an authorized onsite representative available to assist as required.

Cisco shall provide a monthly Elective Change Report.

Cisco shall provide the Customer with the option to purchase additional Elective Change Hours as needed. Minimum hour purchase blocks may apply.

#### 3.1.1 Submitting an Elective Change

Please see section 3.0 on the process to submit an Elective change.

### 3.2 Proactive Problem Management

Elective Change Services can include proactive Problem Management which may assist to prevent the occurrence or limit the adverse impact of future Incidents in two ways:

Periodic reviews of Customer Network are conducted to identify potential error conditions that can be corrected before Incidents occur. When these conditions are identified, the Change Management (for conditions with Known Errors) or the Problem control process (for conditions that require further evaluation) is initiated

Periodic reviews of Incidents, Problems, Known Errors, and the Incident Management process are conducted to improve efficiency and effectiveness of Cisco in responding to Incidents. These activities can include major problem reviews in which the processing of P1 Incidents is reviewed to identify opportunities for process improvement. Other activities include reviewing past Incidents and problems with the goal of updating the Known Error database and improving remediation procedures.

Customer must submit an Elective Change Request for proactive Problem Management activities. However, Cisco will conduct proactive Problem Management activities at its sole discretion to improve the results of the Incident Management process.

### 3.3 Carrier Management

Carrier management activities are an important but very unpredictable task performed within the Service. To provide flexibility for the Customer, Cisco will deliver carrier management services within the structure of Elective Change services. Carrier Management is provided as a standard service for Foundation Service Offering and is an Elective Service for all other service offerings. Elective Service change hours will be used to perform carrier management activities such as coordination of outages with the Customers' circuit provider, notify Customer of carrier status and update tickets for accurate record keeping. Cisco will take efficient and expeditious steps to bring a circuit back into service involving the Customer along the entire process.

## 4 Service Level Management

Service Level Management is a process to manage our Customer relationship and is a component of Services. Service Level Management process is managed by a Cisco Customer Relationship Manager (CRM).

### 4.1 Service Level Reviews

Cisco gathers and tracks ticket data and generates Operational Report to track performance. The Operational Report provides ticket information and response times generated every month and distributed to designated Customer contacts via email or Service Portal. The Operational Reports are also reviewed remotely on a regular basis in the Service Level Management Review meeting with the Customer.

Cisco will schedule at a minimum quarterly service reviews with the Customer. The quarterly service reviews are delivered remotely using a conference bridge or collaborative tools. In the quarterly service reviews, the CRM presents ticket information, ticket response times, ticket trends, and reviews SLO performance. The meetings provide general Network performance reporting suitable and available for trending and analysis.

The annual business review meeting is an interactive and collaborative session that reviews the trends over the past year and discusses the Service Plan for the next year of service.

### 4.2 Service Level Agreements

Cisco offers Service SLAs for Incident Management, which are available upon request.

### 4.3 Service Level Objectives

SLOs apply to Managed Components that are managed exclusively by Cisco within the Service. Due to the nature of the implementation process, Cisco cannot adhere to the SLOs during the Transition Management phase. Customer and Cisco must agree and document within the SAK to acknowledge the completion of the Transition Management

process. The Service Delivery phase begins after Cisco receives agreement from the Customer to when this phase begins. Cisco adheres to the SLOs during the Service Delivery phase.

SLO's will be delivered around Time to Change (TTC), Time to Notify (TTN) and Time to Resolve (TTR) by the Service.

#### 4.3.1 Time to Change

Cisco assesses Standard and Elective Change Requests to determine level of complexity and the amount of time required to complete the change. Standard change activities are part of Incident and Problem management steps which may be schedulable by nature. All Elective Change requests are scheduled events. Cisco SLOs for executing the Standard and Elective Changes are as follows:

Cisco estimated time duration to perform change	Time to completion from receipt of change request
< 2 Hours	Next business day
2 to 4 Hours	Second business day
> 4 hours	Scheduled service

Business days are Monday through Friday, excluding Cisco-observed holidays.

#### 4.3.2 Time to Notify (TTN)

Customers may have specific incident notification requirements of which the Service will offer a Time to Notify objective. Cisco will respond to incidents raised through the management platform by electronically notifying a specified Customer contact(s) within the TTN timeframe. Cisco SLO for meeting this objective is as follows:

Cisco estimated time to notify Customer contact	Incident Level
15 Minutes	P1 and P2 Incidents

#### 4.3.3 Time to Resolve (TTR)

Incidents go through many stages with resolution being a primary objective. Time to Resolve tickets includes all remote incident management activities (alarm or call receipt through resolve, excluding maintenance or carrier cycle time). Time to Resolve shall mean the time period for a priority 1 or 2 severity from occurrence of the Incident until Cisco restores the Managed Component to a usable level of functionality. Cisco SLO for meeting this objective is as follows:

Cisco estimated time	Incident Level
----------------------	----------------

to resolve a ticket	
6 Hours	P1 incidents
12 Hours	P2 incidents
24 Hours	P3 incidents
48 Hours	P4 incidents

SLO measurements exclude the following:

- Delays caused by Customer (example waiting for response on change window or on-site resources) in resolving the qualifying issue
- Delays caused by third parties, such as Telecarriers, in resolving the qualifying issue
- Scheduled wait time
- SMARnet cycle time is not included in the SLO measurement.
- Customized calling trees

## 5 Services Not Covered

This Service Description should be read in conjunction with the **List of Services Not Covered** document posted at <http://www.Cisco.com/go/servicedescriptions/>, which is hereby incorporated into, and made part of, this Service Description by this reference.

## 6 Customer Responsibilities

### 6.1 Management Connectivity

#### 6.1.1 Termination Device

Customer will use reasonable efforts to provide and maintain the Termination Device in good working order. The Customer shall not, nor permit others to, rearrange, disconnect, remove, attempt to repair, or otherwise tamper with the Termination Device. Should this occur without first receiving written consent from Cisco, the Customer will be responsible for reimbursing Cisco for the cost to repair any damage thereby caused to the Customer Premise Equipment. Under any circumstances, Cisco will not be held liable to the Customer or any other parties for the interruption of Service, missed SLAs or SLOs, or for any other loss, cost, or damage that results from the improper use or maintenance of the Termination Device.

Unless otherwise agreed upon, title to all Termination Devices shall remain in possession of Cisco Systems, Inc. Cisco expects that, at the time of removal, the Termination Device shall be in the same condition as when installed, with the expectation of normal wear and tear. Customer shall reimburse Cisco for the depreciated costs of any Termination Device that is deemed beyond normal wear and tear.

Cisco, or its subcontractors, shall be allowed access to the Customer Premises (location occupied by Customer or

Customer's end user) to the extent reasonably determined by Cisco for the inspection or emergency maintenance of Cisco-supplied Termination Device. Failure to allow timely access may invalidate SLAs and SLOs and delay restoration of Managed Services.

#### 6.1.2 Install Termination Device

The Customer shall provide the following with respect to the installation of the Termination Device:

- Provide appropriate secure rack-mount location for the Termination Device with suitable environmental conditions for computer operation.
- Install the Termination Device and Network connectivity per Cisco-supplied guidelines.
- Provide communications facilities and services including internet and Network configuration. Communication facilities and services must be maintained for the duration of the Service term.
- Provide a resource to support the installation of the Termination Device. These activities include:
  - Racking
  - Connection to Network
  - Power connection to uninterruptible power system (UPS) or other facility with continuous uninterrupted power
  - Power-up

Provide suitable commercial power, and an UPS or other acceptable power back-up facilities providing a minimum of 1kVA dedicated for the Termination Device.

Provide mutual agreement of date concerning completion of Transition Management activities.

#### 6.2 Training

The Customer shall provide training coordination support including identifying trainees and trainee contact information.

#### 6.3 Transition Management

To enable Cisco to provide Services for Managed Components, Cisco requires the Customer to:

- Assign a project manager to represent the Customer during the Transition Management phase.
- Assign a technical lead to assist Cisco with establishing the Network access required for remote management.
- Project manager and technical lead attend Customer Project Kickoff meeting and training sessions.

##### 6.3.1 Perform a discovery audit

The discovery audit will be conducted by the Customer using Cisco-supplied processes and tools for the Cisco Unified Communications and Unified Contact Center Remote Management Services.

The discovery audit must be completed and submitted to Cisco 14 calendar days after placing the order for the Service.

If the Customer so elects, Cisco can perform this audit as an Elective Change Service. The audit process requires Customer to run Cisco-supplied macro 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 Customer 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)
- Available 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

### 6.3.2 Service Activation Kit

Complete the SAK which provides the key information critical to success for Transition Management and includes:

- Location of management applications
- Network connectivity detail for the Management Application Platform
- Device location and naming scheme
- Management IP addresses and system detail, SNMP community strings
- Telnet and password access
- Management system User names and contact detail
- Definition of Customer-specific support policies including:
  - Points of contact and profile data
  - Case category access
  - Notification policy
  - Escalation policy
  - Dispatch policy
- Managed Component support contract information (e.g., Cisco SMARTnet, etc.)

Complete tasks defined in the SAK to enable management access to managed systems which may include setting up SNMP, traps, system log, and traps.

Provide as-built documentation including detailed design, Network implementation plan(s), site survey(s), and bill of materials. Data and documentation will be obtained from Cisco Partner as necessary to facilitate Transition Management.

### 6.3.3 Install Management Application Platform

For those cases where the Cisco Management Application Platform or components of the Cisco Service Management Application resides on the Customer Premises then the Customer must provide an appropriate secure rack-mount location for the Cisco Management Application Platform (or components) and termination devices with suitable environmental conditions for computer operation.

The Customer is also expected to provide the following:

Installation of the Management Application Platform and Network connectivity per Cisco-supplied guidelines.

Provide communications facilities and services including internet and Network configuration. Communication facilities and services must be maintained for the duration of the Service term.

Provide a resource to support the installation of the Management Application Platform. These activities include:

- Racking
- Connection to Network
- Power connection to UPS or other facility with continuous uninterrupted power
- Power-up

Provide suitable commercial power, and an uninterruptible power system (UPS) or other acceptable power back-up facilities providing a minimum of 1kVA dedicated for the Server Management Application and termination device.

Provide mutual agreement of date concerning completion of Transition Management activities.

Provide training coordination support including identifying trainees and trainee contact information.

### 6.4 Service Connectivity and Network Access

Cisco Remote Management Services are delivered using a collection of protocols and ports. The Customer must allow the collection of data for Managed Components.

Provide Read and Write management access to Managed Components as defined by SAK. Provide Read management

access for components that are monitored only. Access must be implemented in a timely manner in accordance to the SAK. This includes SNMP, syslog, Unified Communications Manager call detail record (CDR) interface, and other defined protocols as necessary to support Services.

### 6.5 Incident Resolution

The Customer must provide support contracts, letters of agency and all other end Customer documentation and authorization required to facilitate incident resolution.

Customer is required to maintain hardware maintenance and/or software maintenance as may be applicable on all System components identified in Purchase Order for the duration of the contract.

### 6.6 Managed Components

The Customer will:

- Ensure that all Managed Components are in good working order prior to completion of Transition Management. This means that Managed Components are fully configured, deployed and functioning properly prior to the commencement of Incident and Problem Management services. Good working order status will be verified by Cisco during the management readiness assessment process and using availability and performance reports during Transition Management. Required remediation steps will be provided to Customer by Cisco. Customer is responsible for all activities required to bring Managed Components up to good working order, including but not limited to system administration, configuration changes, scripting, and MAC (moves, adds and changes). Necessary services may be acquired from Cisco as Elective Change Services.
- Approve all Standard and Elective Change Requests prior to Cisco taking change action
- Provide physical security of the Managed Components.
- Contact Cisco to report Incidents via telephone or other means in accordance with policies established
- Allow Cisco to retain and publish aggregate statistics and metrics for non-identifiable trending analysis.
- Back-up Cisco Unified Communications and Contact Center applications and operating systems. The

Customer is responsible for ensuring the backups run successfully.

- Perform back-up on devices not running Cisco Catalyst OS or Cisco IOS. The Customer is responsible for ensuring the backups run successfully.

### 6.7 Non-Managed Components

The Customer is responsible for monitoring and managing the Non-Managed Components and applications.

### 6.8 Communication and Change Management

Cisco has a co-management approach to Managed Services, allowing the Customer and other Customer-approved vendors to retain access to Customer devices. Because multiple parties can make changes to the environment, Cisco requires that anyone with access to the Customer's environment follow a consistent and documented Change Management process. This process is reviewed and agreed upon prior to completion of the Transition Management phase.

The Customer will:

- Provide Cisco with changed data with respect to the Customer and Managed Components, as needed, via the Portal.
- Provide timely delivery of information required for configuration of Managed Components notification procedures.
- Submit maintenance window and other scheduled maintenance activity using the calendar on the Portal, by telephone or email. Cisco requires 72 hours advanced notification. Cisco will suppress Incident tickets during the scheduled maintenance period.
- Maintain sole responsibility for informing Cisco of Customer employee status changes.
- Provide and maintain a list of Customer employees authorized to request changes.
- Provide and maintain an escalation path within the Customer's employee base.

Provide Cisco product training for end-users.

**APPENDIX A:**

**Cisco Unified Communication Remote Management Services**

Cisco Unified Communication Remote Management Services has two levels of services – Standard and Premier. This Appendix describes the services capabilities, supported devices, elective changes, and reports delivered with each service level.

**Service Capabilities**

<b>Activities &amp; Deliverables</b>	<b>Standard</b>	<b>Premier</b>
Transition management	✓	✓
Management connection	✓	✓
Intelligent monitoring & event correlation	✓	✓
Incident notification	✓	✓
Voice QOS monitoring & ticketing	✓	✓
Incident management	✓	✓
Self-Diagnostics and Business Rules Engine	✓	✓
Management portal	✓	✓
Reactive problem management (root cause analysis)	✓	✓
Standard changes	✓	✓
Review/assess Cisco Field Notices	✓	✓
Ticket Trending and problem analysis	✓	✓
Problem resolution	✓	✓
Create configuration management database for managed devices	✓	✓
Execute elective changes	✓	✓
Device-level reports	✓	✓
CDR & CUCMR collection & storage		✓
Premier Reports		✓
Enables DIY support model with leave behind application		✓
Knowledge base accessible to end users		✓
Synthetic transactions supported		✓
CMDB and Ticketing level integration with Customer platform available		✓
Mobility management		✓
Presence management		✓
Unified messaging management		✓

**Supported Devices:**

The following table identifies the devices managed by Cisco Unified Communications Remote Management Service

<b>Supported Devices</b>	<b>Standard</b>	<b>Premium</b>
Cisco Series Routers	✓	✓
Cisco Series Switches	✓	✓

Supported Devices	Standard	Premium
Universal Gateways and Access Servers	✓	✓
AS5200	✓	✓
AS5300 Series	✓	✓
AS5400	✓	✓
AS5800	✓	✓
Wireless	✓	✓
Cisco 500 Series	✓	✓
Cisco 1100	✓	✓
Cisco 1130	✓	✓
Cisco 1200	✓	✓
WLAN Controller	✓	✓
WSLE	✓	✓
<b>Core Infrastructure</b>		
DNS	✓	✓
NTP	✓	✓
<b>Core Software Subcomponents</b>		
Exchange	✓	✓
SQL	✓	✓
Domino	✓	✓
<b>OS Components</b>		
WIN 2000 OS	✓	✓
WIN 2003 OS	✓	✓
Linux OS	✓	✓
<b>General Hardware Components</b>		
Cisco MCS Hardware	✓	✓
Cisco Approved HP, IBM, Sun Hardware	✓	✓
<b>Unified Communications</b>		
Unified Communications Manager 7.x	✓	✓
Unified Communications Manager Express (IOS)	✓	✓
Unified Communications Manager Business	✓	✓
Unity Express 2.x-3.x	✓	✓
Unity 4.x-7.x	✓	✓
Unity Connection 1.x-2.x	✓	✓
Cisco Gatekeeper	✓	✓
Cisco SRST	✓	✓
VG248	✓	✓
IP Communicator	✓	✓
Cisco IP Phone	✓	✓
Cisco TDM Gateways	✓	✓
Cisco Unified Presence 6.x		✓
Unified Mobility Manager 1.x		✓

Supported Devices	Standard	Premium
Meeting Place 5.x -6.x		✓
Meeting Place Express		✓
Unified Contact Center Express		✓
Unified Mobile Communicator		✓
Unified Personal Communicator		✓
VoIP Trunking Gateways		✓
VXML Gateways		✓
<b>Unified Contact Center</b>		
Unified Contact Center Express 7.x		✓
ICM 5.x & 6.x		✓
Unified Contact Center Enterprise 7.x		✓
Unified Customer Voice Portal 7.x		✓
CRS 4.X-5.x		✓
Administrative Workstation		✓
Peripheral Gateway		✓
Router (ICM)		✓
Logger		✓
Historical Data Server		✓
CTI OS/CAD (PG CTI Server)		✓
ICM Carrier NIC		✓
Ingress Gateway		✓
Egress Gateway		✓
Gatekeeper		✓
CVP VXML Server		✓
Media Servers		✓
CSS Boxes		✓
ASR/TTS Servers		✓
Outbound Dialer		✓
Third Party Connectors		✓
CVP Report Servers		✓
Cisco WebView Servers		✓
CVP Application Server		✓
CVP Call Director Server		✓

\* Services provided by Cisco include monitoring of foundation elements associated with Unified Communications. As part of the monitoring service, incidents associated with monitored foundation elements will be assigned to the Customer for remediation. Should an escalation occur, or Cisco determines that a foundation element is affecting voice services, then Cisco will engage and assist Customer support staff. Responsibility for remediation of monitored – but not Cisco managed elements resides with the Customer.

### Elective Change Services

Elective Change Services are Customer requested changes and are scheduled activities. The table below identifies the changes that are available for Cisco Remote Management Services.

Elective Changes	Standard	Premium
Phone Administration (MAC) <ul style="list-style-type: none"> <li>• Add new phones</li> <li>• Configure/change/ delete lines</li> <li>• Configure speed dials</li> <li>• Configure XML services (e.g. Extension Mobility, CS QRT)</li> <li>• Configure device profiles for extension mobility</li> <li>• Device association for user management and for UC clients</li> <li>• Manage phone button templates and softkey templates</li> <li>• Manage UC user accounts</li> <li>• Perform phone load upgrades on Unified Call Manager</li> </ul>	✓	✓
Gateway administration <ul style="list-style-type: none"> <li>• Configure new voice gateways</li> <li>• Add/remove/ change trunks</li> <li>• Allocate directory numbers to trunks for analog ports</li> <li>• Configure hardware media resources (e.g. conference bridges, transcoders)</li> <li>• Upgrade IOS</li> <li>• H.323 gateway/ gatekeeper dial plan updates</li> <li>• Gateway/ gatekeeper/trunk capacity planning</li> </ul>	✓	✓
Dial plan administration <ul style="list-style-type: none"> <li>• Planning and design</li> <li>• Auditing dial plan and implementing changes</li> <li>• Translation patterns and CTI route points for forwarding calls</li> <li>• Manage route lists and route groups for trunk preference</li> <li>• Route patterns for tie lines and fax servers</li> <li>• Creating and updating dial plans for new sites</li> <li>• Time of day routing of calls</li> <li>• Configuring line and hunt groups</li> <li>• Configuring and administering UC Attendant Console</li> <li>• Media resource plan auditing and updates</li> </ul>	✓	✓
Cisco Media Convergence Server (MCS) administration <ul style="list-style-type: none"> <li>• Apply operating system patches</li> </ul>	✓	✓
Cisco application software administration <ul style="list-style-type: none"> <li>• Apply software updates and patches</li> </ul>	✓	✓
Licensing <ul style="list-style-type: none"> <li>• Apply license updates and changes</li> </ul>	✓	✓
Managing CDR Analysis and Reporting service	✓	✓
MeetingPlace/ MeetingPlace Express <ul style="list-style-type: none"> <li>• Managing user accounts and groups</li> <li>• License updates and changes</li> </ul>	✓	✓
Configuration changes to Cisco software and devices	✓	✓
Cisco software upgrades for feature enhancements and security-related purposes	✓	✓
Cisco Unity <ul style="list-style-type: none"> <li>• End -user MACs</li> <li>• Class of control/ distribution list administration</li> <li>• Microsoft Active Directory &amp; Exchange configuration Call handler MACs</li> <li>• Directory handler MACs</li> <li>• Ports and TDM integration</li> <li>• Apply patches to Microsoft Active Directory, Microsoft Exchange</li> </ul>	✓	✓

Elective Changes	Standard	Premium
<ul style="list-style-type: none"> <li>Failover support</li> </ul>		
TELCO / Carrier Coordination <ul style="list-style-type: none"> <li>Coordination of service engagement</li> </ul>	✓	✓
Capacity Planning <ul style="list-style-type: none"> <li>Evaluation of Network performance and current resource utilization</li> <li>Determining impacts and required modifications to support new applications and services</li> </ul>	✓	✓

### Premier Reports

The following reports available with Cisco Unified Communications Remote Management Premier Service:

Report Name	Description
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, 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 shall contain 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; create 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 lists 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); date of last back-up.
Global Ticket Report	Identifies the devices in the system that has been impacted by an Incident or Problem and extent of AutoCase activity. The device names indicate the location in production environments. End user selects the system, time frame and generates a report via Web portal.
Service Experience Report	Identifies top ten sites that have experienced the most tickets and causes. The report consists of: site names, site location, # of Change tickets, # of Incident tickets, device type, device name, major cause
Application Server Report	Identifies the following key server statistics: Utilization of CPU, Memory, Disk space, Network. Service status of all monitored services on Cisco UC servers. End user selects the server time frame and generates a report via Web portal.
Voice Service Level Summary Report	Cisco Unified Communications Manager cluster-based report representing: mean opinion score (MoS), latency, jitter, packet loss, disconnect cause summary, call type report and inbound/outbound call report.
Elective Change Report	A monthly summary report of elective change hours expended in support of the elective changes requested by the Customer.
Operations Report	A monthly report that provides ticket information and response times.

**APPENDIX B:**

**Cisco Unified Contact Center Remote Management Services**

This Appendix describes the services capabilities, supported devices, elective changes, and reports delivered in Cisco Unified Contact Center Remote Management Services.

**Service Capabilities**

Activities & Deliverables
Transition management
Management connection
Intelligent monitoring & event correlation
Incident notification
Voice QOS monitoring & ticketing
Incident management
Self-Diagnostics and Business Rules Engine
Management portal
Reactive problem management (root cause analysis)
Standard changes
Review/assess Cisco Field Notices
Ticket Trending and problem analysis
Problem resolution
Create configuration management database for managed devices
Execute elective changes
Device-level reports
CDR & CUCMR collection & storage
Premier Reports
Enables DIY support model with leave behind appliance
Knowledge base accessible to end users

**Supported Devices:**

The following table identifies the devices managed by Cisco Unified Contact Center Remote Management Services:

Supported Devices	
Unified Contact Center - Applications	Network Devices
ICUCM 5.x & 6.x	Cisco Series Routers*
Unified Contact Center Enterprise 6.x & 7.x	Cisco Series Switches*
Unified Customer Voice Portal 3.x-7.x	Unified Communications
CRS 4.X-5.x	Unified Communications Manager 4.x-7.x
Unified Contact Center - Hardware	Unity 4.x-7.x
Administrative Workstation	Cisco Unified Presence 6.x
Peripheral Gateway	Unified Mobile Communicator

Supported Devices	
Router (ICUCM)	Unified Personal Communicator
Logger	IP Communicator
Historical Data Server	Cisco IP Phone
CTI OS/CAD (PG CTI Server)	Cisco PSTN Gateway
ICUCM Carrier NIC	<b>Core Software Subcomponents</b>
Ingress Gateway	Exchange
Egress Gateway	SQL
Gatekeeper	Domino
CVP VXML Server	<b>OS Components</b>
Media Servers	WIN 2000 OS
CSS Boxes	WIN 2003 OS
ASR/TTS Servers	Linux OS
Outbound Dialer	<b>General Hardware Components</b>
Third Party Connectors	Cisco MCS Hardware
CVP Report Servers	Cisco Approved HP, IBM, Sun Hardware
Cisco WebView Servers	<b>Core Infrastructure</b>
CVP Application Server	DNS
CVP Call Director Server	NTP

\* Services provided by Cisco include monitoring of foundation elements associated with Unified Communications. As part of the monitoring service, incidents associated with monitored foundation elements will be assigned to the Customer for remediation. Should an escalation occur, or Cisco determines that a foundation element is affecting voice services, then Cisco will engage and assist Customer support staff. Responsibility for remediation of monitored – but not Cisco managed elements resides with the Customer.

### Elective Change Services

Elective Change Services are Customer requested changes and are scheduled activities. The table below identifies the changes that are available for Cisco Unified Contact Center Remote Management Services.

Elective Changes
Phone Administration <ul style="list-style-type: none"> <li>• Add new phones</li> <li>• Configure/change/ delete lines</li> <li>• Configure speed dials</li> <li>• Configure XML services (e.g. Extension Mobility, CS QRT)</li> <li>• Configure device profiles for extension mobility</li> <li>• Device association for user management and for UC clients</li> <li>• Manage phone button templates and softkey templates</li> <li>• Manage UC user accounts</li> <li>• Perform phone load upgrades on Unified Call Manager</li> </ul>
Gateway administration <ul style="list-style-type: none"> <li>• Configure new voice gateways</li> <li>• Add/remove/ change trunks</li> <li>• Allocate directory numbers to trunks for analog ports</li> <li>• Configure hardware media resources (e.g. conference bridges, transcoders)</li> <li>• Upgrade IOS</li> <li>• H.323 gateway/ gatekeeper dial plan updates</li> <li>• Gateway/ gatekeeper/trunk capacity planning</li> </ul>
Dial plan administration <ul style="list-style-type: none"> <li>• Planning and design</li> <li>• Auditing dial plan and implementing changes</li> <li>• Translation patterns and CTI route points for forwarding calls</li> </ul>

Elective Changes
<ul style="list-style-type: none"> <li>• Manage route lists and route groups for trunk preference</li> <li>• Route patterns for tie lines and fax servers</li> <li>• Creating and updating dial plans for new sites</li> <li>• Time of day routing of calls</li> <li>• Configuring line and hunt groups</li> <li>• Configuring and administering UC Attendant Console</li> <li>• Media resource plan auditing and updates</li> </ul>
Cisco Media Convergence Server (MCS) administration <ul style="list-style-type: none"> <li>• Apply operating system patches</li> </ul>
Cisco application software administration <ul style="list-style-type: none"> <li>• Apply software updates and patches</li> </ul>
Licensing <ul style="list-style-type: none"> <li>• Apply license updates and changes</li> </ul>
Managing CDR Analysis and Reporting service
MeetingPlace/ MeetingPlace Express <ul style="list-style-type: none"> <li>• Managing user accounts and groups</li> <li>• License updates and changes</li> </ul>
Configuration changes to Cisco software and devices
Cisco software upgrades for feature enhancements and security-related purposes
Cisco Unity <ul style="list-style-type: none"> <li>• End -user MACs</li> </ul> Class of control/distribution list administration <ul style="list-style-type: none"> <li>• Microsoft Active Directory &amp; Exchange configuration call handler MACs</li> <li>• Directory handler MACs</li> <li>• Ports and TDM integration</li> <li>• Apply patches to Microsoft Active Directory, Microsoft Exchange</li> <li>• Failover support</li> </ul>
TELCO / Carrier Coordination <ul style="list-style-type: none"> <li>• Coordination of service engagement</li> </ul>
Capacity Planning <ul style="list-style-type: none"> <li>• Evaluation of Network performance and current resource utilization</li> <li>• Determining impacts and required modifications to support new applications and services</li> </ul>
CTI <ul style="list-style-type: none"> <li>• Port and route point integration updates</li> <li>• Scripting updates</li> </ul>
Routing script adjustments <ul style="list-style-type: none"> <li>• Perform changes to routing scripts in support of call routing applications</li> </ul>
Administration script adjustments <ul style="list-style-type: none"> <li>• Perform changes in support of administrative applications</li> </ul>
Configuration Manager Changes <ul style="list-style-type: none"> <li>• Perform updates to Configuration Manager</li> </ul>
Provisioning applications and interfaces <ul style="list-style-type: none"> <li>• Provisioning of integration elements between applications</li> </ul>
Creation of custom reports <ul style="list-style-type: none"> <li>• Consultation</li> <li>• Definition</li> <li>• Configuration</li> </ul>
Creation of custom dashboards <ul style="list-style-type: none"> <li>• Consultation</li> <li>• Definition</li> <li>• Configuration</li> </ul>
Management Reporting Optimization <ul style="list-style-type: none"> <li>• Review and recommendations for modifications to database to support advanced reporting</li> <li>• Perform recommended database changes</li> </ul>
Port Administration <ul style="list-style-type: none"> <li>• Modifications</li> </ul>

Elective Changes
<ul style="list-style-type: none"> <li>Turn up/down</li> </ul>
License Administration <ul style="list-style-type: none"> <li>Administer modifications to licenses, including additions and deletions</li> </ul>
Wave File, TTS and ASR Administration <ul style="list-style-type: none"> <li>Changes to, prompts, vocabulary, administration, tuning and basic call transfer.</li> <li>File additions, modifications and deletions</li> </ul>
Email Administration <ul style="list-style-type: none"> <li>Administration of application</li> <li>Configuration of the email management system</li> </ul>
Ingress Gateway Administration <ul style="list-style-type: none"> <li>Service changes for new application deployments, call service additions and dial peers</li> <li>Administer changes to the ingress gateway</li> </ul>
Gatekeeper Administration <ul style="list-style-type: none"> <li>Changes to gatekeeper configuration</li> </ul>
Outbound campaign modifications <ul style="list-style-type: none"> <li>Administer the system configuration</li> <li>Administer outbound campaign application</li> <li>Changes to dialer lists, modes and scripts.</li> </ul>
CVP self-service applications in Audium/Design Studio <ul style="list-style-type: none"> <li>Application changes and enhancements</li> <li>File additions, modifications and deletions</li> </ul>
SIP Proxy Server <ul style="list-style-type: none"> <li>Configuration and Table changes</li> <li>Upgrades, additions, modifications and deletions</li> </ul>
CVP Operations Console and Reporting server and Database <ul style="list-style-type: none"> <li>Application changes and enhancements</li> <li>File additions, modifications and deletions</li> </ul>

## Reports

The following reports available on the Portal:

Report Name	Description
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, 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 shall contain 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; create 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 lists 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); date of last back-up.
Global Ticket Report	Identifies the devices in the system that have been impacted by an Incident or Problem and extent of AutoCase activity. The device names indicate the location in production environments. End user selects the system, time frame and generates a report via Web portal.
Service Experience Report	Identifies top ten sites that have experienced the most tickets and causes. The report consists of: site names, site location, # of Change tickets, # of Incident tickets, device type, device name, major cause

Report Name	Description
Application Resource Report	Provides daily and monthly reports on the availability of resources and ports configured on Cisco voice and contact center applications. The report also provides resource availability Incident ticket information. End user selects the server, time frame and generates a report via Web portal.
Application Server Report	Identifies the following key server statistics: Utilization of CPU, Memory, Disk space, Network. Service status of all monitored services on each Cisco voice and contact center server. End user selects the server time frame and generates a report via Web portal.
System Activity Report	User generated report that can be generated by site or geography and provides the following info: CVP: Calls active, Total Calls handled/day/hour ICUCM: Calls active, Total calls handled, Dialer: Calls active, Total calls handled WIM: Chats active, total chats handled. EIM: Mails open, total mails handled
Voice Service Level Summary Report	Cisco Unified Communications Manager cluster-based report representing: mean opinion score (MoS), latency, jitter, packet loss, disconnect cause summary, call type report and inbound/outbound call report.
Elective Change Report	A monthly summary report of elective change hours expended in support of the elective changes requested by the Customer.
Operations Report	A monthly report that provides ticket information and response times.

**APPENDIX C:**

**Cisco Foundation Technologies Remote Management Services**

This Appendix describes the services capabilities, supported devices, elective changes, and reports delivered with Cisco Foundation Technologies Remote Management Services.

Activities & Deliverables
Management readiness assessment
Intelligent monitoring
Incident resolution
Advanced Event Correlation (device, time, syslogs)
Self-Diagnostics and Business Rules Engine
Incident notification
Root cause analysis
Standard Changes
Review/assess Cisco Field Notices
Ticket Trending and problem analysis
Problem resolution
Backup of Cisco IOS Routers and Switches
Create Configuration Management Database for managed devices
Execute Elective Changes
Device-level reporting
Web-accessible portal
Carrier Coordination
<ul style="list-style-type: none"> <li>• Coordination of Service Engagement</li> </ul>

**Supported Devices:**

The following table identifies the devices managed by Cisco Foundation Technologies Remote Management Services:

Supported Devices	
Networking Routers	Switches
800 Series	6500
1000 Series	6500 Module: Firewall Services Module (FWSM)
1400 Series	6500 Module: Content Switching Module (CSM)
1600 Series	6500 Module: 8 Port E1 PSTN interface modules
1700 Series	6500 Module: 8 Port T1 PSTN interface modules
1800 Series	6500 Module: 4 Port FXS analog interface module
2000 Series	Catalyst 4900
2500 Series	Catalyst 1200 Series
2600 Series	Catalyst 1600 Series
2800 Series	Catalyst 1700 Series
3000 Series	Catalyst 1800 Series
3600 Series	Catalyst 2100 Series

Supported Devices	
3700 Series	Catalyst 2600 Series
3800 Series	Catalyst 2800 Series
4000 Series	Catalyst 2900 Series
7000 Series	Catalyst 2960
7100 Series	Catalyst 3550
7200 Series	Catalyst 3560
7300 Series	Catalyst 3560E
7400 Series	Catalyst 3750
7500 Series	Catalyst 3750E
7600 Series	Catalyst 3750 Metro Series Switches
	Catalyst 4000
	Catalyst 4500
	Catalyst 4500E
	Catalyst Express 500 Series
	Catalyst Express 520 Series
	Cisco Catalyst 4800 Series Switches
	Cisco Catalyst 4900 Series Switches

### Elective Change Services

Elective Change Services are Customer requested changes and are scheduled activities. The table below identifies the changes that are available for Cisco Foundation Technologies Remote Management Services.

Elective Changes
Licensing <ul style="list-style-type: none"> <li>Apply license updates and changes</li> <li>Track &amp; report on software license usage</li> </ul>
Configuration changes to Cisco software and devices
Cisco software upgrades for feature enhancements and security-related purposes
Patches for Cisco devices and Cisco applications
Connectivity and Path Maintenance <ul style="list-style-type: none"> <li>Packet capture and traffic analysis</li> <li>Device mapping and packet flow monitoring</li> <li>SNMP and non-SNMP-based administration agents</li> </ul>

**APPENDIX D:**

**Cisco Application Delivery Remote Management Services**

This Appendix describes the services capabilities, supported devices, elective changes, and reports delivered with Cisco Application Delivery Remote Management Services.

Activities & Deliverables
Management readiness assessment
Incident Monitoring
Incident resolution
Advanced Event Correlation
Incident notification
Root cause analysis
Standard Changes
Review/assess Cisco Field Notices
Ticket Trending and problem analysis
Problem resolution
Backup of Cisco IOS Routers and Switches
Create Configuration Management Database for managed devices
Execute Elective Changes
Device-level and Component-Level Reporting
Web-accessible portal

**Supported Devices:**

The following table identifies the devices managed by Cisco Application Delivery Remote Management Service:

Supported Devices	
WAAS WAE 512	ACE NME ACE20 *
WAAS WAE 612	ACE4710 Appliance
WAAS WAE 674	ACE AXG
WAAS WAE 7326	GSS 4492
WAAS WAE 7341	CSS 1150X
WAAS WAE 7371	<b><i>Core Infrastructure</i></b>
Cisco WAVE-274	6500
Cisco WAVE-474	7600
Cisco WAVE-574	ISR 1800
WAAS NME 302 *	ISR 2800
WAAS NME 502 *	ISR 3800
WAAS ACNS	
WAAS Central Manager	
ACE NME ACE10 *	

\* Management of the Network Modules requires a purchase of Foundation support for the Host Device as well

## Reports

The following reports are available with this Service:

Reports	Content
ATM PVC Traffic	<p>Inbound Throughput (bps) – Average rate of inbound traffic (bits per second) on this resource during the last measurement interval.</p> <p>Outbound Throughput (bps) – Average rate of outbound traffic (bits per second) on this resource during the last measurement interval.</p> <p>Inbound Volume (PDUs) - The number of PDUs (packets, cells, frames, etc.) received by this resource.</p> <p>Outbound Volume (PDUs) - The number of PDUs (packets, cells, frames, etc.) sent by this resource.</p> <p>Inbound CRC Errors (PDUs) - Number of PDUs received that contained CRC errors</p> <p>Reassembly Timeouts (PDUs) - Number of PDU reassemblies which timed out.</p>
Availability Summary	<p>Interface Availability (percent) - The percentage of time that this Interface was in an operational state.</p> <p>Device Availability (percent) - The percentage of time that this resource was in an operational state.</p>
Cisco CPU Memory Usage	<p>CPU Utilization (percent) - The overall CPU busy percentage over the last 5 minute period.</p> <p>Memory Pool Utilization (percent) - Indicates the percentage of the memory pool that is currently used on the managed device.</p> <p>Memory Pool Free - Indicates the number of bytes from the memory pool that are currently unused on the managed device.</p> <p>Memory Pool Largest Free - Indicates the largest number of contiguous bytes from the memory pool that are currently unused on the managed device</p>
Cisco Catalyst Backplane	Backplane Bandwidth utilization percentage
Cisco Sensor	<p>Voltage Level - Value is in millivolts. "format clean" is required to ensure that negative values are presented correctly.</p> <p>Voltage Status - Value is in millivolts. "format clean" is required to ensure that negative values are presented correctly.</p> <p>Fan State - State values are normal(1), warning(2), critical(3), shutdown(4), notPresent(5), notFunctioning(6).</p> <p>Power Supply State - State values are normal(1), warning(2), critical(3), shutdown(4), notPresent(5), notFunctioning(6).</p> <p>Temperature Level - Value is in degrees Celsius.</p> <p>Temperature Status - Value is in degrees Celsius</p>
Device ICMP	<p>ICMP Messages Received (per second) - The total number of ICMP messages which the entity received.</p> <p>ICMP Messages Sent (per second) - The total number of ICMP messages which the entity attempted to send.</p> <p>Ping Replies Received (per second) - The total number of ICMP echo request (ping) messages received.</p> <p>Ping Replies Sent (per second) - The total number of ICMP echo reply messages sent.</p> <p>Pings Sent (per second) - The total number of ICMP echo request (ping) messages sent.</p> <p>Ping Replies Received (per second) - The total number of ICMP echo reply messages received</p>
Device IP Statistics	<p>IP Packets Received (per second) - The total number of input datagrams received from interfaces, including those received in error.</p> <p>IP Packets Forwarded (per second) - The number of input datagrams for which this entity was not their final IP destination</p> <p>IP Out Requests (per second) - The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP for transmission.</p> <p>No Route (per second) - The number of IP datagrams discarded because no route could be found to transmit them to their destination.</p> <p>Fragmentation Failures (per second) - The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be.</p> <p>Reassembly Failures (per second) - The number of failures detected by the IP re-assembly algorithm (for</p>

Reports	Content
	whatever reason: timed out, errors, etc).
Frame Relay Errors	<p>Inbound BECN (percent) - Out of all frames received by this resource, the percentage that had their forward congestion bit set</p> <p>Inbound FECN (percent) - Out of all frames received by this resource. the percentage that had their forward congestion bit set</p> <p>Inbound Discard Priority (percent) - Out of all inbound traffic received by this resource, the percentage marked priority for discard (CLP=1 for ATM, DE=1 for Frame Relay)</p> <p>Outbound Discard Priority (percent) - Out of all outbound traffic to be sent by this resource, the percentage marked priority for discard (CLP=1 for ATM, DE=1 for Frame Relay)</p> <p>Outbound Discarded (percent) - The percentage of outgoing traffic dropped due to congestion / resource limitations.</p> <p>Availability (percent) - The percentage of time that this resource was in an operational state (in active service) during the last measurement interval. Some reasons that would cause a resource to be out of service include hardware / software faults, manual and automatic resets, and Network maintenance procedures. For interfaces and virtual interfaces, this percentage includes downtime resulting from the entire device being out of service.</p>
Frame Relay Throughput **	<p>Inbound Throughput (bps) - Average rate of inbound traffic (bits per second) on this resource during the last measurement interval.</p> <p>Outbound Throughput (bps) - Average rate of outbound traffic (bits per second) on this resource during the last measurement interval.</p> <p>Inbound Volume (octets) - The volume of traffic (in octets) in the Ingress/Inbound direction to this resource.</p> <p>Outbound Volume (octets) - The volume of traffic (in octets) in the Egress/Outbound direction from this resource.</p> <p>Inbound Volume (PDUs) - The number of PDUs (packets, cells, frames, etc.) received by this resource.</p> <p>Outbound Volume (PDUs) - The number of PDUs (packets, cells, frames, etc.) sent by this resource.</p>
Interface DSX1	<p>Errored Seconds</p> <p>Unavailable Seconds</p> <p>Severely Errored Seconds</p> <p>Severely Errored FrameSeconds</p>
Interface DSX3	<p>Unavailable Seconds</p> <p>Severely Errored Seconds</p>
Interface Error Discard	<p>Delivered (inbound) Packets - Total number of packets delivered to a higher layer, during the last polling period. This metric excludes any packets that were received by an interface but not passed on.</p> <p>Inbound Errors - The number of incoming PDUs that were discarded due to errors.</p> <p>Inbound Discards - The number of incoming PDUs dropped due to congestion / resource limitations.</p> <p>Transmitted (outbound) Packets - The number of PDUs (packets, cells, frames, etc.) sent by this resource.</p> <p>Outbound Errors - The number of outgoing PDUs that were discarded due to errors.</p> <p>Outbound Discards - The number of outgoing PDUs dropped due to congestion / resource limitations.</p>
Interface LAN Error	<p>Inbound Abort - Valid on packet-oriented interfaces only. The number of (error-free) packets dropped during the last polling period. Packets may be dropped for capacity reasons (no buffer space) or for traffic-shaping reasons.</p> <p>Inbound CRC - Number of input packets which had cyclic redundancy checksum errors.</p> <p>Inbound Frame - Number of input packet which were misaligned.</p> <p>Inbound Giants - Number of input packets which were larger then the physical media permitted.</p> <p>Inbound Ignored - Number of input packets which were simply ignored by this interface.</p> <p>Inbound OverRun - Count of input which arrived too quickly for the to hardware receive.</p>
Interface Multicast	<p>Inbound Unicast Packets per Second - The number of packets received on an interface and delivered to a higher layer. Does not include packets addressed to a multicast or broadcast address at this layer.</p> <p>Outbound Unicast Packets per Second - The number of packets presented to an interface for</p>

Reports	Content
	<p>transmission, including those that were not transmitted. Does not include packets addressed to a multicast or broadcast address at this layer.</p> <p>Inbound Multicast Packets per Second - The number of packets received on an interface and delivered to a higher layer which were addressed to a multicast address at this layer.</p> <p>Outbound Multicast Packets per Second - The number of packets presented to an interface for transmission, including those that were not transmitted, which were addressed to a multicast address at this layer.</p> <p>Inbound Broadcast Packets per Second - The number of packets received on an interface and delivered to a higher layer which were addressed to a broadcast address at this layer.</p> <p>Outbound Broadcast Packets per Second - The number of packets presented to an interface for transmission, including those that were not transmitted, which were addressed to a broadcast address at this layer.</p>
Interface Throughput Bandwidth**	<p>Inbound Utilization (percent) - The average percentage of inbound capacity utilized on this resource during the last measurement interval. Half-Duplex Note: Interfaces such as Ethernet are full-duplex, meaning that applied to such, this metric only reports the percentage of the interface's total capacity that is being utilized by incoming traffic. This percentage needs to be added to the outbound utilization percentage to get an idea of the total utilization on a full-duplex interface.</p> <p>Outbound Utilization (percent) - The average percentage of outbound capacity utilized on this resource during the last measurement interval. Half-Duplex Note: Interfaces such as Ethernet are full-duplex, meaning that applied to such, this metric only reports the percentage of the interface's total capacity that is being utilized by outgoing traffic. This percentage needs to be added to the inbound utilization percentage to get an idea of the total utilization on a full-duplex interface.</p> <p>Inbound Throughput (bps) - Average rate of inbound traffic (bits per second) on this resource during the last measurement interval.</p> <p>Outbound Throughput (bps) - Average rate of outbound traffic (bits per second) on this resource during the last measurement interval.</p>
Interface Volume Health	<p>Inbound Volume (octets) - The volume of traffic (in octets) in the Ingress/Inbound direction to this resource.</p> <p>Outbound Volume (octets) - The volume of traffic (in octets) in the Egress/Outbound direction from this resource.</p> <p>Inbound Errors - The number of incoming PDUs that were discarded due to errors.</p> <p>Outbound Errors - The number of outgoing PDUs that were discarded due to errors.</p> <p>Unknown Protocols - The number of incoming PDUs discarded due to an unknown or unsupported protocol.</p>
Top 10 Utilization Exception Report	Top 10 Utilization Exception Report (for each, Tx and Rx ) (per cust)
Top 10 Interface Errors Exception Report	Top 10 Interface Errors Exception Report: (per cust)

\*\* These reports should be used judiciously due to the additional cost of Network resources (BW, platform licensing, server capacity,...) they incur. They should only be used when necessary to help Cisco manage the Network.

### Elective Change Services

Elective Change Services are Customer requested changes and are scheduled activities. The table below identifies the changes that are available for Cisco Application Delivery Remote Management Services.

Elective Changes
Licensing <ul style="list-style-type: none"> <li>• Apply license updates and changes</li> <li>• Track &amp; report on software license usage</li> </ul>
Cisco software upgrades for feature enhancements and security-related purposes
Connectivity and Path Maintenance <ul style="list-style-type: none"> <li>• Packet capture and traffic analysis</li> <li>• Device mapping and packet flow monitoring</li> </ul>

<b>Elective Changes</b>
<ul style="list-style-type: none"><li>• SNMP and non-SNMP-based administration agents</li></ul>
NetworkCarrier Coordination
<ul style="list-style-type: none"><li>• Coordination of Service Engagement</li></ul>
Patches to Cisco equipment and Cisco applications

**APPENDIX E:**

**Cisco Wireless Remote Management Services**

This Appendix describes the services capabilities, supported devices, elective changes, and reports delivered with Cisco Wireless Remote Management Services.

<b>Activities &amp; Deliverables</b>
Management readiness assessment
Backup of Cisco IOS Devices
Incident Monitoring
Incident resolution
Advanced Event Correlation
Incident notification
Root cause analysis
Standard Changes
Review/assess Cisco Field Notifications
Ticket Trending and problem analysis
Problem resolution
Create Configuration Management Database for managed devices
Execute elective changes
Device-level and Component-Level Reporting
Web-accessible portal

**Supported Devices:**

The following table identifies the devices managed by Cisco Wireless Remote Management Services

<b>Supported Devices</b>
AP1100* series
AP1130 AG series
AP1200* series
AP1230 AG series
AP1240 AG series
AP1250* AG series
500 series Express Access Points
Wireless LAN Controller 2000
Wireless LAN Controller 2100
Wireless LAN Controller 4400
Wireless Service Module (WiSM) 6500 *
Wireless Service Module (WiSM) 7600 *
Network Module WLC12 for ISR 2800 *
Network Module WLC8 for ISR 2800 *
Network Module WLC6 for ISR 2800 *
Network Module WLC12 for ISR 3800 *

Supported Devices
Network Module WLC8 for ISR 3800 *
Network Module WLC6 for ISR 3800 *
Integrated WLAN Controller S25 for 3750G
Integrated WLAN Controller S50 for 3750G

- Management of the Network Modules only. Management of the Host Device is included in Cisco Foundation Technologies Remote management Services (see Appendix C).

### Elective Change Services

Elective Change Services are Customer requested changes and are scheduled activities. The table below identifies the changes that are available for Cisco Wireless Remote Management Services.

Elective Changes
Licensing
<ul style="list-style-type: none"> <li>• Apply license updates and changes</li> </ul>
Configuration changes to Cisco software and devices
QoS to support wireless phones and prioritize mission critical traffic.
Rogue AP detection and optional blocking.
Centralized configuration repository with change detection and escalation.
Investigation and resolution of authentication issues
Management of digital certificates and encryption keys
Analysis of logs and protocol sampling to develop a protocol catalog
Adjustment of power levels to delineate coverage zones.
Cisco software upgrades for feature enhancements and security-related purposes
Licensing
<ul style="list-style-type: none"> <li>• Apply license updates and changes</li> <li>• Track &amp; report on software license usage</li> </ul>
Cisco software upgrades for feature enhancements and security-related purposes
Connectivity and Path Maintenance
<ul style="list-style-type: none"> <li>• Packet capture and traffic analysis</li> <li>• Device mapping and packet flow monitoring</li> </ul>
SNMP and non-SNMP-based administration agents
NetworkCarrier Coordination
<ul style="list-style-type: none"> <li>• Coordination of service engagement</li> </ul>
Patches to Cisco devices and applications

## APPENDIX F:

### Glossary of Terms

Glossary of Terms should be read in conjunction with this Service Description. Capitalized terms not defined herein have the meanings assigned to them in the Glossary of Terms.

**Analog Telephony Devices** means devices such as fax machines, modems, and analog phones connected to FXS or gateway ports and that require call processing by a managed Cisco Unified Communications Manager.

**Advanced Event Correlation (device-level, component-level, time-based)** means the act of combining disparate data sources to obtain root cause.

**Backup Management** means the process and actions needed to backup and restore Cisco IOS router and switches. May include backup policies outlining retention policies, ad-hoc configuration backups and restores as well as standard backup reports.

**Carrier** means a provider of data transport services.

**Change Management** means the process used by the Cisco to receive, authorize, execute, and communicate changes to Managed Components.

**Change Request** means any request for service made by the Customer or Partner, who Customer has granted the authority to act on its behalf, in electronic format (submitted via the Portal).

**Cisco** means Cisco Systems, Inc., a California corporation having its principal place of business at 170 West Tasman Drive, San Jose, California 95134.

**Cisco Field Notice** means an electronic notification about product related issues.

**Cisco Remote Operations Services (ROS)** means the Cisco Services team that delivers Cisco Remote Management Services.

**Configuration Management** means the process to create and maintain an inventory of the Managed Components.

**Customer** means the entity purchasing Services for its own internal use either directly or through an Authorized Channel.

**Customer Acceptance** means a mutual agreement with Cisco to acknowledge completion of the Transition Management phase.

**Customer Notification** means a communication to inform the Customer that an Incident has been recorded.

**Customer Premises** means the physical Customer location where the Managed Components reside.

**E-notification** means the act of sending notification of Incidents and the status of Tickets electronically.

**Elective Change** means a change requested by the Customer and is often the result of changes in the Customer Network, business processes, or the business. Elective Changes are not the result of Cisco Incident Management and Problem Management processes.

**Elective Change Request** means any request for service made by the Customer or Partner, in electronic format (submitted via the Portal).

**Host Device** means chassis.

**IOS** means Cisco Internet Operating System.

**Unified Communications (UC)** means the functionality of providing traditional voice services, to include but not limited to, phones calls, convergence calls, or voicemail services, over an IP enabled Network.

**Incident** means any event that is not part of the standard operation of a service and that causes or may cause an interruption to, or reduction in, the quality of that service.

**Incident Management** means the process to detect an incident, notify the Customer about the incident and resolve the incident.

**Incident Resolution** means the process to restore services on Managed Components.

**Intelligent Monitoring** means advanced correlation and automation of tools and scripts to enable quick response to Incidents.

**IT** means Information Technology.

**Knowledge Base** means a searchable database of knowledge and known errors.

**Known Error** means Incidents with a defined root cause and resolution.

**Letter of Agency** means a letter which authorizes Cisco to act as the Customer's agent for purposes of ordering, facilitating, tracking and/or providing services with Carriers, maintenance contract providers, and other general-service providers.

**Managed Component** means an element for which remote IT-infrastructure management services are provided by Cisco.

**Management Application Platform** is suite of management applications and tools that Cisco uses to deliver ITIL based Service Management.

**Management Connection** means the physical communication link between the Cisco and the Customer Premise.

**Management Connectivity** means a bi-directional communication between the Customer Premise and Cisco for Management Data to be securely and consistently transmitted between Managed Components and Cisco.

**Management Data** means events, alerts, performance information, traps and/or log messages that are collected by the Service Management Application.

**Management Readiness Assessment** means an assessment that determines whether all Managed Components are in good working order prior to completion of Transition Management. Requires Managed Components are fully configured, deployed and functioning properly prior to the commencement of Incident and Problem Management services.

**Management Services** means a service that provides Monitoring, Incident Resolution, Reactive Problem Management, service level management and Standard Changes to resolve all Incidents.

**Monitoring** means detecting events on Managed Components.

**Network** means a set of interconnected and interworking Cisco supported hardware and software that is implemented, operated, and supported by Customer from a single Network operations center (NOC).

**Network Component** means a device or link that makes up part of a Network.

**Non-Managed Component** means any element for which management services is not provided by Cisco.

**Normal Service Operation** means service operation within Cisco service levels as defined in *Section 4 Service Level Management*.

**OSI** means the Open System Interconnection Reference Model.

**Partner** means the third party contracted by Customer to act as its technical point of contact with respect to the Services.

**Patch** means a small fix to a problem using a piece of software code.

**Point of Presence** means a carrier aggregation point for access to carrier-provided Internet and wide area Network services.

**Portal** means the online Web user interface supplied for Customers and Partners to receive and submit information to and from the NOC.

**Primary Management Connectivity** means the management connection provided by Cisco.

**Proactive Problem Management** means the process to prevent Incidents.

**Problem** means the underlying cause of one or more Incidents.

**Problem Analysis** means the activity of investigating problems to determine the root cause.

**Problem Management** means the process to find and resolve the root cause of a Problem and prevention of Incidents.

**Problem Resolution** means the process of providing remediation based on the root cause for unknown Incidents.

**Project Coordinator** means the Cisco project manager who is the single point of contact thru the Transition Management phase.

**PSTN** means Public Switched Telephone Network.

**PVC** means Private Virtual Circuit.

**Quote** means quote for services.

**Reactive Problem Management** means the Problem Management sub-process that primarily supports Incident Management. These processes are initiated when an Incident cannot be matched to a Known Error.

**Read** means the ability to view system logs, configuration files and other device and system-level information.

**Release Management** means the process focused on the actual implementation of approved Changes.

**Reseller** means the business that sold Cisco management to the Customer.

**Self-Diagnostic and Business Rules Engine** means the ability to gather further diagnostic data and provide additional actionable recommendations.

**Service Description** means Cisco will provide the Services and perform Cisco responsibilities described in the standard Cisco Service Description located at [www.cisco.com/go/servicedescriptions/](http://www.cisco.com/go/servicedescriptions/) (or such other location of which Cisco may notify Customer from time to time).

**Service Activation Kit (SAK)** means a document that is completed by the Customer during the Transition Management phase.

**Service Delivery** means the phase after Transition Management when Cisco begins to deliver Services.

**Service Desk** means a single point of contact for Customers for the Service.

**Services** mean Cisco Remote Management Services which consist of the activities and the processes used by Cisco to monitor manage and make changes to your Network, voice and application services.

**Standard Business Hours** means 8AM to 5PM in the time zone of the Customer's headquarters.

**Standard Change** means a Cisco ROS recommended change that is often as a result of Incident Management and Problem Management processes or Cisco Field Notice.

**Standard Change Request** means a request for change to solve an Incident or Problem.

**Start Date** means the date Services commence.

**SLA** means Service Level Agreement.

**SLO** means Service Level Objective.

**Termination Device** means Customer Premises equipment that terminates the Management Connection.

**Ticket** means the tracking mechanism for Incidents and service requests within the NOC. The NOC activities are detailed within the Ticket that contains the complete history of record for an Incident or service request.

**Transition Management** means a phased process approach in which Cisco prepares Customer infrastructure for the Management Services.

**Ticket Trending** means analyzing tickets and ticket trends so that proactive steps can be taken to reduce or eliminate potential future incidents from occurring in the Network.

**VPN** means Virtual Private Network.

**Write** means the ability to make and save changes to device configurations.