Service Description for Cisco Managed Services

This document describes the service elements, features and components of the Cisco Managed Services.

General

Related Documents. This document should be read in conjunction with the following documents: (1) Glossary of Terms for the Service Description for Cisco Managed Services; (2) List of Services Not Covered (posted at www.cisco.com/go/servicedescriptions/); (3) the methodology and associated terminology used in determining the priority level of an Incident, which is included in Appendix A of this Service Description; and (4) Exhibit 1 to the Service Description for Cisco Managed Services ("Exhibit 1").

Direct Sale from Cisco. If you have purchased these Services directly from Cisco, this document is incorporated into your Master Services Agreement (MSA) or equivalent services agreement executed between you and Cisco, including Cisco's End User License Agreement as it related to Cisco's Data Collection Tools. 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 description purposes only and is not a contract between you and Cisco. The contract, if any, governing the provision of this Service will be the one between you and your Cisco Authorized Reseller. Your Cisco Authorized Reseller should provide this document to you, or you can obtain a copy of this and other Cisco service descriptions at www.cisco.com/go/servicedescriptions/.

Order of Preference. In the event of a conflict between the Service Order, the Agreement, this Service Description, any Addendum(s) to this Service Description, and the Exhibit 1, the following priority will apply (from highest to lowest): (a) the Service Order; (b) any Addendum(s); (c) the Service Description; (d) the Exhibit 1 and (e) the applicable Agreement.

Service Order

An accompanying Customer Service Order will reference this Service Description and Exhibit 1, which details the quantity, type, pricing, payment terms, and any additional commitments by Customer.

Defined Terms

Unless otherwise defined in the body of this Service Description, capitalized terms used in this Service Description are defined in this Service Description for Cisco Managed Services Glossary of Terms, in the Service Order, or in the Agreement.

Service Summary

Cisco Managed Services consists of a set of multi-technology managed services described below that involve the monitoring, management, and troubleshooting of the Managed Components. Service components common to all Cisco Managed Services are based upon the Information Technology Infrastructure Library (ITIL) Service Lifecycle Processes.

Service components associated with specific technologies are provided in the applicable Addendum to the Service Description for Cisco Managed Services.

Contents

ITIL Service Design

ITIL Availability Management

Availability Management

Cisco will track system uptime and reachability of Managed Components.

Cisco Responsibilities

- Create a list of Key Performance Indicators (KPIs) related to service availability that will be monitored
- Create mutually defined availability thresholds for the KPIs
- Manage KPIs by generating Threshold Crossing Alerts (TCAs)
- Notify mutually agreed relevant parties or systems when KPI thresholds are exceeded
- Create Incidents based on TCA notifications
- Analyze Incidents to identify potential issues
- Provide availability reports about the managed infrastructure and applications

Customer Responsibilities

- Review and agree to the KPIs and TCAs
- Review reports and discuss as needed

ITIL Capacity Management

Capacity Management

Cisco will monitor the capacity of the Managed Components.

Cisco Responsibilities

- Create a baseline of the environment’s throughput and/or capacity by establishing KPI related to capacity that will be monitored
- Create mutually defined capacity TCAs associated with the KPIs
- Notify mutually agreed relevant parties or systems when KPI thresholds are crossed
- Create Incidents based on TCA notifications
- Analyze Incidents to identify potential issues

Customer Responsibilities

- Review and agree to the KPIs and TCAs
- Review reports and discuss as needed

Performance Management

Cisco will monitor the performance of the Managed Components against defined performance standards and provide reporting.

Cisco Responsibilities:

- Create a list of KPIs that will be monitored
- Create mutually defined performance TCAs associated with the KPIs
- Notify mutually agreed relevant parties or systems when TCAs are triggered
- Create Incidents based on TCA notifications
- Analyze performance Incidents to identify potential issues

Customer Responsibilities:

- Review and agree to the KPIs and TCAs

ITIL Service Catalog Management

ITIL Supplier Management

Non-Standard Managed Device Management

Cisco will oversee the interactions with and management of third party suppliers who provide certain third party supplier products and/or services to Customer that are included as Non-Standard Managed Components in the Exhibit 1.

Cisco Responsibilities

- Support Non-Standard Managed Components as set forth in the Exhibit 1
- Manage Non-Standard Managed Components through their lifecycle, provide periodic license utilization reports and provide support services to Customer via terms described in the Exhibit 1
- Advise of Non-Standard Managed Component dependencies

Customer Responsibilities

- Identify Non-Standard Managed Components and the associated third party suppliers
- For customer-held licenses for third party Non-Standard Managed Components, obtain appropriate rights-to-use for Cisco in any third party agreement, manage the contracts through their lifecycle, and provide a Letter of Agency (LoA) as required by vendors authorizing Cisco's management

ITIL Service Transition

ITIL Change Management

Emergency Change Management

Cisco will coordinate the scheduling and application of changes related to Incidents and Problems affecting the Managed Components with Customer. Emergency Changes are scoped to restore the service.

Cisco Responsibilities

- Create Emergency Change requests
- Manage the change procedure(s) to restore service, including release packaging, dependencies, deployment, validation, and back-out
- Identify dependencies for each change request
- Coordinate execution of Emergency Change to Managed Components directly between Cisco and Customer Single Point of Contact (SPOC) assigned to the Incident
- Notify relevant parties about Emergency Changes, keeping the parties updated to closure
- Manage all change records using Cisco's Information Technology System Management (ITSM) tool(s)

Customer Responsibilities

- Integrate Cisco Change Management processes into Customer's Change Advisory Board (CAB) processes
- Provide Cisco access to CAB processes
- Facilitate CAB processes for scheduling, communicating, and executing changes
- Perform changes if outside of scope of the services

Normal Change Management

Cisco will interact with Customer SPOC that represents the Customer's CAB to coordinate changes that affect the operation of the Managed Components. Normal Changes are planned changes that typically require CAB approval before they can be deployed.

Cisco Responsibilities

- Create Normal Change requests, as required, resulting from an Incident or Problem, Service Request Fulfillment process, or Service Requests, in accordance with the change management process governed by the CAB
- Notify relevant parties about changes, keeping the parties updated through to closure
- Assign and/or change priorities per mutually agreed CAB processes
- Manage the change procedure(s), including dependencies, deployment, validation, and back-out
- Manage scheduling with Customer SPOC that represents CAB processes
- Manage all change records using Cisco's ITSM tool(s)

Customer Responsibilities

- Integrate Cisco Change Management processes into Customer's CAB processes
- Provide Cisco access to CAB processes
- Represent Cisco in CAB processes for scheduling and communicating changes
- Provide change window

Standard Change Management

Cisco may make changes to the software and configuration of the Managed Components as a part of Change Management. The scope of the changes is mutually agreed to be highly repeatable and not require CAB approvals. Standard Changes are categorized by the original Service Request Types defined in the Appendix of the appropriate Addendum to the Service Description for Cisco Managed Services.

Cisco Responsibilities

- Interact with Customer SPOC that represents the Customer's CAB
- Create Standard Change requests from Service Requests in conjunction with mutually pre-agreed change management processes governed by the CAB
- Manage the change procedure(s), including dependencies, deployment, validation, and back-out
- Manage all change records using Cisco's ITSM tool(s)

Customer Responsibilities

- Represent Cisco in CAB processes as necessary
- Agree to Standard Changes that do not require CAB approvals
- Confirm that a maintenance window is not required for Standard Changes

ITIL Service Asset Management

Service Asset Management

Cisco will collect and maintain inventory information about the environment.

Cisco Responsibilities

- Provide an inventory of all Managed Components
- Facilitate addition/deletion of Managed Component inventory within the inventory management system
- Provide support for management and use of inventory and infrastructure configuration baselines
- Provide periodic reporting regarding Cisco's Configuration Management Database (CMDB)
- Manage and protect the integrity of Managed Components and configurations via a policy that requires in-scope components are used and only authorized changes are made consistent to Customer's CAB processes

Customer Responsibilities

- See General Customer Responsibilities below

ITIL Service Transition Planning and Support

Local Language Support

Cisco will provide mutually agreed spoken language support in a language other than English during standard business hours. Exhibit 1 will provide the selected language(s), their hours of availability, and the locations at which they are available.

Cisco Responsibilities

- Provide local language support via a Cisco team and/or language translation services
- Agree to language selection(s) during contracting

Customer Responsibilities

- Agree to language selection(s) during contracting
- Customer must contact Cisco during standard business hours as defined per location to receive the agreed spoken language support

Portal

Cisco will provide access to a web-based Portal that contains Customer reports and information related to the services purchased.

Cisco Responsibilities

- Implement and manage a Cisco hosted, web-based Portal
- Provide capability to generate and download reports and download past reports
- Provide administrative user interface for Customer to manage user profiles

Customer Responsibilities

- Implement and administer Role Based Access Control (RBAC) for user profiles in accordance with good industry practice

Service Transition

Cisco will aid in the discovery of components and will prepare the Managed Components to be monitored and/or managed. Cisco will gather information about, and onboard Customer's Managed Components on to Cisco's management systems.

Cisco Responsibilities

- Provide a transition plan for onboarding Customer's Managed Components into the Cisco's management system
- Provide a VPN end point to enable Cisco's remote connectivity
- Manage the schedule and lead the Service Transition
- Create and update a Runbook based on standardized templates and services
- Identify a SPOC to engage with Customer during the Service Transition
- Discover components and assist in determining candidates for onboarding or retiring
- Onboard and or retire Managed Components per Customer guidance
- Establish a go live date (or set of dates) when Cisco will begin to managed and/or monitor the Managed Components
- In addition to the above, perform tasks specified in any transition plan

Customer Responsibilities

- Timely provide functional host names, IP addresses, SNMP strings, passwords, and similar information for all Managed Components
- Provide a single point of contact/technical lead to assist Cisco with establishing access required for remote management
- Implement all activities needed to ensure connectivity between all Managed Components and Cisco's management system
- Review and approve Runbook
- Agree to the go live date(s)
- Perform tasks specified as Customer's responsibility in the transition plan by the dates described in the transition plan
- Return Cisco owned assets, uninstall Data Collection Tools, and close VPN endpoint upon termination of the Service

Note: Cisco owned or license hardware or software based data collection tool(s) may be used at Customer's site(s) to aid in the performance of the Cisco Managed Services ("Data Collection Tools"). Cisco will provide the requirements (power, HVAC, etc.) for these tools as a part of Service Transition. Customer will be responsible for any loss, theft or damage to the tool(s) until they are returned, except to the extent caused by Cisco.

ITIL Application Management

Application Management

Cisco will manage applications that are listed as Managed Components (application-based Managed Components) in Exhibit 1.

Cisco Responsibilities

- Maintain proper working order of the application-based Managed Component, as provided in Exhibit 1
- Confirm the application-based Managed Component is configured for Simple Network Management Protocol (SNMP) management and/or syslog messages, as appropriate

Customer Responsibilities

- Provide Cisco with SNMP and Secure Shell (SSH) access to the application-based Managed Components that support these access protocols
- Ensure Cisco has administrative access to the application-based Managed Components

ITIL Service Operation

ITIL Event Management

Event Management

Cisco will monitor for Events on the Managed Components.

Cisco Responsibilities

- Create and implement Event Management policies
- Detect that an Event has occurred by monitoring Syslog, Simple Network Management Protocol (SNMP) trap messages, KPIs, and/or TCAs from Managed Components
- Implement Event correlation and filtering though Event Management policies when an Event occurs
- Help identify meaningful Events by creating filtering rules

Customer Responsibilities

- Provide access and configuration changes for Cisco to receive messages from the Managed Components

ITIL Incident Management

eBonding

Cisco will provide Information Technology System Management (ITSM) integration points to allow Customer's ITSM system to communicate with the Cisco Managed Services ITSM to facilitate the exchange of ticketing, status, and workflow processes, and other information.

Cisco Responsibilities

- Provide an ITSM integration interface between Cisco's ITSM and Customer's ITSM that facilitates the exchange of Change Management, Incident Management, and Service Request Fulfillment workflow ticketing and status updates
- Provide a Customer accessible interface to Cisco's ITSM process
- Notify Customer of any material changes to Cisco's ITSM interface

Customer Responsibilities

- Instrument Customer ITSM system to interoperate with Cisco ITSM integration interface
- Provide a SPOC for eBonding operations
- Notify Cisco when any material changes are made to Customer's ticketing systems
- Contact Cisco if Customer believes eBonding ticketing data or information is incorrect

Incident Management

Cisco will identify, troubleshoot, and restore normal operational functionality if an Incident is detected in a Managed Component.

Cisco Responsibilities

- Create Tickets from detected or reported Events
- Manage Incidents by classifying, prioritizing, troubleshooting, and restoring normal operation
- Assign and reassess Incident priorities in accordance with the process defined in Appendix A of this Service Description
- Notify mutually agreed relevant parties about Incidents, keeping the parties updated through Incident closure
- Provide Incident reports pertaining to the Managed Components

Customer Responsibilities

- Provide means for Cisco to access, troubleshoot, and resolve Managed Components
- Provide details about support contracts and other documentation/authorization required to facilitate Incident resolution
- Contact Cisco if Customer believes an Incident is in-progress
- Review reports and discuss as needed
- Perform recommended changes to Managed Components or third party hardware, software, or services if outside of control of Cisco

Managed Component Management

Cisco will manage the operation of the Managed Components.

Cisco Responsibilities

- Confirm that the Managed Components can successfully send and receive and/or process data traffic and report failed passwords and community SNMP strings
- Confirm the Managed Component is properly configured to send Simple Network Management Protocol (SNMP) and/or syslog messages as appropriate

Customer Responsibilities

- Provide Cisco with current passwords and SNMP strings for the Managed Components or alternatively, provide Cisco with the means to modify passwords and SNMP strings

ITIL Problem Management

Proactive Problem Management

Cisco will proactively identify situations that may cause an Event on a Managed Component and provide solutions to reduce the recurrence of similar events.

Cisco Responsibilities

- Analyze Events or Incidents to identify common situations and trends that trigger an Event to identify common root cause or errors and create a Problem Record
- Analyze Cisco Product Security Incident Response Team (PSIRT) notifications, Cisco security vulnerabilities, and field notices to determine if action is necessary
- Provide actionable recommendations to Customer and/or CAB to resolve Problem Record and reduce the recurrence of similar Events
- Maintain Problem Records to determine if action taken resolved the root cause and provide actionable recommendations to a Known Error database maintained by Cisco
- Help identify situations in which the Problem may occur

Customer Responsibilities

- Provide additional information regarding Managed Component configurations, Non-Standard Managed Components, and/or similar information which may be related to the Incident(s) or Problem(s)
- If applicable, coordinate with third party suppliers to address situations or incompatibilities where a Non-Standard Managed Component is the cause of a Problem
- Review Problem Record report(s) and discuss, as needed
- Implement recommended changes if outside the scope of the Service

Reactive Problem Management

Cisco will reactively respond to Customer-reported Problems that may impact the Managed Components and provide solutions to reduce the recurrence of similar events.

Cisco Responsibilities

- Analyze Problem Record from Customer, including history of the Problem
- Characterize and prioritize Problem Record from Customer, and determine appropriate actions
- Provide actionable recommendations to Customer and Known Error database maintained by Cisco
- Provide up to eight (8) Root Cause analysis or major Problem review documents, if necessary
- Close Problem Record

Customer Responsibilities

- Submit a request for reactive Problem Management support to Cisco

- Provide additional information regarding Managed Component configurations, Non-Standard Managed Components, and/or information that may relate to the Problem Record
- Coordinate with third party suppliers to address situations or incompatibilities where a Non-Standard Managed Component is the cause of a Problem Record, if applicable
- Implement recommended changes if outside the scope of the Service
- Review Problem Record report and discuss, as needed

ITIL Request Fulfillment

Service Requests

Cisco will manage handling of submitted requests for service. Service Requests are categorized by Request Types that are specified in the Appendix of the appropriate Addendum to the Service Description of Cisco Managed Services.

Cisco Responsibilities

- Provide a web-based Portal for Customer to request and Cisco to, categorize, approve, prioritize, and manage received Service Requests
- Manage the request through validation, completion, and closure
- Follow appropriate procedures to fulfill the Service Request

Customer Responsibilities

- Create a request for service with the required information
- Provide acknowledgement if requested when the service request is completed
- Provide a list of authorized users permitted to submit Service Requests

Service Request Fulfillment

Cisco will fulfill approved changes and Service Requests to the Managed Components.

Cisco Responsibilities

- Execute approved Service Requests and associated Standard and Normal Changes
- Manage Service Request record disposition post implementation
- Manage change record(s) and Service Requests in Cisco's Information Technology System Management (ITSM) CMDB as appropriate
- Evaluate Service Requests that are not defined in the Appendix of the appropriate Addendum to the Service Description for Cisco Managed Services or Services Requests that may require additional fees

Customer Responsibilities

- Provide means for Cisco to access, and make changes to the environment's Managed Components
- Provide reasonably requested additional details pertaining to Service Request(s)

ITIL Continual Service Improvement

ITIL Service Measurement

Business Review

Cisco will host a business review on a frequency as defined in Exhibit 1. Additional operational reviews may be held as reasonably requested by Customer.

Cisco Responsibilities

- Provide an agenda and schedule for the business review with Customer
- Provide information about tickets trends, response times, and performance metrics as applicable
- Provide analysis of historical, trended, performance, and operational data about service delivery

- Provide recommendations for improving the Service
- Implement generally available improvements to Cisco's tools and processes

Customer Responsibilities

- Provide a representative to attend and acknowledge any Customer actions discussed during the review
- Evaluate, and if agreed, approve recommended actions and provide updates regarding past actions

ITIL Service Reporting

Reporting

Cisco will make reports available to Customer as listed in the applicable Service Addendum.

Cisco Responsibilities

- Provide standardized, preconfigured reports related to the services purchased via the online Portal
- Provide exportable report data in Portable Document Format (PDF) and/or Comma Separated Value (CSV) formats

Customer Responsibilities

- Provide a list of authorized users eligible to receive reports

General Customer Responsibilities and Exclusions

Cisco's provisions of the services are dependent on certain assumptions, including Customer's compliance with its responsibilities as listed in this Service Description. If any of the assumptions materially change or are inaccurate or if Customer fails to comply with its responsibilities under this Service Description, the parties will promptly work in good faith to adjust the scope, pricing, or other elements in writing via Cisco's change management processes. Unless expressly provided in writing as a Cisco responsibility, in addition to the Customer responsibilities listed above, Customer shall also be responsible for the following:

- Customer will provide any specialized training of Cisco personnel required for onsite access.
- All pluggable optics will be installed by Customer prior to the start of the services.
- Customer will be responsible for receipt of all inventory and delivery of all equipment and Managed Components at all Customer facilities.
- All quoted work will be performed during Standard Business Hours, unless expressly agreed otherwise.
- Customer will supply Cisco with reasonably requested and necessary technical data (e.g. network diagram) and other information to enable Cisco to provide the Services in a timely manner.
- Customer will provide and maintain the facilities and environmental conditions, including power, HVAC, connectivity, space (physical and rack space), security, raised floors, fire containment, connectivity, reliable out of band access, and other requirements necessary for the proper operation of the Managed Components and Customer's other infrastructure managed infrastructure and applications in Customer facilities.
- Customer will obtain all approvals and licenses required by any third parties related to Customer's facilities, systems, software, and network reasonably necessary for Cisco to provide the services.
- Customer agrees to perform, and cooperate with Cisco in the performance of, all tasks approved via the CAB process.
- Customer is responsible for backing-up and protecting its own data against loss, damage, theft or destruction according to at least generally accepted industry practices.
- Customer will provide Cisco timely physical and remote access to the Managed Components and Customer's other infrastructure, as reasonably required.
- Customer will provide reasonable physical, administrative and technical security to prevent the loss, theft, damage or destruction of any Cisco provided software or hardware for use in conjunction with the Services.
- Customer is responsible for maintaining reasonable technical, administrative, and procedural safeguards to protect its data that may be processed using the services.
- Customer will be responsible for selecting the Managed Components appropriate for the anticipated use.
- Customer will manage all third party products and/or services that are not in the scope of Services.
- Customer will identify any dependencies for out of scope hardware, software and services.
- Customer will provide functional host names, IP addresses, SNMP strings, passwords, and similar information for all Managed Components and applications.
- Customer will maintain Cisco SMARTnet support on all Managed Components.
- Cisco will not provide Services for any Managed Components that are EoX (e.g. End of Life, End of Support, etc.) unless expressly provided in the Exhibit 1.
- Customer will be responsible for obtaining appropriate permissions to use data related to the Managed Components (including third party components) when necessary to provide the Services.
- Upon cessation or termination of the Services, the license to the Data Collection Tools will automatically terminate and Customer will return all Cisco-owned hardware and software licensed for the receipt of the Services.

- Customer will enforce any third party supplier contract terms (and Service Level Agreements, as applicable) and release Cisco from resulting obligations to the extent customer fails to do so.

Exclusions

Products and services that are not described in this Service Description are not part of the services, including, but not limited to, the following examples:

- Customer's Internet connectivity or any equipment necessary to establish such connectivity
- Services or software to resolve any Incidents or problems resulting from a third party product or causes beyond Cisco's control unless specifically described as in scope
- Maintenance on any third-party hardware or software that is not provided by Cisco
- Software or hardware upgrades unless expressly referenced in this Service Description or Addendum(s) to this Service Description
- Migration services unless specifically described as in scope
- Support of equipment not managed by Cisco
- Unless otherwise expressly provided, all services will be performed in English.

Appendix A

This Appendix describes the methodology and associated terminology used in determining the priority level of an Incident.

Cisco classifies Incidents according to “Impact” and “Urgency” and subsequently defines the priority of the Incident by applying the Impact and Urgency terms to the chart below.

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, often equal to the extent to which an Incident leads to availability of the Solution. The impact levels are described below. Cisco will work with Customer during Transition Management to specify the impact for specific Managed Components if necessary. There are four impact levels:

- Widespread: Entire service 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)

Urgency Definition

Urgency defines the criticality of the Incident and its impact on the Services or ability for Customer to receive the Services.

Cisco Incident urgency levels are defined as follows:

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

Priority Definitions

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

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				
URGENCY		Widespread	Large	Localized	Individualized
	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 Priority of impact or Incident resolution.

The case may be left open for a prescribed period while operational stability is being assessed.