Service Description for Cisco Managed Services

This document (this "Service Description") describes the Service elements, features, and components of the Cisco Managed Services. The specific quantity and type of the Services purchased by Customer will be documented in a written Ordering Document between the parties.

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 (available at www.cisco.com/go/servicedescriptions); (2) List of Services Not Covered (available 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) any Ordering Document(s).

Order of Preference. If there is a conflict between this Service Description, an Ordering Document, the applicable Agreement, or any Addendum to this Service Description, the following priority will apply (from highest to lowest): (a) any Ordering Document, as applicable; (b) any Addendum(s); (c) the Service Description; and (d) the applicable Agreement.

Service Summary

The Services are a set of multi-technology managed services, as further described below, that consist of the monitoring, management, and troubleshooting of Managed Components and Third Party Managed Components. Service components common to all Cisco Managed Services are based upon practices recommended by the Information Technology Infrastructure Library (ITIL). Cisco may provide supplemental services as described in an addendum to this Service Description (each an "Addendum") as purchased by Customer pursuant to any relevant Ordering Documents. Service components associated with specific technologies (e.g. networking, data center, collaboration, and/or security) are provided in the applicable Addendum to this Service Description. Unless otherwise expressly provided for in the applicable Ordering Document(s), all Services will be delivered remotely from global NOCs using the "follow-the-sun" delivery model and all Services will be provided 24x7x365, except where noted.

Summary Table, Reporting, Custom Scoped Changes, and Service Levels

The following tables summarize the Service elements that Cisco provides for each tier of the Services:

Service Elements	Foundation	Standard	Comprehensive
Service Transition – Planning and Support	✓	✓	✓
Service Transition – Managed Component Onboarding	✓	✓	✓
Service Asset Inventory Management	✓	✓	✓
High Availability	✓	✓	✓
Event Management	✓	✓	✓
Incident Management	✓	✓	✓
Change Management	✓	✓	✓
Operations Support Portal	✓	✓	✓
Reactive Problem Management	✓	✓	✓
Configuration Management	✓	✓	✓
Exit Assistance	✓	✓	✓
Operations Service Review - Quarterly	✓	✓	✓
Service Delivery Management		✓	✓
Capacity and Performance Reporting		✓	✓
Operations Service Review – Monthly			✓
Availability Management			✓
Proactive Problem Management			✓
Business Review			✓

Optional Service Elements*	Foundation	Standard	Comprehensive
Smart Bonding for CMS	✓	✓	✓
TACACS	✓	✓	✓
Geo-Redundancy	✓	✓	✓
Enhanced Authentication	✓	✓	✓
Service Request Management	✓	✓	✓
Service Fulfillment Portal	✓	✓	✓
Local Language Support	✓	✓	✓
Management of Third Party Managed Components	✓	✓	✓
Proactive Problem Management		✓	✓
Operations Service Review – Monthly		✓	✓

*subject to additional charges and separate purchase

Monitored Components

As part of Service Transition – Managed Component Onboarding, Cisco will identify which devices, hardware, or equipment on Customer's network may be Onboarded as Managed Components and Third Party Managed Components. As part of this process, Cisco will also identify certain devices, hardware, or equipment on Customer's network that may be monitored (but not managed) by

Cisco ("**Monitored Components**"). With respect to these Monitored Components, Cisco's responsibilities will be limited to including any Events recorded by Cisco with respect to the Monitored Components in any applicable reports provided to Customer.

Cisco and Customer acknowledge and agree that, during the course of Change Management, certain Cisco changes to Managed Components may have a resulting impact on the Monitored Components. Any such changes would be discussed and agreed with Customer via Customer's CAB process.

Reporting
Cisco will provide, or make available via the Portal, the reports listed in Reporting Appendix for Cisco Managed Services. Reports which will be provided, based on the tier of Service purchased by Customer.

Custom Scoped Changes
In addition to any Service Requests in the Service Catalog, Cisco will work with Customer to accommodate custom Service Requests, utilizing Cisco's change management process to define the scope and price of, each requested change. Custom Service Requests, describing the scope and associated charges, will be agreed in writing between Cisco and Customer before Cisco proceeds.

Service Level Agreements – Standard and Comprehensive Tiers Only
Cisco will perform and manage the Services in order to meet or exceed the Service Levels described in (and subject to) the applicable Service Level Agreement appendix. This applies only to the Standard Tier and Comprehensive Tier of Services.

Foundation Tier of Service

Service Elements included with Foundation Tier
The following Service elements are included with the Foundation tier:

Service Transition – Planning and Support
Cisco and Customer will work together as described below to define the scope of the Services, including identifying the Managed Components on Customer's Network, and to define the requirements for establishing connectivity between the Managed Components and Cisco.

Cisco Responsibilities

- Host and lead a kick-off meeting via phone or web conference
- Define the high-level scope of work required to transition Customer's existing Network to readiness for management of the Managed Components by Cisco, including assessing changes required to Customer's platform, Network, and processes in order to commence the Services
- Provide and manage a transition plan ("**Transition Plan**") that defines the overall service transition scope, establishes milestones against which project progress will be measured, defines the requirements for establishing connectivity and access for the Service (often requiring a secure VPN end point to enable remote connectivity), and establishes a go-live date (or set of dates) when Cisco will begin to manage and/or monitor the Managed Components
- Define the required inventory information and topology requirements necessary to activate or onboard the Managed Components
- Identify a SPOC to engage with Customer during the Service Transition Perform any other tasks specified in the Transition Plan
- Perform any other tasks designated as Cisco's responsibility in the Transition Plan

Customer Responsibilities

- Unless as otherwise agreed in writing, provide the inventory information and topology requirements, as well as host names, IP addresses, SNMP strings, passwords, and other similar information, necessary to activate or Onboard the Managed Components, as requested by Cisco and as aligned to the milestones agreed in the Transition Plan
- Review and approve Transition Plan, including go-live dates
- Identify a SPOC to engage with Cisco during the Service Transition
- Perform activities and changes, including any required installations
- Obtain all permissions needed to establish and maintain connectivity between all Managed Components and the Cisco Managed Services Platform (CMSP)
- Perform tasks specified as Customer's responsibility in the Transition Plan
- To enable Portal access, make any routing/firewall changes reasonably required by Cisco
- Agree to the go-live date(s) when Cisco will begin to provide operate services on the Managed Components
- Upon termination of the Services, de-install Data Collection Tools, close VPN endpoint and return, at customer cost, all Cisco owned assets as directed by Cisco

Service Transition – Managed Component Onboarding
Cisco will Onboard the Managed Components onto the CMSP with Customer-supplied information and Customer's assistance and will establish connectivity between the Managed Components and Cisco.

Cisco Responsibilities

- Provide a secure VPN end point to enable Cisco's remote connectivity to the Managed Components
- Provide Customer with hardware- or software-based Data Collection Tools and define the technical requirements (e.g. rack space, VM type, power, cooling, etc.) for operation of the Data Collection Tools as part of the CMSP
- Design, implement, and test bidirectional management connectivity and communication
- Remotely assist customer in installing and configuring the Data Collection Tools for installation and use on Customer's Network
- Onboard and/or retire Managed Components, per the applicable Ordering Document(s) and Customer guidance
- Discover Managed Component candidates and determine which candidates should be: (i) Onboarded as Managed Components, (ii) monitored (but not managed) by Cisco as Monitored Components, (iii) out of scope, or (iv) retired
- Provide notification to Customer that Activation is complete
- Provide a Customer Runbook
- Facilitate addition/deletion of Managed Components list within the CMSP via the Change Management process
- Implement CMSP as the system of record

Customer Responsibilities

- Install and configure the Data Collection Tools, including any secure VPN endpoint required, at Customer location(s)
- Provide the environment necessary to meet the technical requirements (e.g. rack space, VM type, power, cooling, etc.) for Data Collection Tools
- Provide private IP address and associated connectivity for the Managed Components
- Provide and validate bidirectional management connectivity through internal firewalls between the Data Collection Tools and Managed Components using the ports and protocols described above
- Provide onsite resources to assist Cisco in establishing and testing connectivity and management of the Management Components
- If desired, review and monitor Cisco's ready for use testing and results
- Review and approve Customer-specific elements in the Runbook
- Make available TCP, UDP, and ICMP ports and IP protocols to Cisco as specified in the Runbook

Service Asset Inventory Management

Cisco will collect and maintain inventory information about the Managed Components and the associated environment.

Cisco Responsibilities

- Provide a list of all Managed Components from Cisco's CMSP, upon Customer request
- Complete addition or deletion of Managed Components listed within Data Collection Tool via the Service Request Process

Customer Responsibilities

- See General Customer Responsibilities below

High Availability

Cisco will provide a second instance of the Data Collection Tools based on location of first instance

of Data Collection Tools.

Cisco Responsibilities

- Deploy dual instances of the Data Collection Tools in a redundant fashion within the same site (onsite or hosted)
- Where the parties mutually agree in writing, deploy an instance of Data Collection Tools at a Customer site, as well as a Cisco-hosted version
- Manage the Data Collection Tools as Managed Components

Customer Responsibilities

- See General Customer Responsibilities below

Event Management
Cisco will monitor for Events on Managed Components.

Cisco Responsibilities

- Create and implement Event Management policies
- Detect that an Event has occurred by monitoring syslog, SNMP trap messages, KPIs, and/or Threshold Crossing Alerts from Managed Components
- Help identify meaningful Events by creating filtering rules
- Implement Event correlation and filtering though Event Management policies when an Event occurs

Customer Responsibilities

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

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, where required
- 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 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 or has occurred, per Runbook
- Perform Cisco or third-party recommended changes to Managed Components or third-party hardware, software, or services, if outside of the scope of the Managed Services
- Provide Cisco with updates to Customer initiated and related to the Incident(s). Please note: Incident Tickets will be on “hold” for any period of time Cisco is delayed in receiving required information from Customer, the End User, or applicable third-party service providers.

Change Management
Cisco will manage the deployment of technical changes to the Managed Components (e.g. configuration changes), in Customer's environment as a result of a change activity. Change types supported by Change Management are Emergency Changes, Normal Changes, Standard Changes and Informational Changes.

Cisco Responsibilities

- Manage the lifecycle of Change Management Requests, as required, resulting from an Incident, Problem, Service Request, as otherwise mutually agreed to in writing or as required in accordance with the Change Management Process
- Coordinate, provide governance and execute changes to Managed Components, using commercially reasonable efforts to minimize any adverse impacts of those changes to Customer's environment
- Provide a Single Point of Contact who will attend up to two hours of Customer CAB meetings per week
- Validate and prioritize Change Requests based on urgency, including PSIRTs where applicable
- Manage end-to-end lifecycle of Change Requests
- Manage all Change Requests using the CMSP
- Provide notifications of change request start and completion for Customer-impacting changes
- Work with Customer to identify and approve Standard Changes
- As part of Customer's CAB process, discuss with Customer any changes to Monitored Components that may result from Changes approved with respect to the Managed Components
- Perform pre- and post-change Health Check

Customer Responsibilities

- Notify Cisco of and review with Cisco any Informational Changes
- Submit Requests for Change (RFCs) for Cisco Managed Components as Service Requests, Incidents via the Portal, Smart Bonding, email, or Customer ITSM
- Submit Requests for Change (RFCs) for Customer Managed Components as Informational Changes via the Portal, Smart Bonding, email, or Customer ITSM
- Review, implement, and execute Cisco-initiated Change Requests in accordance with Cisco's instructions as described in the Change Request
- Inform Cisco on Customer scheduling, communicating, and executing of changes
- Provide Cisco access to Customer CAB meetings and facilitate communication between Cisco and Customer's CAB
- Confirm and maintain scheduled windows for change activities
- Determine and mitigate any impacts to the Monitored Components or out-of-scope devices as a result to a change to the Managed Components
- Review and approve (within 48 hours or less) Cisco-initiated Changes to the Managed Components
- Follow the Change Management Process as described in the Runbook

Operations Support Portal
Cisco will provide a web-based Portal that provides Customer reports and information related to the Services. For security reasons, the Portal is accessible only via the VPN tunnel to Cisco and is not accessible via the public internet.

Cisco Responsibilities

- Implement and make available to Customer a Portal for the Services
- Provide capability to generate and download reports
- Provide administrative user interface for Customer to manage user profiles for access to the Operations Support Portal

Customer Responsibilities

- Make any routing/firewall changes reasonably required by Cisco to enable the Portal
- Provide end user profiles for RBAC in accordance with relevant industry practice
- Review Incident tickets

Reactive Problem Management

Cisco will analyze Incidents after Incident Management has restored Services to identify a Root Cause for P1 Incidents (as defined in Appendix A).

Cisco Responsibilities

- Analyze Cisco Product Security Incident Response Team (PSIRT) notifications, Cisco security vulnerabilities, Known Error databases, and field notices to determine if action is necessary
- Define remediation of PSIRT notifications, if necessary
- Correlate and organize Incidents to create a Problem Record
- Analyze the Problem Record, including any available history
- Characterize and prioritize the Problem Record and determine appropriate actions
- Provide actionable recommendations to Customer, consulting Cisco's Known Error database where needed.
- Work with Customer's Change Management team to deploy a permanent fix
- Provide Root Cause analysis for P1 Incidents (as defined in Appendix A)
- Once resolved, close the Problem Record

Customer Responsibilities

- Provide additional information regarding Managed Component or third party Device configurations and/or information that may relate to the Problem Record
- Coordinate with third-party suppliers to address situations or incompatibilities where a Third Party Managed Component is the cause of a Problem Record, if applicable
- Implement Cisco-recommended changes
- Review the Problem Root Cause Analysis report and discuss, as needed
- Approve PSIRT remediation recommendations

Configuration Management

Cisco will backup and manage the configuration(s) of IOS-based Managed Components.

Cisco Responsibilities

- Implement and manage a Configuration Management system that will import and archive configurations of Managed Components
- Backup Managed Components supported by Cisco CatOS®, Cisco-IOS® and Cisco NX-OS® and IOS-XR® device configurations
- Provide change management processes for updating configurations
- Provide change management reports with recommendations about Managed Components

- Where needed, load configurations onto Managed Components in response to a Service Request

Customer Responsibilities

- Provide Cisco with access to the Managed Components through the Configuration Management system
- Perform and verify backups on devices not running Cisco CatOS®, Cisco-IOS® and Cisco NX-OS® IOS-XR® device configurations

Exit Assistance

Prior to the termination or expiration of the Services, Cisco will make available or provide (as applicable) the following to Customer in connection with the migration of the Services back to Customer or to Customer's third-party provider:

- Runbook
- Four (4) hours of virtual knowledge transfer based on the Runbook
- High level and low-level network design documents, as available; and
- Cisco will disconnect the Cisco VPN from Customer followed by email confirmation

Customer Responsibilities

- Develop and implement staffing skills, tools, and plans to take over the management and monitoring of the Managed Components
- Download applicable reports before termination or expiration date, as desired
- Remove Cisco access to Managed Components

Operations Service Review – Quarterly

Cisco will host a remote service review meeting on a quarterly basis and review operational data including incident tickets and historical trends.

Cisco Responsibilities

- With Customer input, provide an agenda and schedule for the Operations Service Review with Customer
- Provide recommendations for improving the Service delivery
- Where applicable, discuss with Customer the performance of the Services with respect to the Service Levels

Customer Responsibilities

- Provide a representative to attend and agree to perform any Customer actions agreed during the meeting
- Evaluate and approve Cisco-recommended actions and provide updates regarding past actions

Standard Tier of Service

Service Elements included with Standard Tier
The Standard tier includes all Service elements and reports included with the Foundation tier plus the following:

Service Delivery Management
To support high quality service and confirm that service delivery processes are in place, Cisco will provide Service Delivery Management as a part of the Service.

Cisco Responsibilities
- Provide a single point of contact for Customer during business escalations, resolution of commercial issues, and contract renewals discussions
- Monitor, control, and support service delivery so that systems, methodologies, and procedures are followed
- Discuss alignment of Services with the changing business needs and consult on service improvements when out-of-scope changes are needed
- Maintain Runbook to ensure operational activities are up-to-date

Customer Responsibilities
- Provide a key point of contact for Cisco for escalations, commercial issues and contract renewals discussions
- Provide a representative to attend and agree to perform any Customer actions discussed during the Service review
- Evaluate and approve Cisco-recommended actions and provide updates regarding past actions

Capacity and Performance Reporting
Cisco will monitor the capacity and performance of the Managed Components.

Cisco Responsibilities
- Create a baseline of the throughput and/or capacity of Customer's environment by establishing KPIs related to the capacity that will be monitored
- Create defined capacity TCAs associated with the KPIs
- Notify agreed relevant parties or systems when KPI thresholds are crossed
- Create a list of KPIs that will be monitored
- Create defined performance TCAs associated with the KPIs
- Notify agreed relevant parties or systems when TCAs are triggered

Customer Responsibilities
- Provide a quarterly view of upcoming activities/events that may impact capacity

Comprehensive Tier of Service

Service Elements Included with Comprehensive Tier
The Comprehensive tier of the Service includes all Service elements and reports included with the Foundation and Standard tiers, plus the following:

Operations Service Review – Monthly
Cisco will host a remote service review meeting on a monthly basis and review operational data including incident tickets and historical trends.

Cisco Responsibilities
- With Customer input, provide an agenda and schedule for the Operations Service Review with Customer
- Provide information about Incident tickets, response times, and performance metrics and other KPIs as applicable
- Provide report of historical, trended, and operational data about Service delivery
- Provide recommendations for improving the Service delivery
- Where applicable, discuss with Customer the performance of the Services with respect to the Service Levels

Customer Responsibilities
- Provide a representative to attend and agree to perform any Customer actions agreed during the meeting
- Evaluate and approve Cisco-recommended actions and provide updates regarding past actions

Availability Management
Cisco will track system uptime and reachability of Managed Components.

Cisco Responsibilities
- Provide a list of KPIs related to Service availability that will be monitored
- Implement defined availability thresholds for the KPIs
- Manage KPIs by generating TCAs
- Notify relevant parties or systems when KPI thresholds are exceeded
- Create Incidents based on TCA notifications
- Where needed, create and analyze Incidents to identify potential issues according to Incident Management
- Provide availability reports about the managed infrastructure and applications

Proactive Problem Management
Cisco will proactively perform activities aimed at identifying and resolving Problems before Events and Incidents occur. Proactive activities include the following: trend analysis, health checks, and platform tuning.

Cisco Responsibilities
- Analyze Cisco Product Security Incident Response Team (PSIRT) notifications, Cisco security vulnerabilities, Known Error databases and field notices to determine if action is necessary
- Analyze Events and Incidents to assist in identifying trends or errors
- Provide actionable recommendations to Customer to resolve the Problem Record and reduce the recurrence of similar Events

- Provide Root Cause analysis of major Problems
- Maintain Problem Records to determine if the action taken resolved the Root Cause for P1 Incidents

Customer Responsibilities

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

Business Review

Cisco will host a periodic (up to quarterly) meeting to review business outcomes for the previous review period and to confirm alignment of the service with in Customer's business priorities.

Cisco Responsibilities

- With Customer input, provide an agenda and schedule for the business review
- Provide previous period view of historical, trended, and operational data for Service delivery performance
- Highlight operational risks and provide recommendations for improving Service delivery
- Discuss with Customer additional requirements and needs for services based on technology market trends
- Highlight new technology features and propose knowledge transfer, where applicable

Customer Responsibilities

- Provide a representative to attend and agree to perform any Customer actions discussed during the review
- Evaluate and approve recommended actions and provide updates regarding past actions

Optional Service Elements

Customer may purchase one or more optional Service elements as described below and as available with the tier of Service purchased.

Optional Service Elements Available for Any Service Tier

One or more of the following Service elements may be purchased as optional Service elements in addition to the purchase of any tier of Service:

Smart Bonding for CMS

Cisco will provide CMSP integration points to allow Customer's ITSM system to communicate with the CMSP to facilitate the exchange of tickets, status updates, workflow processes, and with other related information.

Cisco Responsibilities

- Provide ITSM integration interface between the CMSP and Customer's ITSM to facilitate the exchange of Change Management, Incident Management, and Service Request Management workflow Incident ticketing and status updates
- Provide Customer an API specification to enable integration of Customer's ITSM with the CMSP
- Notify Customer of any material changes to Cisco's API interface

Customer Responsibilities

- Customize and configure Customer's ITSM system to interoperate with CMSP API interface
- Provide a SPOC for Smart Bonding operations
- Follow requirements contained in documentation to enable the integration
- Notify Cisco when any material changes are made to Customer's ticketing systems
- Contact Cisco if Customer believes Smart Bonding ticketing data or information is incorrect

TACACS

Cisco will utilize a family of related protocols that support remote authentication and authorization services for networked access control through a centralized server deployed and managed by customer in its own data center.

Cisco Responsibilities

- Use centralized authentication to authenticate and control access to Managed Components
- Establish and maintain the list of authorized Cisco users
- Develop process for management of remote authentication
- Maintain Customer authentication credentials
- Notify Customer when user credentials have been revoked
- Publish logs and reports associated with activities of authorized users

Customer Responsibilities

- Assign a project manager to assist Cisco with understanding Customer requirements for Network access
- Notify Cisco when user credentials should be revoked

Geo-Redundancy

Where Data Collection Tools are located at a Customer site, Cisco will implement and maintain the Data Collection Tools in two separate Customer data centers to enhance Cisco's ability to recover

or continue to provide the Services in the event of a disaster impacting the Data Collection Tools.

Cisco Responsibilities
- Deploy the Data Collection Tools in an alternate and regionally diverse data center as identified in the Runbook
- Provide Transition Planning and Support services for the Data Collection Tools in the alternate location, if necessary
- When needed (e.g. there is an outage affecting the first instance of the Data Collection Tools), update network configurations to route network traffic to the appropriate Data Collection Tools

Customer Responsibilities
- Provide Cisco with access to an alternate and regionally diverse data center meeting Cisco's requirements
- Perform obligations contained in Transition Planning and Support of this Service Description with respect to the Data Collection Tools

Enhanced Authentication
Cisco will utilize multi-factor authentication methods and processes for Cisco's access to the Managed Components.

Cisco Responsibilities
- Notify Customer when user credentials need to be revoked
- Upon request, provide logs and reports associated with authorized users for review
- Utilize Customer's multi-factor on-demand system with an email notification option
- Provide Customer with a list of Cisco users, along with such users' Cisco email addresses

Customer Responsibilities
- Assign a project manager to assist Cisco with the authentication required for network access
- Assist in authentication issues
- Publish logs and reports associated with Cisco authorized users for review

Service Request Management
Cisco will implement Service Requests as described in the Service Catalog and in accordance with Service Requests for Managed Components.

Customer's applicable Ordering Document(s) will list the aggregate number of Service Request Units (SRUs) included in the Service purchased. If Customer uses all of its available SRUs, then Customer may purchase additional SRUs, subject to additional charges.

Cisco Responsibilities
- Provide the Portal for Customer to make, and for Cisco to categorize, approve, prioritize, and manage, Service Requests
- Manage the Service Requests through validation, completion, and closure
- Fulfill the Service Requests
- Execute approved Service Requests
- Manage Service Request record disposition post implementation
- Manage Service Requests in Cisco's ITSM system, as appropriate
- Evaluate Service Requests that are not defined in the Service Catalog to the applicable Addendum and any Services Requests requiring additional charges
- Handle Urgent Service Requests as a priority during Standard Business Hours on an as-available basis and per the Service Catalog

Customer Responsibilities

- Create Service Requests
- Provide acknowledgement, if requested, when each Service Request is completed
- Provide a list of authorized users permitted to submit Service Requests
- Provide details with respect to authorized user attributes
- Provide the means for Cisco to access and make changes to Managed Components within Customer's environment to fulfill the Service Requests (if different than the access provided by Customer for Cisco's provision of the Services)
- Perform any physical or onsite changes to Managed Components reasonably required by Cisco to help fulfill Service Requests
- Provide reasonably requested additional details pertaining to Service Requests

Service Fulfillment Portal

Cisco will implement a web-based cloud services brokerage platform. The Service Fulfillment Portal, for site onboarding, provides three optional functions: a Service Fulfillment Portal business catalog, custom workflows, and orchestration.

Cisco Responsibilities

- Provide Customer with access to the Service Fulfillment Portal
- Customize orchestration workflows according to Customer requirements
- Customize Customer's Business Catalog according to mutually agreed Customer requirements
- Manage the Service Orders according to custom workflows through to final fulfillment of such Service Orders
- Provide notifications in accordance with the applicable orchestration workflow
- Enable Service Reporting for Customer Service Fulfillment cycle and Service Inventory

Customer Responsibilities

- Provide a list of users authorized to access the Service Fulfillment Portal with their respective roles
- Provide service details for entries in the Service Catalog design
- Provide details for customization of Service orchestration workflows
- Use Service Fulfillment Portal to initiate Service Orders
- Provide future roadmap and assist in the implementation of Service Fulfillment Portal Business Catalog changes
- Provide single point of contact (SPOC) with respect to the management and oversight of Customer's responsibilities with respect to the Service Fulfillment Portal
- Follow Change Management Process for Change Requests with respect to Service Fulfillment Portal Business Catalog, Service Orchestration workflow

Local Language Support

Cisco will provide spoken language support in Spanish or Portuguese during Standard Business Hours. The applicable Ordering Document(s) will provide the selected language(s) and the locations at which such language will be available. All ticket information will be in English.

Cisco Responsibilities

- Provide local language support via a Cisco team and/or language translation services

Customer Responsibilities

- Contact Cisco during Standard Business Hours per location in order for local language support

Management of Third Party Managed Components
Cisco will manage Third Party Managed Components as described in this Service Description and any applicable Ordering Document(s). Cisco will oversee the interactions with, and management of, third-party suppliers who provide certain third-party products and/or services to Customer that are included as Third Party Managed Components in the applicable Ordering Document(s).

Cisco Responsibilities
- Support Third Party Managed Components identified in the applicable Ordering Document(s) as Managed Components except as otherwise expressly provided in this Service Description and any Ordering Documents
- Manage Third Party Managed Components through their lifecycle and provide support services to Customer as described in the applicable Ordering Document(s)
- Advise Customer of Third Party Managed Component dependencies

Customer Responsibilities
- Identify Third Party Managed Components and the associated third-party suppliers
- Obtain Letter of Agency (LOA) (See General Responsibilities)
- Manage all security incidents, notifications, and/or alerts and notify Cisco of any such security incidents, notifications, and/or alerts with respect to Third Party Managed Components

Optional Service Elements Available for Standard and Comprehensive Tiers
If Customer has purchased the Standard tier of Services, Customer may also purchase one or more of the following Service elements as described under the section entitled “Service Elements included with Comprehensive Tier” above:

- Proactive Problem Management
- Operations Service Review – Monthly

General Responsibilities, Exclusions, and General Terms

Cisco's provision of the Services is dependent on Customer's compliance with its responsibilities as listed in this Service Description. If Customer fails to comply with its responsibilities or if the Exclusions specified below should no longer apply under this Service Description, the parties will promptly work in good faith to adjust the scope, pricing, and other elements in writing via Cisco's Change Request processes or the execution of additional Ordering Documents.

General Cisco Responsibilities

Unless expressly provided in writing as a Customer responsibility, in addition to the Cisco responsibilities listed above, Cisco will also be responsible for the following:

- Cisco will participate in any reasonable Customer training required relating to Cisco's performance of the Services for Customer (up to a maximum of 8 hours per year).
- Cisco will materially comply with Customer's reasonable security policies, as applicable, provided that such policies do not: conflict with Cisco's policies, amend or conflict with the Agreement or this Service Description, or cause Cisco to incur materially increased risks or costs to comply with such policies.
- Cisco will maintain a reasonable information security and data privacy program with appropriate technical, administrative, and physical safeguards designed to prevent any (i) unauthorized access, use, distribution, or deletion of Customer's data and (ii) compromise of the Managed Components. More information on Cisco's security and privacy policy can be found here: http://www.cisco.com/c/en/us/about/trust-transparency-center/data-protection.html.

General Customer Responsibilities

Unless expressly provided in writing as a Cisco responsibility, in addition to the Customer responsibilities listed above, Customer will also be responsible for the following:

- When the Managed Components are located on a Customer site, Customer will provide Cisco and/or its subcontractors timely physical and remote access to the Managed Components and Customer's other infrastructure (including obtaining any internal approvals), as reasonably required for Cisco to perform the Services.
- Customer will provide functional host names, IP addresses, SNMP strings, passwords (or means to modify passwords and SNMP strings), and similar information for all Managed Components, Monitored Components, Third Party Managed Components, and Customer applications.
- Data Collection Tools may be used to aid the performance of the Services. Cisco will provide Customer the technical and environmental requirements (e.g. power, rack spaces, HVAC, etc.) for the Data Collection Tools as a part of the Services, which Customer must provide.
- To the extent Cisco personnel (including any Cisco subcontractors) are required to perform any Services at a Customer site, Customer will provide any specialized training of Cisco personnel required for onsite access.
- Customer will resolve any configuration issues and stabilize each site before handing over operations to Cisco.
- All pluggable optics will be installed by Customer prior to the start of applicable Services.
- Unless, provided for in a separate SOW or Service Description, Customer will be responsible for receipt of all inventory and delivery of all equipment and Managed Components at all Customer locations.
- All onsite work will be performed during Standard Business Hours, unless expressly agreed otherwise by Cisco in writing.

- Customer will promptly supply Cisco with reasonably requested and necessary technical data (e.g., network diagrams) and other information to allow Cisco to provide the Services in a timely manner.
- Customer will provide and maintain the locations 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, Third Party Managed Components, Monitored Components, and Customer's other infrastructure, managed infrastructure, and applications in Customer locations as they relate to the Services.
- Customer agrees to perform, and cooperate with Cisco in the performance of, all tasks approved via Customer's CAB process.
- Customer is responsible for backing-up and protecting its own data against loss, damage, theft or destruction.
- Customer will maintain a reasonable information security and data privacy program with appropriate technical, administrative, and physical safeguards designed to prevent any: (i) unauthorized access, use, distribution, or deletion of Customer's data and (ii) compromise of the Managed Components, Third Party Managed Components, and Monitored Components.
- Customer will provide reasonable physical, administrative and technical security to prevent the loss, theft, damage or destruction of any Data Collection Tools and other Cisco software or hardware provided by Cisco for Customer's use in conjunction with the Services.
- Customer is responsible for maintaining reasonable technical, administrative, and procedural data security and data privacy safeguards to protect its data that may be processed using the Services.
- Customer will be responsible for selecting Managed Components appropriate for its anticipated use.
- Customer will be responsible for managing 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/or services.
- Customer must maintain Cisco SMARTnet support on all Managed Components.
- Customer will provide a change window for Cisco to implement changes to the Managed Components.
- Customer will represent Cisco in, or permit Cisco to be directly involved in, any CAB processes related to third party products and services, as necessary.
- Customer will be responsible for reviewing, analyzing, and (if needed) discussing with Cisco the information contained in the reports provided. Customer will notify Cisco within a reasonable timeframe if Customer believes there is an inaccuracy in any report.
- Customer will notify Cisco in advance of any updates or changes planned in Customer's environment. Failure to notify Cisco of such updates or changes may result in Customer being charged for additional Service Request Units.
- Third-party products covered as part of the Services and managed by Cisco are supported on an up/down basis only, unless otherwise specified in writing by Cisco.
- Where applicable (e.g., for Customer-held licenses for Third Party Managed Components or other third party software, products, or services), Customer must provide a Letter of Agency (LOA) between any applicable third party vendor and Cisco authorizing Cisco and its contractors to act as Customer's agent with respect to the management of any applicable Third Party Managed Components or other software, products, or services. Additionally, Customer must maintain a valid service agreement with such third-party vendor.
- Internet Link speed for the VPN connection with Cisco: The minimum speed is 5Mbps for both download and upload (symmetric circuit). Delay of the internet connection to be within acceptable limits

- The Portal is accessible only via the VPN tunnel to Cisco and is not accessible via the public internet.

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:

- 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 applicable Ordering Document(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 specified otherwise in the applicable Ordering Document(s)
- 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, Addendum(s) to this Service Description, or the applicable Ordering Document(s)
- Migration services unless specified otherwise in the applicable Ordering Document(s)
- Providing Services with respect to equipment not managed by Cisco and identified by the parties as Managed Components
- Change Management or implementation of changes with respect to equipment not managed by Cisco
- Unless otherwise expressly provided for in the applicable Ordering Document(s), all Services will be provided in English.
- Unless otherwise agreed in writing, SmartBonding is limited to a single bond from Cisco's CMSP and Customer's ITSM.

Additional Terms

1. **Direct Sale from Cisco**. If you have purchased these Services directly from Cisco, this Service Description is incorporated into your Master Services Agreement, Advanced Services Agreement or equivalent services agreement executed between you and Cisco ("Direct Agreement"), including Cisco's End User License Agreement as it related to Cisco's Data Collection Tools.

2. **Sale via Cisco Authorized Reseller**. If you have purchased these Services through a Cisco Authorized Reseller, then this Service Description is incorporated into the agreement between the Cisco Authorized Reseller and Customer governing the Authorized Reseller's provision of the Services to Customer ("Reseller Agreement").

3. **No Direct or Reseller Agreement.** If you have purchased these Services either directly from Cisco or indirectly through a Cisco Authorized Reseller and are not a party to a Direct Agreement or Reseller Agreement, respectively, then Cisco's sale of, and your purchase and use of the Services, shall be governed by the terms and conditions of Cisco's standard Advanced Services Agreement, which is located at: http://www.cisco.com/c/dam/en_us/about/doing_business/legal/docs/Advanced_Services_Click-to-Accept_Agreement_sample.pdf ("Advanced Services Agreement").

4. **No Termination for Convenience.** In the event that your Agreement contains any right to terminate such Agreement or any order or SOW with respect Cisco services purchased by you thereunder for convenience, any such right to terminate for convenience shall be null and void with respect to the Services described in this Service Description.

5. **Compliance with Laws.** Cisco will comply with applicable laws, rules and regulations, including, but not limited to, all applicable export control laws and regulations. Customer will comply with all applicable laws, rules, and regulations related to the receipt and use of the Services and will obtain all approvals and licenses required by any third parties related to the Managed Components, Customer's locations, systems, software, and network as are reasonably necessary for Cisco to provide the Services.

6. **Cisco Recommendations.** To the extent that Customer fails to implement any Cisco recommendations or requirements with respect to the Managed Components or the Services or to the extent that Customer makes changes to the Managed Components in violation of this Service Description, Cisco shall have no liability for any failure(s) with respect to the performance of the Services.

7. **Data Collection Tools.** Customer receives a limited, non-transferable, internal use, license to use the Data Collection Tools only to the extent and duration reasonably required to receive the Services. Upon cessation or termination of the Services, the license to the Data Collection Tools will automatically terminate and to the extent applicable, Customer will return all Cisco-owned hardware and software licensed for the receipt of the Services (e.g., Data Collection Tools). Except to the extent caused by Cisco, Customer will be responsible for any loss, theft or damage to the Data Collection Tools until they are returned. The following document is incorporated into this Service Description: http://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/data-collection-tools-supplement.pdf.

8. **Data Retention.** Upon cessation or termination of the Services, and within 30 calendar days of receipt of all Cisco-owned hardware and software licensed for the receipt of the Services Cisco will destroy any Customer Data, Telemetry Data or Cisco Operations Data from the Data Collection Tools.

9. **Third Party Contracts.** Customer will be responsible for enforcing any third-party supplier contract terms (and Service Level Agreements, as applicable) and will release Cisco from any affected performance obligations to the extent Customer fails to do so.

10. **Confidential Information.** The information provided in this document is confidential information of and proprietary to Cisco and is being furnished with the understanding that Customer will keep such information confidential. The information provided in this document may not be used for any purpose other than in connection with Customer's use of the relevant services provided by Cisco. To that end, this document, and the information contained in it, must not be disclosed to any person other than an employee or advisor of Customer who requires the information.

11. **Usage Data.** Cisco may collect data on User's usage of the Services ("**Usage Data**") in order to maintain, improve, market or promote the Services. Partner acknowledges and agrees that Cisco owns all Intellectual Property Rights in, and may freely use, the Usage Data. In any event, Cisco will comply at all times with Applicable Law related to Cisco's collection and use of all Usage Data and will use reasonable physical, technical, and procedural means to protect the Usage Data in accordance with the Cisco Online Privacy Statement, which is made available at http://www.cisco.com/c/en/us/about/legal/privacy-full.html or such other site(s) as Cisco may publically communicate from time to time.

12. **Subcontractors.** Cisco may use subcontractors to provide services to Customer on its behalf for the purposes of providing the Services. Cisco will remain responsible for its subcontractors' compliance with the obligations under this Service Description, any Addendum, and the applicable agreement between Cisco and Customer. References to Cisco in this Service Description and any Addendum shall include its subcontractors, as applicable.

13. **Services to Devices Not Covered.** Any Services provided by Cisco with respect to devices that are not Managed Components are provided on an "as-is" basis.

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 the breadth of its impact on Customer's 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 affects the availability of the Service. Cisco will work with Customer during the provision of Transition Planning and Support Services 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, locations or Managed Components)
- Large: Multiple locations are affected (between one-half and three-quarters of individuals, locations or Managed Components)
- Localized: A single location and/or multiple users are affected (between one-quarter and one-half of individuals, locations or Managed Components)
- Individualized: A single user is affected (less than one-quarter of individuals, locations or Managed Components)

Urgency Definitions
The Urgency of an Incident is classified according to its impact on the Services or ability for Customer to receive the Services and the financial impact to Customer's business. 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 Customer's business.
- Major – Primary function is severely degraded and supported by backup or redundant system. There is a probable significant financial impact to Customer's business.
- Minor – Non-critical function is stopped or severely degraded. There is a possible financial impact to Customer's business.
- Low/Notice – Non-critical business function is degraded. There is no impact. Customer perceives the issue as low.

Priority Definitions
Priority defines the level of effort that will be expended by Cisco and 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: Cisco and Customer will commit any necessary resources 24x7 to resolve the situation.
- P2: Cisco and Customer will commit full-time resources during Standard Business Hours to resolve the situation.
- P3: Cisco and Customer are willing to commit resources during Standard Business Hours to restore service to satisfactory levels.
- P4: Cisco and 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
	Major	P1	P2	P2	P3
	Minor	P2	P3	P3	P3
	Low/Notice	P4	P4	P4	P4

Cisco will adjust the case priority in accordance with updated Priority of Impact or Incident resolution.

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

Appendix B

Additional Commercial Terms

This Appendix B sets out Customer's pricing terms and payment obligations relating to the Services. This Appendix does not include any charges that may be agreed upon by the Parties pursuant to a separate Ordering Document, which, if applicable, will be invoiced separately and as agreed in such applicable Ordering Document. Additionally, to the extent that any terms in this Appendix B conflict with terms set forth in any Addendum to the Service Description, the terms in the Addendum will take precedence over any conflicting terms in this Appendix B.

1. **Pricing Summary**. The charges for the Services ("Charges") will be detailed in the applicable Ordering Document.

2. **Invoicing Start Date.** Unless the Customer has prepaid for the Services, Cisco will begin invoicing as Managed Components are Activated or on the original scheduled start date of the Services, whichever occurs first. Cisco may delay invoicing if it is the primary cause of the delay in Activation.

3. **Additional Devices Added as Managed Components**. If Customer wishes to add new Devices as Managed Components entitled to management via the Services, the parties will follow Cisco's standard change request process ("**Change Request**").

4. **Service Request Fees**. Cisco will invoice Customer for any Service Requests that are fulfilled by Cisco during the applicable billing month. To the extent that Customer makes any change to the number of Managed Components from the number of Managed Components quoted/priced in the applicable Ordering Document, the monthly Charges for the Services will be adjusted accordingly. For the avoidance of doubt, Service Request Units may not be used to offset the additional monthly Charges associated with such an increase in the total number of Managed Components. To the extent that Customer submits a Service Request not designated as a Service Request type that is either included in the quoted/priced Services or designed with a number of SRUs in the Service Request Catalog (a "Custom Service Request"), Cisco will issue a quote to Customer specifying the pricing and/or the Service Request Units to be charged to implement the Custom Service Request.

5. **Minimum Commitments and Minimum Term**. The Ordering Documents will contain any minimum term or minimum fees commitment associated with the Services.

6. **Monthly Management Information (MI) Report and Invoicing Process**.

   (a) On or before the 7th calendar day of every Month, Customer will receive notification from the Cisco requesting review and approval of a report outlining usage of the Services (e.g., number of Managed Components Cisco manages, Service Requests fulfilled, etc.) for the previous Month (the "MI Report").
   (b) In addition to the information above, the MI Report will also set out all of the charges for the Services that are payable by Customer for the previous month.
   (c) Within seven (7) calendar days of notification being given for Customer to review the MI Report (the "Review Period"), Customer will notify Cisco in writing that, either:
      (i) Customer approves the MI Report; or
      (ii) Customer believes that the MI Report contains errors, in which case Customer shall provide Cisco with reasonable details of where it believes such errors arise.

(d) If notified by Customer of errors in the MI Report, Cisco promptly will correct any mathematical or other errors in the MI Report and re-issue the MI Report to Customer.

(e) If Customer fails to notify Cisco before the end of the Review Period, the MI Report will be deemed approved by Customer.

(f) Within seven (7) days from:

(i) the approval of the MI Report in accordance with Section 5(c)(i) or Section 5(e) above; or

(ii) if notification under Section 5(c)(ii) has been given, Cisco making a corrected MI Report available or providing Customer written notification (together with reasonable supporting details) that the original MI Report did not contain errors,

Cisco will issue the relevant monthly invoice through the Cisco billing tool.

(g) Cisco's rights to invoice for the charges for the Services and Customer's obligation to pay will not be affected by (i) any delays caused by Customer (or anyone acting on Customer's behalf), (ii) Customer's failure to perform or delay in performing its obligations under the Addendum or (iii) any finance system integration or finance process issues.

7. Purchase Orders.

(a) Customer need not provide Cisco a Purchase Order for the purchase of the Services. This Service Description and the Ordering Documents shall serve in lieu of a Purchase Order and/or will act as a valid Purchase Order from Customer.

(b) However, if Customer is required to issue a Purchase Order, Customer will inform Cisco of this within 10 days of the Effective Date and shall either provide Cisco a blanket Purchase Order covering the anticipated charges for the entire term specified in the Ordering Document or separate Purchase Orders covering the anticipated charges of each year of the term specified in the Ordering Document.

(c) The terms contained in any purchase orders shall be for administrative purposes only and shall have no contractual effect.

(d) Customer will be obliged to pay all invoices submitted by Cisco in compliance with the terms of this Addendum regardless of whether Customer has issued a corresponding Purchase Order.