Cisco Managed Service for Enterprise Service Level Objectives

This document describes the Service Level Objectives for the following Cisco Managed Service for Enterprise:

- Collaboration
- Data Center
- Enterprise Networks
- Security

This Service Level Objective Description defines the service level metrics that Cisco tracks for each Service. The document contains two major sections: Network Operation Center SLOs and Security Operations Center SLOs.

Related Documents: This document should be read in conjunction with the following documents also posted at www.cisco.com/go/servicedescriptions/: (1) Cisco Managed Service for Enterprise Common Service Description ("Common Service Description"); (2) Glossary of Terms; (3) List of Services Not Covered.

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/.

Network Operations Center Service Level Objectives

1.0 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 objectives, 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.

1.1 Incident Prioritization

Cisco classifies and prioritizes incidents according to impact and urgency.

Activities:

- Evaluate Incident severity and prioritize all Incidents into Priority 1 (P1), Priority 2 (P2), Priority 3 (P3) and Priority 4 (P4) Incident categories
- Classify Incidents into Fault or Performance Incident categories as appropriate

Deliverable(s):

- Properly prioritized Incidents based on Incident Ticketing attributes
- Properly classified Incident based on the Incident Ticketing attributes

1.1.1 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, room and/or multiple users are affected (between one-quarter and one-half of individuals, sites or devices)
- **Individualized:** A single user or meeting is affected (less than one-quarter of individuals, sites or devices)

1.1.2 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.

1.2 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:

1. **P1: Critical** – Cisco and the Customer will commit any necessary resources 24x7 to resolve the situation.
2. **P2: High** – Cisco and the Customer will commit full-time resources during Standard Business Hours to resolve the situation.
3. **P3: Medium** – Cisco and the Customer are willing to commit resources during Standard Business Hours to restore service to satisfactory levels.

4. **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 ticket 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.

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

2.0 Service Level Objectives

Service Level Objectives apply only to Managed Components that are managed exclusively by Cisco within the Service. Cisco adheres to the SLOs during the Service Delivery phase.[1] Within the Service Activation Kit, the Customer and Cisco must document their agreement to formally acknowledge the completion of the Transition Management process. The Service Delivery phase commences upon mutual agreement between Cisco and the Customer that the Transition Management phase is complete and that the Service Delivery phase has been reached.

The following Incident metrics are tracked as Service Level Objectives:

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

2.1 Time to Change

Cisco has categorized Defined Changes into Types based on level of complexity and the amount of time required to complete the change. All Elective Changes are scheduled events and are dependent on coordination with Customer schedule. A change request must be fully qualified and scheduled with the customer before the Time to Change metric starts. All custom scope Elective Change requests are scheduled events and follow Change Management procedures.

Additional details are available in the individual technology addendums and outline the specific change types. The chart below provides a break-down of the available categories and durations for Small, Medium, and Large changes.

[1] Cisco cannot adhere to the SLOs during the Transition Management phase. Within the Service Activation Kit, the Customer and Cisco must document the exit criteria for the Transition Management phase.

Category	Size
Type 1	*Small*
Type 2	*Small*
Type 3	*Med*
Type 4	*Med*
Type 5	*Med*
Type 6	*Large*
Type7	*Large*
Type 8	*Large*

Cisco Service Level Objectives (SLO) for completing approved Change request is as follows:

Change Type*	Time to completion from receipt of fully qualified and scheduled change request
Types 1 and 2 Up to 12 changes per customer per business day	3 Business Days
Types 3 and 4 Up to 6 changes per customer per business day	Within 5 business Days**
Type 5 - 8	No SLO, scheduled

*Note: See specific Technology Addendums for individual change type categories.
**Note: SLO time commences when all necessary detail to execute the change is available.

Business days are Monday through Friday, excluding Cisco-observed holidays.
SLO measurements exclude the following:

- Delays caused by Customer in executing the requested change (for example, waiting for response on change window)
- Any mutually agreed schedule of activities that causes service levels to fall outside of measured SLO defined obligations.
- Other factors outside of Cisco's reasonable control for which Cisco is not responsible
- Cisco or third party hardware dispatch and replacement
- SMARTnet cycle time is not included in the SLO measurement.
- Ticket closure time may be different than change completion time. For example: a ticket may be kept open for review after the change has been executed.

Any Customer-requested changes that are considered by the Customer as “emergency” or “urgent” changes will be treated on a commercially reasonable effort by the Cisco NOC/SOC and will depend on Cisco NOC/SOC engineer availability at the time of submittal. Additional charges may apply. See the Common Service Description for details.

2.2 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:

- “Electronic notifications may be generated automatically and sent to customer contacts as specified during the Transition Management phase.”

Cisco estimated time to notify designated Customer contact	Incident Level
15 Minutes from ticket creation	All Priority Incidents

2.3 Time to Restore (TTR)

Incidents go through many stages with restoration being a primary objective. Time to restore tickets includes all remote incident management activities (alarm or call receipt through restore, excluding maintenance or carrier cycle time). Time to Restore shall mean the time period 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 to restore an incident ticket	Incident Level
4 Hours	P1 incidents
12 Hours	P2 incidents
72 Hours	P3 incidents
120 Hours	P4 incidents

SLO measurements exclude the following:

- Delays caused by Customer in resolving the qualifying issue (for example, waiting for response on change window or on-site resources)
- Any mutually agreed schedule of activities that causes service levels to fall outside of measured SLO defined obligations.
- Delays or faults caused by third party equipment or vendors, such as Carriers in resolving the qualifying issue
- Other factors outside of Cisco’s reasonable control for which Cisco is not responsible
- Cisco or third party hardware dispatch and replacement

- Acquisition and installation time of new software to be installed on the Managed Component due to software defects or bugs
- SMARTnet cycle time is not included in the SLO measurement.

3.0 Security Operations Center Service Level Objectives

The nature of Security Operations differs from Network Operations sufficiently to demand separate Service Level Objectives. The Service Level Objectives for the following Cisco Managed Service for Security Service Levels are described in the document below:

- Monitoring
- Management

Service Level Objectives

The following Incident metrics are tracked as Service Level Objectives specifically for Security Managed Service and pertain to security events and not fault events.

A fault or performance event is specific to the availability and performance of the actual security device.

A security event is defined as anything detected which is considered malicious in nature or intended to cause degradation to the network resources and / or assets.

Service Level Management for Cisco Managed Service for Security

Once the event is determined to be anomalous in nature or a security threat, that event is then classified within the Mean Time to Classify (MTTC) objective.

Security Incident Classification Codes:

- **Benign:** Traffic that is not harmful to network integrity.
- **Attack:** An attempt to gain unauthorized access to protected data or deny access to networks.
- **Denial of service (DoS):** An attempt to saturate the network resources.
- **Malware:** Detection of software designed to infiltrate or cause damage to resources.
- **Misuse:** Internal misuse of network and data resources.
- **Recon:** Scanning a network for vulnerabilities.
- **Suspicious traffic:** Not enough data available to rule out an attack and classify it as benign.

The MTTC SLO objective is 30 minutes