



Service Level Objectives for Cisco Remote Management Services

This document describes the Service Level Objectives for the following Cisco Remote Management Services:

- Cisco Unified Communications Remote Management Services
- Cisco Unified Contact Center Remote Management Services
- Cisco Foundation Technologies Remote Management Services
- Cisco Application Delivery Remote Management Services
- Cisco Wireless Remote Management Services
- Cisco Unified Computing Remote Management Services
- Cisco Advanced Performance Monitoring Services
- Cisco Remote Monitoring Services for Security
- Cisco Remote Management Services for Security
- Cisco Server Networking and Virtualization Remote Management Services

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.

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 levels, initiating Change Management as needed for restoration
- Coordinate the dispatch of support personnel to the Customer Premises to perform necessary onsite repairs as per the end-Customer maintenance and support contracts. This requires a signed Letter of Agency by the Customer.
- Remotely assist onsite personnel as needed to facilitate service restoration.
- Remotely facilitate hardware replacement and software updates determined to be required by Cisco.

1.1 Incident Prioritization

Cisco classifies and prioritizes incidents according to impact and urgency.

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 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)

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:

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

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

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

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

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

2.0 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 Phase is complete and that the Service Delivery Phase has been reached.

The following Incident metrics are tracked as Service Level Objectives:

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

2.1 Time to Change

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

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.

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

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

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:

Cisco estimated time to notify Customer contact	Incident Level
15 Minutes	P1 and P2 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 for a priority 1 or 2 severity from occurrence of the Incident until Cisco restores the Managed Component to a usable level of functionality. Cisco SLO for meeting this objective is as follows:

Cisco estimated time to restore a ticket	Incident Level
4 Hours	P1 incidents
12 Hours	P2 incidents
24 Hours	P3 incidents
48 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)
- Delays caused by third parties, such as Telecarriers, in resolving the qualifying issue
- Scheduled wait time
- SMARTnet cycle time is not included in the SLO measurement.
- Customized calling trees

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 Remote Operations Security Services are described in the document below:

- Cisco Remote Monitoring Services for Security
- Cisco Remote Management Services for Security

1 Incident Management

Incident Management is the process used by the Cisco Remote Management Services for Security (RMS) Security Operations Center (SOC) to identify incidents and restore service or remediate declared incidents as quickly as possible. The Cisco SOC will proactively monitor key events and thresholds on managed devices to support the Customer's Security infrastructure. Additionally, the Customer may declare an incident by contacting the Cisco RMS Service Desk, communicating via telephone or the Cisco RMS Web Portal.

Upon automatic or manual submission of an incident (Incident) to the Cisco RMS Service Desk, an Incident Ticket is created. The Cisco RMS Service Desk will coordinate with the Cisco SOC during the lifespan of the declared Incident. The Cisco RMS Service Desk is responsible for coordinating the management of the Incident, which includes communicating with the Customer throughout the Incident management process. This communication also includes notification to the Customer that the Incident has been resolved or remediated.

1.1 Incident Priority and Classification

Incidents will be managed according to the Severity level as determined by Cisco according to its IT Infrastructure Library (ITIL) service support framework. Incident Severity level depends on a variety of factors including pre-defined Incident Ticketing attributes such as business impact and business urgency. Incident Severity level will determine the Incident Priority level set by the Cisco RMS Service Desk on a per-incident basis.

Activities:

- Evaluate Incident Severity and prioritize all Incidents into Priority 1 (P1), Priority 2 (P2) and Priority 3 (P3) 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

Priority Definitions

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

Cisco Incident Management priorities are defined as follows:

- P1: Critical - The Managed Component is unavailable and severely disrupting / impacting the Customer's business. Cisco and the Customer will commit any necessary resources 24x7 to resolve the situation.
- P2: High – The Managed Component is unavailable or its functionality is severely degraded and Customer's business is moderately disrupted.
Cisco and the Customer will commit full-time resources during Standard Business Hours Monday through Friday to resolve / remediate the Incident to resolve the situation.

- P3: Medium – The Managed Component is unavailable or its functionality is moderately degraded and Customer's business is minimally disrupted.

Cisco and the Customer are willing to commit resources as available during Standard Business Hours to resolve/remediate the Incident and restore service to satisfactory levels.

2.0 Service Level Objectives

Service Level Objectives (SLOs) apply only to Managed Components that are managed exclusively by Cisco within the Service. Cisco adheres to the SLOs during the Service Delivery phase.² 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 Phase is complete and that the Service Delivery Phase has been reached.

The following Incident metrics are tracked as Service Level Objectives:

Service Level Management for Cisco Remote Management Services for Security

SLO Name	SLO Detail	SLO Targets
Mean Time To Notify (MTTN)	Notify Customer of all Service Impacting Incidents within X minutes	15 Minutes
Mean Time To Investigate (MTTInv)	Investigate Incidents within X minutes	30 Minutes
Mean Time To Isolate (MTTIso)	Isolate root cause of all Incidents within X minutes	90 Minutes
Mean Time To Resolve (MTTR)	Resolve all Incidents within X hours	Priority 1 (P1) within 4 Hours Priority 2 (P2) within 24 Hours Priority 3 (P3) within 72 Hours
Mean Time To Complete (MTTC) ³	Complete Customer-initiated Service Requests within X hours	Logical Priority 2 (P2) within 24 Hours Logical Priority 3 (P3) within 72 Hours Physical moves handled on case-by-case with Customer

² 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.

³ All Customer-requested RFCs associated to the service are, by default, classified as either Priority 2 with a MTTC target of 24 hours or Priority 3 with a MTTC target of 72 hours.

Any Customer-requested RFC's that are considered by the Customer as "emergency" or "urgent" RFCs will be treated on a commercially reasonable effort basis by the Cisco SOC and will depend on Cisco SOC engineer availability at the time of submittal. The MTTC SLO target aims to complete the emergency RFC within 4 hours like a Priority 1 classified incident. P1 incidents related to hardware replacement will be exempted from the normal 4 Hour P1 SLO. These incidents will still be P1 incidents, and replacement within 24 hours (or 1 business day) is the norm with shipments delivered to Customer's site the next business day by 10:30 am local time (second business day if shipped on Sunday or US holiday). This may vary for international shipments.

2.1 Time to Change

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

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

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.

2.3 Time to Resolve (TTR)

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

SLO measurements exclude the following:

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