Service Description: Cisco IronPort Managed Email Security

This document describes the Cisco IronPort Managed Email Security.

Related Documents: The following documents posted at www.cisco.com/go/servicedescriptions/ should be read in conjunction with this Service Description and are incorporated into this Service Description by this reference: (1) Cisco RMS Supported-Device List, (2) Cisco RMS Glossary of Terms, (3) List of Services Not Covered, and (4) Severity and Escalation Guidelines

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. In the event of a conflict between the MSA and this Service description this Service description shall prevail.

Sales via 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 this document to you, or you can obtain a copy of this and other Cisco service descriptions at www.cisco.com/go/servicedescriptions/.

Cisco IronPort Managed Email Security:

The objective of the Cisco IronPort Managed Email Security is to manage and monitor the identified security components of the customer's (Customer) IronPort Messaging infrastructure, targeting malicious spam and e-mail virus activity that may threaten a Customer's business and providing the Customer with a 24x7 incident handling, analysis and response capability on their Messaging Security infrastructure.

Incident Management for Cisco IronPort Managed Email Security:

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. Restoration of service may involve implementing temporary work-arounds. The Cisco SOC will proactively monitor for key events and thresholds on IronPort email appliances in the Customer's Messaging Security infrastructure. In the case of undetected events, Customers may declare an incident by contacting the Cisco RMS Service Desk, communicating via telephone or the Cisco RMS Web Portal, any priority incidents involving issues such as missing emails, the inability to send or receive e-mail, receiving spam or degraded performance in receiving emails.

Upon automatic detection 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 ultimately 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.

Example of an incident and the associated resolution by the Cisco SOC Support Team:

Incident: Customer's email administrator calls into the Cisco RMS Service Desk to report that several users are receiving spam and then asks if this can be corrected.

Resolution: Cisco RMS Service Desk records the details of the issue and opens an Incident Ticket for the Cisco SOC. The Cisco SOC engineer may recommend that

the Customer's email administrator sends instructions to their user community to submit perceived spam messages directly to IronPort's Senderbase through a "missed spam" submission plug-in in their email application or through email forward. The Cisco SOC engineer may also access the IronPort email appliance and analyze the configuration to determine if any spam settings need to be adjusted. If so, the Cisco SOC engineer will recommend a configuration change to the IronPort email appliance.

Incident Detection:

Cisco's IronPort Managed Email Security Security monitoring system indicates a fault condition was declared or a performance threshold was exceeded which has triggered an incident

Activities:

- Monitor (24x7x365) manageable elements of the Customer's IronPort Messaging infrastructure

- Perform ongoing Hardware, Operating System and Security Service incident monitoring (re: alerting) on the IronPort email appliances of the Customer's IronPort Messaging infrastructure

  - Hardware incidents: Failure, capacity errors, pairing failures, RAM utilization
  - Operation System incidents: Quarantine capacity, Quarantine messaging, application failures, key expiration, DNS connectivity, LDAP connectivity, work queue messaging, engine failures
  - Security Service incidents: Anti-Virus engine failure, Anti-Virus update failure, Anti-Virus engine time outs, malformed messages, quarantine capacity, Anti-Spam engine failure, Anti-Spam update failure

- Detect incidents

- Correlate incidents where applicable

Deliverable(s):

- Confirmed incidents logged in the Cisco RMS Configuration Management Database (CMDB)

Incident Recording:

Cisco's IronPort Managed Email Security Security ticketing system captures alarm / event / correlation data, enriches with relevant Configuration Item (CI) information and creates incident ticket

Activities:

- Enrich alarm information with relevant CI information from the Cisco RMS CMDB

Deliverable(s):

- Create incident Ticket

- Post incident Ticket online via the Cisco Portal for the Customer to view all ticket handling details and milestones

Incident Communication (E-notification)

Cisco's IronPort Managed Email Security notification system will electronically notify (e-notify) designated Customer contacts for new Incidents or milestones achieved during the Incident Management process. E-notifications are sent to any email address or email-capable mobile device and will include the Incident

Ticket number. The Customer can always view Incident status and detailed information via the Cisco web portal.

Automated electronic notification (e-notification) to specific Customer contact(s) based on Customer's notification requirements as agreed on during the Service Activation process.

Activities:

- Match customer's notification profile with Incident Ticket milestones

Deliverable(s):

- Perform e-notification of Incident Tickets per Customer's notification profile within the Mean Time To Notify (MTTN) Service Level Objective (SLO) goal of 15 minutes.

- Log e-notification records in the Incident Ticket

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

Incident Investigation and Diagnosis

Cisco SOC engineers utilize Incident Remediation procedures to collect any additional data required to fully diagnose and match the Incident to a known error in the Cisco RMS Knowledge Base (KB). Cisco SOC engineers will work to quickly isolate the root cause of the Incident. Once root cause isolation has occurred, Cisco SOC engineers will update the Incident Ticket with information related to root cause isolation and then proceed to the Incident resolution and restoration phase.

Activities:

- Initial investigation of Incident by a Tier-2 Cisco SOC engineer

- Collect additional data to properly diagnose root cause of the Incident

- Attempt to match Incident to a known error in the Cisco RMS Knowledge Base (KB)

Deliverable(s):

- Begin investigation activities within Mean Time To Investigate (MTTInv) SLO of 30 minutes

- Isolate the Root Cause of the Incident within Mean Time To Isolate (MTTIso) SLO of 90 minutes

- Update Incident Ticket with root cause isolation information for Incidents

- Perform e-notification for this Incident Ticket event milestone (if requested by the Customer)

Incident Resolution and Restoration

Cisco SOC engineers utilize Incident Remediation procedures and work to restore services within agreed service levels, initiating any Requests for Change (RFCs) as needed for restoration.

After the Incident has been isolated down to its root cause, Cisco SOC engineers will work to resolve the Incident. Resolution is complete when functionality is restored to the affected IronPort email appliance(s) The resolution process includes any action the Cisco SOC requires to restore functionality to a IronPort email appliance on the Customer's Messaging Security infrastructure.

The Cisco SOC will utilize work-around solutions to restore all or partial functionality when full functionality cannot be restored within committed timeframes as defined in the Service Level Management section of this document. When a work-around is utilized, the Incident will continue to remain open and will be worked by Cisco SOC engineers until resolved, in accordance with the priority level of the Incident.

Incident resolution and restoration may include Cisco SOC engineers working directly with the Customer's Messaging Security infrastructure team (including email or network administrators) to resolve Incidents on the IronPort email appliances on the customer's Messaging Security infrastructure. The Customer is ultimately responsible for any patching of infected hosts on their network if it is determined that is the root cause of the declared Incident.

Should the Cisco SOC require a configuration change in an IronPort email appliance to resolve an issue or implement a work-around, the Cisco SOC will follow the Change Management Process established with the Customer.

Activities:

- Resolve declared Incidents on IronPort email appliances

- Submit, when needed, a Cisco-recommended Request For Change (RFC) in accordance with the Change Management Process established with the Customer to resolve a Incident (including implementing a temporary work-around)

- Initiate the Reactive Problem Management process if no Known Error exists in the Cisco RMS Knowledge Base (KB)

- Update Incident Ticket to include notes detailing Incident resolution

- Perform e-notification for Incident Ticket milestones, if requested by the Customer

Deliverable(s):

- Updated Incident Ticket with resolution or recommendation details on the declared Incident

- If needed, initiate Cisco-recommended Request for Change (RFC) to resolve the Incident or implement a temporary work-around as determined by Cisco SOC engineers

- Resolve Incident within the Mean Time To Resolve (MTTR) Service Level Objective (SLO) according to priority level. See table in Service Level Management section of this document for details.

Incident Escalations

Escalations of Incident will be primarily driven by elapsed time against Service Level Objectives (SLOs) ensuring effective routing of Incidents to appropriate Cisco SOC technical resources as required. A Customer may request escalation of an Incident Ticket at any time via the Cisco Remote Management portal or Telephone call to the Cisco RMS Service Desk. The Cisco SOC will refer Incidents to the Customer as

needed and escalate the Incident with the Customer within the Customer's defined escalation guidelines until the Incident is resolved.

Activities:

- Handling of the Incident by appropriate level Cisco SOC technical resources

- Escalation of the Incident as appropriate in the Cisco SOC or with the Customer per the established escalation procedures

Deliverable(s):

- Updated Incident Ticket to include escalation notes

- Incidents resolved or remediated in accordance with all defined SLO targets for the Cisco IronPort Managed Email Security service offering (see Service Level Management section of this document for SLOs)

- Perform e-notification for Incident Ticket event milestone, if requested by the Customer

Example:

- Cisco IronPort Managed Email Security monitoring system automatically detects an incident with the IronPort email appliance. The Cisco RMS Service Desk initially handles the Incident and routes the Priority 1 (P1) Incident Ticket to the Cisco SOC for analysis. For this P1 Incident, a Cisco SOC engineer may determine at any time during the 4 hour MTTR SLO that the Incident needs to be escalated. The P1 Incident ticket is then escalated within the Cisco SOC to focus a higher level of attention and management oversight on the incident to ensure the 4 hour MTTR SLO is met.

Incident Closure

Once the Cisco SOC declares an Incident resolved and verified, the Incident will be closed. In the event that the Incident reoccurs, a new Incident Ticket will be created to accurately reflect the recurring nature of the Incident and aid in the identification of Problems. Depending on frequency, recurring Incidents may trigger the Reactive Problem Management process that may include a Cisco-recommended Request For Change (RFC) to resolve the recurring Incident.

Any authorized Customer agent may also proactively request Incident Ticket closure via the Portal or Telephone. The Cisco SOC will work in conjunction with the Cisco RMS Service Desk to close the Incident Ticket or follow up with the Customer for more information as needed.

Activities:

- Confirm Incident is resolved with the Customer

- If Incident reoccurs, depending on frequency and attributes of the Incident, initiate the Reactive Problem Management process which may include a Cisco-recommended RFC to resolve recurring Incident

Deliverable(s):

- Update Incident Ticket to include notes detailing the reason for closing the Incident

- Close the Incident Ticket

- Perform e-notification for Incident Ticket event milestone, if requested by the Customer.

Problem Management for Cisco IronPort Managed Email Security Service

The goal of Problem Management is to minimize the adverse impact of Incidents resulting from errors in the Customer's network by delivering a systematic approach for diagnosing the root causes of Incidents and preventing their reoccurrence by recommending the elimination of the underlying errors whenever possible. To achieve this goal, Cisco SOC engineers will endeavor to diagnose the root cause of Incidents and then propose actions to improve or correct the situation.

Reactive Problem Management

Reactive problem management describes the problem management processes that primarily support incident management. These processes are initiated when an incident cannot be matched to a known error. A problem is declared for the purpose of tracking the activities that lead to identifying a root cause and a resolution to the incident's underlying error. The process concludes when a known error, including its root cause and resolution, has been identified and recorded in the known error database. The known error will then be used to resolve and close all associated open and future incidents.

Activities:

- Utilize Problem Management procedures to collect additional data required to analyze the root cause

- Utilize error data, technical expertise, and product and development resources (if needed) to isolate a root cause for the error

- Document recommended remediation and resolution procedures in the Cisco Known Error Database and assist Incident Management team in the resolution of the underlying error(s) that caused the incident

- Error is closed and handed back to the Incident Management team for any further Incident Management activity

Deliverable(s):

- Aid Incident Management resources to meet MTTR SLO according to priority level. See table in Service Level Management section of this document for details.

- Keep the Cisco Known Error Database accurate and up-to-date

Example:

- A Customer's email administrator reports that their users are having trouble receiving certain types of attachments. After initial investigation of the incident and an unsuccessful search of the Known Error Database, a Cisco SOC Incident Management engineer opens a problem management ticket. A Cisco SOC Problem Management engineer investigates further and determines that the attachments are being removed by content filtering. The Cisco SOC Problem Management engineer then recommends to the Customer's email administrator that a Request for Change ticket be opened to update the content filter on the IronPort email appliance to allow the delivery of emails with specific attachments.

Proactive Problem Management

Proactive Problem Management minimizes the occurrence or limits the adverse impact of future incidents. The Cisco SOC engineers will analyze Incident trends to identify patterns and systemic conditions. In the event a trend is detected, the results will be introduced into the Problem Management process. The Cisco SOC engineers analyze different data sets based upon a variety of triggers that would indicate that an

IronPort email appliance should be further evaluated. Not all the aforementioned triggers are necessarily indicative of a problem requiring resolution.

Activities:

- Identify recurring Incidents and refer to Incident Management for resolution

- Analyze trends for Incidents on IronPort email appliances

- Monitor the resolution of Incidents on IronPort email appliances

- Document applicable error, remediation, recovery, and resolution information in the Cisco Knowledge Base

Deliverables:

- Reduce the number of errors in the Customer's messaging security infrastructure over time

Example:

- During the proactive Problem Management process a Cisco SOC Problem Management engineer notices that one of the spam quarantines on the IronPort email appliance is routinely near its capacity. The Cisco SOC engineer then recommends to the Customer's email administrator to either increase the size of the quarantine or reduce its retention period. If accepted by the Customer's email administrator, a Request for Change (RFC) ticket is opened for the required change to be executed.

Change Management for Cisco IronPort Managed Email Security Service

Change Management is the process used by the Cisco SOC to apply standardized methods and procedures for authorizing, documenting, and performing all changes. The objective of Change Management is to make necessary Cisco-recommended and Customer-requested changes in an efficient and accountable manner, utilizing standard processes. The following table details Cisco-recommended and Customer-requested changes that are applicable to the Managed Email Security service.

Cisco-recommended Changes		
Changes required To:	**Category**	**Change description**
Resolve an Incident or implement a work-around for an Incident	Change	Logical or Physical change to a IronPort email appliance software or hardware configuration
Respond to a critical vulnerability or threat directed at entitled IronPort email appliances	Change	Logical change to a IronPort email appliance configuration
Resolve a Known Error identified during the Problem Management process	Change	Logical or Physical change to a IronPort email appliance software configuration
Software update to a entitled IronPort email appliance	Change	Logical change to a IronPort email appliance software configuration
Physically Add or Delete of a entitled IronPort email appliance	Add or Delete	Physically add or delete a IronPort email appliance[1]
Customer-requested Changes		
Changes required To:	**Category**	**Change description**
Change logical functionality	Change	Logical change to a entitled IronPort email appliance

		software configuration
Physically move a IronPort email appliance	Move	Physically relocate an entitled IronPort email appliance from one location to another[2]

[1] *The customer may be asked to assist with physically connecting, disconnecting and/or relocating entitled IronPort email appliance(s).*
[2] *The customer will be responsible for physically connecting, disconnecting and/or relocating entitled IronPort email appliance(s) when they initiate this type of Service Request.*

Any customer request for change requiring more than 4 hours of engagement will be considered as an additional Cisco IronPort professional service engagement, which will incur additional charges negotiated with end customer on a case-by-case basis.

Change Origination

The first step in initiating the Change Management process is the origination of a Request for Change (RFC). For the Cisco IronPort Managed Email Security service, RFCs may originate from two categories: Cisco-recommended changes and Customer-requested changes. These changes are summarized in the table above.

Activities:

- A Request for Change (RFC) Ticket is initiated by Cisco or the Customer via the Portal

- The Request for Change (RFC) Ticket is categorized as described in the table above.

- The Customer tracks the progress of the RFC ticket throughout its lifecycle.

Deliverable(s):

- Creation of a Request for Change (RFC) Ticket on the Cisco Portal for the Customer to view

Cisco-Recommended Changes

Cisco-recommended changes originate from the Cisco SOC engineers. Before executing a Cisco-recommended change, the Cisco SOC change assignee will evaluate the change and make a recommendation to the Customer that will include details regarding the criticality and timeframe for implementation of the change. The Cisco SOC change assignee will not execute a change until the Customer has authorized or pre-authorized the change to be made.

Activities:

- Communicate to the Customer the criticality and timeframe associated to the change

- Obtain Customer approval for executing the change

- Follow established Change Management process including updating all activities in the Change Ticket

Deliverables:

- Release changes in the Customer's messaging security infrastructure within Mean Time to Complete (MTTC) Service Level Objectives

Cisco-recommended changes required to resolve an incident or implement a work-around

During the course of the Incident management process, the Cisco SOC engineers may need to make changes to IronPort email appliances in order to resolve Incidents. These changes are typically logical changes to the IronPort email appliance configurations for the purpose of troubleshooting and implementing temporary workarounds.

Changes required to resolve Incidents are implemented as needed by the Cisco SOC engineers in accordance with agreed upon Change Management processes established with the Customer.

Activities:

- Logical configuration changes to implement a temporary work-around or aid in troubleshooting an Incident during the Incident Management process

- Logical configuration changes to apply software updates during the Incident Management process or the normal service support activities associated to the Managed Email Security service and the entitled IronPort email appliance(s)

- Communicate to the Customer the criticality and timeframe associated to the change

- Obtain Customer approval for executing the change

- Follow established Change Management process including updating all activities in the Change Ticket

Example:

- A Customer's email administrator calls in to the Cisco RMS Service Desk to report an Incident involving missing email messages. A Cisco SOC engineer determines that the IronPort email appliance is blocking legitimate e-mail traffic on the Customer's network due to sender mail transfer agent (MTA) Senderbase Reputation Score. The Cisco SOC engineer recommends a configuration change to the IronPort email appliance to always e-mail from that MTA (or domain).

Cisco-recommended Changes to respond to a critical Vulnerability or Threat directed at the IronPort email appliance(s)

Cisco recognizes that certain critical vulnerabilities have the capability to degrade a Customer's email system and severely limit email services. As new vulnerabilities are released or threats become known, the Cisco SOC will evaluate the severity and potential impact to the IronPort email appliance(s). If the vulnerability or threat is judged by the Cisco SOC to be critical with respect to Customer safeguards, or the Customer's IronPort email appliances are impacted by the vulnerability, the Cisco SOC will recommend changes to correct the issue and/or mitigate the threat. If requested by the Customer, changes will be executed according to the priorities and terms contained in Customer-Requested Change section of this service description.

Changes to address critical vulnerabilities will be performed at the earliest possible time, in coordination with the Customer and the agreed upon Change Management processes established between Cisco and the Customer.

Activities:

- Logical configuration changes to respond to a critical vulnerability or threat identified by the Cisco SOC and directed at the IronPort email appliance(s)

- Communicate to the Customer the criticality and timeframe associated to the recommended change

- Obtain Customer approval for executing the change

- Follow established Change Management process including updating all activities in the Change Ticket

Example:

- A Cisco security advisory is released to the public detailing vulnerability on a particular model and version of the IronPort email appliance. The Cisco SOC initiates an RFC and coordinates with the Customer's email administrator to apply the AsyncOS hot patch to the IronPort email appliance(s) to mitigate the threat of a successful exploit.

Cisco-recommended Changes to address Known Errors identified during the Problem Management process

During the course of the Problem Management process, the Cisco SOC engineers may recommend changes to the IronPort email appliance in order to resolve an underlying error whose root cause was identified and logged in to the Cisco Known Error Database.

Changes required to resolve known errors are implemented as needed by the Cisco SOC engineers in accordance with agreed upon Change Management processes established between Cisco and the Customer.

Activities:

- Logical configuration changes to the IronPort email appliance(s) to resolve a known error identified during the Problem Management process

- Communicate with the Customer the criticality and timeframe associated to the change

- Obtain Customer approval for executing the change

- Follow established Change Management process including updating all activities in the Change Ticket

Example:

- During the proactive Problem Management process a Cisco SOC engineer notices that one of the spam quarantines is routinely near its capacity. The Cisco SOC engineer then recommends to the Customer to either increase the size of the quarantine or reduce its retention period. The Cisco SOC engineer then initiates an RFC to make the necessary changes to the Customer's IronPort email appliance to alleviate the quarantine capacity issue.

Cisco-recommended software update to IronPort email appliances

Cisco SOC engineers may recommend software updates to improve or enhance the features and functionalities of the IronPort email appliances as a normal course of delivering the Cisco IronPort Managed Email Security service. Software updates may include AsyncOS upgrades as well as hot patches and bug fixes.

Activities:

- Logical software upgrades to the IronPort email appliance(s)

- Communicate with the Customer the criticality and timeframe associated to the change

- Obtain Customer approval for executing the change

- Follow established Change Management process including updating all activities in the Change Ticket

Example:

- Cisco publishes the latest release of the IronPort AsyncOS software. A Cisco SOC engineer then initiates an RFC to make the necessary changes to the Customer's IronPort email appliance to enhance the features and functionality of the IronPort email appliance(s).

Cisco-recommended Physical Add or Delete of IronPort email appliance(s)

Throughout the Cisco IronPort Managed Email Security service term, Cisco SOC engineers may recommend physical adds or deletes of IronPort email appliances as a normal course of delivering the Cisco IronPort Managed Email Security service. This type of change would normally be associated to situations where a Customer's email messaging capacity requirements change due to a Customer's business needs.

Activities:

- Physical adds or deletes of IronPort email appliance(s)

- Communicate with the Customer the criticality and timeframe associated to the change

- Obtain Customer approval for executing the change

- Follow established Change Management process including updating all activities in the Change Ticket

Example:

- Cisco SOC Problem Management engineers determine that the current deployment of IronPort email appliances are no longer optimally meeting the needs of the Customer in regards to the scope of the Cisco IronPort Managed Email Security service offering. The Cisco SOC Problem Management engineer then initiates an RFC to evaluate the current IronPort email appliance deployment on the Customer's network and, if needed, an escalation to Cisco IronPort service activation resources to execute the RFC for an upgrade to the IronPort email appliances currently deployed on the Customer's messaging security infrastructure.

Customer-Requested Changes

Customer-requested changes are changes that originate with the Customer. The Customer uses the Cisco Portal to submit Customer Requests for Changes (RFCs). This will automatically initiate the Change Management process. The Customer can also call the Cisco RMS Service Desk and describe the RFC over the phone. The Cisco RMS Service Desk will make the initial evaluation of the RFC and coordinate with the Cisco SOC Change Manager in compliance with the agreed upon Change Management process established between Cisco and the Customer.

The specifics of the Change Management Process are outlined and reviewed with the Customer during the Service Activation phase. All change requests will have an associated Mean Time to Complete (MTTC) Service Level Objective to execute the change. See Service Level Management section of this document for details on all Service Level Objectives (SLOs).

The Cisco SOC Change Manager evaluates the potential impact of Customer-requested changes and will determine if a Cisco SOC engineer will need to discuss the implications of a requested change with the Customer. If the Cisco SOC Change Manager determines that the change requires additional information, planning, diligence or testing, the Cisco SOC Change Manager may coordinate the Cisco SOC Change Advisory Board (CAB) which may, in their discretion, refuse the Customer-requested change if they determine that the change may adversely affect the functionality of the IronPort email appliance or disrupt the Customer's business. The Cisco SOC Change Manager will have responsibility for communicating acceptance or rejection of the Request for Change (RFC) to the Customer.

Activities:

- Cisco RMS Service Desk makes initial evaluation of the RFC and coordinates with the Cisco SOC Change Manager

- Cisco SOC Change Manager classifies the change into Priority 1 (P1), Priority 2 (P2) and Priority 3 (P3) Incident categories.

- Cisco SOC Change Manager may coordinate with the Cisco SOC Change Advisory Board (CAB) as needed to determine the level-of-effort and business risk associated to the change request as defined in the IT Infrastructure Library (ITIL) Change Management framework under the following change categories: Priority 1 (P1), Priority 2 (P2) and Priority 3 (P3) Incident categories.

- Cisco SOC Change Manager or Cisco SOC Change Assignee communicates with the Customer regarding the criticality and timeframe associated to the change in accordance with the change attributes

- Cisco SOC Change Manager obtains approval from the Customer for executing the change

- Cisco SOC follows the established Change Management process including updating all activities in the Change Ticket

Customer-requested Logical Change

A Logical Change includes changes to software on IronPort email appliances. The Cisco SOC Change Manager will have the responsibility of determining the level-of-effort to support the Logical Change request per the specific details of the RFC.

The Customer will be entitled to a set amount of Change Management activity on a monthly basis based on a formula involving the size of their User community, the number of entitled IronPort email appliance(s) on the Customer's Cisco IronPort Managed Email Security infrastructure, and their business needs.

Activities:

- Cisco SOC Change Manager evaluates the Customer's Request For Change (RFC) and categorizes the RFC into Priority 1 (P1), Priority 2 (P2) and Priority 3 (P3) Incident categories.

- Cisco SOC Change Manager or Change Assignee coordinates with the Customer according to the Change Management process established with the Customer

- Customer request configure the IronPort email appliance to accept mail for additional domains.

Deliverables:

- Complete the Customer-requested RFC within the Mean Time To Complete (MTTC) Service SLO according to priority level. See table in Service Level Management section of this document for details.

Example:

- The Customer's email administrator is deploying a mail server (groupware) in their network and wants to ensure that this particular email traffic is not going to be blocked by the IronPort email appliance. The Customer's email administrator submits a RFC on the Cisco Web Portal and instructs the Cisco SOC to update the IronPort email appliance configuration to include a relay list to always allow this particular email traffic from this specific mail server.

Customer-requested Physical Move

A Physical Move is a change required to physically move an IronPort email appliance from one location to another. For a Physical Move, the Customer or a qualified Cisco Partner is responsible for physically moving the component from one location to the next. The Cisco SOC is responsible for making the necessary changes in the Cisco RMS CMDB as well as the configuration of the IronPort email appliance so that management can continue in the new physical location. A Physical Move may involve physically moving the Cisco RMS VPN termination router along with the IronPort email appliance(s). The Cisco SOC will work with the Customer to coordinate the Physical Move and re-establish remote management connectivity to the IronPort email appliance.

Activities:

- Cisco SOC Change Manager evaluates the Customer's Request For Change (RFC) and categorizes the RFC into Priority 1 (P1), Priority 2 (P2) and Priority 3 (P3) Incident categories.

- Cisco SOC Change Manager or Change Assignee coordinates with the Customer according to the Change Management process established with the Customer

Deliverables:

- Re-establish connectivity to the Customer's messaging security infrastructure and resume monitoring and management of IronPort email appliances under the scope of the Cisco IronPort Managed Email Security service
- Complete the Customer-requested RFC within the MTTCSLO according to priority level. See table in Service Level Management section of this document for details.

Example:

- The Customer is shutting down a hub site and is moving the IronPort email appliance to its headquarters site. The Customer coordinates the move with the Cisco SOC to ensure that management connectivity is re-established at the new location, all information is updated in the Cisco RMS Configuration Management Database (CMDB), and remote monitoring resumes on the entitled IronPort email appliance(s) deployed in the Customer's messaging security infrastructure.

Executing changes

After changes are executed, the Cisco SOC will notify the Customer that the change has been executed. Once the Customer accepts the change, the Ticket will be closed. The status of changes can be viewed on the Cisco Remote Management Services for Security Web Portal.

Activities:

- Maintain a ticket history of changes visible through the Portal

- Evaluate change requests

- Authorize and schedule change requests

- Coordinate changes

- Update Web Portal change tickets to include change status

- Review and close change requests

Deliverable(s):

- Executed change

- Change Ticket updated with detailed notes and viewable on the Cisco Web Portal

Service Level Management for Cisco IronPort Managed Email Security

Service Level Objectives (SLOs) for Cisco IronPort Managed Email Security[1]

SLO Name	SLO Detail	SLO Targets
Mean Time To Notify (MTTN)	Notify Customer of Hardware, Operating System and Security Service Incidents within X minutes	15 Minutes
Mean Time To Investigate (MTTInv)	Investigate Hardware, Operating System and Security Service Incidents within X minutes	30 Minutes
Mean Time To Isolate (MTTIso)	Isolate root cause of Hardware, Operating System and Security Service Incidents within X minutes	90 Minutes
Mean Time To Resolve (MTTR)	Resolve Hardware*, Operating System and Security Services 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)^2	Complete Customer's Logical Request for Changes (RFCs) 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

[1] All Service Level Objectives (SLO) goals are established to provide operational benchmarks for the Cisco Ironport MMS service on a "commercially reasonable efforts" basis.

2 Priority 1 Incidents on an entitled Managed Component where the Managed Component is unavailable and severely disrupting / impacting the Customer's business. Cisco and the Customer will commit any necessary resources 24x7 until the Incident is resolved / remediated

3 Priority 2 Incidents on an entitled Managed Component where 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 normal business hours Monday through Friday to resolve / remediate the Incident

4 Priority 3 Incidents on an entitled Managed Component where 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 normal business hours to resolve / remediate the Incident and restore service to satisfactory levels.

[5] All Customer-requested RFCs associated to the Cisco Ironport Managed Messaging Security 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 would be 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 normally replacement is made within 24 hours (or 1 business day). 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.

Customer Responsibilities for Cisco IronPort Managed Email Security

Service Activation

To ensure that Cisco is enabled to provide Cisco IronPort Managed Email Security Services for IronPort email appliances, Cisco requires the Customer to:

- Assign a project manager to represent the Customer during the service activation phase

- Assign a technical lead that will assist Cisco with establishing the network access required for remote management of the IronPort email appliances

- Supply all required information contained in the Cisco Remote Management Services for Security Service Activation Kit (SAK) provided during the service activation phase.

Connectivity and Network Access

- Cisco Remote Management Services for Security will supply a VPN termination router to establish a remote network management connection into the Customer premise. As necessary, the Customer will allow logical network access to the other IronPort email appliances via the connection to the VPN termination router.

- Cisco IronPort Managed Email Security is delivered using specific ports and protocols. The Customer will open up the required ports and protocols to enable Cisco Remote Management Services for Security to collect the data for all IronPort email appliances entitled under the Cisco IronPort Managed Email Security service.

- To ensure that the Cisco Remote Management Services for Security can provide Cisco IronPort Managed Email Security, the Cisco SOC requires the Customer to provide Cisco SOC engineers with full read/write access using network management protocols that include enabling full administrative privileges (re: administrative access) to all IronPort email appliances entitled under Cisco IronPort Managed Email Security service.

Operations Support

- A Customer contact will be assigned for each IronPort email appliance entitled under Cisco IronPort Managed Email Security service in order to assist Cisco SOC engineers and support personnel with technical and non-technical troubleshooting and administrative tasks as normal course of action for delivering the Cisco IronPort Managed Email Security service.

- Customer is responsible for assigning a Process Manager that will review and coordinate the approval of changes in the normal course of providing the Cisco IronPort Managed Email Security service.

IronPort email appliances

- The Customer is responsible for the physical security of the IronPort email appliances

- The Customer must agree to allow Cisco to retain and publish aggregate statistics and metrics for non-identifiable trending analysis

Communications and Change Management

- Cisco takes a co-management approach to Cisco IronPort Managed Email Security allowing the Customer and other Customer-approved vendors to retain access to Customer's IronPort email appliances. Because multiple parties may be able to make changes to the managed IronPort email appliances deployed in the Customer's managed email security infrastructure, the Cisco SOC requires that anyone with access to the Customer's IronPort email appliances follow a consistent and documented Change Management Process. This process will be reviewed and agreed upon prior to completion of the service activation phase.

- The Customer is responsible for updating the Cisco SOC with current data with respect to the Customer information as well as all IronPort email appliances, as needed, via the Portal

- The Customer is responsible for the timely delivery of information required for configuration of IronPort email appliances and Customer information (including notification procedures)

- The Customer should notify the Cisco Remote Management Services for Security Service Desk at least 72 hours in advance of any scheduled maintenance windows

- The Customer maintains sole responsibility for informing Cisco of Customer employee status changes

- The Customer is responsible for providing and maintaining a list of Customer employees authorized to request or submit Request for Changes (RFCs) to the Cisco Remote Management Services for Security Service Desk

- The Customer is responsible for providing and maintaining an escalation path within the Customer's employee base

- The Customer is responsible for end-user training of the Cisco Web Portal.

- The customer is responsible for the evaluation and monitoring of the deployed Data Loss Prevention (DLP) policies with respect to regulations compliance, policy effectiveness, etc. Cisco can assist with enabling one or more of the 100+ policies available as part of the Cisco IronPort DLP software. Cisco Advanced Services can be utilized to provide additional Data Loss Prevention consulting.

Transition Management for Cisco IronPort Managed Email Security

The Cisco IronPort Managed Email Security Transition Management phase uses a Service Activation process in which Cisco prepares the Customer's Messaging Security infrastructure for Cisco remote management. Using our proven Service Activation methodology enables an efficient and low-impact effort of enabling the Customer's Messaging Security infrastructure to receive Cisco Remote Management Services for Security management services. This framework includes:

- Discovering the IronPort email appliances on the Customer's messaging security infrastructure

- Planning the transition from service activation phase to full lifecycle management

Discovering the Managed Email Security Infrastructure

Discovering the Managed Email Security Infrastructure phase includes the pre-implementation activities that provide Cisco Remote Management Services for Security with a high-level understanding of the Customer's business and messaging security infrastructure needs. This assists the Cisco Remote Management Services for Security team in having an accurate understanding of the Customer's requirements before the planning and implementation processes begin.

Activities:

- Identify key Customer participants and setup initial kick-off meeting

- Have initial engagement with the Customer

Cisco Remote Management Services for Security will work with the Customer to discover and get an understanding of the managed email security infrastructure. In this case, the purpose of planning the transition of Cisco IronPort Managed Email Security Activation is to prepare both the Customer and the Cisco SOC for a smooth management transition. This process involves collecting and validating all technical details required to enable remote IT infrastructure management, ensuring the Customer has a clear understanding of service features, and establishing joint interaction methods. Each IronPort email appliance will be assessed to ensure that no further work is needed before remote management begins.

Transition to Cisco IronPort Managed Email Security Activation

The purpose of planning the transition phase is to prepare both the Customer and Cisco Remote Management Services for Security for a smooth management transition. This phase involves collecting and validating all technical details required to enable remote messaging security infrastructure management, ensuring that the Customer has a clear understanding of service features, and establishing joint interaction methods. Each site will be assessed to ensure that no further work is needed before the IronPort email appliances located at the physical site are brought under management.

Activities:

- Establish key relationships with the Customer

- Work with the Customer to develop an implementation plan

- Cisco IronPort System Engineer (SE) to gather all required Customer information via the Service Activation Kit (SAK)

- Cisco IronPort System Engineer (SE) to gather the required IronPort email appliance information via the Service Activation Kit (SAK)

- Cisco Remote Management Services for Security service activation resources enter all required Service Activation Kit (SAK) information into the Cisco Remote Management Services for Security Configuration Management Database (CMDB)

- Cisco Remote Management Services for Security service activation resources to work with the Customer to define an escalation plan for the Cisco SOC and the Customer

- Cisco Remote Management Services for Security and the Customer align on the Change Management Process that will be followed

- Cisco Remote Management Services for Security service activation resources to configure, ship and deliver the remote network management VPN termination router

Deliverable(s):

- Completed Service Activation Kit (SAK)

- Remote network management VPN termination router(s) configured, shipped and installed on customer premise

Implementing Management Operations for Cisco IronPort Managed Email Security

Implementing management operations phase involves executing the implementation plan. To provide a single point of contact to apply ongoing focus on established timelines and commitments, Cisco Remote Management Services for Security will appoint a designated project coordinator.

During this phase, Cisco Remote Management Services for Security will establish management connectivity and ensure the Customer contacts are aware of how to interact with the Cisco Remote Management Services for Security Service Desk and Cisco Remote Management Services for Security SOC during delivery of services.

Activities:

- Cisco Remote Management Services for Security service activation resources will work with the Customer and the Cisco IronPort SE to install the VPN termination router and establish remote network management connectivity to effectively manage the IronPort email appliance(s)

- Cisco Remote Management Services for Security service activation resources will establish remote management access for each IronPort email appliance via the VPN connection between Cisco Remote Management Services for Security and the Customer

- Cisco Remote Management Services for Security service activation resources and a Cisco IronPort System Engineer (SE) will review the configuration of all IronPort email appliances to ensure readiness for remote management

- Cisco IronPort System Engineer and Cisco Remote Management Services for Security service activation resources will work with the Customer on any initial management configuration issues and/or changes required for successful management of the IronPort email appliances

- Begin ongoing Incident monitoring of IronPort email appliances

Deliverable(s):

- Establish Cisco Remote Management Services for Security Portal access and verify IronPort email appliances inventory

- Publish scheduled service activation events via notes in the master Service Activation Ticket viewable on the Portal

- Train primary Customer contacts for the Cisco IronPort Managed Email Security service on how to use the Cisco Portal

- Provide the Customer with a complete inventory of IronPort email appliances published on the Portal

- Remote Management Connectivity installed and verified

- Configure Cisco Remote Management Services for Security management platform(s) to backup the configuration of all entitled IronPort email appliances on the Customer's Cisco IronPort Managed Email Security infrastructure. The Cisco Remote Management Services for Security management platform will retrieve configuration backups of the entitled IronPort email appliances 4 times per day and store them in a secure location in the Cisco Remote Management Services for Security management platform for up to one year

- Perform gap analysis between IronPort email appliances inventory and what is on the original Purchase Order, resolving any discrepancies

As necessary, for Cisco Remote Management Services for Security to perform its responsibilities as stated in this Service Description, Cisco Remote Management Services for Security will maintain an information repository of data in the Cisco Remote Management Services for Security Configuration Management Database (CMDB) with respect to the Customer and entitled IronPort email appliances.

-END-