# Service Description: Cisco ScanSafe Web Security Service

**Direct Sale from Cisco IronPort.** If you have purchased these services directly from Cisco IronPort, this document is incorporated into your purchase agreement with Cisco IronPort.

**Sale via Authorized Reseller.** If you have purchased these services through an authorized IronPort reseller, this document is for description purposes only; and the contract, if any, governing the provision of the services will be the one between you and your authorized reseller. Your authorized reseller should provide this document to you, or you can obtain a copy of this service description at: www.cisco.com/legal/services.html.

This Service Description should be read in conjunction with the other applicable documents found at: www.cisco.com/legal/services.html. Capitalized terms are defined in the Glossary of Terms at the end of this document.

## 1. Overview

1.1 ScanSafe Web Security is delivered through hardware and software deployed in IronPort managed data centers. IronPort and/or its parent company will retain ownership, as applicable, of all hardware infrastructure used in IronPort data centers as part of providing the ScanSafe Web Security service.

1.2 The ScanSafe Web Security component includes hardware infrastructure powered by IronPort technology together with 24x7 monitoring, management and support.

1.3 The Services do not include Customer's access connection to the Internet or any equipment necessary for Customer to make such connection, which are Customer's sole responsibility.

1.4 Services that are not expressly set forth in this Service Description are not covered, including, without limitation, the following:

a) Any customization of, or labor to install, Software and Hardware.

b) Any expenses incurred to visit Customer's location, except as required during escalation of problems by IronPort.

c) Services or software to resolve Software or Hardware problems resulting from third party product or causes beyond IronPort's control or failure by Customer to perform its responsibilities set out in this Service Description.

d) Services for non-IronPort products used in connection with IronPort Services.

1.5 Except as otherwise agreed, Software entitlement, including media, documentation, binary code, source code or access in electronic or other form is not provided.

## 2. IronPort Responsibilities

2.1 As long as Customer has paid all applicable fees, IronPort will:

a) Provide the Services set forth in the Service Description as ordered by the Customer;

b) Provide all Updates and Releases commercially released by IronPort; and

c) Use its reasonable commercial endeavors to resolve technical problems identified within IronPort's Services. IronPort does not provide technical support for any third-party hardware or software not purchased and/or authorized by IronPort.

## 3. Functionality

3.1 The Web security services comprise Web Malware Scanning and Web Filtering as described below.

3.2 The Customer's external HTTP, HTTPS and FTP over HTTP requests (including all attachments, macros or executables) are directed through the Services. The configuration settings required to direct this external traffic via the Services are made and maintained by the Customer (with assistance and support from IronPort as reasonably required) and are dependent on the Customer's technical infrastructure. The Customer should ensure that internal HTTP/HTTPS/FTP over HTTP traffic (e.g. to the corporate intranet) is not directed via the Services.

**Web Malware Scanning ("MS")**

3.3 Once the relevant configuration changes are made, unencrypted Web pages and attachments will be scanned by Outbreak Intelligence$^{TM}$, a proprietary security platform that detects malware threats by using a combination of multiple, correlated detection technologies, including industry leading anti-malware engines.

3.4 MS will scan as much of the Web page and its attachments as possible. It may not be possible to scan certain Web pages or attachments (for example, password protected). Unscannable attachments will be blocked. Encrypted traffic (i.e. HTTPS/SSL) cannot be scanned and will be passed through MS unscanned (unless HTTPS Inspection is enabled as described in paragraph 3 below).

3.5 If a requested Web page or attachment is found to contain malware (or deemed unscannable in accordance with paragraph 1.2, except for SSL traffic), then access to that Web page or attachment is denied and the user will be displayed an automatic alert Web page. Notification may also be sent by email to a customer administrator.

**Web Filtering ("WF")**

3.6 Once the relevant configuration changes are made, Web pages and attachments will be filtered using industry leading URL categorization and content analysis. URLs are categorized by reference to a number of predefined categories as specified in the Portal (see below).

3.7 The Customer can configure WF to create access restriction policies (based both on categories and types of content) and deploy these at specific times to specific Internet users or groups. A number of additional features (for example, 'blocked' and 'allowed' list functionality) are also available.

3.8 WF will filter as much of the Web page and its attachments as possible. It may not be possible to filter certain Web pages or attachments (for example, password protected). The Customer may also configure specific exceptions for web sites that should not be filtered. Encrypted traffic (i.e. HTTPS/SSL) cannot be filtered and will be passed through WF unless otherwise specified by the Customer in relation to specific categories of content. WF will only filter Web pages that are categorized by WF in accordance with the category that the Customer has chosen to filter.

3.9 The Customer can use individual and/or group administration and reporting capabilities by utilizing the Connector software described in paragraph 6.

3.10 If a user requests a Web page or attachment where an access restriction policy applies, then access to that Web page or attachment is denied and the user will be displayed an automatic alert Web page. Notification may also be sent by email to a customer administrator.

**HTTPS Inspection**

3.11 Where enabled, HTTPS Inspection allows the administrator to set a policy determining which domains and categories of HTTPS traffic are decrypted and inspected on the scanning infrastructure. Data is encrypted from the Web server to the scanning tower in the normal way; however, for sites which the customer wishes to be inspected, the scanning tower will terminate the SSL-based connection, inspect the data in the same way as for HTTP traffic, and then re-encrypt the traffic from the scanning towers to the end user using a different certificate. The corresponding certificate authority will need to be rolled out to the Customer's Web browsers as a trusted certificate authority to prevent domain mismatch warnings appearing to end users. HTTPS Inspection can be used for both malware detection and enhanced Web filtering actions such as Outbound Content Control.

**Outbound Content Control**

3.12 Outbound Content Control gives Web filtering Customers the flexibility to define rules based on the HTTP protocol's POST function. These filters look for specific files with certain characteristics (e.g. MD5 or SHA1 checksums), keyword analysis, outbound file types, preconfigured IDs (e.g. credit card numbers or social security numbers) and DFA-based regular expressions.

**Block Alert Pages**

3.13 Block alert pages are dynamically generated HTML pages displayed to end users when they are prevented from accessing prohibited Web content. The Customer can choose a standard block alert page or your own customized content which can be uploaded via the Portal (see below). IronPort will host the Blocked pages.

**Connector**

3.14 If ordered by the Customer, IronPort will provide the Connector software for the Customer to install in its network in accordance with IronPort's installation guidelines. The Connector does not support all potential customer systems and set-ups.

3.15 The Connector enables users to connect to the Services even without a static IP address by using an authentication key. If users have other services that rely on a fixed IP address for identification, they can configure direct connections for specific websites, domains, hosts or networks.

3.16 Administrators can create, revoke, activate, and deactivate authentication keys for Connectors per group or per users.

**Anywhere+ or AnyConnect (Secure Mobility)**

3.17 If ordered by the Customer, IronPort will provide the Anywhere+ or AnyConnect software for the Customer to install on its end users' PCs or laptops in accordance with our installation guidelines. Anywhere+ and AnyConnect do not support all potential customer setups.

3.18 Anywhere+ or AnyConnect allow the end user's PC or laptop to connect to the Services from a remote location outside the customer's internal network. They do not rely on provisioned IP addresses.

**Portal**

3.19 The Customer will be provided access to a Web-based portal, hosted by IronPort, to administer and report on the Services. Access to the Portal is via a secure (HTTPS) website and is password-protected.

3.20 The Customer may have multiple administrators for a single account. The Customer can give each administrator a unique login and provide full access or read only privileges specific to each user. This functionality allows a unique, single Super User account that can create multiple administrators.

3.21 The Portal enables the customer administrator to:

a) review statistics of all malware stopped and other Web content blocked;

b) create access restrictions and apply these to specific users or groups (if the Connector has been installed);

c) customize browser alert pages seen by users when access to a particular website or file is denied;

d) update administration details for real-time email alerts; and

e) configure and schedule automated system auditing and reporting.

3.22 Automated reports are available on overall traffic, bandwidth, blocked URLs and Web malware stopped. The Portal also offers a comprehensive selection of additional reports, generated daily, which provide in-depth analysis in the form of graphs, tables, and exportable data files. The Customer can schedule regular reports for different service functionality and specify users, times, and email it to certain users or groups.

3.23 Audit Logging functionality records administration, configuration, filtering, and policy changes made for the Services, and can be configured by full access administrators or the Super User. Auditing includes who made the change, what was changed, and when it was changed. Audit logs can be searched by specifying a time period, category or type of logs, and type of action taken.

3.24 Privacy Logging functionality, when enabled, will log when web pages are blocked according to web filtering policy, but will obfuscate private details such as source username and IP address. This feature is for customers who must comply with local privacy policies or regulations.

## 4. Maintenance

4.1 From time to time, IronPort performs scheduled maintenance, to update the servers (IronPort and third-party servers at the datacenter(s)) and software that are part of the ScanSafe Web Security service. IronPort will make all reasonable attempts to notify Customer at least five business days in advance of any planned downtime or scheduled maintenance. Notwithstanding the foregoing, Customer acknowledges that IronPort may, in certain situations, need to perform emergency maintenance on less than 48 hours advance notice.

## 5. Pricing Conditions

5.1 The Customer must notify IronPort within 14 days if the number of Seats increases by more than 5% of the then declared number of Seats. IronPort reserves the right to require the Customer to purchase additional Seats if the number of actual distinct users (as shown by IronPort's Web traffic logs) exceeds the number of licensed Seats from time to time.

5.2 Pricing is subject to the Customer's peak bandwidth per seat (the higher of inbound and outbound, measured on a 95th percentile basis) not exceeding an average of 5 kb/s in any calendar month. Charges will be increased pro rata if this level is exceeded for three or more calendar months. IronPort will notify the Customer if this level is exceeded in any one calendar month, such notification to be given within 10 business days after the end of such month.

## 6. Customer Responsibilities

6.1 Customer shall supply IronPort with all technical data and all other information IronPort may reasonably request from time to time to allow IronPort to supply the Services to the Customer, including a completed deployment questionnaire and site matrix.

6.2 Customer recognises that information sent to and from Customer will pass through IronPort's systems and accordingly Customer undertakes to comply with all relevant legislation applicable to its use of the Internet.

6.3 Customer is responsible for implementing and using strong passwords for accessing IronPort dedicated infrastructure and the associated support portal.

*The following are common guidelines for choosing strong passwords. These are designed to make passwords less easily discovered by intelligent guessing:*

- *Include numbers, symbols, upper and lowercase letters in passwords*
- *Password length should be around 12 to 14 characters*
- *Avoid any password based on repetition, dictionary words, letter or number sequences, usernames, relative or pet names, or biographical information (e.g., dates, ID numbers, ancestors' names or dates...)*

6.4 In performing the Services, IronPort may instruct the Customer to perform certain tasks or checks relating to Customer's network. Customer shall, at its expense, perform all such checks and tests. Customer will also provide IronPort, or its authorized representative, reasonable and free access to Customer's networking equipment. Customer shall not be required to furnish specialized equipment or know-how. Customer agrees to pay IronPort, at IronPort's then-current rates, plus any reasonable actual out-of-pocket expenses, for any rework or additional work resulting from modification of the Services requested by Customer (and accepted by IronPort) or any act or omission of Customer, including providing inaccurate information to IronPort. IronPort shall seek Customer's approval in advance of incurring such costs if it knows costs will be incurred as a result of such act or omission of Customer.

6.5 Customer is responsible for obtaining all approvals required by any third parties in order for IronPort to perform any Service under this Service Description. IronPort shall not be in default of its obligations to the extent it cannot perform the Services either because such approvals have not been obtained or any third party otherwise prevents IronPort from performing such Services.

6.6 Customer agrees that it shall not resell the Product and/or Services or create or offer derivative versions of the Services either directly or through a third party.

6.7 Customer assumes full responsibility for the control and use of the data contained in any reports provided by IronPort hereunder. Customer acknowledges the potential privacy and other issues associated with the collection and use of this data.

6.8 Customer assumes full responsibility to back-up and/or otherwise protect all data against loss, damage, or destruction. Customer acknowledges that it has been advised to back-up and/or otherwise protect all data against loss, damage or destruction.

6.9 Customer shall comply with such laws and regulations governing use, export, re-export, and transfer of IronPort Products and technology and will obtain all required U.S. and local authorizations, permits, or licenses.

6.10 The failure of Customer to comply with this Section may be deemed a material breach.

## 7. Data Privacy

7.1 Subject to the IronPort Privacy Statement at http://www.ironport.com/privacy.html or a successor site location, as the same may be amended from time to time by IronPort with notice to Customer, Customer hereby consents and grants to IronPort a license to collect and use the data from the

Customer as described in the Documentation, as the same may be updated from time to time by IronPort ("Data"). To the extent that reports or statistics are generated using the Data, they shall be disclosed only in the aggregate and no End User identifying information may be surmised from the Data, including without limitation, user names, phone numbers, unobfuscated file names, email addresses, physical addresses and file content.

## 8. Licenses and Ownership

8.1 Subject to Customer's compliance with the terms of this Service Description, IronPort grants to Customer a worldwide, non-exclusive and non-transferable license to use, for Customer's internal business use only and for the duration of the relevant purchase order: (i) the Services; (ii) other Deliverables specified in an applicable SOW, if any, and (iii) Data Collection Tools, if any (collectively and individually, the ***"Licensed Materials"***). These license grants do not include the right to sublicense; provided that Customer may permit its suppliers, subcontractors and other related third parties to use the Licensed Materials solely on Customer's behalf for Customer's benefit, provided that Customer ensures that any such use is subject to license restrictions and confidentiality obligations at least as protective of IronPort's rights in such Licensed Materials as are specified in this Service Description.

8.2 Except as otherwise expressly set forth in this Service Description, Customer shall not (and shall not permit a third party to): make error corrections or derivative works of, or otherwise modify, decompile, decrypt, reverse engineer, disassemble or otherwise reduce all or any portion of any Deliverable, Data Collection Tool or the Services to human-readable form; or transfer, sublicense, rent, lease, distribute, or sell, any Services, Deliverables or Data Collection Tools. Customer agrees that it receives no implied licenses under this Service Description, and all rights not expressly granted herein are reserved to IronPort.

8.3 Each party will retain the exclusive ownership of all its Pre-Existing Technology.

8.4 Except as otherwise expressly set forth in this Service Description, IronPort owns and will continue to own all right, title and interest in and to the Hardware, Services, Deliverables, Data Collection Tools, Reports, sketches, diagrams, text, know-how, concepts, proofs of concepts, artwork, software, algorithms, methods, processes, identifier codes or other technology provided or developed by IronPort (or a third party acting on IronPort's behalf) pursuant to this Service Description, including modifications, enhancements, improvements or derivative works of any of the foregoing, regardless of who first conceives or reduces to practice, and all Intellectual Property in any of the foregoing (collectively, "***IronPort Intellectual Property***").

8.5 As between Customer and IronPort, Customer shall at all times retain all right, title and interest in and to all of Customer's Pre-Existing Technology and all Intellectual Property that is developed by Customer or by a third party on Customer's behalf thereafter, other than IronPort Intellectual Property. Products supplied to Customer by any third party shall at all times be owned by the applicable third party, and will be subject to any applicable third party license terms.

8.6 Customer hereby grants to IronPort a perpetual, irrevocable, royalty free, worldwide right and license to all Intellectual Property in the Customer Feedback (as defined below) to use and incorporate Customer Feedback into any Services, Products, Deliverables, Data Collection Tools, Reports or IronPort Pre-Existing Technology, and to use, make, have made, offer to sell, sell, copy, distribute and create derivative works of such Customer Feedback for any and all purposes whatsoever, and Customer acknowledges and agrees that it will obtain no rights in or to any Services, Products, Deliverables, Data Collection Tools, Reports or IronPort Pre-Existing Technology as a result of IronPort's use of any such Customer Feedback. For purposes of this Service Description, "Customer Feedback" means all oral or written communications regarding improvements or changes to any Services, Products, Deliverables, Data Collection Tools, Reports or IronPort Pre-Existing Technology that Customer provides to IronPort.

## 9. Acceptable Use Policy

9.1 The Customer is responsible for ensuring that all users of the Services are aware of this policy. The Customer is also responsible for ensuring that these regulations are complied with at all times, and shall indemnify IronPort against liability, whether civil or criminal, for any violation by such users as the Customer permit to use the Services.

9.2 Users must not under any circumstances whatsoever commit, or attempt to commit, nor aid or abet any action that may threaten the Services – this shall include but is not limited to:

- Using the Services for any unlawful, invasive, infringing, defamatory, or fraudulent purpose;
- Intentionally sending any virus, worm, Trojan horse or harmful code or attachment with the Services;
- Interfering with the use of the Services by other authorized users;
- Altering, tampering with or circumventing any aspect of the Services;
- Any attempt to crash a Services host or network;
- "Denial of service" attacks, or "flooding" attacks;
- Reselling, passing-through, renting, leasing, timesharing or branding the Services or otherwise providing the Services to any party which is not contractually authorized by us to receive the Services;
- Testing or reverse-engineering the Services in order to find limitations, vulnerabilities or evade filtering capabilities;
- Supplying proprietary information about the Services, including but not limited to screen shots, product documentation, demonstrations, service descriptions, announcements, or feature roadmaps to unauthorized third parties;

- Any attempt to circumvent the user authentication or security of a Services host or network;
- Any profligate use of the Services (i.e. peak bandwidth, measured on a 95th percentile basis, exceeding an average of 6 kb/s per licensed used in any calendar month);
- The creation, transmission, storage, or publication of any kind of virus or corrupting program or corrupted data;
- Any other action that may adversely affect the Services or their operation.

9.3 IronPort shall have the right to suspend or terminate the Services, and to take such defensive action as may at its sole discretion be deemed necessary in the event of any attack upon the Services or network. Furthermore, IronPort may instigate civil and/or criminal proceedings as appropriate against the perpetrators of such prohibited action.

## 10. Service Level Agreements

### Web Service Availability

10.1 IronPort warrants that its network will process and deliver Customer's Web requests at least 99.999% of the total hours during every month Customer uses the Services ("Availability"). Availability will be determined on an aggregate basis across all Customer sites. IronPort provides both primary and secondary proxy addresses for each site from which Web traffic may be directed. As a result, non-Availability occurs only where Web content sent from a site to both proxy addresses is not being received, scanned, analyzed, filtered, or transmitted after filtering to end users at the affected Customer site.

10.2 If IronPort breaches the Availability warranty, IronPort shall provide service credits of a portion of Customer's monthly Services fees on the following basis:

| Monthly Service Availability | % reimbursement of monthly Web Service fee |
|---|---|
| 99.999 - 99.5 % | 10 |
| 99.49 - 99.0 % | 20 |
| 98.99 - 98.5 % | 30 |
| 98.49 - 98.0 % | 40 |
| 97.99 - 97.5 % | 50 |
| 97.49 - 97.0 % | 60 |
| 96.99 - 96.5 % | 70 |
| 96.49 - 96.0 % | 80 |
| 95.99 - 95.5 % | 90 |
| Below 95.5% | 100 |

### Web Filtering Latency

10.3 Web Filtering Latency refers to the additional Web page load time attributable to the Web Services. Web Filtering Latency is assessed by reference to the average elapsed time between:

- a Web page request being sent to us at the datacenter where the applicable scanning towers are located; and
- receipt of the requested Web-page data by the requesting party.

10.4 Web Filtering Latency shall be assessed solely by reference to the time taken to download a discrete resource from a selection of popular websites. For the avoidance of doubt the Web Filtering Latency SLA does not apply to the Anywhere+ service.

10.5 To calculate the average Web Filtering Latency, IronPort shall measure the average elapsed time taken to download a discrete resource from each of the websites referred to above ("Filtered Response Time") and compare this time to the average elapsed time taken for identical Web page requests by the same requesting party during the same testing period which are not processed through the Services ("Unfiltered Response Time"). Each such sample of the Filtered Response Time and Unfiltered Response Time is referred to as a "Sampled Pair". Such samples shall be taken every 60 minutes.

10.6 IronPort warrants that the Filtered Response Time (averaged over all of the Sampled Pairs) in any one calendar month will not exceed the greater of:

- one second more than the Unfiltered Response Time; and
- three times the Unfiltered Response Time.

10.7 If IronPort breaches the above warranty, IronPort will provide service credits of an amount equal to 10% of the Customer's monthly Service fees for the Services provided for that month.

### False-Positive Web Filtering Rate

10.8 The "False-Positive Filtering Rate" Service Level measures the percentage of URLs and domains that were blocked by the Service but, based on the Customer's chosen categorization policies, should not have been blocked ("Bad Blocks"). For the avoidance of doubt, if a URL is in the 'unclassified' category it shall be required to be blocked if the Customer has elected to block all unclassified URLs.

False-Positive Filtering Rate =

100

x total number of Bad Blocks in a calendar month at all Sites

÷ total number of URLs scanned by the Web Filtering Service at all Sites during the same calendar month

where the Bad Blocks are determined by IronPort acting reasonably.

10.9 If the False-Positive Filtering Rate is greater than or equal to 0.0004%, IronPort will provide service credits of an amount equal to 10% of the Customer's monthly fees for the Web Filtering Service. IronPort shall respond within seven days of receipt of notification that the Customer believes there to have been a Bad Block, and shall give reasons for its decision as to whether there has been a Bad Block or not.

### False-Negative Web Filtering Rate

10.10 The False-Negative Filtering Rate Service Level measures the percentage of URLs and domains that were not blocked by the Service but, based on the Customer's chosen categorization policies, should have been blocked (“Missed Blocks”). For the avoidance of doubt, if a URL is in the ‘unclassified’ category it shall only be required to be blocked if the Customer has elected to block all unclassified URLs.

False-Negative Filtering Rate =

100

x total number of Missed Blocks in a calendar month at all Sites

÷ total number of URLs scanned by the Web Filtering Service at all Sites during the same calendar month

where the Missed Block are determined by IronPort acting reasonably.

10.11 If the False-Negative Filtering Rate is greater than or equal to 0.0004%, IronPort will provide service credits of an amount equal to 10% of the Customer’s monthly fees for the Web Filtering Service. IronPort shall respond within seven days of receipt of notification that the Customer believes there to have been a Missed Block, and shall give reasons for its decision as to whether there has been a Missed Block or not.

**General**

10.12 If Customer believes that IronPort has not met any of the above warranties, Customer must contact IronPort in writing within 15 business days of the end of the month in which Customer believes the relevant warranty was not met.

10.13 IronPort will implement, maintain and use appropriate processes, procedures and tools to monitor, calculate and report on the performance of the Services against the service levels set forth in this Section. If a dispute arises about this Clause, IronPort will make a determination in good faith based on its system logs, monitoring reports and configuration records.

10.14 All remedies referred to in this Section are subject to the Customer having paid all applicable fees and fulfilled all of its obligations under this Service Description.

10.15 The remedies in this Section do not apply to any matters arising due to any of the following:

- Customer-requested hardware or software upgrades, moves, facility upgrades, etc.
- a scheduled maintenance period that was announced at least 24 hours in advance
- hardware, software or other data center equipment or services not in the control of IronPort or within the scope of the ScanSafe Web Security Service
- hardware or software configuration changes made by the Customer without the prior written consent of IronPort
- Denial of Service attacks on the installed email security infrastructure or ancillary services
- events outside of IronPort’s reasonable control, including without limitation acts of God, earthquake, labor disputes, industry wide shortages of supplies, actions of governmental entities, riots, war, terrorism, fire, epidemics, or delays of common carriers.

10.16 The remedies set out in this Section shall be Customer’s sole and exclusive remedy in contract, tort or otherwise in respect of the relevant events. No more than one category of credit may be claimed in respect of any one issue.

## 11. Support and Escalation Matrix

11.1 IronPort operates a 24/7 helpdesk which comprises both Tier 1 and Tier 2 engineers. All issues must be logged with Tier 1 engineers in the first instance. If an issue is not resolved by Tier 1 engineers, the issue will be escalated to Tier 2 engineers for resolution. If Tier 2 engineers are unable to resolve the issue they will escalate the issue internally to Operations Engineers for resolution.

11.2 Customer is responsible for using reasonable efforts to resolve internally any support questions prior to contacting IronPort. Customer is responsible for reporting any and all errors promptly in writing in English and for providing sufficient information to IronPort to enable IronPort to duplicate the circumstances indicating a reported Software defect or error. Customer shall provide technical information as may be required by IronPort systems engineers or security analysts, including but not limited to IP addresses for Customer's existing solution.

**Help Desk Numbers**

| | **Telephone** | **Email** |
|---|---|---|
| **EMEA** | +44 (0)20 7034 9400 | support@scansafe.com |
| **US / APAC** | +1 877 472 2680 | support@scansafe.com |

**Severity Definitions**

11.3 IronPort helpdesks shall assign a severity to all problems submitted by Customer.

- Severity 1: An existing network is down or there is a critical impact to the End User's business operation. End User and IronPort will commit full-time resources to resolve the situation.
- Severity 2: Operation of an existing network is severely degraded, or significant aspects of the End User's business operation are being negatively impacted by unacceptable network performance. IronPort and End User will commit full-time resources during Standard Business Hours to resolve the situation.
- Severity 3: Operational performance of the network is impaired while most business operations remain functional. IronPort and End User are willing to commit reasonable resources during Standard Business Hours to restore service to satisfactory levels.
- Severity 4: Information or assistance is required on a Supplier's product capabilities, installation, or configuration. There is clearly little or no impact to the End User's business operation. IronPort and End User are willing to provide resources during Standard Business Hours to provide information or assistance as requested.

11.4 For the purposes of this document:

a) "Business Days" means the generally accepted days of operation per week within the relevant region where the Services shall be performed, excluding local holidays.

b) "Local Time" means Central European Time for Services provided in Europe-Middle-East and Africa, Australia's Eastern Standard Time for Services provided in Australia, Japan's Standard Time for Services provided in Japan, and Pacific Standard Time for Services provided in all other locations.

c) "Standard Business Hours" means 8:00 AM to 5:00 PM, Local Time at location, on Business Days.

**Escalation process**

11.5 Customers should engage the below contacts when an issue requires escalation.

11.6 Severity 1 escalation times are measured in calendar hours - 24 hours per day, 7 days per week. Severity 2, 3, and 4 escalation times correspond with Standard Business Hours.

| **Elapsed Time** | **Severity 1** | **Severity 2** | **Severity 3** | **Severity 4** |
|---|---|---|---|---|
| **1 hour** | Senior Customer Service Technician | | | |
| **4 hours** | Service Level Manager | Senior Customer Service Technician | | |
| **24 hours** | Technical Support Manager | Service Level Manager | | |
| **48 hours** | Director, Technical Support | Technical Support Manager | | |
| **72 hours** | | Director, Technical Support | Service Level Manager | |
| **96 hours** | | | Technical Support Manager | Service Level Manager |

## GLOSSARY OF TERMS

**Data Collection Tools** means Hardware and/or Software tools that support IronPort's ability to provide troubleshooting on cases, data analysis, and report generation capabilities

**Documentation** means user manuals, training materials, Service descriptions and specifications, technical manuals, license agreements, supporting materials and other information relating to Services offered by IronPort, whether distributed in print, electronic, CD-ROM or video format.

**Hardware** means any tangible IronPort equipment, devices, or components made available to Customers.

**Intellectual Property** means any and all tangible and intangible: (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

**Pre-Existing Technology** in relation to either party means all of such party's pre-existing Intellectual Property, confidential information and materials, including, without limitation, proprietary ideas, sketches, diagrams, text, know-how, concepts, proofs of concepts, artwork, software, algorithms, methods, processes, identifier codes or other technology that are owned by a party prior to commencement of any Services hereunder, or that are otherwise developed by or for such party outside the scope of this Service Description.

**Release** means an incremental Software release that provides maintenance fixes and/or provides additional functionality.

**Reports** means reports, recommendations, network configuration diagrams, and any related items provided by IronPort to Customer.

**Services** means one or more of the services options selected by the Customer and described at www.cisco.com/legal/services.html .

**Software** means the software programs provided to Customer by IronPort, including any copies, Updates, upgrades, modifications, enhancements, and any derivative works thereof.

**Update** means IronPort Releases containing the same configuration or feature set as originally acquired, unless the Customer has upgraded the applicable Services to a configuration or feature set other than what was originally acquired, and the applicable license fee for that upgrade has been paid. Updates do not include any separately licensed and priced Software release that contains an enhanced configuration or feature set.