

Service Description: Security Software Extended Support

This document describes the Security Software Extended Support.

Related Documents: This document should be read in conjunction with the following documents also posted at <http://www.cisco.com/go/servicedescriptions/>: (1) Glossary of Terms; (2) List of Services Not Covered; and (3) Severity and Escalation Guidelines. All capitalized terms in this description have the meaning ascribed to them in the Glossary of Terms.

Direct Sale from Cisco. If you have purchased these Services directly from Cisco, this document is incorporated into your Master Services Agreement (MSA), Cisco Services Agreement (ASA), or equivalent services agreement executed between you and Cisco. If you have no applicable agreement in place, the following terms will apply: http://www.cisco.com/c/dam/en_us/about/doing_business/legal/docs/Advanced_Services_Click-to-Accept_Agreement_sample.pdf (the applicable terms being the, "Agreement"). All capitalized terms not defined in in any supplemental definitions within this document have the meaning ascribed in the Agreement. If not already covered in your Agreement, this document should be read in conjunction with the Related Documents identified above. In the event of a conflict between this Service Description and your 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 description purposes only; is not a contract between you and Cisco. The contract, if any, governing the provision of this Service will be 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 <http://www.cisco.com/go/servicedescriptions/>. All capitalized terms not defined in any supplemental definitions within this document have the meaning ascribed in the Glossary of Terms at the above URL.

Table of Contents

1.0	Services Summary	3
1.1	Services Not Covered	3
1.2	Supplemental Definitions.....	4
2.0	Security Software Extended Support	4
2.1	API Compatibility Maintenance	4
2.2	In-House Utility Execution	5
2.3	Problem Resolution	5
2.4	Software Upgrade.....	5
2.5	General Responsibilities	6
2.6	Security Software Extended Support Escalation Guideline.....	7
3.0	Assumptions and Additional Terms	8

1.0 Services Summary

Service Overview. The Security Software Extended Support Service (the “Services”) provides activities designed to help support the Customer with the software purchased and implemented using the Cisco Security Software Development Service (“Security Software”) and listed in the Ordering Documents (defined below).

This Service Description is intended to provide an indicative summary of the Services Cisco will provide to Customer. The details of the Services will be provided in paper or electronic document (e.g. Service Order, Statement of Work (SOW), quote, proposal or online order submission) signed or otherwise agreed to by the Customer, that references or incorporates this Service Description and specifies the details of the Services purchased by Customer, and items such as pricing, payment terms, and other commercial terms, identifies Products to be implemented or migrated, and describes any additional Customer and Cisco Responsibilities (“Ordering Documents”).

1.1 Services Not Covered

The following services are not supported under the Services:

- Any customization, upgrade, and/or porting of the Security Software.
- Any usage, configuration, hardware or software, or any other such modification of the Cisco Security Extended Software outside of the intended use as defined in the Instructions for use.
- Support of Security Software problems that are diagnosed by Cisco to be Enhancement requests or changes by Customer to the system configuration.
- Resolution of the problems is viewed by Cisco as an Enhancement for which a separate statement of work between the parties is required.
- Any hardware or third-party product that Customer may need to acquire that is related to this Service Description (e.g. hardware to run the Security Software).
- Support or replacement of Security Software that has been altered, modified, mishandled, destroyed, or damaged by natural causes beyond Cisco’s control or Customer’s failure to perform its responsibilities under this Service Description.
- Any support, upgrade or maintenance for Product other than Security Software as defined by this Service Description.
- Services for non-Cisco development tools or any non-Cisco software installed in the Product.
- Any hardware upgrade required to run new or updated Security Software.
- Customer acknowledges that it is only entitled to receive support services against the Support Option for which it has paid a separate support fee. If additional Cases (defined below) or Custom Software (defined below) are supported by Cisco beyond that which Customer has ordered, Cisco reserves the right to charge for support if Cisco determines that unauthorized support is being provided.
- Customer acknowledges that it is not entitled to support on Cisco products not covered under this Agreement. Support for other Cisco products is covered under separate service maintenance agreements.

- The base Services do not include any on-site support under this Service Description. If Cisco is requested to perform on-site diagnostics and remedial maintenance, Customer shall reimburse Cisco for all labor and travel expenses at Cisco's then-current time and material rates, except where mutually agreed.
- Any support for Cisco Security Extended Software design, implementation and upgrades not covered by this Service Description, including solution redesign, solution expansion, onsite implementation/upgrade assistance etc.
- Custom Security Extended Software enhancements not developed and implemented by Cisco Services.
- Custom Software enhancements post acceptance.

1.2 Supplemental Definitions

- Bug Fix means any modification or revision to the Security Software, other than an Enhancement, that corrects an error or provides other incidental corrections.
- Case means a single support issue and the reasonable effort(s) needed to resolve it such as technical assistance provided by Cisco personnel to Customer regarding questions, clarifications, problems, Bug Fixes, status of a Case and escalation of Case with respect to the Security Software. A single support issue cannot be broken down into subordinate issues. If a Case consists of multiple issues, each subordinate issue shall be considered a separate Case. A Case may require multiple telephone calls and off-line research to achieve final resolution. Cisco has the right to close a Case if Cisco determines: a) the Case is not a problem but an Enhancement request; b) the Case is not a problem but an inherent feature of the product; or c) a workaround was provided for resolution.
- Enhancement(s) means a change, addition or new release, other than Bug Fix to the Security Software that adds new functions or features, or improves functions or performance by changes to system design.
- Services means the Security Software support provided herein.

2.0 Security Software Extended Support

2.1 API Compatibility Maintenance

2.1.1 Service Summary

Cisco will update the Application Programming Interface and/or Security Software for Cisco Products and the Security Software covered in this Service Description and described in the Ordering Documents.

2.1.2 Cisco Responsibilities may include the following:

- Update Security Software or API to continue functioning using the new API.

2.1.3 Customer Responsibilities include:

- Include Cisco in the planning of migrations to the new version of the Cisco Product that would warrant this activity.

2.2 In-House Utility Execution

2.2.1 Service Summary

Cisco will execute the software in-house on a periodic basis to: conduct testing, gather inventory, generate reports, and assist in operating the Security Software, install updates, and similar functions as described in this Service Description and the Ordering Documents.

2.2.2 Cisco Responsibilities may include the following:

- Cisco will execute the software in-house on a periodic basis.
- Cisco will notify customer when the execution completes with summary information relevant to the execution.

2.2.3 Customer Responsibilities include:

- If execution requires customer input, customer must provide such input to Cisco in a timely manner.

2.3 Problem Resolution

2.3.1 Service Summary

The Problem Resolution Service element provides activities to help the Customer resolve identified issues with the Security Software.

2.3.2 Cisco Responsibilities may include the following:

- Perform Tier 2/3 solution-level incident and problem management by managing identified incidents, from escalation to resolution with known fixes or workaround and closure
- Provide minor releases or generate workaround solutions for identified issues with the Security Software covered by this Service using commercially reasonable efforts which may include a patch to the implemented Security Software.

2.3.3 Customer Responsibilities include:

- Provide information to Cisco relevant for incident or problem resolutions. This may include but not be limited to: logs, network information, sample user profiles, network diagrams, etc.
- Provide a test environment similar to the production environment, whereby Cisco and Customer may jointly replicate the problem and test possible resolutions.
- Provide Cisco access to aforementioned test environment.

2.4 Software Upgrade

2.4.1 Service Summary

The Software Upgrade Service provides support for implementing maintenance releases, Enhancements minor releases, and major releases for the Security Software during the service term.

2.4.2 Cisco Responsibilities may include the following:

- Perform configuration and change management by maintaining an inventory of the Cisco managed

elements in the Security Software.

- Coordinate any changes to the Security Software by addressing availability and performance issues as a result of an incident or upon Customer request.
- Implement software patches, minor releases, Enhancements and workaround solutions for identified issues for the Security Software using commercially reasonable efforts.
- Provide a Bug Fix for Security Software experiencing issues along with instructions of how to retrieve Bug Fix. If the electronic medium does not work for the Customer, the Customer may request the Bug Fix be sent next-day delivery service or some other shipment medium.

2.4.3 Customer Responsibilities include:

- Provide information to Cisco relevant for upgrade. This may include but not be limited to: logs, network information, sample user profiles, network diagrams, etc.
- Provide a test environment similar to the production environment, whereby Cisco and Customer may jointly test updates to the Security Software before deploying into production.
- Provide Cisco access to aforementioned test environment.

2.5 General Responsibilities

2.5.1 Cisco Responsibilities may include the following:

- Provide process for Customer to access Security Software Extended Support team, and to the extent necessary, Cisco implementation team access, during Standard Business Hours, five days per week, to assist by electronic mail, or the Internet for use, integration, configuration, and troubleshooting issues.
- Use commercially reasonable efforts to respond to Customer within one (1) hour for Severity 1 and 2 requests calls received during Standard Business Hours
- Use commercially reasonable efforts to respond to Customer on next business day for Severity 3 and 4 requests received during Standard Business Hours and for all requests received outside Standard Business Hours.
- Manage problems according to the Cisco Severity and Escalation Guidelines except where noted in this Service Description.
- Verify (and if needed, update) severity level consistent with Cisco Security Severity and Escalation Guidelines

2.5.2 Customer Responsibilities include:

- Provide severity level as described in the Cisco Security Severity and Escalation Guidelines when contacting Cisco to report a problem with the Security Software
- Provide, at no charge to Cisco, reasonable access to the Security Software through the internet or via VPN to establish a data communication link between Customer and Cisco so issues can be diagnosed and, where possible, corrected remotely.
- Customer is responsible for any hardware required to perform fault isolation.

- Provide current shipment information including contact name, address, telephone number, email address, and fax number.
- Provide Cisco with valid, applicable serial numbers / license key for product covered by this Service experiencing an issue as well as the location details for the software including address and zip code.
- Verify any in-transit damage of Software media shipped to Customer when performing updates.
- Implement the latest Software release and latest third-party releases not covered by the Services, if required by Cisco, to correct a reported issue.
- Make all reasonable efforts to isolate Software issues prior to requesting support from Cisco.
- Use the keyword “Security Software Extended Support” when opening a support case with Cisco.
- Acquire, install, configure, and provide technical support for:
 - Third-party products, including upgrades required for Cisco related services.
 - Network infrastructure, including, but not limited to, local and wide-area data Networks and equipment required by Cisco for operations of software covered by this Service.
- No software packages may be added, and existing software packages must not be modified (either by configuration changes or service-level changes, except for required service upgrades to Windows, Linux, and anti-virus software).
- Designate a single point of contact to act as the primary technical interface to the designated Cisco engineer.
- Ensure key personnel are available to participate during the course of Service delivery to provide information and evaluate issues, as needed.
- Customer shall respond within two (2) Business Days of Cisco’s request for documentation or information necessary to provide this Service, unless otherwise agreed to by Cisco.
- Provide documented information on Customer’s existing network infrastructure design including features and services, route plans, addressing schema, call/data flow, dial plans, security policies, network management, and operational processes.

2.6 Security Software Extended Support Escalation Guideline

Table 1 Security Software Extended Support Escalation Guidelines

Elapsed Time	Severity 1	Severity 2	Severity 3	Severity 4
1 hr.	Solution Engineering Manager			
4 hrs.	Technical Support Director	Solution Engineering Manager		
24 hrs.	VP Cisco Services	Technical Support Director		
48 hrs.	SVP Cisco Services	VP Cisco Services		
72 hrs.			Solution Engineering Manager	
96 hrs.		SVP Cisco Services	Technical Support Director	Solution Engineering Manager

3.0 Assumptions and Additional Terms

- Customer is responsible for determination and implementation of Customer design requirements, implementation of any recommendations provided by Cisco and for determining if the receipt and use of any Services or Deliverables complies with applicable laws. Cisco recommendations are based upon information provided to Cisco at the time of the services. In no event shall Cisco be liable for the accuracy or completeness of the information contained in the Cisco recommendations.
- Service Description should be read in conjunction with the Advanced Services General Assumptions and Exclusions document posted at: www.cisco.com/go/servicedescriptions which is hereby incorporated for reference. To the extent there is a conflict between the terms of this Service Description and such document, the terms of this Service Description shall control.
- All services will be provided in the English language unless otherwise agreed to by Customer and Cisco.
- The basis in which to accept or reject Deliverables is substantial conformance with its specifications or description. Where any Service element contains Deliverables, the Customer will have five business days in which to accept the Deliverables or they are deemed accepted. If Customer rejects any Deliverable, it will notify Cisco in writing of its rejection and provide written details as to basis for the rejection.
- Cisco may collect information about your network and the type of traffic traversing the network (“Network Data”). Network Data does not include the network content. Cisco uses Network Data in order to provide, maintain, improve, market or promote the Services. You acknowledge that Cisco may freely use the Network Data as long as it does not include any network content, is in a form that does not identify or imply Customer or any Customer end users, and is aggregated with other Network Data. In any event, Cisco will comply at all times with applicable law related to Cisco’s collection and use of all Telemetry Data and will use reasonable physical, technical, and procedural means to protect the Network Data in accordance with Cisco’s privacy policy found here: <http://www.cisco.com/c/en/us/about/trust-transparency-center/overview.html>.
- CUSTOM SOFTWARE TERMS AND CONDITIONS

Any software delivered as part of Services is considered to be custom software incidental to the Services (e.g., software adaptors as part of integration Services), and is hereinafter referred to as “Custom Software”. Cisco or its subcontractors(s) own all intellectual property rights and all other proprietary rights, including all derivatives and modifications in and to the Custom Software. Custom Software shall be delivered in object code or script format.

If Custom Software is provided under this SOW, it is licensed in accordance with the terms and conditions set forth in the Agreement.

DISCLAIMER OF WARRANTY AND SUPPORT. NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THE AGREEMENT: (A) THE CUSTOM SOFTWARE IS PROVIDED “AS IS,” AND CISCO MAKES NO WARRANTY, EXPRESS, IMPLIED, OR STATUTORY, AND DISCLAIMS ANY AND ALL WARRANTIES WITH RESPECT TO THE CUSTOM SOFTWARE, IN WHOLE OR IN PART, OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY OR NONINFRINGEMENT AND (B) CISCO SHALL HAVE NO OBLIGATIONS WITH RESPECT TO SUPPORT OR MAINTENANCE, INCLUDING WITHOUT LIMITATION, UPGRADES, UPDATES, MAINTENANCE RELEASES, OR MODIFICATIONS, OF THE CUSTOM SOFTWARE.

