



Service Description: Cisco Security Agent Implementation Service

This document describes Cisco Security Agent Implementation Service.

Related Documents: This document should be read in conjunction with the following documents also posted at 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), Advanced Services Agreement (ASA), or equivalent services agreement executed between you and Cisco. In the event of a conflict between this Service Description and your MSA or equivalent services agreement, this Service Description shall govern.

Sale via Cisco Authorized Reseller. If you have purchased these Services through a Cisco Authorized Reseller, this document is for 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 www.cisco.com/go/servicedescriptions/.

Cisco shall provide the Cisco Security Agent Implementation Service described below as selected and detailed on the Purchase Order for which Cisco has been paid the appropriate fee. Cisco shall provide a Quote for Services ("Quote") setting out the extent of the Services and duration that Cisco shall provide such Services. Cisco shall receive a Purchase Order that references the Quote agreed between the parties and that, additionally, acknowledges and agrees to the terms contained therein.

Service Summary

The CSA Implementation Service offers requirements analysis, planning, design, and implementation consulting to help the Customer design and deploy an effective Cisco Security Agent solution. The scope of this Service is structured into three tiers of user groups as follows:

- Up to 50 CSA licenses and 1 CSA policy group
- 51 to 500 CSA licenses and 1 to 4 CSA policy groups
- Over 500 CSA licenses and/or over 4 CSA policy groups

Cisco Security Agent Implementation Service

Under this Service, Cisco shall provide the Cisco Security Agent Implementation Service during Standard Business Hours, unless stated otherwise. Cisco shall provide the following General Support provisions for Services selected by Customer:

General Support

- Designate an engineer ("Advanced Services Engineer") to act as the primary interface with Customer for its Network.

Detailed Discovery and Analysis

- Team with the Customer to collect and document Customer's business requirements and Network information to be used by the Network design. These may include the following:
 - Cisco Security Agent deployment goals, objectives, and requirements.
 - Features and functionality that are required to meet Customer's business objectives.
 - Analysis of existing network security architecture, design and policies.
 - Analysis of threat levels in all environments where a personal computer is used.
 - Perform system readiness assessment. Cisco will perform a detailed evaluation of Customer's Network's ability to support a Cisco Security Agent solution. The system readiness assessment typically includes, amongst other things, the following:
 - Assessing the readiness of the Customer's Network infrastructure to support the Cisco Security Agent.
 - Reviewing Customer's current security management procedures including security alerts and notification requirements.
 - Reviewing Customer's existing software operations procedures and escalation processes.

- Analyzing key device configurations including firewalls and intrusion detection systems.

Design, Server Build, and Agent Deployment Support

- Low Level Design. Cisco will develop an implementation-ready low-level design for the Customer's CSA solution. Cisco will perform detailed design development, which typically includes, amongst other things, the following:
 - Review CSA infrastructure design.
 - Create appropriate CSA desktop group policies with user-interaction configuration to satisfy business function requirements.
 - Create administrative groups and policies to facilitate ongoing management of the CSA solution.
- Develop Acceptance Test Plan. Cisco will identify the testing processes required to verify the CSA aligns to Customer's identified solution requirements and that the solution is ready for the deployment. Cisco will develop an acceptance test plan which typically includes, amongst other things, the following:
 - Compile and review the following:
 - Customer requirements document
 - Solution requirements document
 - Detailed design document
 - Operations plan document
 - Network readiness remediation plan
 - Operational readiness remediation plan
 - Identify tools required for executing the test cases.
 - Test schedule, test case priorities, test lab topology, role and responsibilities, testing processes, and severity levels.
 - Provide Customer-approved acceptance test plan
- Develop Implementation Plan. Cisco will identify the processes required to implement the solution components and Software in the Customer's Network. Cisco will develop a Network implementation plan which typically includes, amongst other things, the following:
 - Compile required documentation which may include:
 - Site Requirements Specification.
 - Detailed Design.
 - Supplier/customer roles and responsibilities.
 - Site-specific implementation human resource requirements.
 - Site contacts, location and considerations.
 - High level site specific installation requirements.
 - Site specific information from Bill of Materials ("BOM"), and delivery of equipment for staging and/or installation.
 - Third-party support contacts and agreements, in the event that such support is necessary for cutover or migration strategies required for this implementation.
 - Review detailed design with emphasis on order of implementation within Customer's Network.
 - Verify that all time-dependent functions built into the Network implementation schedule align to scheduled delivery and implementation.
 - Identify and add site dependencies to the rollout schedule.
 - Define Customer-agreed deployment parameters that will be used to assess implementation-readiness at each site.
 - Define timelines for post-implementation testing.
 - Create and track actions list.
 - Maintain Issues log.
 - Develop contingency plans.
 - Provide Network implementation schedule.
- Team with the Customer for the CSA controlled deployment in a protected environment. Cisco activities during controlled deployment may include:
 - CSA Management Center server deployment.
 - Creation of CSA installation kit.
 - Assist the Customer's electronic software distribution team with the testing and controlled deployment (i.e., the CSA will be in "Test Mode") of CSA.

Policy Tuning

- Assist the customer with the tuning of CSA policies and resolving system conflicts.
- Run application (i.e., agents).

- Monitor the system, fine tune policies as needed.
- Finish acceptance testing.
- Help the Customer teams with switching CSA to “Protect Mode” for active protection of the Network (i.e., Agents will be enforcing the new policies), and monitor the system. Cisco activities may include providing remote escalation support for technical issues.

Knowledge Transfer

- Provide on-site knowledge transfer session with Customer’s CSA analysts and senior help desk staff during deployment.
- Provide on-site knowledge transfer session with Customer’s server operations team.
- Provide remote knowledge transfer session for CSA help desk staff (up to eight (8) attendees) on CSA troubleshooting.
- Run a workshop with Customer to:
 - Present executive summary of the CSA implementation methodology and production deployment.
 - Run a question and answer session.
 - Perform project closure with Customer.

Documentation

- Document Cisco Security Agent policies and operational procedures

Service Responsibilities of Customer

Customer shall comply with the following obligations:

- Provide a list of all of the networking components including but not limited to Hardware, Software and solution configurations;
- Provide a high-level architectural drawing showing the type of Hardware, Software, and application solutions configurations and where they are physically located (for example, geographical location or location within the Network);
- Detailed definitions of the type of application (for example mobile traveler, corporate workforce or verticals) and features; detailed definition of Customer’s implementation strategy and schedule;
- Provide copies of product configuration templates.
- Provide a network topology map, configuration information, and information of new features being implemented as needed.
- Retain overall responsibility for any business process impact and any process change implementations
- Ensure key Customer networking and operational personnel are available to participate in interview sessions as required.
- Unless otherwise agreed to by the parties, Customer shall respond within two (2) business days of Cisco’s request for documentation or information needed for the Service.
- Customer acknowledges that Cisco’s obligation is to only provide assistance to Customer with respect to the tasks detailed and that such assistance may not result in some or all of the tasks being completed.