



Service Description: Cisco IronPort – Onsite Email Security Appliance Installation

This document describes the Cisco IronPort Systems LLC (“IronPort”) Onsite Email Security Appliance Installation services (“Services”) to be performed for the customer (“Customer”) pursuant to an appropriately accepted purchase order reflecting the IronPort Services SKU: **PRO-SER-ONSITE-ESA**.

Direct Sale from IronPort. If you have purchased these Services directly from IronPort, this document is incorporated into your Product Sales and Services Agreement or other master services agreement covering Advanced Services between IronPort and Customer (“Agreement”), or if no such Agreement exists, then the terms and conditions set forth in the IronPort Standard Terms and Conditions of Sale (and AS Addendum) posted under the IronPort offerings heading at www.cisco.com/legal/services.html, which is hereby incorporated into and made a part hereof by this reference.

Sale via Authorized Reseller. If you have purchased these Services through an authorized reseller, this document is for description purposes only; and the contract, if any, governing the provision of the Service 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 under the IronPort offerings heading posted at: www.cisco.com/legal/services.html.

Project Objective and Scope

Project Objectives and Scope: The project objective is to install, configure, and test the IronPort Email Security Appliance (ESA) email gateway security solution in the Customer production environment and to provide ‘side-by-side’ training to Customer team member(s) responsible for managing the system.

Installation Services / Appliances: The following IronPort products are to be installed and configured:

- IronPort Email Security Appliance (ESA): [up to 2 appliances]
- IronPort Secure Management Appliance (SMA): [up to 1 appliance]

Responsibilities and Limitations

IronPort Responsibilities:

IronPort will be responsible for the following activities during the installation:

- Pre-Installation Consulting and Project Planning
- Messaging Architecture and IronPort System Design
- Evaluation Unit Installation and Initial Configuration
- Evaluation Unit Hands-On Training
- Evaluation Unit Tuning (altering configuration for more aggressive spam filtering)
- LDAP/AD Integration
 - Recipient Verification Configuration
 - Email Routing Configuration
- Customer-Specific Policy Configuration
- Message Filter and Content Filter Design and implementation
 - Attachment Filtering and Acceptable-Use Policies
 - Customer-specific Contents Scanning Options
- Outbound Policy Configurations:
 - Configuration of Smarthost (if required)
 - Configuration of PXE via CRES (if required)
 - Configuration of TLS delivery (if required)
 - Basic configuration of DLP services (if required)
- Configuration of Centralized Management (if required)
- SMA Configuration:
 - Configuration of Centralized Reporting (if required)
 - Configuration of Centralized Quarantine (if required)
 - Configuration of Centralized Message Tracking (if required)
- Hands-On Training (Overview of the Management Interface)
- Solution testing
- Production Cutover Planning Discussion
- Post-Installation Follow-up

Customer Responsibilities:

Prior to the Onsite Installation, the Customer team is expected to have performed the following:

- All non-ESA solution components procured, installed, and configured.
- ESAs racked and placed onto the Customer network.
- SMA racked and placed onto the Customer network (if required)
- Firewalls configured such that:
 1. Port 80/443 opened to the ESAs from within Customer network.
 2. Port 80/443 to the internet open for updates.

3. SSH / SCP access to the ESAs from the installation desktop is allowed.
 4. Port 389 (or as required) opened between ESAs and any LDAP server, if required.
- Port 25 between internet and ESAs opened
 - Port 25 between Customer mail server and ESAs opened
 - The 'Pre-Arrival Checklist' (to be provided by IronPort) is reviewed and returned to IronPort.

In addition, during any time that IronPort is onsite, the IronPort team will require:

- Internet access from a machine within the Customer environment
- Standard telephone access; physical desk space (for 1 person)
- Access to IronPort devices to be configured

Limitations:

The following activities are outside the scope of this Services Description and require a separate professional engagement for completion:

- Configuration of policies based LDAP Group membership
- DKIM/Domain Keys Configuration
- SSL Certificate Configuration
- Inbound TLS Configuration
- SMTP Authentication Configuration
- Optimization and customization of DLP Policies
- Migrating policies from previous mail security solutions
- Integration with third party services (such as but not limited to Vontu, PGP, etc)
- Custom filtering policies
- Custom PXE and CRES configurations (i.e. custom logo, TLS-Reply deliveries, etc.)
- External User Authentication

Assumptions

The following assumptions underlie the effort and schedule defined above:

- IronPort is normally able to begin a project of this scope within 5 days of the negotiated date between Customer and IronPort.
- Installation will occur on up to 2 ESAs, and 1 SMA, installed at a single location.
- All Customer preparation steps (listed above) will be performed prior to the planned start date.
- Team member responsible for owning the solution will be assigned to the project on a full time basis.
- The solution will not integrate with any Customer system unless specifically stated within this Services Description.

- Complex policy implementations may require additional Services, which will be negotiated separately.
- The configuration of any component other than IronPort devices is outside the scope of this Services Description.
- Customer must ensure that all relevant personnel and participants are available during the course of the Services to assist if network related issues are encountered and for any necessary knowledge transfer.
- All information (such as, but not limited to: designs, topologies, requirements) provided by Customer is assumed to be valid and up-to-date for Customer's current environment. IronPort Services are based upon information provided by Customer at the time of the Services.
- Customer must have installed and tested network and Internet connectivity to the site of the installation prior to commencement of Services.

Additional Costs

For Onsite Services, all costs incurred by IronPort for travel to a single Customer installation site will be included in the cost of the Services.

Please Note: The parties recognize that IronPort's ability to perform the Services or meet schedule estimates is dependent upon Customer satisfying its obligations hereunder in a timely manner. Any additional costs for services beyond the scope, including any costs incurred as a result of Customer not taking the necessary preparation steps or other schedule delays outside of IronPort's control, will be performed on a time and materials basis on an agreed upon schedule at rates specified in the IronPort Services price list at the time of such work.

Completion Confirmation

IronPort will provide an email notification upon completion of the Services to Customer. The Customer shall within five (5) Business Days of receipt of such notification provide written acknowledgement via email of IronPort's completion of the Services.

Customer's failure to acknowledge completion or to provide reasons for rejection of the Services within the five (5) Business Day period, signifies Customer's acceptance of completion of the Services in accordance with this Services Description.