Cisco IronPort Email Security Plug-in 7.3 Administrator Guide

May 01, 2013

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco IronPort Email Security Plug-in 7.3 Administrator Guide

CONTENTS

CHAPTER 1

Getting Started with the Cisco IronPort Email Security Plug-in

This chapter contains the following sections:

What's New in this Release

This release includes the following new features:

- Ability to configure Cisco Ironport Email Security Plug-in to use a Cisco Ironport Encryption appliance (IEA) or Cisco Registered Envelope Service (CRES) as the hosted key server.
- Outlook 2010 64-bit Support.
- **Automatic Configuration**. The Cisco Ironport Email Security Plug-in is automatically configured by an XML file attachment received from the administrator.
- **Configuration Per Email Account**. The Cisco Ironport Email Security Plug-in is deployed in three modes that determine the configuration per email account as Decrypt Only, Flag, or Encrypt.

- **Desktop Encryption Secure Envelope Options**.
  - **Lock or unlock encrypted email**. The end user is able to lock or unlock encrypted email. They can also set and modify the reason for locking the encrypted email.
  - **Set the expiration date and time for encrypted email**. The end user can set or clear an expiration date and time.

Supported Configurations

The *Cisco Encryption Compatibility Matrix* lists the supported operating systems and can be accessed from the following URL:

http://www.cisco.com/en/US/docs/security/iea/Compatibility_Matrix/IEA_Compatibility_Matrix.pdf

Related Documents

To use the Encryption plug-in, you need to have a Cisco IronPort Encryption appliance running and properly configured to work with the Encryption plug-in or have a Cisco Registered Envelope Service (CRES) account. To understand how to configure the Cisco IronPort Encryption appliance, you may want to review the following guides:

- *IronPort Encryption Appliance Installation Guide*. This guide provides instructions for installing and configuring email encryption, and it may help you to understand how to configure your encryption appliance settings to work with the plug-in settings you configure. See:

http://www.cisco.com/en/US/products/ps10154/prod_installation_guides_list.html

To better understand how Cisco IronPort Email Security works, you may want to review some basic information about how email is classified as spam, virus, or as non-spam. For more details on these subjects, you may want to review the following guide:

- *Cisco IronPort AsyncOS for Email Configuration Guide*. This guide contains information on spam and virus protection. Users can improve the efficacy of the SenderBase network by employing the spam and virus plug-in. When users marks an email as “spam,” “virus,” or “not spam,” they can train the filters to become more effective and improve the performance of all Cisco IronPort appliances. See:

http://www.cisco.com/en/US/products/ps10154/products_user_guide_list.html

How to Use This Guide

Use this guide as a resource to learn about the features in your Cisco IronPort Email Security Plug-in. The topics are organized in a logical order, but you might not need to read every chapter in the book. Review the Table of Contents and the section called How This Book Is Organized, page 1-3 to determine which chapters are relevant to your particular configuration.

This guide is distributed electronically as a PDF. The electronic versions of the guide are available on the Cisco IronPort Customer Support Portal. You can also access an HTML online help tool in the appliance GUI:

- In Outlook 2010, go to **Tools** > **Options** > **Cisco Email Security**. Click the **Help** button in Outlook, then click **Actions** > **Cisco Email Security.**
- In Outlook 2003/2007, go to **Tools** > **Options** > **Cisco Email Security** > **Help**.

How This Book Is Organized

Chapter 1, “Getting Started with the Cisco IronPort Email Security Plug-in” provides an introduction to the Cisco IronPort Security plug-in and defines its key features and role in network security configurations. New features of the current release are described along with information about other resources for information and support contact information.

Chapter 2, “Overview” introduces the Reporting Plug-in and the Encryption plug-in. This section provides an overview of each of these tools.

Chapter 3, “Performing a Mass Installation” describes how to perform a mass installation. The instructions provide steps for running the install.

Chapter 4, "Configuring and Using the Cisco IronPort Email Security Plug-in for Outlook" provides instructions for configuring the Cisco IronPort Email Security Plug-in for Outlook. It includes steps for installing the encryption plug-in, sending or receiving encrypted email, and managing secure messages.

Appendix A, "Cisco IronPort Systems, LLC Software License Agreement" contains detailed information about the licensing agreements for Cisco IronPort products.

Where to Find More Information

Cisco offers the following resources to learn more about the Cisco IronPort Email Security Plug-in.

Security Training Services & Certification

Cisco Security Training Services deliver exceptional education and training for Cisco security products and solutions. Through a targeted curriculum of technical training courses, the program provides up-to-date knowledge and skills transfer to different audiences.

Use one of the following methods to contact Cisco Security Training Services:

Training. For question relating to registration and general training:

- http://training.ironport.com
- stbu-trg@cisco.com

Certifications. For questions relating to certificates and certification exams:

- http://training.ironport.com/certification.html
- stbu-trg@cisco.com

Knowledge Base

You can access the Cisco IronPort Knowledge Base on the Cisco IronPort Customer Support site at the following URL:

http://www.cisco.com/web/ironport/knowledgebase.html

The Knowledge Base contains a wealth of information on topics related to Cisco IronPort products.

Articles generally fall into one of the following categories:

- **How-To.** These articles explain how to do something with a Cisco IronPort product. For example, a how-to article might explain the procedures for backing up and restoring a database for an appliance.
- **Problem-and-Solution.** A problem-and-solution article addresses a particular error or issue that you might encounter when using a Cisco IronPort product. For example, a problem-and-solution article might explain what to do if a specific error message is displayed when you upgrade to a new version of the product.
- **Reference.** Reference articles typically provide lists of information, such as the error codes associated with a particular piece of hardware.
- **Troubleshooting.** Troubleshooting articles explain how to analyze and resolve common issues related to Cisco IronPort products. For example, a troubleshooting article might provide steps to follow if you are having problems with DNS.

Cisco Support Community

Cisco Support Community is an online forum for Cisco customers, partners, and employees. It provides a place to discuss general email and web security issues, as well as technical information about specific Cisco products. You can post topics to the forum to ask questions and share information with other Cisco and Cisco IronPort users.

You can access the Cisco Support Community from the following URL:

https://supportforums.cisco.com

Cisco Customer Support

Note The level of support available to you depends upon your service level agreement. Cisco IronPort Customer Support service level agreement details are available on the Support Portal. Check this page for details about your level of support.

You can request support by phone, email, or online 24 hours a day, 7 days a week. You can contact Cisco Customer Support using one of the following methods:

- Cisco Support Portal: http://www.cisco.com/support
- Phone support: Contact Cisco Technical Assistance Center (TAC) within U.S. /Canada at 800-553-2447 and at Worldwide Phone Numbers.
- Email: tac@cisco.com

If you purchased support through a reseller or another supplier, please contact that supplier directly with your product support issues.

Cisco Content Security Welcomes Your Comments

The Cisco Content Security Technical Publications team is interested in improving the product documentation. Your comments and suggestions are always welcome. You can send comments to the following email address:

`contentsecuritydocs@cisco.com`

Cisco IronPort Email Security Plug-in Overview

The Cisco IronPort Email Security Plug-in installs reporting and encryption menus onto Outlook Email. The reporting plug-in enables users to submit feedback about the type of mail they receive (for example, users can report spam, phishing, and virus emails), and the encryption plug-in places an “encrypt message” button on the toolbar which enables users to either send encrypted email from their email programs or to flag the email to be encrypted before it leaves their organizations.

When the Cisco IronPort Email Security Plug-in is installed, it enables components on an Outlook mail client. This single interface allows end-users to seamlessly report emails or send encrypted email. End users can lock or unlock encrypted emails, adding or modifying a lock reason. End users can also set an expiration date and time for the encrypted email. Combining these plug-ins simplifies installation and provides a single interface for users and Administrators to install and modify.

The reporting and encryption plug-ins provide a convenient interface that enables you to submit feedback and send encrypted messages by using toolbar buttons and right-click context menus. If you are using the reporting plug-in to report a message, a dialog box appears indicating that the message was submitted. The Encryption Plug-in places an **Encrypt Message** button in the menu bar of an email message to provide an easy way for senders to email encrypted messages. The Encryption plug-in requires the presence and proper configuration of a Cisco IronPort Encryption appliance or have a Cisco Registered Envelope Service (CRES) account.

CHAPTER 2

Overview

The Cisco IronPort Email Security Plug-in framework supports several Cisco IronPort Email Security Plug-ins, including the Reporting plug-in and the Encryption plug-in.

This chapter contains the following sections:

The Cisco IronPort Email Security Plug-in

The Cisco IronPort Email Security Plug-in consists of two commonly used email security plug-ins: the Reporting plug-in and the Encryption plug-in. You may deploy the Cisco IronPort Email Security Plug-in on your Outlook email program. When you deploy the Cisco IronPort Email Security Plug-in, it installs one or both of the following applications:

- **The Reporting Plug-in**. The Reporting Plug-in enables Outlook users to submit feedback to Cisco IronPort Systems about unsolicited and unwanted email messages, such as spam, viruses, and phishing messages. For details, see The Reporting Plug-in, page 2-2.
- **The Encryption Plug-in**. The Encryption Plug-in places an Encrypt Message button in the menu bar of an email message to provide an easy way for a sender to mark a message to be encrypted. For details, see The Encryption Plug-in, page 2-2.

The Reporting Plug-in

The Reporting Plug-in enables Outlook users to submit feedback to Cisco IronPort Systems about unsolicited and unwanted email messages, such as spam, viruses, and phishing messages. Cisco IronPort uses this feedback to update its filters to stop unwanted messages from being delivered to your inbox.

You can also report false positives, which are legitimate email messages that are marked as spam, to IronPort Systems by using the Not Spam button. Legitimate email messages are often referred to as "ham." Cisco uses reports about false positives to adjust its spam filters to avoid misclassifying legitimate email in the future. Any valid email can be reported as **Not Spam** and will help to increase filter efficacy.

This plug-in provides a convenient interface that enables you to submit feedback by using toolbar buttons and right-click context menus. When you report a message, a dialog box appears indicating that the message was submitted. The message data that you submit is used by automated systems to improve the Cisco IronPort filters. By submitting message data, you help to reduce the volume of unsolicited email in your inbox.

The Encryption Plug-in

The Encryption Plug-in places an **Encrypt Message** button in the menu bar of an email message to provide an easy way for senders to mark messages to be encrypted and secured before it leaves the organization.

There are two types of encryption available: Flag Encryption and Desktop Encryption. The Flag Encryption option allows you to flag the email for encryption, and the email is encrypted by the Cisco IronPort Encryption appliance or Email Security appliance before the email is sent out of the network. Desktop

Encryption allows you to encrypt email from within your email program using the Cisco IronPort encryption technology. Then, it sends the encrypted email from your desktop. You may want to use Desktop Encryption if you want to ensure that mail sent *within* your organization is encrypted.

The Encryption plug-in is designed to work with a functioning and configured Cisco IronPort Encryption appliance or a Cisco IronPort Email Security appliance (if you have one in your network). The configuration you use for the Encryption plug-in should be developed in conjunction with the settings on these appliances. If you do not use the same configurations for these appliances, issues may occur when sending encrypted messages.

Installing the Plug-in

To install the Cisco IronPort Email Security Plug-in for groups of users, you will likely want to perform a silent installation. A silent installation allows you to perform an installation without prompting the end user for input. For instructions on performing the silent installation, see Chapter 3, "Performing a Mass Installation."

Configuration Modes

The Cisco IronPort Email Security Encryption Plug-in is deployed in three separate configuration modes. The default configuration mode is Decrypt Only.

In order to enable the other configuration modes, the Outlook email account is configured by an updated attachment file received from the administrator. The administrator sends a *BCE_Config_signed.xml* file attachment to the end user's email account. The end user will receive this file as a *securedoc.html* file. When the end user clicks the *securedoc.html* attachment, the Outlook application detects the configuration information attached to the message and applies the updated configuration.

Note The default envelope name is *securedoc.html*.The attachment name value can be changed by the administrator and the envelope will reflect the newly specified name.

The three configuration modes are:

- **Decrypt Only**—Allows decrypting of secure email messages received.
- **Decrypt and Flag**—Allows decrypting and flagging of secure emails messages. The flag option allows the end user to flag the email for encryption, and the email is encrypted by the Cisco IronPort Encryption appliance or Email Security appliance before the email is sent out of the network. The server must be configured to detect the flagged messages and encrypt them at the server.
- **Decrypt and Encrypt**—Allows encrypting and decrypting of secure email messages.

The following table specifies which features are supported in each configuration mode.

Feature	Decrypt Only	Decrypt and Flag	Decrypt and Encrypt
Send encrypted message			X
Flag message for encryption		X	
Open encrypted email	X	X	X
Reply/Reply All/Forward Message			X
Email lock and unlock			X
Email expiration			X
Email diagnostic (Uses for Reporting and Encryption Plug-ins)	X	X	X
Read-receipt			X
Envelope settings			X
Settings	X	X	X

Deploying the Cisco IronPort Email Security Plug-in with the Cisco Registered Envelope Service (CRES) Key Server

Use the following instructions to deploy the Cisco IronPort Email Security Plug-in so that it is used directly with the Cisco Registered Email Service (CRES) key server.

To begin, log into your CRES account: https://res.cisco.com/admin and go to the **Accounts** tab. Select the account from which you want to enable the Email Security Plug-in. Then, go to the **BCE Config** tab.

Step 1 Choose the token to use with the configuration template:

- **CRES**—Select if your key server is CRES.
  - **SecureCompose**—Do not choose this option as your CRES token.
  - **Token <Account number>**—Choose this option as your CRES token.

Step 2 Click **Download Template** to download the template file in order to edit it. The filename is *BCE_Config.xml*.

Step 3 Edit the configuration file.

The *BCE_Config.xml* file contains detailed instructions for the fields you will need to edit based on your particular environment. Open the file in a text editor and follow the instructions included in the comments to make the necessary modifications.

Note For localization purposes, do not change or reword the existing Message Security labels Low, Medium, or High.

Step 4 Click **Browse** to navigate to the edited *BCE_Config.xml* file, and click **Upload and Sign** after you have located the file.

Once the configuration file is signed, the signed version will be downloaded as *BCE_Config_signed.xml*. Save this file to your local machine.

Step 5 To deploy the configuration file to many end users at once, use the **Distribute Signed Configuration to Bulk List** option. To do so:

a. Browse to the *BCE_Config_signed.xml* file created in Step 4.

b. Browse to a comma separated file containing the email addresses of end users.

c. Change the email subject as needed.

d. Click **Distribute Config**.

Note If the xml configuration file is forwarded to another end user, versus received from the administrator, the auto configuration will not work and an error is received.

Note Do not send the *BCE_Config_signed.xml* file to a mailing list. CRES does not support mailing lists.

Deploying the Cisco IronPort Email Security Plug-in with the IronPort Encryption Appliance (IEA) Key Server

Downloading the IEA Key Server Token

The IEA token is needed for use during the configuration signing process. Before signing the configuration file, download the token to your local machine.

To download the token file from the IEA key server:

Step 1 Log into your IEA administration console: https://<IEA_hostname>/admin. The Administration Console displays.

Step 2 Go to the **Accounts** tab. Go to the account to use with your plug-in installations. This is usually the **Users** account.

Step 3 Go to the **Tokens** tab. Click the Save Token icon (looks like a circle with a down arrow) to the right of the token and save it to your local machine.

Customizing and Signing the Configuration File

Once the IEA token file has been downloaded, the configuration file can be customized and signed. The Cisco Registered Envelope Service (CRES) is a hosted service that provides support for Cisco IronPort Encryption Technology. Because the plug-in configuration file signature verification is performed by the CRES system, customers using an IEA as their key server who want to deploy the Cisco IronPort Email Security Plug-in will also need an administrator account on CRES. If you need a CRES administrator account created for you, contact Cisco IronPort Customer Support at: http://www.cisco.com/web/ironport/index.html

To create a signed configuration file for use with the IEA key server:

Step 1 Log into your CRES account: https://res.cisco.com/admin. The Administration Console displays.

Step 2 Go to the **Accounts** tab and select the account from which you want to enable the Email Security Plug-in. Then, go to the **BCE Config** tab.

Step 3 Choose **IEA** as the token type, then upload the IEA token you previously downloaded from the IEA.

Step 4 Click **Download Template** to download the template file in order to edit it. The filename is *BCE_Config.xml*.

Step 5 Edit the configuration file.

The *BCE_Config.xml* file contains detailed instructions for the fields you will need to edit based on your particular environment. Open the file in a text editor and follow the instructions included in the comments to make the necessary modifications.

Note For localization purposes, do not change or reword the existing Message Security labels Low, Medium, or High.

Step 6 Click **Browse** to navigate to the edited *BCE_Config.xml* file, and click **Upload and Sign** after you have located the file.

Once the configuration file is signed, the signed version will be downloaded as *BCE_Config_signed.xml*. Save this file to your local machine.

Note Do not use Step 5 on the BCE config tab **Distribute Signed Configuration File to Bulk List** (optional) when using the IEA as key server. This option only applies to CRES and will be removed in a future release.

Deploying the Configuration File to the End User

To deploy the configuration file to end users, send the signed configuration file in an email encrypted on the IEA to each end user. The message must be sent from an email address that is listed as an administrator on the IEA and on the CRES account.

Note If the xml configuration file is forwarded to another end user, versus received from the administrator, the auto configuration will not work and an error is received.

Note Do not send the *BCE_Config_signed.xml* file to a mailing list. CRES does not support mailing lists.

To perform a mass installation using the *BCE_Config_signed.xml* file, see Mass Installation Using the BCE_Config.xml File, page 3-18.

Configuring Settings for the Cisco IronPort Email Security Plug-in

After you install the Cisco IronPort Email Security Plug-in, you can make configuration changes from the Cisco Email Security tab in Outlook.

- In Outlook 2010, go to **File > Options > Add-ins > Add-in Options > Cisco Email Security**.
- In Outlook 2003/2007, go to **Tools > Options > Cisco Email Security**.

You can make changes to the Reporting plug-in installation or the Encryption plug-in installation. Or, you can make changes to general options that affect both plug-in installations. For example, you can enable or disable logging for the Cisco IronPort Email Security Encryption Plug-in or you can modify options for a specific encryption mode.

To change the method for marking email for Encryption, you need to make changes to the *BCE_Config.xml* file and perform an auto-configuration. Any of the specified settings must be compatible with your Cisco IronPort Encryption appliance.

To make configuration changes on an Outlook installation, see Chapter 4, "Configuring and Using the Cisco IronPort Email Security Plug-in for Outlook."

TCP/IP Services Required for the Cisco IronPort Email Security Plug-in

Cisco IronPort Email Security Plug-in requires the use of the following TCP/IP services and their associated ports. These ports must be left available for the TCP/IP services to use.

- DNS (Domain Name System).

  The DNS service translates Internet domain and host names to IP addresses. DNS automatically converts the names we type in our Web browser address bar to the IP addresses of Web servers hosting those sites.

  Port number: 53 (TCP/UDP)

For more information, see:
http://en.wikipedia.org/wiki/Domain_Name_System

Impact: High

Resolution: This service must be accessible to all end users.

- SMTP (Simple Mail Transfer Protocol)

  Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.

  Port number: 25, 587, 465, 475, 2525 (TCP)

  For more information, see:
  http://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

  Impact: High

  Resolution: This service must be accessible to all end users.

- DHCP (Dynamic Host Configuration Protocol)

  DHCP is a network protocol used to configure devices that are connected to a network (known as hosts) so they can communicate on that network using the Internet Protocol (IP)

  Port number: 67, 68 (TCP/UDP)

  For more information, see:
  http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

  Impact: High

  Resolution: This service must be accessible to all end users which obtain IP addresses automatically from DHCP server.

- Net BIOS over TCP/IP

  NetBIOS over TCP/IP (NBT, or sometimes NetBT) is a networking protocol that allows legacy computer applications relying on the NetBIOS API to be used on modern TCP/IP networks.

  Port number: 137(UDP) (name services), 138(UDP) (datagram services), 139(TCP) (session services)

  For more information, see:
  http://en.wikipedia.org/wiki/NetBIOS_over_TCP/IP

  Impact: High

  Resolution: This service must be accessible to all end users.

- HTTP (Hypertext Transfer Protocol)

  The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems.

  Port number: 80, 8080 (TCP)

  For more information, see:
  http://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol

  Impact: High

  Resolution: This service must be accessible to all end users.

- HTTPS (Hypertext Transfer Protocol Secure)

  HTTPS is a communications protocol for secure communication over a computer network, with especially wide deployment on the Internet.

  Port number: 443 (TCP)

  For more information, see:
  http://en.wikipedia.org/wiki/HTTP_Secure

  Impact: High

  Resolution: This service must be accessible to all end users.

- IMAP (Internet message access protocol)

  Internet message access protocol allows an e-mail client to access e-mail on a remote mail server.

  Port number: 143, 993 (TCP)

  For more information, see:
  http://en.wikipedia.org/wiki/Internet_Message_Access_Protocol

  Impact: High

  Resolution: This service must be accessible to all end users.

- POP3 (Post Office Protocol)

  Post Office Protocol is used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection.

  Port number: 110, 995 (TCP)

  For more information, see:
  http://en.wikipedia.org/wiki/Post_Office_Protocol

  Impact: High

Resolution: This service must be accessible to all end users.

CHAPTER 3

Performing a Mass Installation

This chapter describes how to perform a mass installation on multiple desktops and contains the following sections:

- Performing the Installation, page 3-1
- Using Custom Configuration Files, page 3-15

Performing the Installation

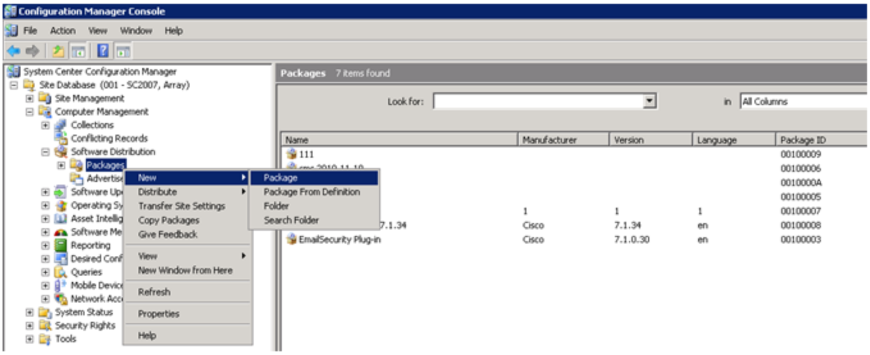
To perform the installation, complete the following steps to create a network shared folder, distribution package, New Package Wizard and New Program Wizard.

To perform the installation:

Step 1 Create a network shared folder that contains the installation package and give users access to the shared folder.

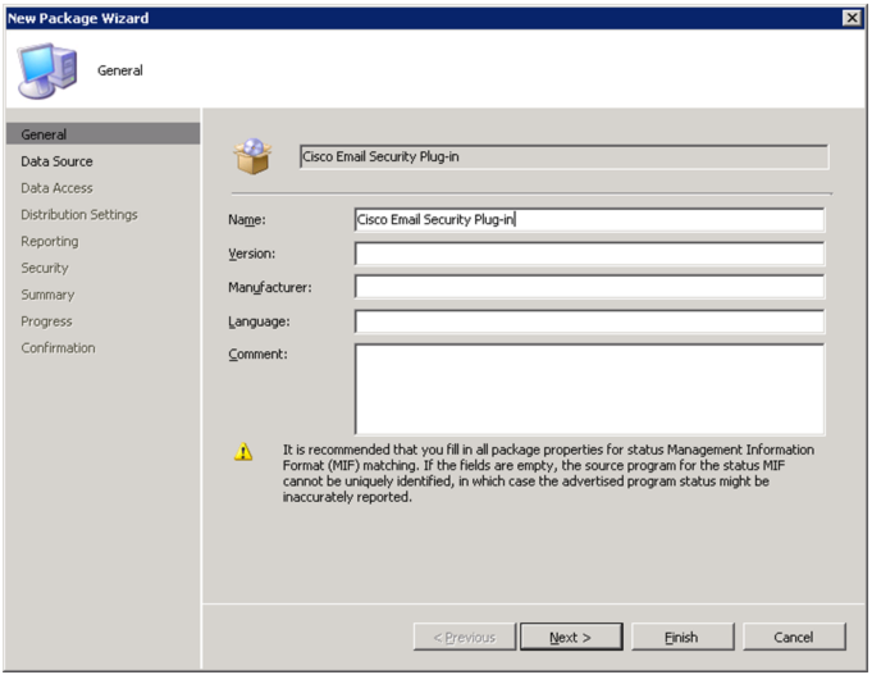
Step 2 Open the SCCM administrative tool.

Step 3 Create a new software distribution package.



Name	Manufacturer	Version	Language	Package ID
111				00100009
sms 2010 11 10				00100006
				0010000A
				00100005
	1	1	1	00100007
7.1.34	Cisco	7.1.34	en	00100008
EmailSecurity Plug-in	Cisco	7.1.0.30	en	00100003

Step 4 Enter a name for the package, and click **Next**.



Cisco Email Security Plug-in

Name: Cisco Email Security Plug-in

Version:

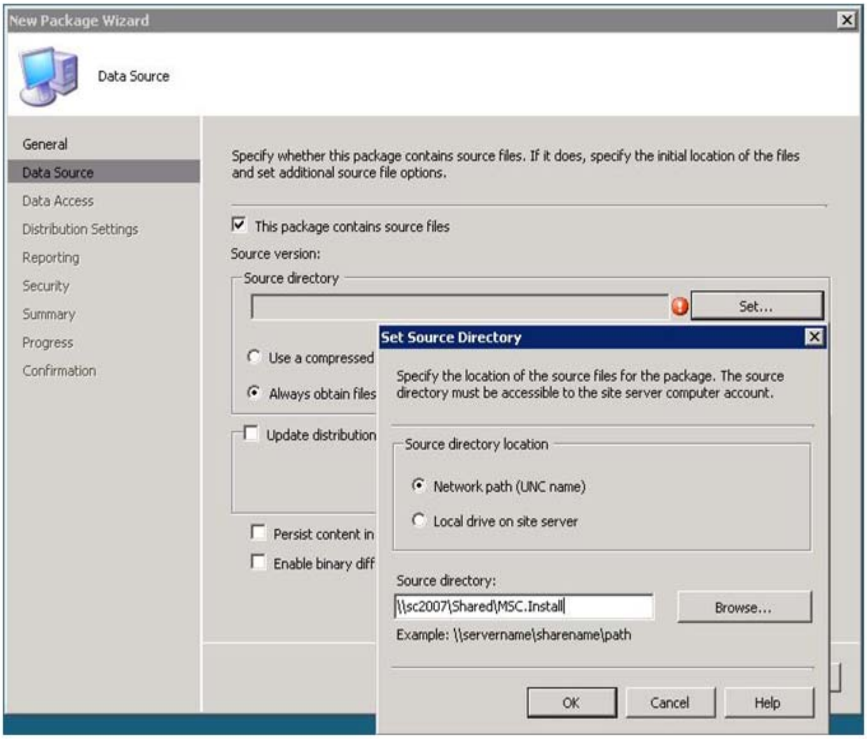
Manufacturer:

Language:

Comment:

It is recommended that you fill in all package properties for status Management Information Format (MIF) matching. If the fields are empty, the source program for the status MIF cannot be uniquely identified, in which case the advertised program status might be inaccurately reported.

Step 5 Specify the network source directory that you created in Step 1 by entering the path to the network shared folder. You can enter the path or browse to the folder. Click **Next**.



Specify whether this package contains source files. If it does, specify the initial location of the files and set additional source file options.

☑ This package contains source files

Source version:

Source directory

○ Use a compressed

● Always obtain files

☐ Update distribution

☐ Persist content in

☐ Enable binary diff

Specify the location of the source files for the package. The source directory must be accessible to the site server computer account.

Source directory location

● Network path (UNC name)

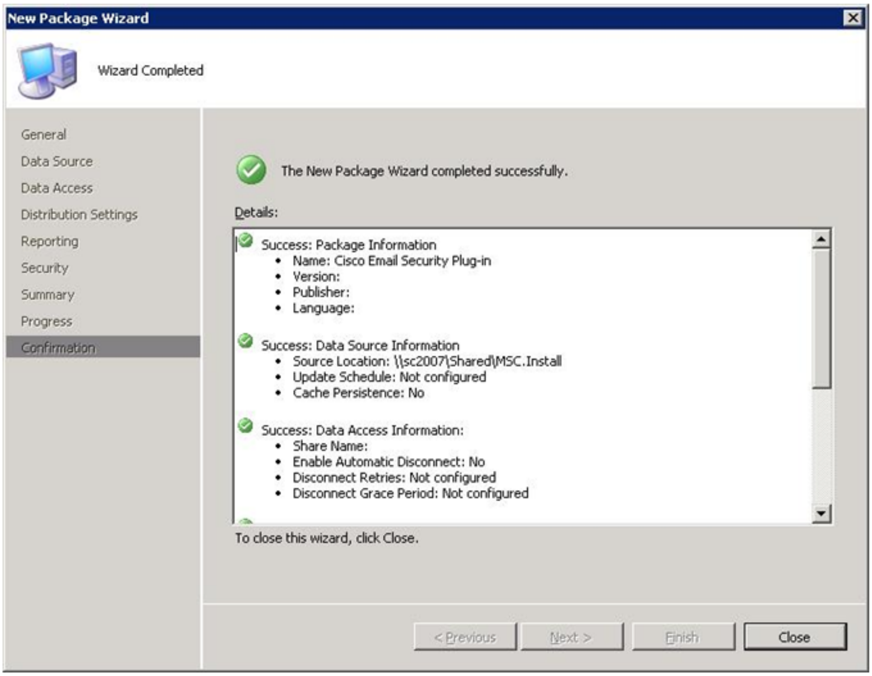
○ Local drive on site server

Source directory: \\sc2007\Shared\MSC.Install

Example: \\servername\sharename\path

Step 6 Continue to the next step in the New Package Wizard, and click **Next**.

Step 7 View the confirmation that the New Package Wizard completed successfully, and click **Close**.



New Package Wizard

Wizard Completed

✓ The New Package Wizard completed successfully.

Details:

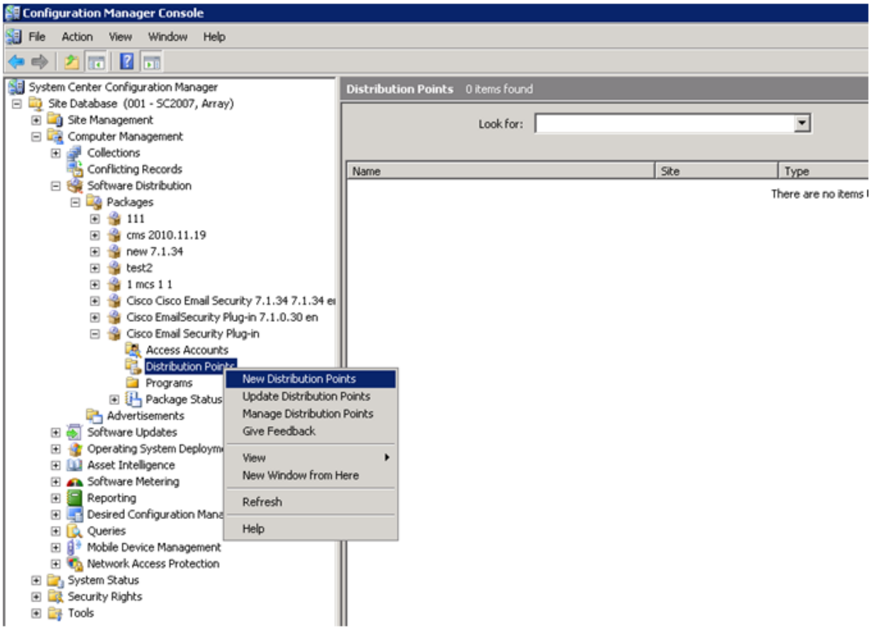
✓ Success: Package Information
- Name: Cisco Email Security Plug-in
- Version:
- Publisher:
- Language:

✓ Success: Data Source Information
- Source Location: \\sc2007\Shared\MSC.Install
- Update Schedule: Not configured
- Cache Persistence: No

✓ Success: Data Access Information:
- Share Name:
- Enable Automatic Disconnect: No
- Disconnect Retries: Not configured
- Disconnect Grace Period: Not configured

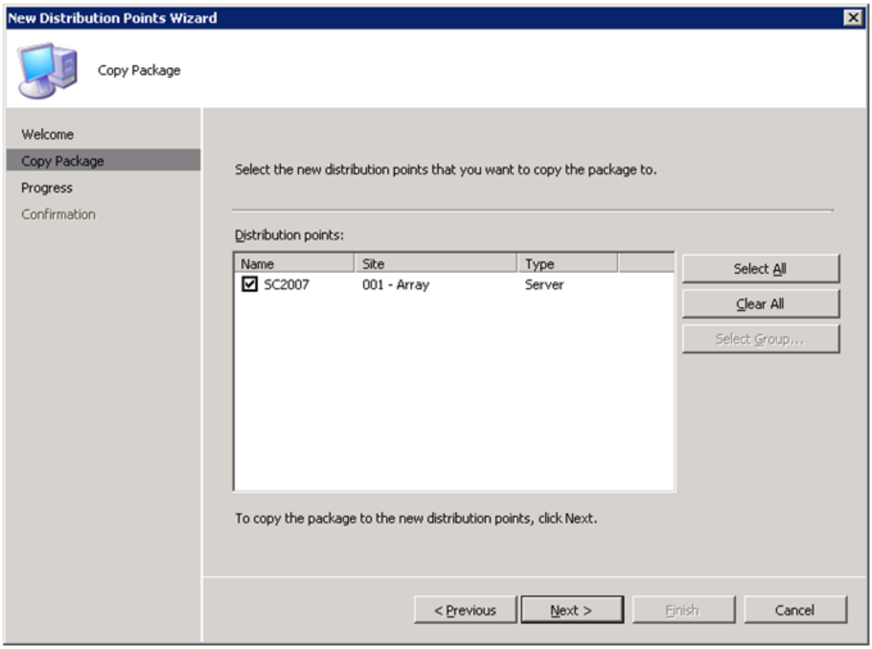
To close this wizard, click Close.

Step 8 Create a new distribution point, and click **Next** on the Welcome page.



There are no items t

Step 9 Select the new distribution point. Click through the next pages on the New Distribution Points Wizard, and click **Close**.



New Distribution Points Wizard

Copy Package

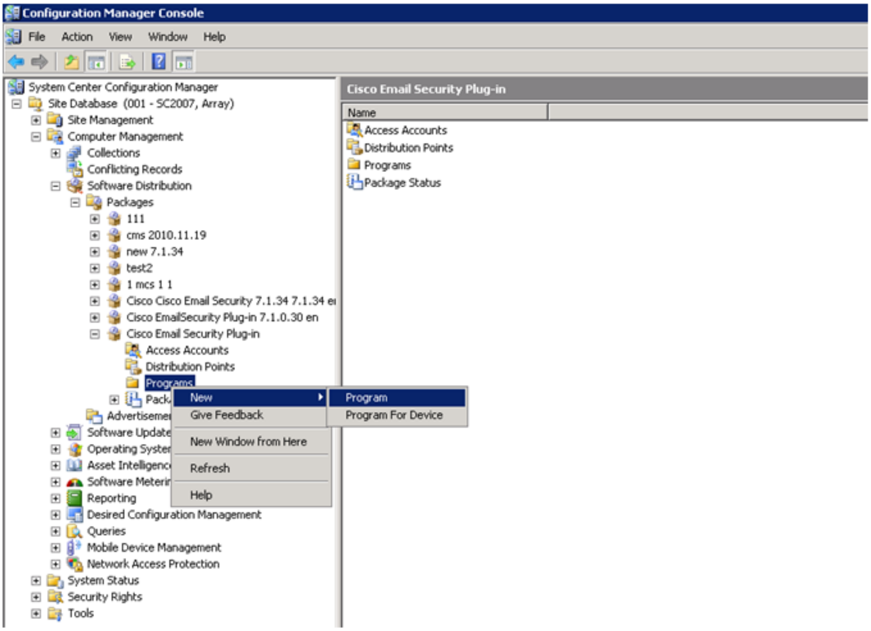
Select the new distribution points that you want to copy the package to.

Distribution points:

Name	Site	Type
☑ SC2007	001 - Array	Server

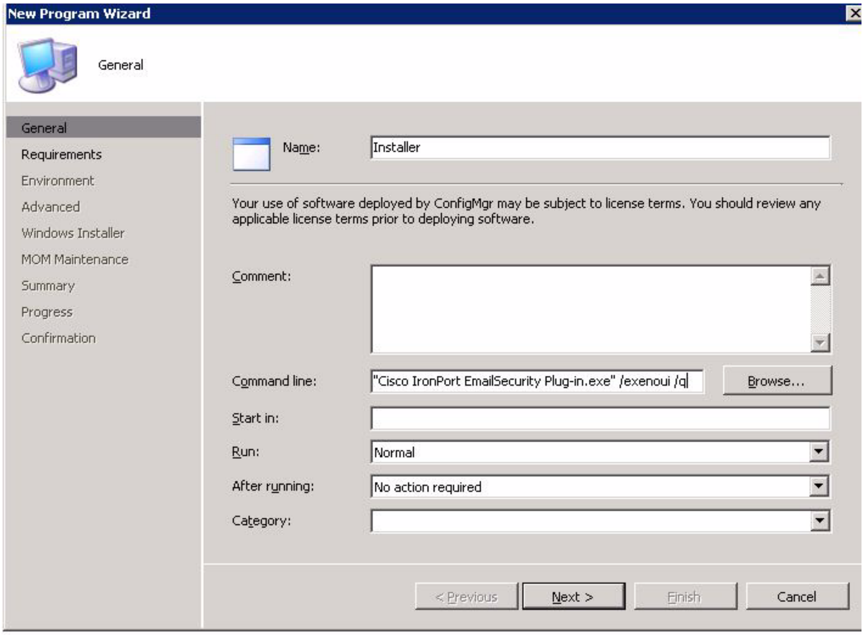
To copy the package to the new distribution points, click Next.

Step 10 Create a new program.



Step 11 In the command line field, enter the following command: *{shared network path}\Cisco IronPort Email Security Plug-in.exe /exenoui /qn*

For example: \\*sc2007\Shared\Cisco IronPort Email Security Plug-in.exe /exenoui /qn* where \\sc2007\Shared\Cisco IronPort Email Security Plug-in.exe is the full network path to the .exe file in the network shared folder.



New Program Wizard

General

Name: Installer

Your use of software deployed by ConfigMgr may be subject to license terms. You should review any applicable license terms prior to deploying software.

Comment:

Command line: "Cisco IronPort EmailSecurity Plug-in.exe" /exenoui /q

Start in:

Run: Normal

After running: No action required

Category:

Note If you want to use customized configuration files, you need to add a special key during this step which enables the installation to use the customized files. You add the special key from the command line (specifying the location of the custom configuration files after the = sign) using the following syntax:

```
Cisco IronPort Email Security Plug-in.exe /exenoui /qn
UseCustomConfig="\\sc2007\Shared\config\"
```

For more information about customizing your configuration files, see Using Custom Configuration Files, page 3-15.

Step 12 In the **Run** field, enter **Hidden**, and then click **Next**.

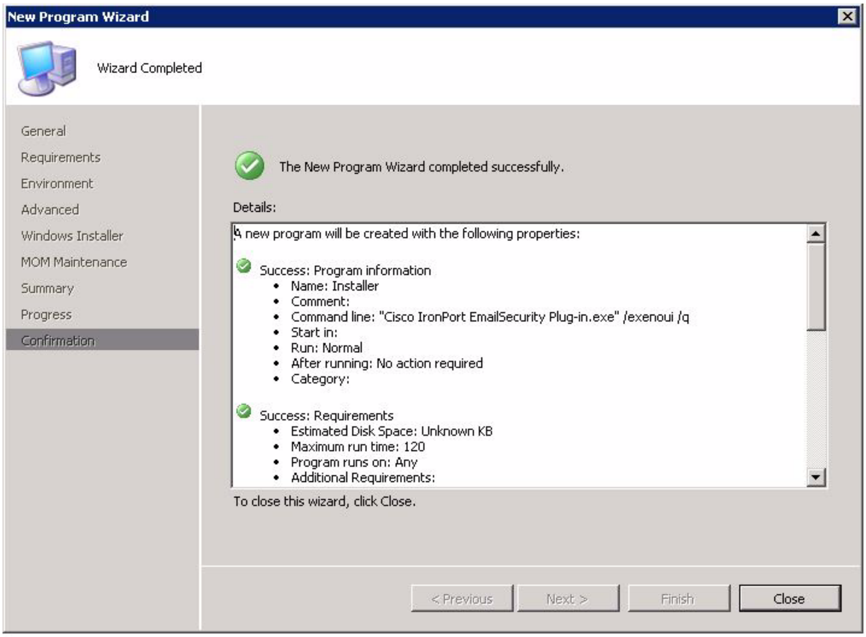
Step 13 Click through the requirements page, and then click **Next**.

Step 14 Select the following environment options:

- **Program can run**: Only when the user is logged on. If Run mode is set to administrative rights, then **Program can run** can be set to **Whenever the user is logged on**.

- **Run mode**: Run with user's rights, or run with administrative rights if users don't have sufficient permissions to install new software.

Step 15 Confirm that the New Program Wizard completed successfully, and click **Close**.



✓ The New Program Wizard completed successfully.

Details:

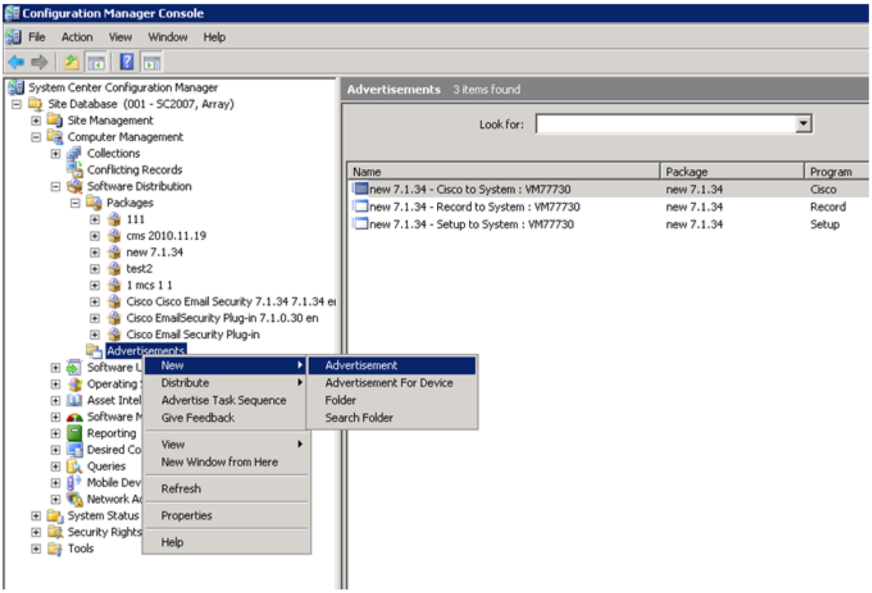
A new program will be created with the following properties:

✓ Success: Program information
- Name: Installer
- Comment:
- Command line: "Cisco IronPort EmailSecurity Plug-in.exe" /exenoui /q
- Start in:
- Run: Normal
- After running: No action required
- Category:

✓ Success: Requirements
- Estimated Disk Space: Unknown KB
- Maximum run time: 120
- Program runs on: Any
- Additional Requirements:

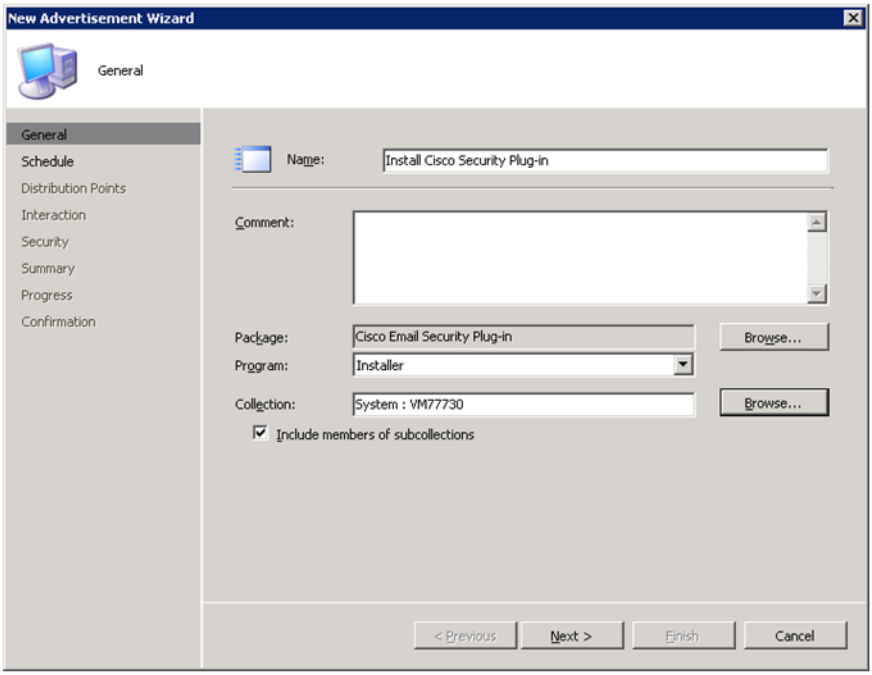
To close this wizard, click Close.

Step 16 Create a new advertisement.



Name	Package	Program
new 7.1.34 - Cisco to System : VM77730	new 7.1.34	Cisco
new 7.1.34 - Record to System : VM77730	new 7.1.34	Record
new 7.1.34 - Setup to System : VM77730	new 7.1.34	Setup

Step 17 Enter a name, select the package and program that you created. Select the collection that contains the group of clients where you want to install the plug-in. Click **Next**.



New Advertisement Wizard

General

Name: Install Cisco Security Plug-in

Comment:

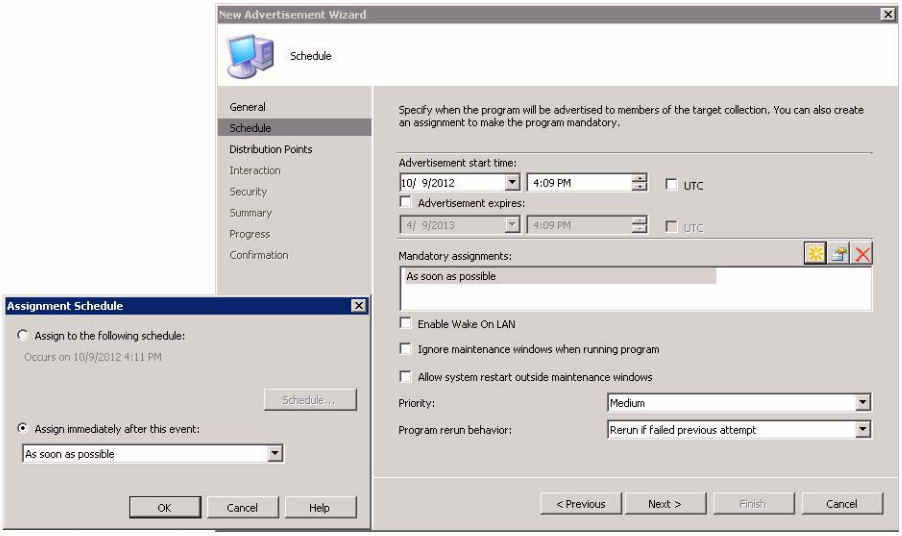
Package: Cisco Email Security Plug-in

Program: Installer

Collection: System : VM77730

☑ Include members of subcollections

Step 18 Set the assignment as mandatory. Click **Next**.



Specify when the program will be advertised to members of the target collection. You can also create an assignment to make the program mandatory.

Advertisement start time: 10/ 9/2012 4:09 PM □ UTC

□ Advertisement expires: 4/ 9/2013 4:09 PM □ UTC

Mandatory assignments: As soon as possible

□ Enable Wake On LAN

□ Ignore maintenance windows when running program

□ Allow system restart outside maintenance windows

Priority: Medium

Program rerun behavior: Rerun if failed previous attempt

○ Assign to the following schedule:

Occurs on 10/9/2012 4:11 PM

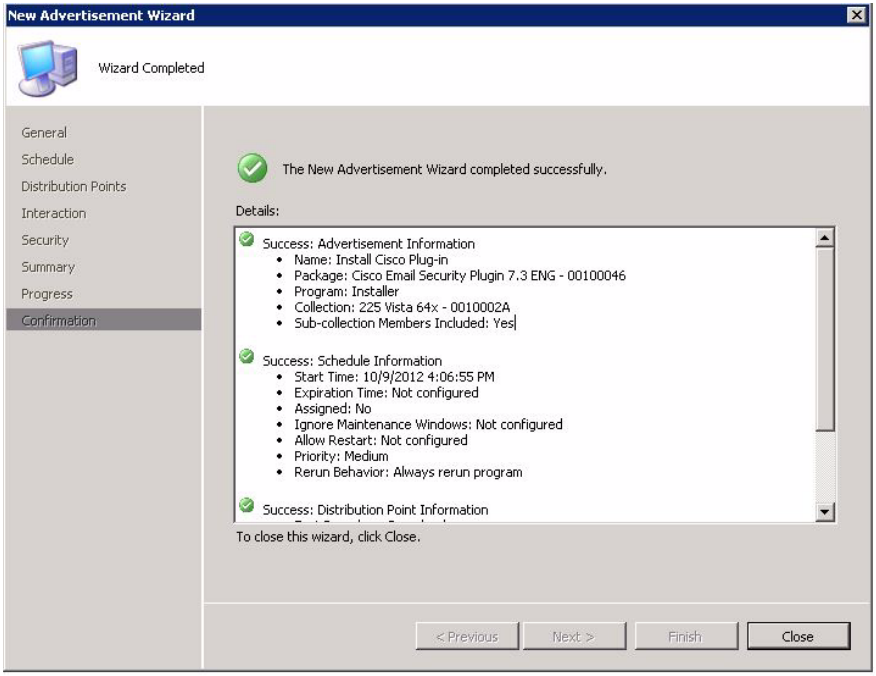
● Assign immediately after this event:

As soon as possible

Step 19 Select the switches based on your preferences. At least one Mandatory assignment should be set. Do not select **Do Not Run Program**, as the program will not start if the connection is slow**.** Click **Next**.

Step 20 Click through the New Advertisement Wizard, and click **Next**.

Step 1 View the confirmation that the New Advertisement Wizard completed successfully, and click **Close**.



The New Advertisement Wizard completed successfully.

Details:

✓ Success: Advertisement Information

- Name: Install Cisco Plug-in
- Package: Cisco Email Security Plugin 7.3 ENG - 00100046
- Program: Installer
- Collection: 225 Vista 64x - 0010002A
- Sub-collection Members Included: Yes

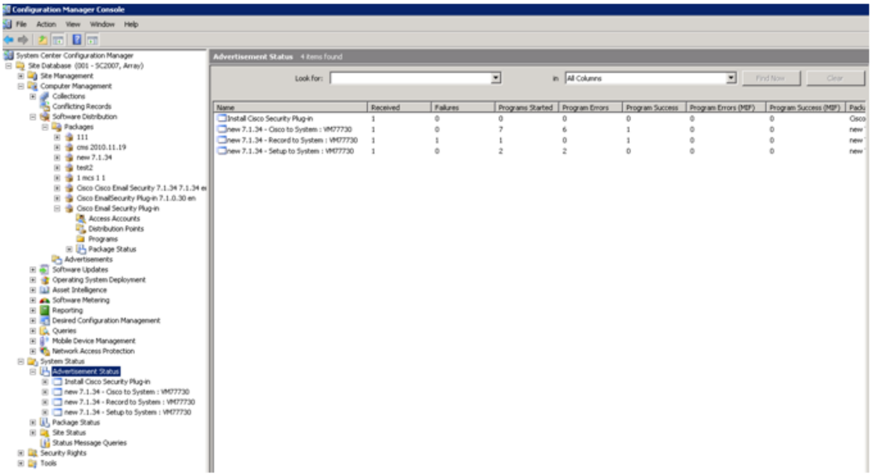
✓ Success: Schedule Information

- Start Time: 10/9/2012 4:06:55 PM
- Expiration Time: Not configured
- Assigned: No
- Ignore Maintenance Windows: Not configured
- Allow Restart: Not configured
- Priority: Medium
- Rerun Behavior: Always rerun program

✓ Success: Distribution Point Information

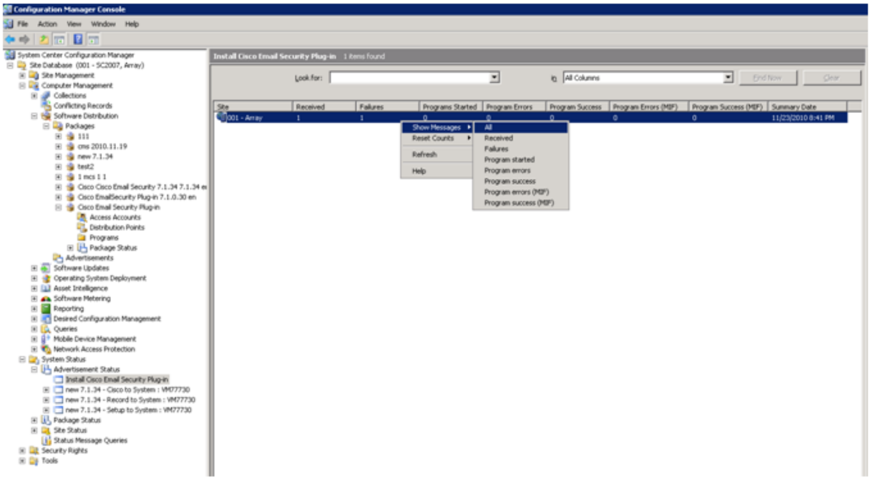
To close this wizard, click Close.

Step 2 View the Advertisement Status in the Advertisement Status window.


Configuration Manager Console
File Action View Window Help
System Center Configuration Manager
Site Database (001 - SC2007, Array)
Site Management
Computer Management
Collections
Conflicting Records
Software Distribution
Packages
111
cms 2010.11.19
new 7.1.34
test2
1 mcs 1 1
Cisco Cisco Email Security 7.1.34 7.1.34 en
Cisco EmailSecurity Plug-in 7.1.0.30 en
Cisco Email Security Plug-in
Access Accounts
Distribution Points
Programs
Package Status
Advertisements
Software Updates
Operating System Deployment
Asset Intelligence
Software Metering
Reporting
Desired Configuration Management
Queries
Mobile Device Management
Network Access Protection
System Status
Advertisement Status
Install Cisco Security Plug-in
new 7.1.34 - Cisco to System : VM77730
new 7.1.34 - Record to System : VM77730
new 7.1.34 - Setup to System : VM77730
Package Status
Site Status
Status Message Queries
Security Rights
Tools
Advertisement Status 4 items found
Look for:
in All Columns
Find Now
Clear

Name	Received	Failures	Programs Started	Program Errors	Program Success	Program Errors (MIF)	Program Success (MIF)	Packa
Install Cisco Security Plug-in	1	0	0	0	0	0	0	Cisco
new 7.1.34 - Cisco to System : VM77730	1	0	7	6	1	0	0	new
new 7.1.34 - Record to System : VM77730	1	1	1	0	1	0	0	new
new 7.1.34 - Setup to System : VM77730	1	0	2	2	0	0	0	new

Step 3 You can create an advertisement report to view more details by selecting **Show Message** > **All** from the Context menu. If an error occurred, you can review the report to see where the error occured.



Site	Received	Failures	Programs Started	Program Errors	Program Success	Program Errors (MIF)	Program Success (MIF)	Summary Date
001 - Array	1	1	0	0	0	0	0	11/23/2010 8:41 PM

Using Custom Configuration Files

The Cisco IronPort Email Security Plug-in allows you to modify the default configuration by editing a set of XML files included in your installation. You might want to use different configuration files to change aspects of the installation. For example, in Encryption configuration file, you might change the file flagging method (Only make this change if you are also able to change the method on the Encryption appliance). In the reporting configuration files, you might change some of the default options, such as the maximum mail size for reporting, or whether to maintain copies of the files after they have been reported. You may also want to customize the button names, or even localize the text used in the user interface.

Overview

To modify and deploy custom configuration files, complete the following steps:

Step 1 Make a copy of the **\\%allusersprofile%\Cisco\Cisco IronPort Email Security Plug-In** directory. It is required to include the Common folder.

Note You must maintain the directory structure of the original files to maintain validity. Make sure that you maintain the structure starting at the Cisco IronPort Email Security Plug-in directory and include all files with configuration files.

Step 2 Edit the XML configuration files. Rather than creating new files, Cisco recommends you modify the XML files included in the installation file. For instructions on modifying these files, see Editing the XML Configuration Files, page 3-16.

Step 3 Run the mass installation as described in Performing the Installation, page 3-1, and deploy the customized XML files as described in Deploying the Custom Configuration Files, page 3-20.

Editing the XML Configuration Files

When you install the Cisco IronPort Email Security Plug-in, configuration data is created and saved in XML files. You can edit the string values to customize the parameter values. However, Cisco does not recommend you remove values or modify the structure of the files.

By default, the plug-in installs configuration files in the %AllUsersProfile% directory in the following locations for Outlook:

```
%allusersprofile%\Cisco\Cisco IronPort Email Security Plug In
```

The XML files are located in the following default locations:

- **\\%allusersprofile%\Cisco\Cisco IronPort Email Security Plug-In\Common\CommonEncryptionConfig.xml**. Contains configuration data related to the Desktop Encryption plug-in.
- **\\%allusersprofile%\Cisco\Cisco IronPort Email Security Plug-In\Common\config_1.xml, config_{N}.xml**. These numbers are dependent on the count of user accounts.
- **\\%allusersprofile%\Cisco\Cisco IronPort Email Security Plug-In\Common\CommonConfig.xml**. Contains basic configuration data that is common to both the Reporting and Encryption plug-ins, such as the location of the log files and the name of the localization file (en-US.xml is the default localization file). You can use your email program settings to change the log file location, and deploy it with your mass installation program. If you want to create a localization file in a language other than the available localization files, you need to reference the name of the new XML file here.
- **\\%allusersprofile%\Cisco\Cisco IronPort Email Security Plug-In\Common\Reporting.xml**. Contains configuration data related to the Reporting plug-in, such as the maximum mail size that can be reported. Cisco does not recommend you modify this file.
- **\\%allusersprofile%\Cisco\Cisco IronPort Email Security Plug-In\Common\Localization\en-US.xml**. Contains data related to local languages. The default language is English. However, there are several localization files available, including de.xml, es.xml, fr.xml, it.xml, zh-CN.xml. If you want to use a language that is not within the scope of these xml files, you can create a custom xml file and reference it in the CommonConfig.xml file.

Warning **Do not change any string id settings that are inside the < or > symbols, as this will prevent your plug-in from functioning properly.**

Example

The following example shows sample changes to the *en-US.xml* file.

To change the text in the Reporting toolbar, find the following section of the *en-US.xml* xml file and edit the text in bold:

```
<group name="Mso.Report.Button.Cations">
 <string id="blockSender">Block Sender</string>
 <string id="spam">Spam</string>
 <string id="ham">Not Spam</string>
 <string id="virus">Virus</string>
 <string id="phish">Phish</string>
</group>
```

For example, if you wanted to add more descriptive titles, you could change the text as follows:

```
<group name="Mso.Report.Button.Cations">
 <string id="blockSender">Block Sender using Outlook</string>
 <string id="spam">Report Spam</string>
 <string id="ham">Report Not Spam</string>
 <string id="virus">Report Virus</string>
 <string id="phish">Report Phishing Attacks</string>
</group>
```

Mass Installation Using the BCE_Config.xml File

To perform a mass installation using the BCE_Config.xml file:

Step 1 Navigate to the **\\%allusersprofile%\Cisco\Cisco IronPort Email Security Plug-In\Common** directory**.**

Step 2 Remove the *config_1.xml file*, if any exists.

Step 3 Copy the *BCE_Config_signed.xml* file to this directory and rename the file back to *config_1.xml*.

Step 4 Navigate to the **\\%allusersprofile%\Cisco\Cisco IronPort Email Security Plug-In\CommonEncryptionConfig.xml** file.

Step 5 Verify that the *CommonEncryptionConfig.xml* file includes these tags:

```
<accountFileNames>
   <accountFileName filePath="config_1.xml" emailAddress="*" />
 </accountFileNames>
```

Note To configure only selected users in a specific domain, you need to modify the *CommonEncryptionConfig.xml* file by specifying the domain as an email address.

For example, to apply the BCE config file to only Cisco users, change the:

```
<accountFileName filePath="config_1.xml" emailAddress="*" />
```

to:

```
<accountFileName filePath="config_1.xml" emailAddress="@cisco.com" />
```

If there is more than one `accountFileName` tag then the `filePath` will be config_2.xml, config_3.xml, etc.

For example:

```
<accountFileName filePath="config_2.xml" emailAddress="@cisco.com" />
```

Step 6 Run the mass installation as described in Performing the Installation, page 3-1 and deploy the customized XML files as described in Deploying the Custom Configuration Files, page 3-20.

Note The **\\%allusersprofile%\Cisco\Cisco IronPort Email Security Plug-In\Common** directory content must be copied to **\\{SHARED_DIR}\{CONFIG_FOLDER}**. The Common folder must exist in {CONFIG_FOLDER}. The UseCustomConfig command parameter enables the installation to use the custom configuration file that you modified.

Deploying the Custom Configuration Files

Once you have completed editing the configuration files, you will need to add a special key during deployment to ensure that the installer uses the custom configuration files you modified. The **UseCustomConfig** command line parameter enables the installation to use custom configuration files and specifies the path to the folder containing configuration files which should be used during the installation.

You add the **UseCustomConfig** key from the command line during Step 11 of the mass installation (see Performing the Installation, page 3-1) using the following syntax:

```
Cisco IronPort Email Security Plugin.exe /exenoui /qn
UseCustomConfigs="\\{SHARED_DIR}\{CONFIG_FOLDER}
```

where the path after the = specifies the path to the customized configuration files.

Additional Commands

In addition to the UseCustomConfig, you can also use the following commands:

- AppDir="C:\CustomInstallDir"—Specifies custom target directory.
- SkipReporting="TRUE"—Disables Reporting plug-in for upcoming installation.
- SkipEncryption="TRUE"—Disables Encryption plug-in for upcoming installation.

CHAPTER 4

Configuring and Using the Cisco IronPort Email Security Plug-in for Outlook

This chapter introduces the features available in the Cisco IronPort Email Security Plug-in for Outlook. The Cisco IronPort Email Security Plug-in includes several types of security plug-ins that work with the Outlook email program. This chapter contains the following sections:

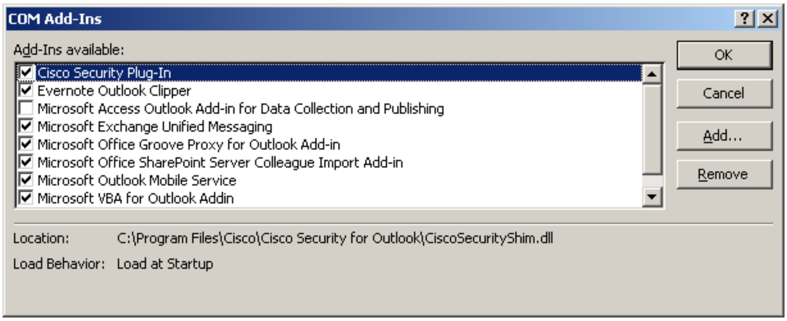
Cisco IronPort Email Security Plug-in For Outlook General Settings

The Cisco IronPort Email Security Plug-in is a platform that supports several Cisco plug-ins, including the Encryption plug-in and the Reporting plug-in. General settings for the Cisco IronPort Email Security Plug-in can be configured from the Options page.

Enable or Disable

By default, the Cisco IronPort Email Security Plug-in is enabled upon installation. The Cisco IronPort Email Security Plug-in can be disabled from the following places:

- In Outlook 2010, go to **File** > **Options** and select **Add-ins** from the left navigation bar. Then, select **COM Add-ins** from the Manage drop-down menu at the bottom of the page, and click **Go**...
- In Outlook2003/ 2007, go to **Tools** > **Options** > **Cisco Email Security**.



Add-Ins available:

☑ Cisco Security Plug-In
☑ Evernote Outlook Clipper
☐ Microsoft Access Outlook Add-in for Data Collection and Publishing
☑ Microsoft Exchange Unified Messaging
☑ Microsoft Office Groove Proxy for Outlook Add-in
☑ Microsoft Office SharePoint Server Colleague Import Add-in
☑ Microsoft Outlook Mobile Service
☑ Microsoft VBA for Outlook Addin

Location: C:\Program Files\Cisco\Cisco Security for Outlook\CiscoSecurityShim.dll
Load Behavior: Load at Startup

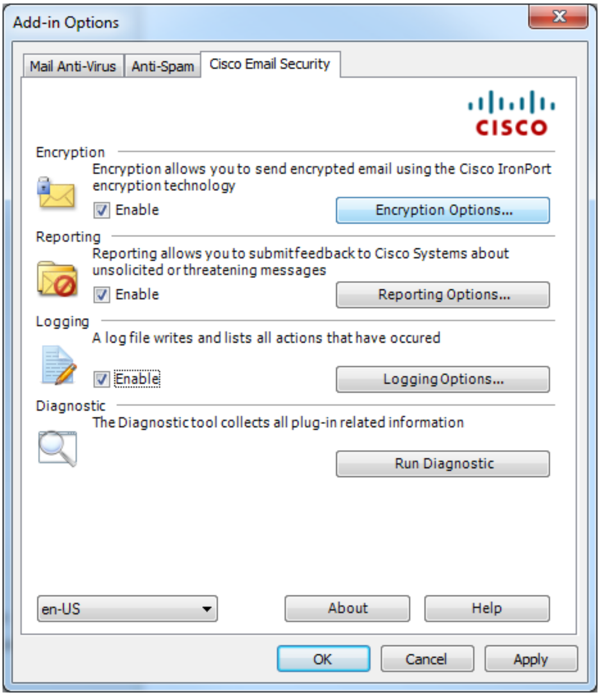
From the COM Add-Ins window, clear the Cisco IronPort Email Security Plug-in check box and click **OK**.

Configuring Basic Settings for the Outlook Plug-in

The end user can configure basic settings from the Cisco Email Security tab.

- In Outlook 2010, go to **File** > **Options** > **Add-ins** > **Add-in Options** > **Cisco Email Security.**
- In Outlook 2003/2007, go to **Tools** > **Options** > **Cisco Email Security.**

Cisco Email Security tab:



Encryption allows you to send encrypted email using the Cisco IronPort encryption technology

☑ Enable

Reporting allows you to submit feedback to Cisco Systems about unsolicited or threatening messages

☑ Enable

A log file writes and lists all actions that have occured

☑ Enable

The Diagnostic tool collects all plug-in related information

en-US

From this tab, the end user can enable encryption, reporting, and logging by selecting the **Enable** check box. To further configure the settings, click the **Encryption Options...**, **Reporting Options...**, or **Logging Options...** buttons. The end user can also use the Diagnostic tool to run a report on the Cisco IronPort Email Security Plug-in to send to Cisco Support when problem-solving.

Reporting Unwanted Emails-Spam, Virus, and Phishing Attacks

The reporting plug-in allows the end user to report to Cisco that an email received is spam, a phishing attack, or a virus. The end user can also report mail that is misclassified as spam, also sometimes called "ham."

The end user can enable the Cisco IronPort Email Security Reporting Plug-in for Outlook via the Options page in Outlook. To enable Reporting:

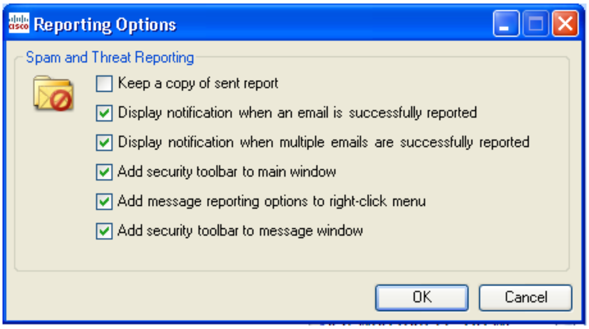
- In Outlook 2010, go to **File** > **Options** > **Add-ins** > **Add-in Options** > **Cisco Email Security.** Select the **Enable** check box in the Reporting field of the Cisco Email Security tab.
- In Outlook 2003/2007, go to **Tools** > **Options** > **Cisco Email Security** tab. Select the **Enable** check box in the Reporting field of the Cisco Email Security tab.

Reporting Options

The Reporting settings are located on the Cisco Email Security page. To modify the Reporting settings:

- In Outlook 2010, go to **File** > **Options** > **Add-ins** > **Add-in Options** > **Cisco Email Security** and click the **Reporting Options** button.
- In Outlook 2003/2007, go to **Tools** > **Options** > **Cisco Email Security** tab and click the **Reporting Options** button.

Reporting Options page:



Reporting Options

Spam and Threat Reporting

☐ Keep a copy of sent report

☑ Display notification when an email is successfully reported

☑ Display notification when multiple emails are successfully reported

☑ Add security toolbar to main window

☑ Add message reporting options to right-click menu

☑ Add security toolbar to message window

Options

This section describes the Reporting options the end user can configure.

Option	Description
Keep a copy of sent report	By default, when the end user reports an email message to Cisco as spam, virus, misclassified spam, or virus, the reporting email the end user sent is deleted. Selecting this option prevents the email from being deleted.
Display notification when an email is successfully reported	When the end user successfully reports an email as spam or virus, they can enable Outlook to display a success message in a dialog box. Clearing this option prevents this dialog box from displaying.
Display notification when multiple emails are successfully reported	When the end user successfully reports a group of emails as spam or virus, they can enable Outlook to display a success message in a dialog box. Clearing this option prevents this dialog box from displaying.

Option	Description
Add security toolbar to the main window	By default, when the end user installs the Cisco IronPort Email Security Plug-in, the plug-in toolbar is added to main Outlook window. Clearing this option prevents this toolbar from being added to main Outlook window.
Add message reporting options to the right-click menu	By default, when the end user installs the Cisco IronPort Email Security Plug-in, the Reporting plug-in menu item is added to the Outlook right-click context menu. Clearing this option prevents this menu item from being added to the right-click context menu.
Add security toolbar to the message window	By default, when the end user installs the Cisco IronPort Email Security Plug-in, the plug-in toolbar is added to the email message window. Clearing this option prevents this toolbar from being added to the email message window.

Using the Reporting Plug-in for Outlook

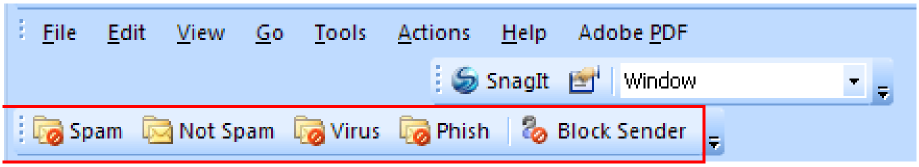
Overview

The Cisco IronPort Email Security Plug-in for Outlook allows the end user to submit feedback to Cisco about spam, virus, or phishing emails that are received in their inbox. The end user can let Cisco know if an email message is misclassified or if it should be treated as spam, for example. Cisco uses this feedback to update the email filters that prevent unwanted messages from being delivered to their inbox.

The Plug-in provides a convenient interface through Outlook’s menu bar and the right-click message menu to report spam, virus, phishing and misclassified emails. After reporting an email, a message appears indicating that the report has been submitted. The messages the end user reports are used to improve Cisco's email filters, helping to reduce the overall volume of unsolicited mail to their inbox.

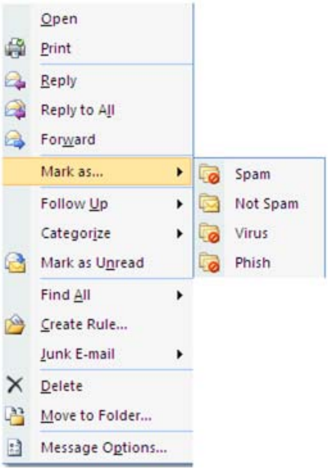
Providing Feedback to Cisco

The Plug-in provides a new toolbar in Outlook containing the following buttons: Spam, Not Spam, Virus, Phish and Block Sender (Block Sender does not block email from the end user's Junk Email Box).

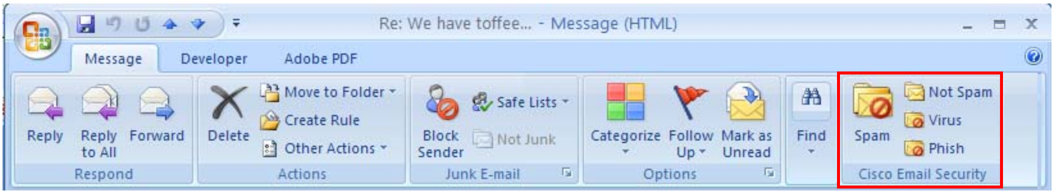


These buttons are used to report spam, virus, and phishing emails (Phishing attacks are emails that link to "spoofed" and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account user names and passwords, social security numbers. For example, the end user might receive an email from *infos@paypals.com* that fraudulently requests their personal banking information). In addition, the end user can click the Block Sender button. Clicking this button invokes the Outlook Junk E-mail action "Add Sender to Blocked Senders List." Please see the Microsoft documentation for more information regarding this feature.

The end user can also use right-click context menu to report spam, misclassified mail, virus, and phish.



And, the end user can use the buttons in the message window to report spam, virus, phish and misclassified mail (misclassified mail is mail that was erroneously marked as spam, virus, or phish).



Message Rotation for Reported Spam, Virus, or Phish Emails

When emails messages are reported as spam, misclassified, virus, or phish, the messages are processed as follows.

Inbox messages:

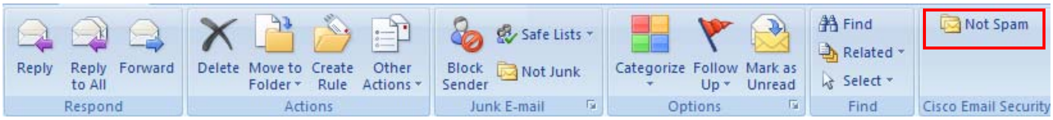
- Inbox messages reported as spam, virus, or phish go into the Junk Email folder.
- Inbox messages reported as Not Spam stay in the Inbox folder.

Junk Messages:

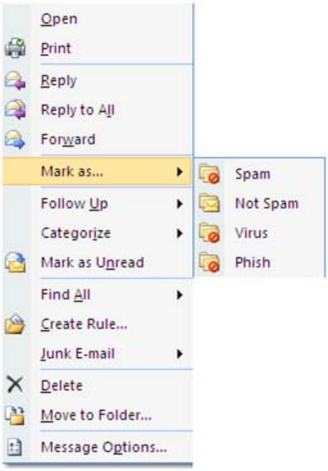
- Junk messages reported as spam, virus, or phish stay in the Junk Email folder.

- Junk messages reported as Not Spam go in the Inbox folder.

If an email received is misclassified as spam (i.e. is filtered and sent to the Junk Email folder), the end user can report the email as misclassified by clicking the **Not Spam** button. This ensures that mail from the sender will not be classified as spam in the future..



The end user can also mark misclassified email from the right-click context menu.

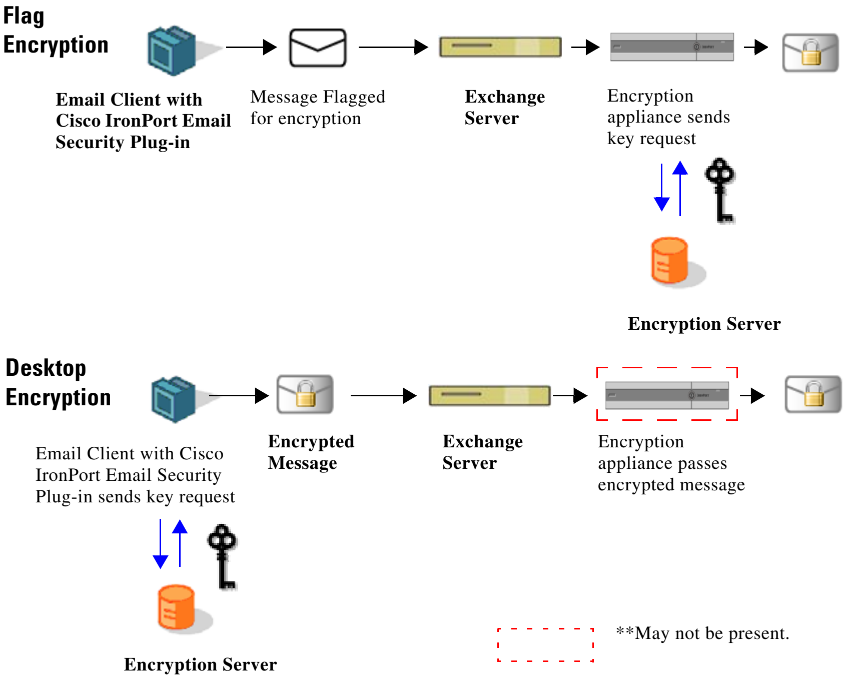


Encrypting Email

The encryption plug-in allows end users to encrypt mail from the desktop or flag email to be encrypted before sending email out of their company network. Choose one of the following encryption options:

- **Flag Encryption**. The Flag Encryption option allows the end user to flag email for encryption, and the email is encrypted by the Cisco IronPort Encryption appliance before it is sent out of the network. You may want to use Flag Encryption if the end user needs to send encrypted mail outside their organization, but don't require the email to be encrypted within their organization. For example, their organization works with sensitive medical documents that need to be encrypted before being sent to patients.
- **Desktop Encryption**. Desktop Encryption allows the end user to encrypt email from within Outlook using the Cisco IronPort encryption technology. Then, it sends the encrypted email from their desktop. You may want to use Desktop Encryption if the end user wants to ensure that mail sent *within* their organization is encrypted. For example, their organization requires all sensitive financial data to be encrypted when sent both within and outside of the organization.

Figure 4-1 Workflows for Flag Encryption vs. Desktop Encryption


Flag Encryption
Email Client with Cisco IronPort Email Security Plug-in
Message Flagged for encryption
Exchange Server
Encryption appliance sends key request
Encryption Server
Desktop Encryption
Email Client with Cisco IronPort Email Security Plug-in sends key request
Encrypted Message
Exchange Server
Encryption appliance passes encrypted message
Encryption Server
**May not be present.

Note The encryption method is determined by decrypting the *BCE_Config_signed.xml* file attachment from the Outlook email account. Decrypt Only mode is enabled by default. The end user can choose to modify their installation in order to change the encryption method by receiving and decrypting an updated *BCE_Config_signed.xml* file from you, the administrator.

Flag and Desktop Encryption Configuration

The default configuration mode for the end user Outlook email account is Decrypt Only. In order to enable the Flag or Encrypt feature, the end user email account is configured by an updated attachment file received from the administrator. Also, the Flag and Encrypt feature can be enabled via Mass Install when a set of configuration files are provided directly to the user's configuration folder. If a decrypted message contains a *BCE_Config_signed.xml* attachment, the Encryption Plug-in for Outlook is automatically configured when the end user launches this configuration file. The Cisco IronPort Encryption appliance or the Cisco Registered Envelope Service (CRES) is used as a key server. If the end user does not have an account, they are prompted to register.

Three configuration modes are available:

- **Decrypt Only**. Allows decrypting of encrypted emails received.
- **Decrypt and Flag**. Allows decrypting and flagging of secure email messages. The flag option allows the end user to flag the email for encryption, and the email is encrypted by the Cisco Email Security appliance before the email is sent out of the network. The server must be configured to detect the flagged messages and encrypt them at the server.
- **Decrypt and Encrypt**. Allows encrypting and decrypting of secure email message.

Launching the Email Security Plug-in Configuration File

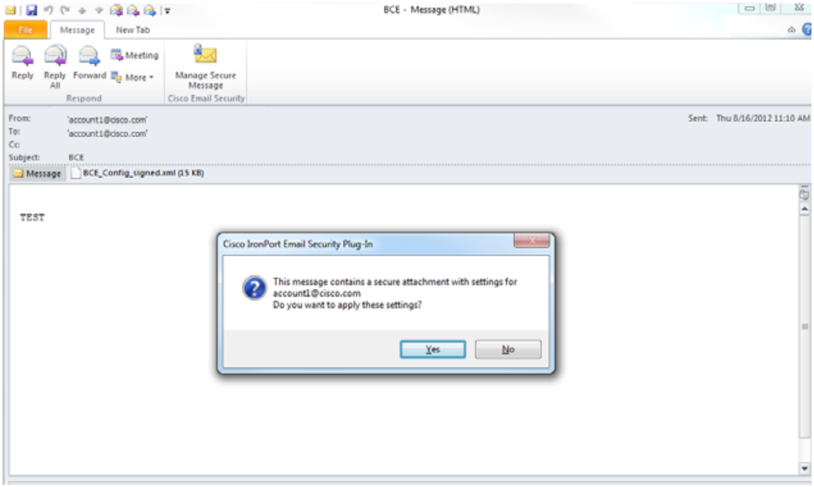
The end user enables and configures the encryption for their Outlook email account by decrypting the *BCE_Config_signed.xml* file attachment from their Outlook email account. If the end user does not see the notification email with the attachment in their inbox, check the spam or junk folder.

When launching the configuration file, the plug-in is configured for the email account that received the notification message with the *BCE_Config_signed.xml* file attachment.

Note Normally, the Jave Runtime Environment (JRE) is automatically installed during the plug-in installation. However, if this does not happen, please install at least version 1.6 to use with the plug-in.

To enable and configure the security plug-in for the Outlook email account:

Step 1 Open the notification email message with the *BCE_Config_signed.xml* file attachment. The end user is asked if they want to apply the settings.



From: 'account1@cisco.com'
To: 'account1@cisco.com'
Cc:
Subject: BCE
Sent: Thu 8/16/2012 11:10 AM
Message | BCE_Config_signed.xml (15 KB)

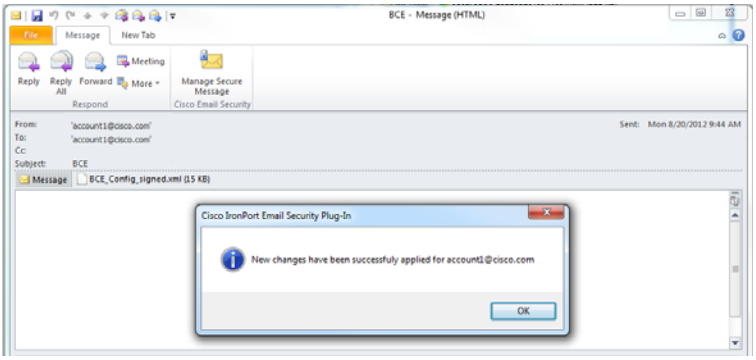
TEST

Cisco IronPort Email Security Plug-In

This message contains a secure attachment with settings for account1@cisco.com
Do you want to apply these settings?

Yes | No

Step 2 Click **Yes** to automatically configure the Cisco IronPort Email Security Plug-In. A message displays after the configuration has been successfully applied.



From: 'account1@cisco.com'
To: 'account1@cisco.com'
Cc:
Subject: BCE
Sent: Mon 8/20/2012 9:44 AM
Message | BCE_Config_signed.xml (15 KB)

Cisco IronPort Email Security Plug-In

New changes have been successfuly applied for account1@cisco.com

OK

Flag Encryption

The Flag Encryption option allows the end user to flag the email for encryption, and the email is encrypted by the Cisco IronPort Encryption appliance or Email Security appliance before the email is sent out of the network. If mail leaving the corporate network needs to be scanned for spam or viruses, the Flag Encryption method should be used.

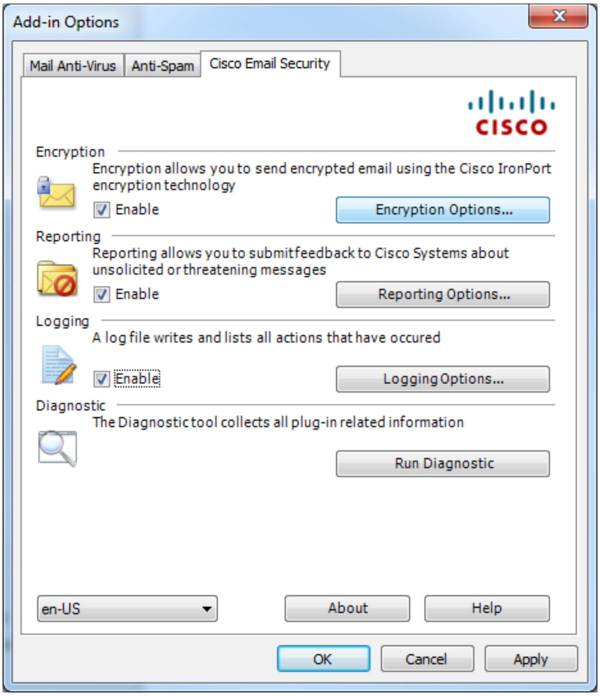
The Flag Encryption settings are located on the Cisco Email Security page. To modify the Flag Encryption settings:

- In Outlook 2010, go to **File** > **Options** > **Add-ins** > **Add-in Options** > **Cisco Email Security** > **Encryption Options**.
- In Outlook 2003/2007, go to **Tools** > **Options** > **Cisco Email Security** > **Encryption Options**.

Enable and disable the Encryption plug-in by selecting or clearing the **Enable** check box in the Encryption field of the Cisco Email Security tab.

Select **Enable** to enable the email program to send sensitive mail via a secure envelope.

Cisco Email Security Add-in Options page:



Encryption

Encryption allows you to send encrypted email using the Cisco IronPort encryption technology

☑ Enable

Reporting

Reporting allows you to submitfeedback to Cisco Systems about unsolicited or threatening messages

☑ Enable

Logging

A log file writes and lists all actions that have occured

☑ Enable

Diagnostic

The Diagnostic tool collects all plug-in related information

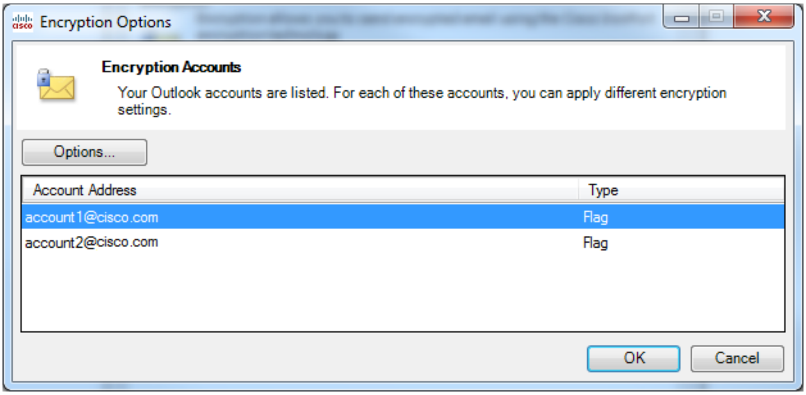
en-US

Flag Encryption Options

Encryption Accounts

The Encryption Accounts page displays all email user accounts for the Flag Encryption Plug-in. Each row indicates a single account and displays the account email address and encryption type. Click **Options** or double-click an Account Address to open the account Encryption Options page.

Encryption Accounts page:



Encryption Accounts

Your Outlook accounts are listed. For each of these accounts, you can apply different encryption settings.

Account Address	Type
account1@cisco.com	Flag
account2@cisco.com	Flag

Note A new account in Outlook will be automatically added in the Encryption Accounts list. And when an Outlook account is removed, that account is automatically removed from the Encryption Accounts list.

Options for Sending Flag Encrypted Email

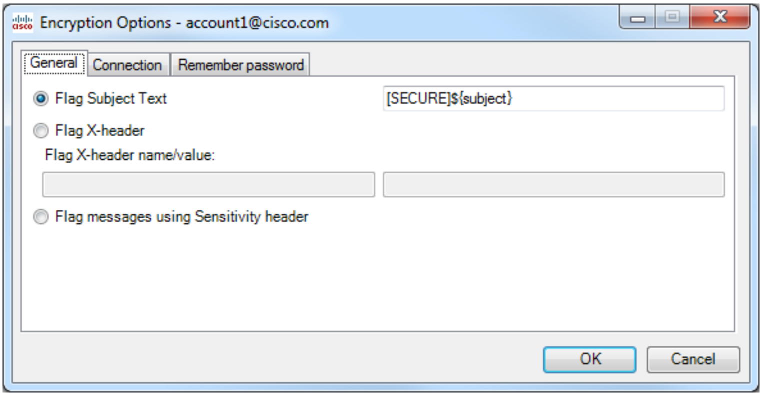
When the end user wants to encrypt outgoing email, you will need to mark or "flag" the email for encryption. This allows filters created by you to identify the messages that need to be encrypted.

Note These methods for flagging email for encryption require changes in email filters to work properly and only an administrator can make these changes.

The Encrypt Message button is available when composing emails. Emails can be marked for encryption using one of the following methods:

General Tab

The following shows the Flag Encryption Options General tab.



● Flag Subject Text [SECURE]${subject}

○ Flag X-header

Flag X-header name/value:

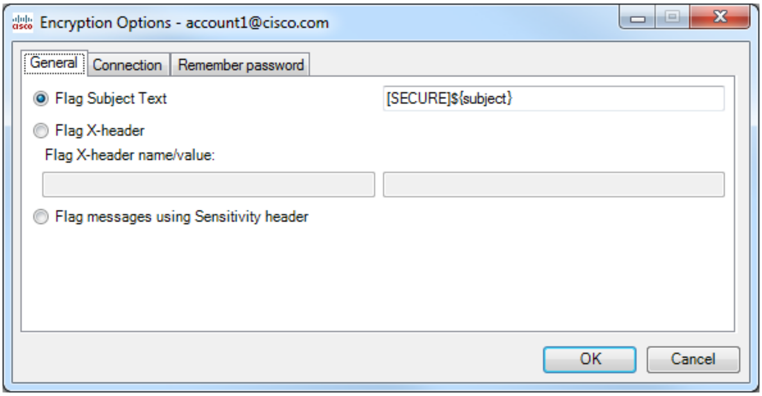
○ Flag messages using Sensitivity header

You can select from the following General options:

General Options	Value
Flag Subject Text	Text can be added to the Subject field of the outgoing email to flag the email for encryption. Enter the text to append to the Subject field to denote the email should be encrypted (the default value is *[SEND SECURE]*).
Flag X-header name/value	An x-header can be added to the outgoing email that will flag the email for encryption. Enter an x-header in the first field (the default value is *x-ironport-encrypt*). In the second field, enter a value of *true* or *false*. If you enter true, then a message with the specified x-header will be encrypted (the default value is true).
Flag messages using Sensitivity header	Outlook can add a sensitivity header to flag the message for email encryption. Selecting this method allows you to use Outlook's sensitivity header to mark emails for encryption.

Connection Tab

The following shows the Encryption Options Connection tab.



Encryption Options - account1@cisco.com

General | Connection | Remember password

● Flag Subject Text: [SECURE]${subject}

○ Flag X-header

Flag X-header name/value:

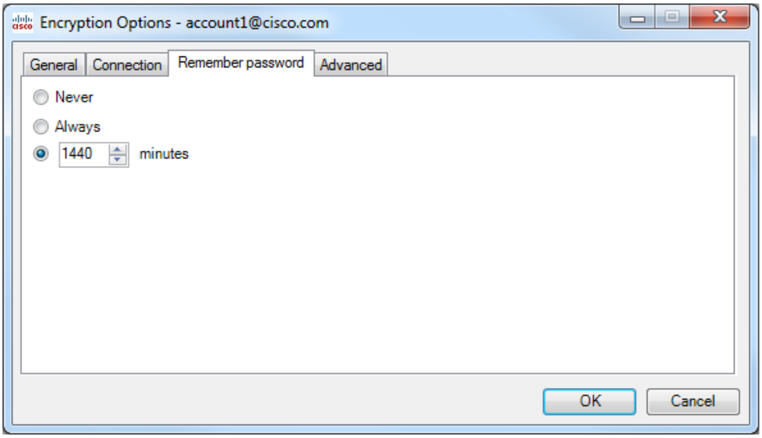
○ Flag messages using Sensitivity header

You can select from the following Connection options:

Connection Options	Value
No proxy	Select if you are not using a proxy.
Use system proxy settings	Select to use the default system proxy settings.
Manual proxy configuration	Select to enter settings for a specific proxy.
Protocol	If you choose not to use default connection settings choose one of the following protocols: HTTP, SOCKS4, SOCKS4a, or SOCKS5.
Host	Specify a host name or IP address for the system or proxy server.
Port	Specify a port for the system or proxy server.
Username	Enter a username if it is required for your server.
Password	Enter the password associated with the username you entered for your system or proxy server.

Remember Password Tab

The following shows the Encryption Options Remember password tab.



○ Never

○ Always

● 1440 minutes

Select from the following Remember Password options:

Password Options	Value
Never	When selected, the encryption password is always required when decrypting and encrypting emails.
Always	When selected, the encryption password is required only for the first time when decrypting an encrypted email. Then the password is cached.
Minutes	Select this option to ensure that the encryption password is cached. Type the number of minutes to remember the password, or use the arrows to modify the entry. After the specified duration, the end user must re-enter the encryption password to decrypt an encrypted email. The default is 1440 minutes.

Desktop Encryption

The Desktop Encrypt option allows the end user to encrypt email from within Outlook and sends the encrypted email from their desktop.

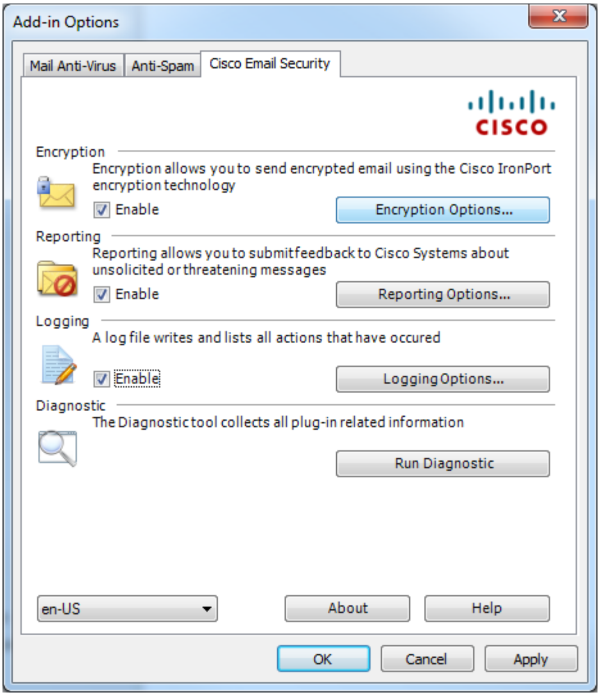
The Desktop Encryption settings are located on the Cisco Email Security page. To modify the Desktop Encryption settings:

- In Outlook 2010, go to **File** > **Options** > **Add-ins** > **Add-in Options** > **Cisco Email Security** > **Encryption Options**.
- In Outlook 2003/2007, go to **Tools** > **Options** > **Cisco Email Security** > **Encryption Options**.

The end user can enable and disable the Encryption plug-in by selecting or clearing the **Enable** check box in the Encryption field of the Cisco Email Security tab. Select **Enable** to enable the email program to send sensitive mail via a secure envelope.

Note The end user can enable or disable the Encryption plug-in from the Cisco Email Security page, although any changes to the encryption mode need to be made by the administrator in the *BCE_config.xml* file.

Cisco Email Security Add-in Options page:



Encryption

Encryption allows you to send encrypted email using the Cisco IronPort encryption technology

☑ Enable

Reporting

Reporting allows you to submitfeedback to Cisco Systems about unsolicited or threatening messages

☑ Enable

Logging

A log file writes and lists all actions that have occured

☑ Enable

Diagnostic

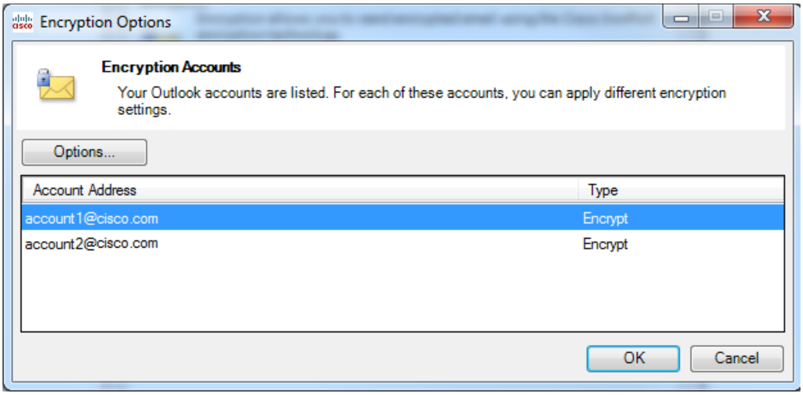
The Diagnostic tool collects all plug-in related information

Desktop Encryption Options

Encryption Accounts

The Encryption Accounts page displays all email user accounts for the Desktop Encryption Plug-in. Each row indicates a single account and displays the account email address and encryption type. Click **Options** or double-click an Account Address to open the account Encryption Options page.

Encryption Accounts page:



Encryption Options

Encryption Accounts

Your Outlook accounts are listed. For each of these accounts, you can apply different encryption settings.

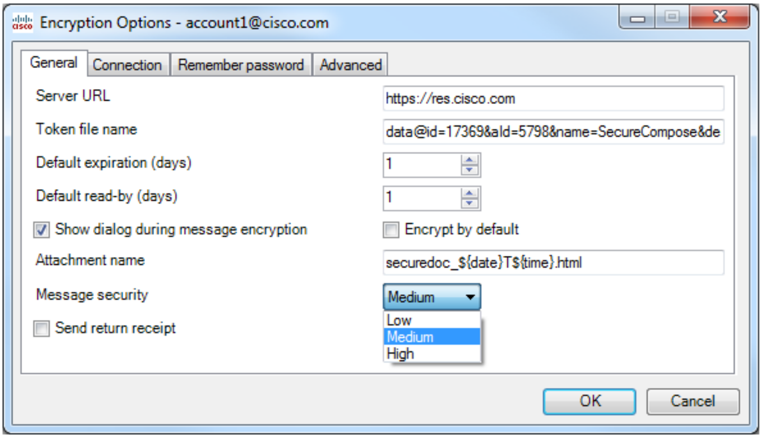
Account Address	Type
account1@cisco.com	Encrypt
account2@cisco.com	Encrypt

Note A new account in Outlook will be automatically added in the Encryption Accounts list. And when an Outlook account is removed, that account is automatically removed from the Encryption Accounts list.

General Tab

The following shows the Desktop Encryption Options General tab.

Note The screen shot and table show all of the possible options in the General tab, although the options displayed vary dependent on the configuration of the *BCE_config.xml file*.



Server URL: https://res.cisco.com

Token file name: data@id=17369&aId=5798&name=SecureCompose&de

Default expiration (days): 1

Default read-by (days): 1

☑ Show dialog during message encryption

□ Encrypt by default

Attachment name: securedoc_${date}T${time}.html

Message security: Medium

Low
Medium
High

□ Send return receipt

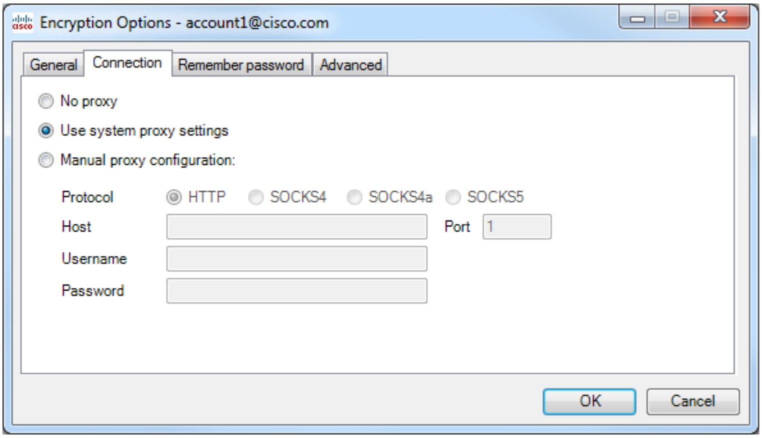
Select from the following General options:

General Option	Value
Server URL	Enter the URL for your Encryption server.
Token File Name	Tokens are customer specific keys used to encrypt data between the email client and the Encryption server. Currently, this information is only used by customer support and should not be modified.
Default Expiration (days)	Specify, in days, how long the encrypted email remains valid. After the number of expiry days is met, the message expires, and it cannot be opened by the recipient after this period.
Default read-by (days)	Specify, in days, the time period during which the recipient is expected to read the encrypted message. If the message is not read within the specified time frame, the sender is notified.
Show dialog during message encryption	Check this option to display the encryption options dialog box for each encrypted message.
Encrypt by default	Select to allow all sent email messages to be encrypted by default.
Attachment name	The default envelope name is *securedoc.html*.The attachment name value can be changed and the envelope will reflect the newly specified name.

General Option	Value
Message security	From the drop-down list, set the security for the encrypted email. The default value is the value set in the *BCE_Config.xml* file. **Note** Changing the message security here applies only to the message being composed. • **High**. A high security message requires a password for authentication every time an encrypted message is decrypted. • **Medium**. If the recipient password is cached, a medium security message does not require a password when the message is decrypted. • **Low.** A low security message is transmitted securely but does not require a password to decrypt an encrypted message.
Send return receipt	Select to request a return receipt when the sent email is opened by the recipient.

Connection Tab

The following shows the Encryption Options Connection tab.



○ No proxy

● Use system proxy settings

○ Manual proxy configuration:

Protocol ● HTTP ○ SOCKS4 ○ SOCKS4a ○ SOCKS5

Host Port 1

Username

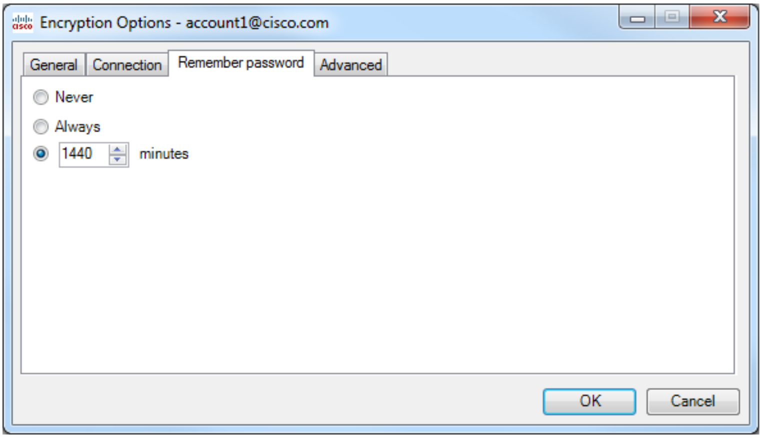
Password

Select from the following Connection options:

Connection Option	Value
No proxy	Select if you are not using a proxy.
Use system proxy settings	Select to use the default system proxy settings.
Manual proxy configuration	Select to enter settings for a specific proxy.
Protocol	If you choose not to use default connection settings choose one of the following protocols: HTTP, SOCKS4, SOCKS4a, or SOCKS5.
Host	Specify a host name or IP address for the system or proxy server.
Port	Specify a port for the system or proxy server.
User Name	Enter a user name if it is required for your server.
Password	Enter the password associated with the user name you entered for your system or proxy server.

Remember Password Tab

The following shows the Encryption Options Remember password tab.



○ Never

○ Always

● 1440 minutes

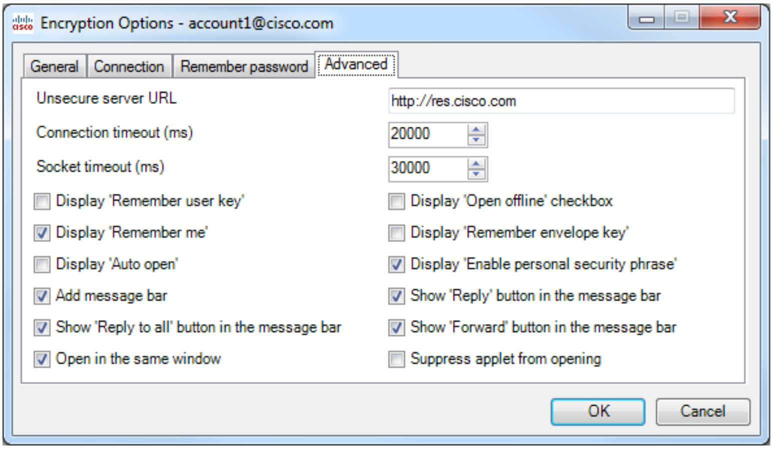
Select from the following Remember Password options:

Password Options	Value
Never	When selected, the encryption password is always required when decrypting and encrypting emails.
Always	When selected, the encryption password is required only for the first time when decrypting an encrypted email. Then the password is cached.
Minutes	Select this option to ensure that the encryption password is cached. From the drop-down, select the cache duration in minutes. After the specified duration, the end user must re-enter the encryption password to decrypt and encrypt emails. The default is 1440 minutes.

Advanced Tab

The following shows the Encryption Options Advanced tab.

Note The screen shot and table show all of the possible options in the General tab, although the options displayed vary dependent on the configuration of the *BCE_config.xml file*.



Unsecure server URL: http://res.cisco.com
Connection timeout (ms): 20000
Socket timeout (ms): 30000

☐ Display 'Remember user key'
☑ Display 'Remember me'
☐ Display 'Auto open'
☑ Add message bar
☑ Show 'Reply to all' button in the message bar
☑ Open in the same window
☐ Display 'Open offline' checkbox
☐ Display 'Remember envelope key'
☑ Display 'Enable personal security phrase'
☑ Show 'Reply' button in the message bar
☑ Show 'Forward' button in the message bar
☐ Suppress applet from opening

Select from the following Advanced options:

Advanced Option	Value
Unsecure server URL	Unsecure base URL to use for message bar help. If omitted, then external secure URL is used. i.e. http://res.cisco.com.
Connection timeout	Length of time to wait for a connection to the key server to be established.
Socket timeout	Length of time to wait for data from the key server.
Display "Open offline" check box	When selected, the check box for Open offline is visible on the envelope.

Advanced Option	Value
Display "Remember envelope key"	When selected, the check box for Remember envelope key is visible on the envelope.
Display "Enable personal security phrase"	When selected, the check box for Enable personal security phrase is visible on the envelope.
Show "Reply" button in the message bar	If the message bar is enabled, show Reply in the message bar.
Show "Forward" button in the message bar	If message bar is enabled, show Forward in the message bar.
Suppress applet for open	Select to suppress opening the envelope with the applet.
Display "Remember me"	When selected, the check box for Remember me is visible on the envelope.
Display "Auto open"	When selected, the check box for Auto open is visible on the envelope.
Add message bar	Select to add the message bar to the secure message.
Show "Reply to All" button in the message bar	If the message bar is enabled, show Reply to All in the message bar.
Open in the same window	Select to open the secure message in the same window as the envelope.

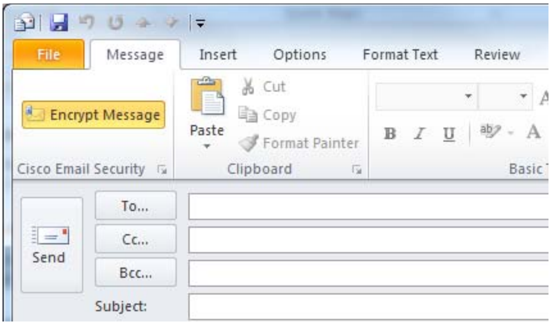
Sending Encrypted Email

Note The default maximum size of an encrypted email is 7 MB before attachments, although this value can be changed by the administrator in the *BCE_Config.xml* file.

The end user can send secure emails by clicking the **Encrypt Message** button while composing an email. Before sending a secure message, verify that the Encrypt Message button is selected.

The Encrypt Message button is available when composing emails.

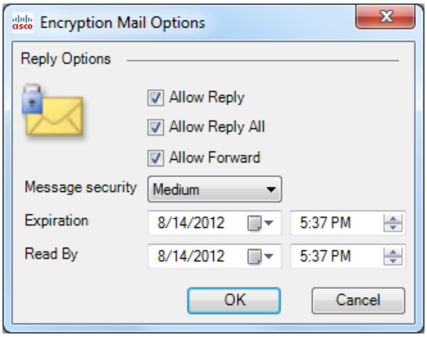
The following shows the Encrypt Message button in the Mail Compose page and the Encryption Mail Options toggle button:



To view the Encryption Mail Options page, click the **Cisco Email Security** launcher in the right-bottom corner.

Encryption Mail Options page:

Note The screen shot and table show all of the possible options in the Encryption Mail Options, although the options displayed vary dependent on the configuration of the *BCE_config.xml file*.



☑ Allow Reply

☑ Allow Reply All

☑ Allow Forward

Message security: Medium

Expiration: 8/14/2012 5:37 PM

Read By: 8/14/2012 5:37 PM

Note When modifying the Encryption Mail Options, the changes are applied only to the email message being composed.

Select from the following Mail options:

Encryption Mail Options	Description
Allow Reply	When selected, the recipient is able to reply to the encrypted email and the reply email message is automatically encrypted.
Allow Reply All	When selected, the recipient is able to reply to all who received the encrypted email and the reply email message is automatically encrypted.
Allow Forward	When selected, the recipient is able to forward the encrypted email and the forwarded email message is automatically encrypted.
Message security	From the drop-down list, set the security for the encrypted email. The default value is the value set in the *BCE_Config.xml* file. **Note** Changing the message security here applies only to the message being composed. • **High**. A high security message requires a password for authentication every time an encrypted message is decrypted. • **Medium**. If the recipient password is cached, a medium security message does not require a password when the message is decrypted. • **Low.** A low security message is transmitted securely but does not require a password to decrypt an encrypted message.

Encryption Mail Options	Description
Expiration	From the drop-down, specify how long (date and time) the encrypted email remains valid. After the expiry date and time is met, the message expires, and it cannot be opened by the recipient after this time.
Read By	From the drop-down, specify the date and time by which the recipient is expected to read the encrypted message. If the message is not read within the specified time frame, the sender is notified.

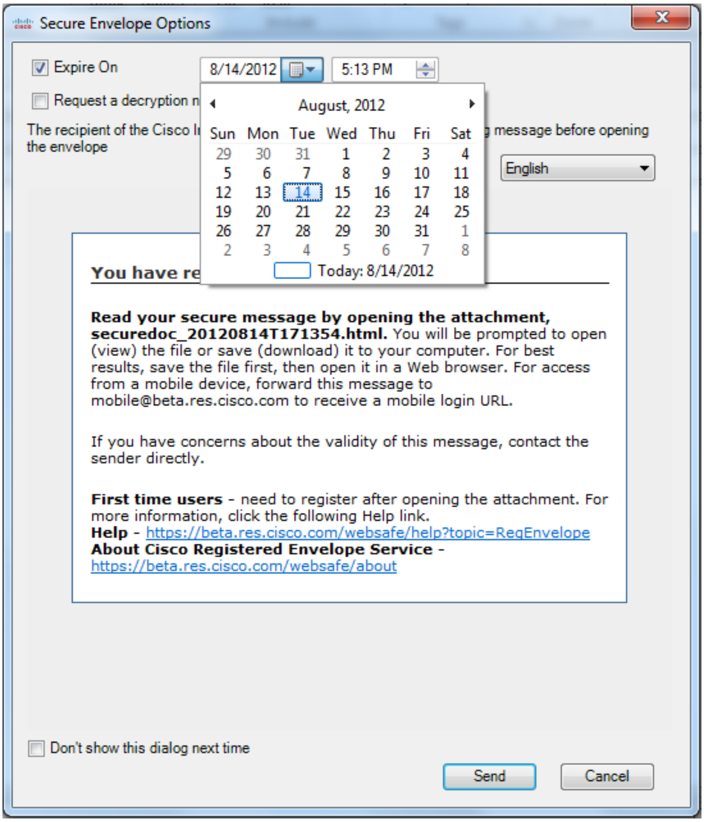
When the end user clicks **Send**, the Secure Envelope Options page displays unless this option is disabled. See Errors and Troubleshooting, page 4-48.

Propagating Reply Options

When a message is decrypted, all settings for the Reply, Reply All, or Forward options and Message Sensitivity options are inherited from the original message and cannot be changed. For example:

- By default, the message is encrypted when replied to or forwarded.
- If the options Reply, Reply All, or Forwarded are not allowed from the original message, a reply or forwarded message cannot be sent and the end user is notified when they click **Send**.
- Recipients included in the original message cannot be removed when the end user performs the options of Reply, Reply All, or Forwarded.
- Recipients not included in the original message cannot be added when the end user performs the options of Reply, Reply All, or Forwarded.
- Recipients cannot be mixed or moved between the To, Cc, or Bcc fields when the end user performs the options of Reply, Reply All, or Forwarded.
- If the account is configured for Decrypt Only or Flag Encrypt, a reply or forwarded message cannot be sent and the end user is notified when they click **Send**.
- If the account Message Sensitivity is set to High, the Reply, Reply All, or Forwarded message will have High sensitivity.
- If the account Message Sensitivity is set to Medium, the Reply, Reply All, or Forwarded message will have Medium sensitivity.
- If the account Message Sensitivity is set to Low, the Reply, Reply All, or Forwarded message will have Medium sensitivity.
- A Reply, Reply All, or Forwarded message is saved in the Sent Items folder and can be decrypted by the sender.
- If a message contains a *BCE_Config_signed.xml* file and is forwarded to another end user, versus received from an administrator, the auto configuration will not work and an error is received.

Secure Envelope Options page:



Secure Envelope Options

☑ Expire On 8/14/2012 5:13 PM

□ Request a decryption n

The recipient of the Cisco I ... message before opening the envelope

English

August, 2012

Sun	Mon	Tue	Wed	Thu	Fri	Sat
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	1
2	3	4	5	6	7	8

Today: 8/14/2012

You have re

Read your secure message by opening the attachment, securedoc_20120814T171354.html. You will be prompted to open (view) the file or save (download) it to your computer. For best results, save the file first, then open it in a Web browser. For access from a mobile device, forward this message to mobile@beta.res.cisco.com to receive a mobile login URL.

If you have concerns about the validity of this message, contact the sender directly.

First time users - need to register after opening the attachment. For more information, click the following Help link.
Help - https://beta.res.cisco.com/websafe/help?topic=RegEnvelope
About Cisco Registered Envelope Service - https://beta.res.cisco.com/websafe/about

□ Don't show this dialog next time

The end user can select from the following Secure Envelope Options:

Secure Envelope Option	Description
Expire on	Select to enable this option. Specify date and time the encrypted email will expire. After date and time is met, the message expires, and it cannot be opened by the recipient after this time. Date and time are displayed in the local time zone of the sender.
Request a Decryption Notification	Allows the sender to request a decryption notification for the message. When the encrypted message is opened, the sender will receive a notification.
Language	Select a language to use for the notification text. Once a language is selected from the drop-down list, the recipient notification displays in the selected language.

If the end user's account is configured for Flag Encryption, the email is flagged to be encrypted before it is sent from their organization. If the end user's account is configured for Desktop Encryption, the email is encrypted at their desktop before it is sent to the Exchange Server.

Manage Secure Messages

The Manage Secure Messages page displays sent encrypted emails. With this option, the end user can perform the following on encrypted emails that they sent:

- **Lock email**. The end user can lock encrypted email that were previously sent. They can also set a lock reason or update the lock reason if the message is already locked. A locked email cannot be opened by the recipient.
- **Unlock email**. The end user can unlock encrypted email that they previously sent, allowing the recipient to decrypt the email.

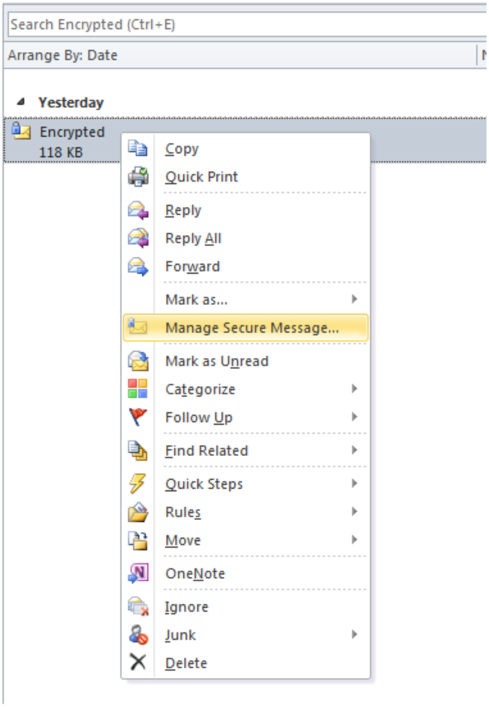
- **Update expiration date**. The end user can set, update, or clear and expiration date on a sent encrypted email. When an encrypted email is expired, the recipient is unable to decrypted the email.

To access the Manage Secure Messages page.

Step 1 Select the encrypted email that you sent and want to modify, then right-click the email to display the **Manage Secure Messages** menu.

The end user can also access the Manage Secure Messages menu when decrypting an encrypted email. If they are a sender of the current email, they will see the Manage Secure Messages button in the toolbar.

Manage Secure Messages Menu Option:



Step 2 Select **Manage Secure Messages**. If the end user password is not cached, they will be asked to enter their password.

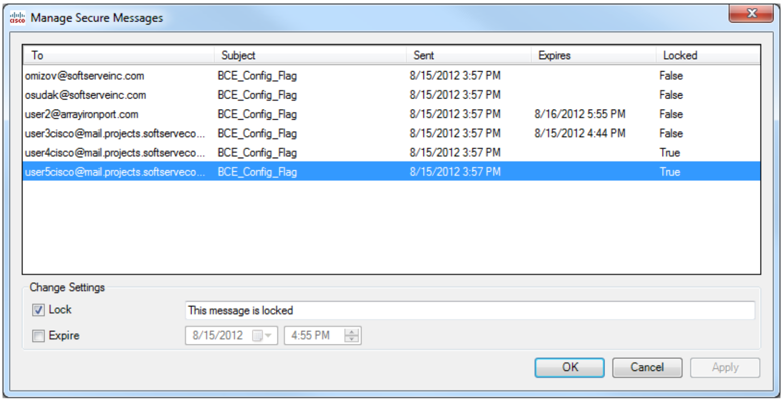
Step 3 To set the lock or expiration option per recipient, select an encrypted email message that you sent, right-click the selected email and select **Manage Secure Messages**.

-OR-

Select multiple encrypted email messages that you sent, right-click the selected emails, select **Manage Secure Messages** and lock all selected encrypted email messages..

Note When accessing the Manage Secure Messages menu from the toolbar, the expiration settings can be applied for only one message at a time.

Manage Secure Messages page:



Manage Secure Messages

To	Subject	Sent	Expires	Locked
omizov@softserveinc.com	BCE_Config_Flag	8/15/2012 3:57 PM		False
osudak@softserveinc.com	BCE_Config_Flag	8/15/2012 3:57 PM		False
user2@arrayironport.com	BCE_Config_Flag	8/15/2012 3:57 PM	8/16/2012 5:55 PM	False
user3cisco@mail.projects.softserveco...	BCE_Config_Flag	8/15/2012 3:57 PM	8/15/2012 4:44 PM	False
user4cisco@mail.projects.softserveco...	BCE_Config_Flag	8/15/2012 3:57 PM		True
user5cisco@mail.projects.softserveco...	BCE_Config_Flag	8/15/2012 3:57 PM		True

Change Settings

☑ Lock This message is locked

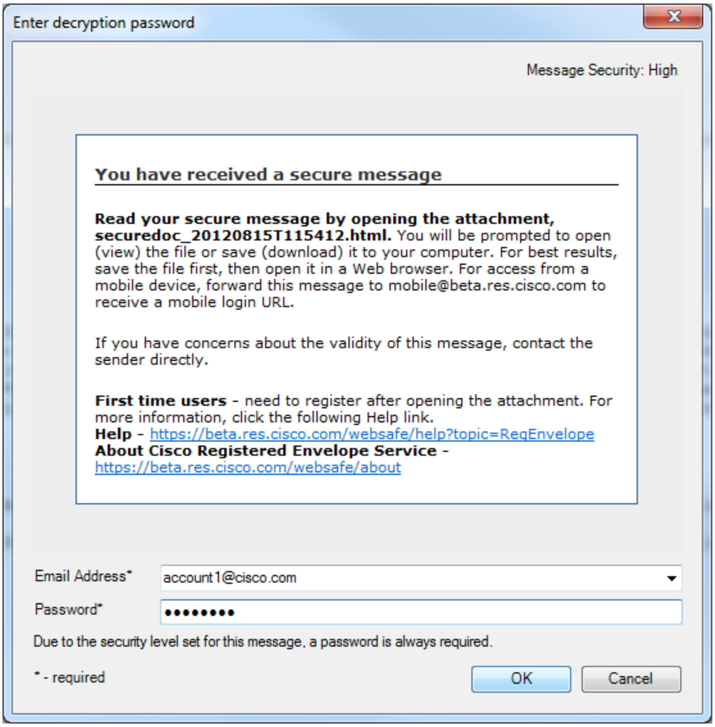
☐ Expire 8/15/2012 4:55 PM

Receiving Secure Emails

The Desktop Encryption plug-in automatically detects secure emails and attempts to decrypt them in Outlook. When the end user receives an encrypted message, they will usually need to enter their encryption password in order to open the envelope. The secure message can be set with a message security of High, Medium, or Low.

Note If the end user receives a password-protected security message, they may need to register and set up a user account with Cisco Registered Envelope Service (CRES) to open their encrypted message. After the end user enrolls with the service, they can use their account password to open all Registered Envelopes that they receive. For more information, see Opening Your First Encrypted Secure Message, page 4-42.

Message Security High page:



You have received a secure message

Read your secure message by opening the attachment, securedoc_20120815T115412.html. You will be prompted to open (view) the file or save (download) it to your computer. For best results, save the file first, then open it in a Web browser. For access from a mobile device, forward this message to mobile@beta.res.cisco.com to receive a mobile login URL.

If you have concerns about the validity of this message, contact the sender directly.

First time users - need to register after opening the attachment. For more information, click the following Help link.
Help - https://beta.res.cisco.com/websafe/help?topic=RegEnvelope
About Cisco Registered Envelope Service - https://beta.res.cisco.com/websafe/about

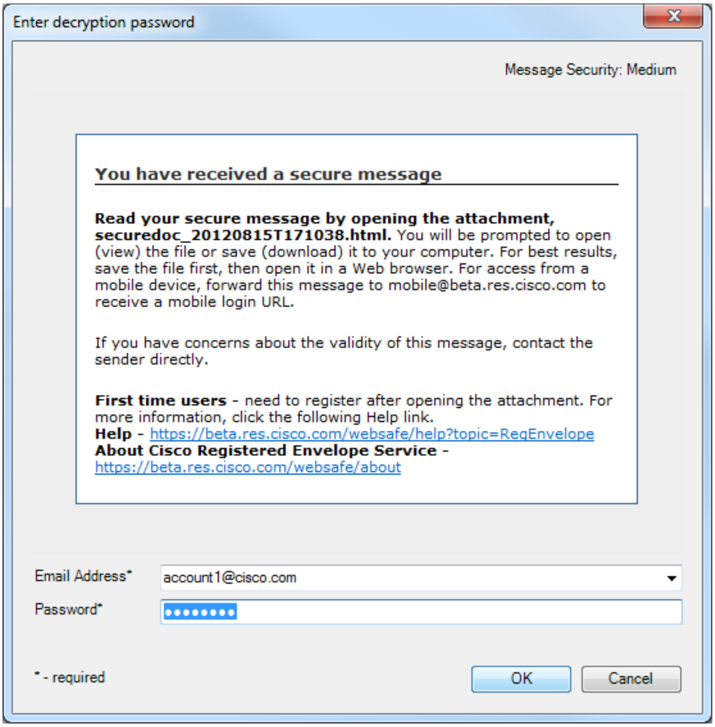
Email Address* account1@cisco.com

Password* ••••••••

Due to the security level set for this message, a password is always required.

* - required

Message Security Medium page:



You have received a secure message

Read your secure message by opening the attachment, securedoc_20120815T171038.html. You will be prompted to open (view) the file or save (download) it to your computer. For best results, save the file first, then open it in a Web browser. For access from a mobile device, forward this message to mobile@beta.res.cisco.com to receive a mobile login URL.

If you have concerns about the validity of this message, contact the sender directly.

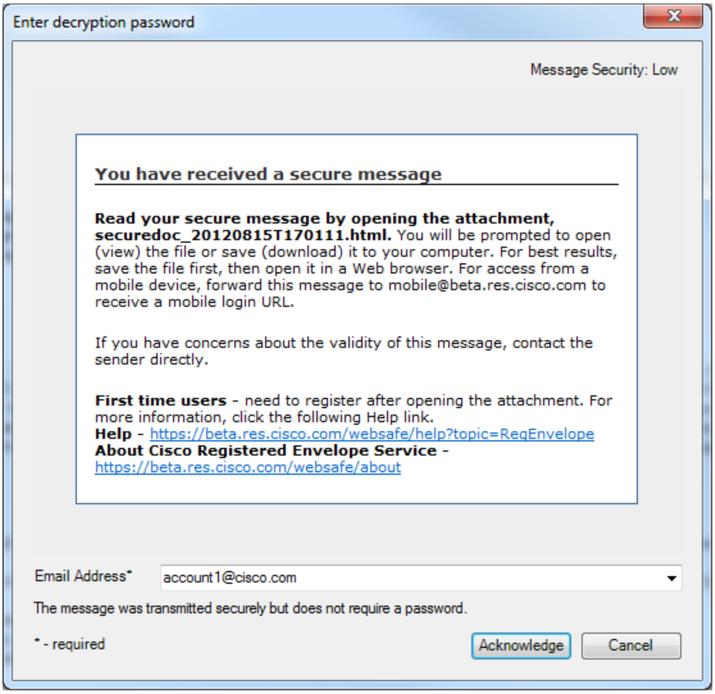
First time users - need to register after opening the attachment. For more information, click the following Help link.
Help - https://beta.res.cisco.com/websafe/help?topic=RegEnvelope
About Cisco Registered Envelope Service -
https://beta.res.cisco.com/websafe/about

Email Address* account1@cisco.com

Password* ••••••••

* - required

Message Security Low page:



Message Security: Low

You have received a secure message

Read your secure message by opening the attachment, securedoc_20120815T170111.html. You will be prompted to open (view) the file or save (download) it to your computer. For best results, save the file first, then open it in a Web browser. For access from a mobile device, forward this message to mobile@beta.res.cisco.com to receive a mobile login URL.

If you have concerns about the validity of this message, contact the sender directly.

First time users - need to register after opening the attachment. For more information, click the following Help link.
Help - https://beta.res.cisco.com/websafe/help?topic=RegEnvelope
About Cisco Registered Envelope Service - https://beta.res.cisco.com/websafe/about

Email Address* account1@cisco.com

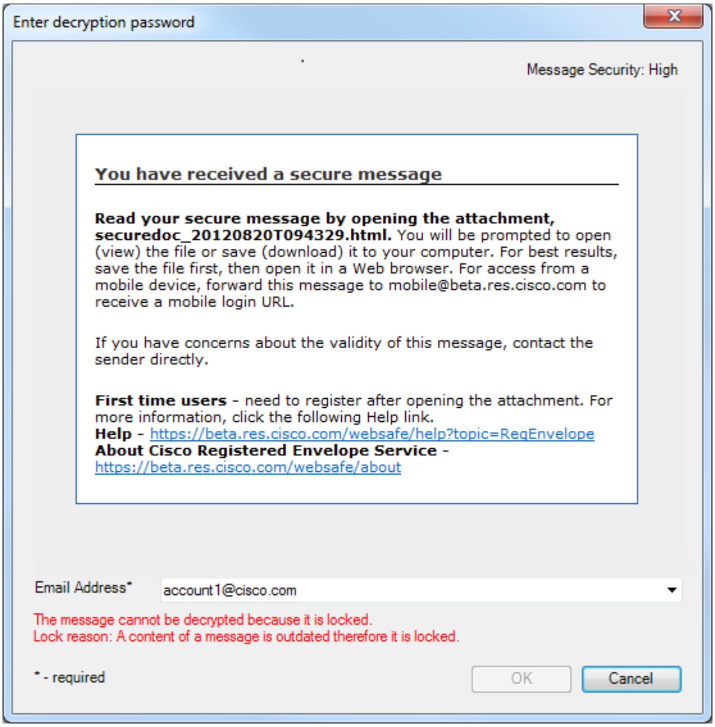
The message was transmitted securely but does not require a password.

* - required

The following describes the Message Security Options:

Message Security Options	Description
High	A high security message requires a password for authentication every time an encrypted message is decrypted.
Medium	If the recipient password is cached, a medium security message does not require a password when the message is decrypted.
Low	A low security message is transmitted securely but does not require a password to decrypt an encrypted message.

If the end user receives a secure message that has been locked or expired, they are notified with a message in red text in the Message Security page.



You have received a secure message

Read your secure message by opening the attachment, securedoc_20120820T094329.html. You will be prompted to open (view) the file or save (download) it to your computer. For best results, save the file first, then open it in a Web browser. For access from a mobile device, forward this message to mobile@beta.res.cisco.com to receive a mobile login URL.

If you have concerns about the validity of this message, contact the sender directly.

First time users - need to register after opening the attachment. For more information, click the following Help link.
Help - https://beta.res.cisco.com/websafe/help?topic=RegEnvelope
About Cisco Registered Envelope Service - https://beta.res.cisco.com/websafe/about

Email Address*: account1@cisco.com

The message cannot be decrypted because it is locked.
Lock reason: A content of a message is outdated therefore it is locked.

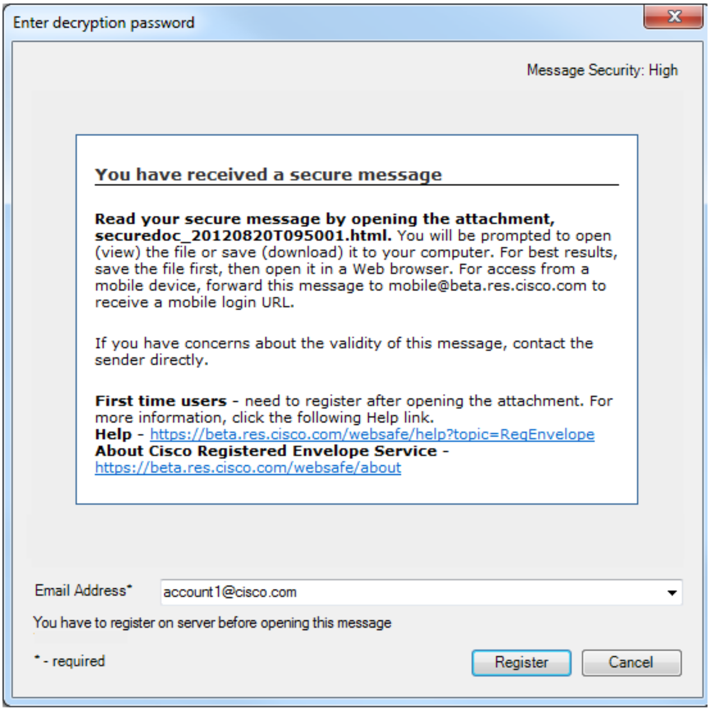
Opening Your First Encrypted Secure Message

If the end user receives an encrypted secure message, they may need to register and set up a user account with Cisco Registered Envelope Service (CRES) to open their encrypted message. After the end user enrolls with the service, they can use their account password to open all encrypted secure messages that they receive.

To open your first encrypted secure message:

Step 1 Double-click the secure email message in your mailbox. Decryption dialog with the register button displays.

Step 2 Click **Register** to enroll with the Cisco Registered Envelope Service (CRES).



You have received a secure message

Read your secure message by opening the attachment, securedoc_20120820T095001.html. You will be prompted to open (view) the file or save (download) it to your computer. For best results, save the file first, then open it in a Web browser. For access from a mobile device, forward this message to mobile@beta.res.cisco.com to receive a mobile login URL.

If you have concerns about the validity of this message, contact the sender directly.

First time users - need to register after opening the attachment. For more information, click the following Help link.
Help - https://beta.res.cisco.com/websafe/help?topic=RegEnvelope
About Cisco Registered Envelope Service - https://beta.res.cisco.com/websafe/about

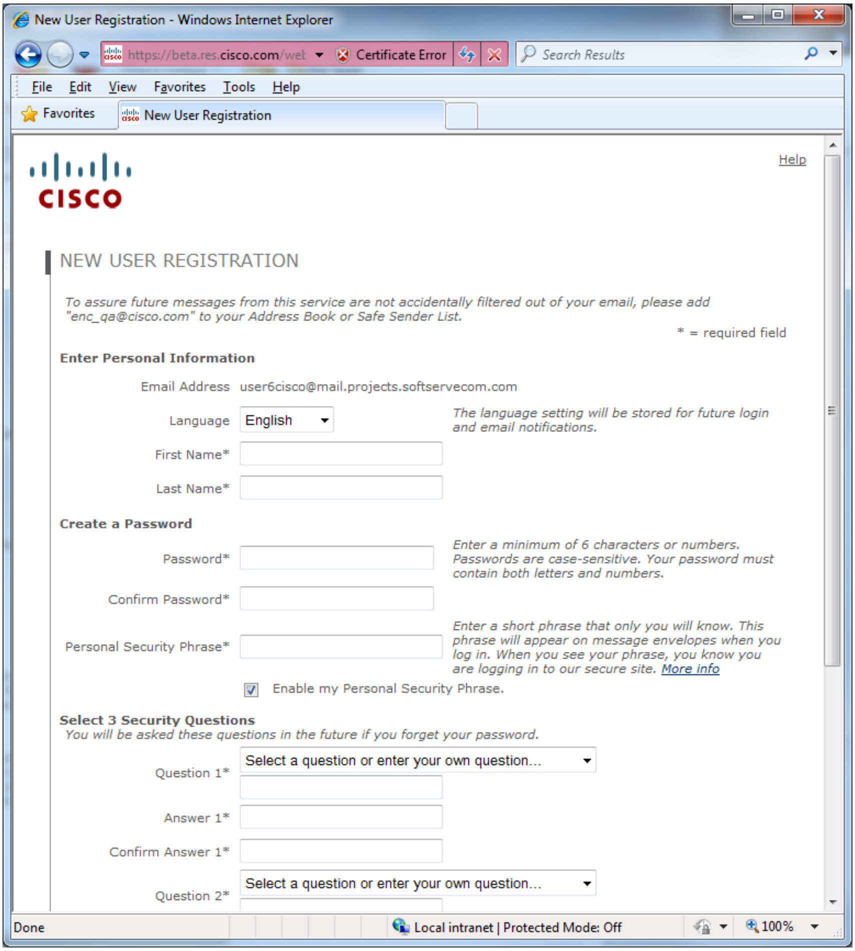
Email Address* account1@cisco.com

You have to register on server before opening this message

* - required

Step 3 Enter the information in the CRES New User Registration page to complete the online registration form.

CRES New User Registration page:



New User Registration - Windows Internet Explorer
https://beta.res.cisco.com/wel
Certificate Error
Search Results
File Edit View Favorites Tools Help
Favorites
New User Registration
Help
Done
Local intranet | Protected Mode: Off
100%

NEW USER REGISTRATION

To assure future messages from this service are not accidentally filtered out of your email, please add "enc_qa@cisco.com" to your Address Book or Safe Sender List.

* = required field

Enter Personal Information

Email Address user6cisco@mail.projects.softservecom.com

Language English — *The language setting will be stored for future login and email notifications.*

First Name*

Last Name*

Create a Password

Password* — *Enter a minimum of 6 characters or numbers. Passwords are case-sensitive. Your password must contain both letters and numbers.*

Confirm Password*

Personal Security Phrase* — *Enter a short phrase that only you will know. This phrase will appear on message envelopes when you log in. When you see your phrase, you know you are logging in to our secure site. More info*

☑ Enable my Personal Security Phrase.

Select 3 Security Questions

You will be asked these questions in the future if you forget your password.

Question 1* Select a question or enter your own question...

Answer 1*

Confirm Answer 1*

Question 2* Select a question or enter your own question...

New User Registration Options:

Field	Description
Language	Optional. Select a language for your CRES account from the drop-down menu. By default the registration page may appear in English but the end user can choose from English, French, German, Spanish, Portuguese, or Japanese.
First Name	Required. Enter the first name of the CRES user account.
Last Name	Required. Enter the last name of the CRES user account.
Password	Required. Enter a password for the account. The password should be at least six characters long and should contain both numbers and letters. **Note** If the end user forgets their password, they can reset it by providing correct answers to the security questions.
Personal Security Phrase	Required. Enter a personal security phrase. A Personal Security Phrase helps protect the end user from password phishing threats. During registration, the end user can specify a short Personal Security Phrase that is known only to the end user and the service. The Personal Security Phrase appears when the end user clicks the password field on Registered Envelopes that they receive. If the end user does not see their Personal Security Phrase, click the link for more information. **Note** If the end user has not selected "Remember me on this computer" then the Personal Security Phrase will not be displayed.

Field	Description
Enable Personal Security Phrase	Optional. Select this check box to enable the personal security phrase.
Security Questions	Required. The end user selects three security questions and must enter and confirm answers to the questions. These questions are used to reset the end user's password if they forget it.

Step 4 Click **Register** at the bottom of the form to create a user account.

Note The end user may need to set up more than one user account if they receive Registered Envelopes at multiple email addresses. A separate user account is needed for each address.

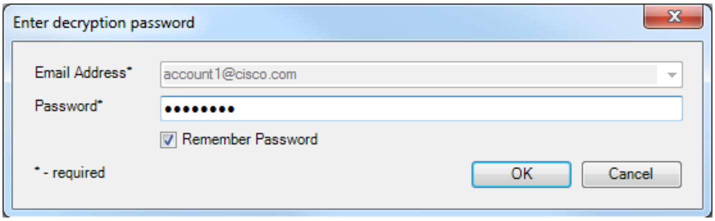
Step 5 Check the email account inbox for an account activation message. In the activation email message, click the **Click here to activate this account** link. A message indicates that the account activation is confirmed and the end user can now view encrypted emails sent to the registered email address.

Step 6 Return to the original email and click the *securedoc_date_time.html* file attachment.

Step 7 Click **Open**. The secure email is decrypted and the message is displayed.

Note Depending on the end user's configuration file settings, some features may not be available. For example, it might not be possible to send a Reply, Reply All, or Forward message.

The password will be saved during the Outlook session. But when Outlook is restarted, the end user needs to enter the password again.



Enter decryption password

Email Address* account1@cisco.com

Password* ••••••••

☑ Remember Password

* - required

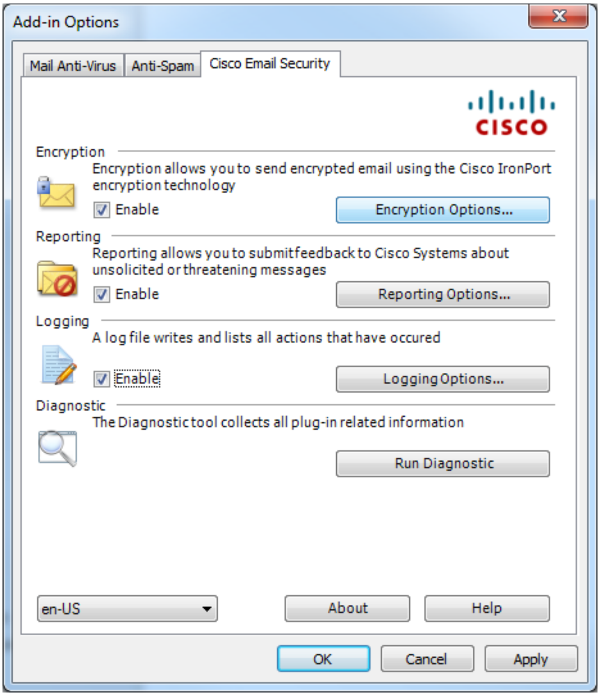
Changing Logging Settings

A log file writes and lists all actions that have occurred.

The Logging Options are located on the Cisco Email Security page. To modify the Logging Options:

- In Outlook 2010, go to **File > Options > Add-Ins > Add-in Options > Cisco Email Security > Logging Options**.
- In Outlook 2003/2007, go to **Tools > Options > Cisco Email Security > Logging Options**.

Cisco Email Security Add-in Options page:



Add-in Options

Encryption

Encryption allows you to send encrypted email using the Cisco IronPort encryption technology

☑ Enable

Reporting

Reporting allows you to submitfeedback to Cisco Systems about unsolicited or threatening messages

☑ Enable

Logging

A log file writes and lists all actions that have occured

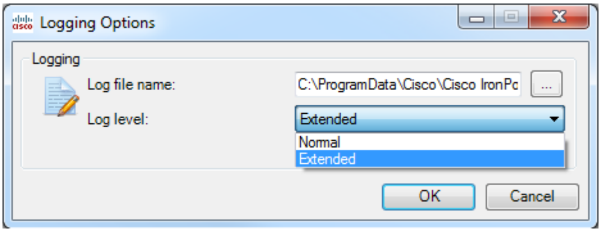
☑ Enable

Diagnostic

The Diagnostic tool collects all plug-in related information

en-US

Encryption Logging Options page:



Logging Options

Logging

Log file name: C:\ProgramData\Cisco\Cisco IronPc

Log level: Extended

Normal
Extended

Logging Options

The end user can configure the following options from the Logging menu.

Option	Description
Log file name	Allows the end user to specify name for the log file that will be stored in %ALLUSERSPROFILE%\Cisco\Cisco IronPort Email Security Plug-in\<username>. The log file name should end with a .log extension.
Log level	• **Normal**. By default, this option is enabled. Normal logging includes fatal, recoverable errors, warnings, and useful information. • **Extended**. Extended logging enables debug log messages in addition to the Normal logging messages.

The end user may want to change logging levels based on the level of troubleshooting they need for a given situation. For example, if they experience issues with the Cisco IronPort Email Security Plug-in, they might set the logging level to **Extended** in order to provide administrators with maximum information, allowing the developers to reproduce issues and run diagnostics.

Errors and Troubleshooting

This section lists some of the common errors that can occur when using the Cisco IronPort Email Security Plug-in for Outlook, and it provides troubleshooting tips for fixing these errors.

Note If the end user receives the same error message several times and the error disrupts the Cisco IronPort Email Security Plug-in for Outlook functionality, they can try running the repair process. See Repairing Cisco Email Security Plug-in for Outlook Files, page 4-53. If the end user encounters the same error after running the repair process, follow the steps to provide Cisco feedback with the Diagnostic tool. See Running the Cisco IronPort Email Security Diagnostic Tool, page 4-55.

Outlook Startup Errors

Error occurred during configuration file initialization

The following messages may appear while Outlook is starting:

- *An error occurred during <file_name> configuration file initialization. Some settings have been set to the default values.*
- *Config validation for account <account_address> has failed. Please set the correct configuration values or contact your administrator.*

These error messages occur if some configuration values are invalid or some configuration files are corrupted in %ALLUSERSPROFILE%\Cisco\Cisco IronPort Email Security Plug-In\<username> folder.

Solution

The Cisco IronPort Email Security Plug-in will not restore default values of some encryption options in corrupted configuration files but will turn off some encryption features instead. If the end user receives an error message repeatedly, run the repair process to fix the configuration files. See Repairing Cisco Email Security Plug-in for Outlook Files, page 4-53.

Configuration file not found

The following error message may display when Outlook is starting:

- *<file_name> configuration file was not found. Settings have been set to the default values.*

Solution

The Cisco IronPort Email Security Plug-in will not restore default values of some encryption options in corrupted configuration files but will set the decryption mode instead. If the end user receives an error message repeatedly, run the repair process to fix the configuration files. See Repairing Cisco Email Security Plug-in for Outlook Files, page 4-53.

Message Reporting Errors

Outlook does not recognize one or more names

The following message may appear when the end user clicks the **Spam, Virus, Phish** or **Not Spam** buttons in Outlook:

- *There was error during email reporting. Description: Outlook does not recognize one or more names.*

This error occurs if the end user is using the Reporting plug-in and Outlook cannot recognize the format of the email message they are attempting to report. The end user will need to repair the Reporting plug-in file to ensure that they can report spam and phishing emails (as well as reporting legitimate mail as "Not Spam").

Solution

Run the repair process. See Repairing Cisco Email Security Plug-in for Outlook Files, page 4-53.

The connection to the server is unavailable

The following message may appear when the end user clicks **Spam, Virus, Phish** or **Not Spam** buttons plug-in buttons in Outlook and use IMAP protocol or "headers only" Outlook property:

- *Error: The connection to the server is unavailable. Outlook must be online or connected to complete this action.*

This error occurs if the end user is trying to report message that downloaded partially (headers only) and the connection to the mail server is off. The Reporting plug-in cannot report a partially downloaded message, and it will attempt to connect to the mail server until it can download a full copy of the message to report.

Solution

Ensure that Outlook has a connection with the mail server before reporting emails with headers only.

Error occurred during connection to server

The following error occurs if Outlook is online but your Internet connection has been lost or the server has become temporarily unavailable.

- *An HTTP error occurred during connection to server.*

Solution

Check your network settings or contact the local administrator.

Decryption and Encryption Errors

When you click **Send**, the Secure Envelope Options page displays unless you have disabled this option. The email account may receive the following status messages:

Your account has been locked

- *Your account has been locked. Please contact your account administrator for more information.*

Solution

Contact the system administrator to unlock the email account.

Your account has been blocked

- *Your account has been blocked and you must reset your password. Please use the forgot password link to reactivate your account. Forgot password?*

Solution

Click the password link and enter the correct answers to the password security challenge questions to reset your password.

Your account has been suspended

- *You have no attempts remaining. Your account is locked for the next 15 minutes.*

Solution

You can attempt to log into https://res.cisco.com/websafe later or contact support at https://res.cisco.com/websafe/help?topic=ContactSupport for assistance.

No recipients

If you do not have a recipent listed in the email that you are sending, you may recieve the following message:

- *An error occurred during encryption: no recipients specified.*

An error occurred during decryption

An unexpected error occurs during message decryption. For example, the SDK returns an unknown error code or the plug-in reports an exception.

- *An error occurred during decryption.*

Solution

Run the diagnostic tool and send the diagnostic report to the support team. See Running the Cisco IronPort Email Security Diagnostic Tool, page 4-55.

An error occurred during encryption

An unexpected error occurs during message encryption. For example, the SDK returns an unknown error code or the plug-in reports an exception.

- *An error occurred during encryption.*

Solution

Run the diagnostic tool and send the diagnostic report to the support team. See Running the Cisco IronPort Email Security Diagnostic Tool, page 4-55.

Exceeds allowable limit

The default maximum size of an encrypted email is 7 MB before attachments, although this value can be changed by the administrator in the *BCE_Config.xml* file. If the encrypted email exceeds the maximum, you may receive one of the following messages:

- *This message exceeds the allowable limit and cannot be decrypted.*
- *This message exceeds the allowable limit and cannot be encrypted.*
- *An error occurred during encryption: an invalid attachment found.*
- *Failed to report this message. This message is too large.*
- *Failed to report {0} messages. {0} messages are too large.*

Note The last two messages for "*Failed to report ...*" are currently in English only.

Repairing Cisco Email Security Plug-in for Outlook Files

To repair Cisco Email Security Plug-in:

Step 1 Make sure Outlook is closed.

Step 2 Go to **Control Panel > Add or Remove Programs**.

Step 3 Find Cisco IronPort Email Security Plug In in the list of programs and click **Uninstall/Change**.

Step 4 Click **Repair**. The installer repair process runs.

Note You are not able to restore or repair the encryption configuration. The encryption configuration is only sent by the administrator in the *BCE_Config.xml* file.

Step 5 Perform the action that caused the error. If the same error occurs after running the repair process, follow the steps to provide Cisco IronPort feedback with the Diagnostic tool. See Running the Cisco IronPort Email Security Diagnostic Tool, page 4-55.

Troubleshooting Using the Diagnostic Tool

The Cisco IronPort Email Security Plug-in includes a diagnostic tool to help Cisco Support in troubleshooting problems. The Diagnostic tool collects important data from the Plug-in tool that can then be sent to Cisco Support to aid them in problem-solving.

The end user may want to use the diagnostic tool if they are receiving errors or if they have issues with the Cisco IronPort Email Security Plug-in that the repair procedure does not resolve. You can also use the diagnostic tool to share critical information with Cisco engineers when reporting a bug.

See Repairing Cisco Email Security Plug-in for Outlook Files, page 4-53 or Running the Cisco IronPort Email Security Diagnostic Tool, page 4-55.

Note If you experience errors, review Errors and Troubleshooting, page 4-48 for troubleshooting tips.

Data Collected by the Cisco IronPort Email Security Diagnostic Tool

The Diagnostic tool collects the following information from your computer:

- Registration information about some COM components
- Environment variables
- Cisco IronPort Email Security Plug-in output files
- Information about Windows and Outlook
- Your system user name and PC name
- Information about other Outlook plug-ins
- Outlook related Windows Event Log entries

Running the Cisco IronPort Email Security Diagnostic Tool

The Cisco Email Security Diagnostic tool can be run from one of the following places:

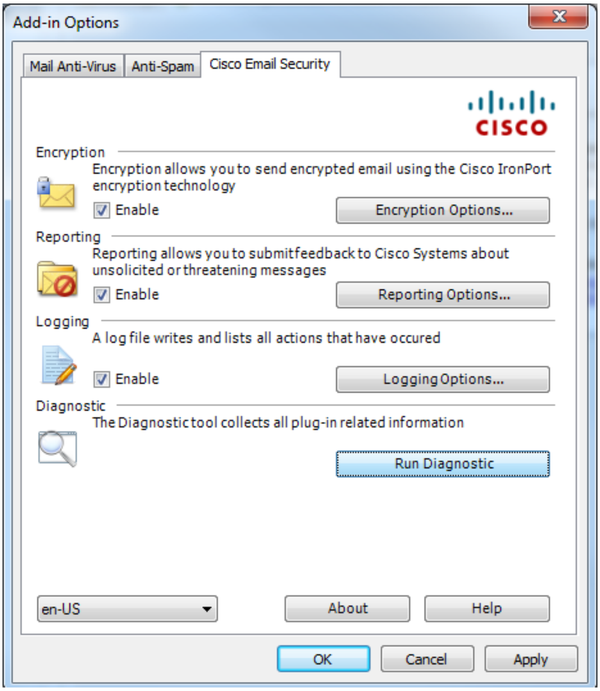
- **From the Cisco Email Security options tab**. Typically, you run the diagnostic tool from the Cisco Email Security options tab.
- **From the "Program Files\ Cisco IronPort Email Security Plug-in" folder** (typically C:\Program Files\Cisco\Cisco IronPort Email Security Plug-in). This is the folder where your Cisco IronPort Email Security Plug-in is installed.
- **From the Start Menu> All Programs > Cisco IronPort Email Security Plug-in > Cisco IronPort Email Security Plug-in Diagnostic.**

Running the Diagnostic Tool from the Outlook Options Page

Step 1 Go to the following to run the Diagnostic tool:

- In Outlook 2010, go to **File > Options > Add-Ins > Add-in Options > Cisco Email Security > Run Diagnostic**.
- In Outlook 2003/2007, go to **Tools > Options > Cisco Email Security > Run Diagnostic**.

Cisco Email Security Add-in Options page:



Add-in Options

Encryption

Encryption allows you to send encrypted email using the Cisco IronPort encryption technology

☑ Enable

Reporting

Reporting allows you to submitfeedback to Cisco Systems about unsolicited or threatening messages

☑ Enable

Logging

A log file writes and lists all actions that have occured

☑ Enable

Diagnostic

The Diagnostictool collects all plug-in related information

en-US

Step 2 Wait a few seconds to allow the Diagnostic tool to collect data. When the Diagnostic tool finishes collecting data, it displays a message indicating that it successfully collected data.

The Diagnostic tool generates the *CiscoDiagnosticReport.zip* file and saves it to the current user's **My Documents** folder. The end user can then send the file to their system administrator or the administrator can send it to their Cisco Support representative. To view the report, double-click the *CiscoDiagnosticsReport.zip* file.

Running the Diagnostic Tool from the Program Files

There are two ways to run the diagnostic tool from the Program files.

- Run the Diagnostic tool from **Start > Programs > Cisco IronPort Email Security Plug-in > Cisco IronPort Email Security Plug-in Diagnostic**.

-OR-

- Go to the folder where Cisco IronPort Email Security Plug-in was installed (typically C:\Program Files\Cisco\Cisco IronPort Email Security Plug-in) and double-click the *Cisco.EmailSecurity.Framework.Diagnostic.exe* file.

Uninstalling the Cisco IronPort Email Security Plug-in

You can uninstall the Cisco IronPort Email Security Plug-in via the **Control Panel** > **Add/Remove Program** option or by running the setup.exe program.

During the uninstall, the following items are removed:

- All registry entries made by the plug-in.
- Entry for the plug-in from the Add/Remove programs listing.
- Some of the files related to the plug-in. Note that not all of the files are removed.
- The plug-in toolbar (removed from Outlook).

Note Uninstalling the plug-in does not affect Outlook performance. Outlook must be closed during the uninstall.

To uninstall the Cisco IronPort Email Security Plug-in for Outlook:

There are two possible ways to uninstall the Cisco IronPort Email Security Plug-in for Outlook:

Step 1 Click **Start** > **Control Panel > Add/Remove Programs**.

Step 2 Select **Cisco IronPort Email Security Plug-In** and click **Uninstall/Change > Next > Remove.**

The second option to uninstall is

- Double-click the plug-in setup file (the file used to install the plug-in) and select the **Remove** option to uninstall the Cisco IronPort Email Security Plug-in.

APPENDIX A

IronPort End User License Agreement

This appendix contains the following section:

Cisco IronPort Systems, LLC Software License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT (“AGREEMENT”) FOR THE LICENSE OF THE SOFTWARE (AS DEFINED BELOW). BY CLICKING THE ACCEPT BUTTON OR ENTERING “Y” WHEN PROMPTED, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY, COLLECTIVELY, THE “COMPANY”) CONSENT TO BE BOUND BY AND BECOME A PARTY TO THE FOLLOWING AGREEMENT BETWEEN CISCO IRONPORT SYSTEMS, LLC, A DELAWARE CORPORATION (“IRONPORT”) AND COMPANY (COLLECTIVELY, THE “PARTIES”). BY CLICKING THE ACCEPT BUTTON OR ENTERING “Y” WHEN PROMPTED, YOU REPRESENT THAT (A) YOU ARE DULY AUTHORIZED TO REPRESENT YOUR COMPANY AND (B) YOU ACCEPT THE TERMS AND CONDITIONS OF THIS AGREEMENT ON BEHALF OF YOUR COMPANY, AND AS SUCH, AN AGREEMENT IS THEN FORMED. IF YOU OR THE COMPANY YOU REPRESENT (COLLECTIVELY, “COMPANY”) DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, CLICK THE CANCEL BUTTON OR ENTER “N” WHEN PROMPTED AND PROMPTLY (BUT NO LATER THAT THIRTY (30) DAYS

OF THE DELIVERY DATE, AS DEFINED BELOW) NOTIFY IRONPORT, OR THE RESELLER FROM WHOM YOU RECEIVED THE SOFTWARE, FOR A FULL REFUND OF THE PRICE PAID FOR THE SOFTWARE.

1. DEFINITIONS

1.1 “Company Service” means the Company’s email or internet services provided to End Users for the purposes of conducting Company’s internal business and which are enabled via Company’s products as described in the purchase agreement, evaluation agreement, beta or pre-release agreement, purchase order, sales quote or other similar agreement between the Company and IronPort or its reseller (“Agreement”) and the applicable user interface and IronPort’s standard system guide documentation that outlines the system architecture and its interfaces (collectively, the “License Documentation”).

1.2 “End User” means the employee, contractor or other agent authorized by Company to access to the Internet or use email services via the Company Service.

1.3 “Service(s)” means (i) the provision of the Software functionality, including Updates and Upgrades, and (ii) the provision of support by IronPort or its reseller, as the case may be.

1.4 “Software” means: (i) IronPort’s proprietary software licensed by IronPort to Company along with IronPort’s hardware products; (ii) any software provided by IronPort’s third-party licensors that is licensed to Company to be implemented for use with IronPort’s hardware products; (iii) any other IronPort software module(s) licensed by IronPort to Company along with IronPort’s hardware products; and (iv) any and all Updates and Upgrades thereto.

1.5 “Updates” means minor updates, error corrections and bug fixes that do not add significant new functions to the Software, and that are released by IronPort or its third party licensors. Updates are designated by an increase to the Software’s release number to the right of the decimal point (e.g., Software 1.0 to Software 1.1). The term Updates specifically excludes Upgrades or new software versions marketed and licensed by IronPort or its third party licensors as a separate product.

1.6 “Upgrade(s)” means revisions to the Software, which add new enhancements to existing functionality, if and when it is released by IronPort or its third party licensors, in their sole discretion. Upgrades are designated by an increase in the Software’s release number, located to the left of the decimal point (e.g., Software

1.x to Software 2.0). In no event shall Upgrades include any new versions of the Software marketed and licensed by IronPort or its third party licensors as a separate product.

2. LICENSE GRANTS AND CONSENT TO TERMS OF DATA COLLECTION

2.1 License of Software. By using the Software and the License Documentation, Company agrees to be bound by the terms of this Agreement, and so long as Company is in compliance with this Agreement, IronPort hereby grants to Company a non-exclusive, non-sublicensable, non-transferable, worldwide license during the Term to use the Software only on IronPort's hardware products, solely in connection with the provision of the Company Service to End Users. The duration and scope of this license(s) is further defined in the License Documentation. Except as expressly provided herein, no right, title or interest in any Software is granted to the Company by IronPort, IronPort's resellers or their respective licensors. This license and any Services are co-terminus.

2.2 Consent and License to Use Data. Subject to Section 8 hereof, and subject to the IronPort Privacy Statement at http://www.IronPort.com/privacy.html, as the same may be amended from time to time by IronPort with notice to Company, Company hereby consents and grants to IronPort a license to collect and use the data from the Company as described in the License 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. Notwithstanding the foregoing, Company may terminate IronPort's right to collect and use Data at any time upon prior written or electronic notification, provided that the Software or components of the Software may not be available to Company if such right is terminated.

3. CONFIDENTIALITY. Each Party agrees to hold in confidence all Confidential Information of the other Party to the same extent that it protects its own similar Confidential Information (and in no event using less than a reasonable degree of care) and to use such Confidential Information only as permitted under this Agreement. For purposes of this Agreement "Confidential Information" means information of a party marked "Confidential" or information reasonably considered by the disclosing Party to be of a proprietary or confidential nature; provided that the Data, the Software, information disclosed in design reviews and any pre-production releases of the Software provided by IronPort is expressly designated Confidential Information whether or not marked as such.

4. PROPRIETARY RIGHTS; OWNERSHIP. Title to and ownership of the Software and other materials and all associated Intellectual Property Rights (as defined below) related to the foregoing provided by IronPort or its reseller to Company will remain the exclusive property of IronPort and/or its superior licensors. Company and its employees and agents will not remove or alter any trademarks, or other proprietary notices, legends, symbols, or labels appearing on or in copies of the Software or other materials delivered to Company by IronPort or its reseller. Company will not modify, transfer, resell for profit, distribute, copy, enhance, adapt, translate, decompile, reverse engineer, disassemble, or otherwise determine, or attempt to derive source code for any Software or any internal data files generated by the Software or to create any derivative works based on the Software or the License Documentation, and agrees not to permit or authorize anyone else to do so. Unless otherwise agreed in writing, any programs, inventions, concepts, documentation, specifications or other written or graphical materials and media created or developed by IronPort or its superior licensors during the course of its performance of this Agreement, or any related consulting or professional service agreements, including all copyrights, database rights, patents, trade secrets, trademark, moral rights, or other intellectual property rights ("Intellectual Property Right(s)") associated with the performance of such work shall belong exclusively to IronPort or its superior licensors and shall, in no way be considered a work made for hire for Company within the meaning of Title 17 of the United States Code (Copyright Act of 1976).

5. LIMITED WARRANTY AND WARRANTY DISCLAIMERS

5.1 Limited Warranty. IronPort warrants to Company that the Software, when properly installed and properly used, will substantially conform to the specifications in the License Documentation for a period of ninety (90) days from the delivery date or the period set forth in the License Documentation, whichever is longer ("Warranty Period"). FOR ANY BREACH OF THE WARRANTY CONTAINED IN THIS SECTION, COMPANY'S EXCLUSIVE REMEDY AND IRONPORT'S ENTIRE LIABILITY, WILL BE PROMPT CORRECTION OF ANY ERROR OR NONCONFORMITY, PROVIDED THAT THE NONCONFORMITY HAS BEEN REPORTED TO IRONPORT AND/OR ITS RESELLER BY COMPANY WITHIN THE WARRANTY PERIOD. THIS WARRANTY IS MADE SOLELY TO COMPANY AND IS NOT TRANSFERABLE TO ANY END USER OR OTHER THIRD PARTY. IronPort shall have no liability for breach of warranty under this Section or otherwise for breach of this Agreement if such breach arises directly or indirectly out of or in connection with the following: (i) any unauthorized, improper, incomplete or inadequate maintenance or calibration of the Software by Company or any third party; (ii) any third party hardware software, services or system(s); (iii) any unauthorized modification or alteration of the Software or Services; (iv) any unauthorized or improper use or operation of the Software or Company's failure to comply with any applicable environmental specification; or (v) a failure to install and/or use Updates, Upgrades, fixes or revisions provided by IronPort or its resellers from time to time.

5.2 WARRANTY DISCLAIMER. THE EXPRESS WARRANTIES SET FORTH IN SECTION 5.1 OF THIS AGREEMENT CONSTITUTE THE ONLY PERFORMANCE WARRANTIES WITH RESPECT TO THE SOFTWARE OR SERVICES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IRONPORT LICENSES THE SOFTWARE AND SERVICES HEREUNDER ON AN “AS IS” BASIS. EXCEPT AS SPECIFICALLY SET FORTH HEREIN, IRONPORT AND ITS SUPERIOR LICENSORS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, OR STATUTORY (EITHER IN FACT OR BY OPERATION OF LAW), AND EXPRESSLY DISCLAIM ALL OTHER WARRANTIES, INCLUDING WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. NEITHER IRONPORT NOR ITS THIRD PARTY LICENSORS WARRANT THAT THE SOFTWARE OR SERVICES (1) IS FREE FROM DEFECTS, ERRORS OR BUGS, (2) THAT OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED, OR (3) THAT ANY RESULTS OR INFORMATION THAT IS OR MAY BE DERIVED FROM THE USE OF THE SOFTWARE WILL BE ACCURATE, COMPLETE, RELIABLE AND/OR SECURE.

6. LIMITATION OF LIABILITY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER FOR ANY LOSS OF PROFITS, COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF BUSINESS, LOSS OF USE OR DATA, INTERRUPTION OF BUSINESS, OR FOR INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES OF ANY KIND, EVEN IF SUCH PARTY RECEIVED ADVANCE NOTICE OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF EITHER PARTY ARISING UNDER ANY PROVISION OF THIS AGREEMENT, REGARDLESS OF WHETHER THE CLAIM FOR SUCH DAMAGES IS BASED IN CONTRACT, TORT, OR OTHER LEGAL THEORY, EXCEED THE TOTAL AMOUNT PAID FOR THE SOFTWARE OR SERVICES DURING THE TWELVE (12) MONTHS PRIOR TO THE EVENT GIVING RISE TO SUCH LIABILITY.

7. TERM AND TERMINATION. The term of this Agreement shall be as set forth in the License Documentation (the “Term”). If IronPort defaults in the performance of any material provision of this Agreement or the License Documentation, then Company may terminate this Agreement upon thirty (30) days written notice if the default is not cured during such thirty (30) day period. If Company defaults in the performance of any material provision of this Agreement or the License Documentation, IronPort may terminate this Agreement upon thirty (30) days written notice if the default is not cured during such thirty (30) day notice and without a refund. This Agreement may be terminated by one Party immediately at any time, without notice, upon (i) the institution by or against the other Party of insolvency, receivership or bankruptcy proceedings or any other proceedings for the settlement of such Party’s debts, (ii) such other Party making a general assignment for the benefit of creditors, or (iii) such other Party’s dissolution. The license granted in Section 2 will immediately terminate upon this Agreement’s termination or expiration. Within thirty (30) calendar days after termination or expiration of this Agreement, Company will deliver to IronPort or its reseller or destroy all copies of the Software and any other materials or documentation provided to Company by IronPort or its reseller under this Agreement.

8. U.S. GOVERNMENT RESTRICTED RIGHTS; EXPORT CONTROL. The Software and accompanying License Documentation are deemed to be “commercial computer software” and “commercial computer software documentation,” respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying License Documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement. Company acknowledges that the Software and License Documentation must be exported in accordance with U.S. Export Administration Regulations and diversion contrary to U.S. laws is prohibited. Company represents that neither the United States Bureau of Export Administration nor any other federal agency has suspended, revoked or denied Company export privileges. Company represents that Company will not use or transfer the Software for end use relating to any nuclear, chemical or biological weapons, or missile technology unless authorized by the U.S. Government by regulation or specific license. Company acknowledges it is Company’s ultimate responsibility to comply with any and all import and export restrictions, and other applicable laws, in the U.S. or elsewhere, and that IronPort or its reseller has no further responsibility after the initial sale to Company within the original country of sale.

9. MISCELLANEOUS. This Agreement is governed by the laws of the United States and the State of California, without reference to conflict of laws principles. The application of the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded. Nothing contained herein shall be construed as creating any agency, partnership, or other form of joint enterprise between the parties. Neither party shall be liable hereunder by reason of any failure or delay in the performance of its obligations hereunder (except for the payment of money) on account of (i) any provision of any present or future law or regulation of the United States or any applicable law that applies to the subject hereof, and (ii) interruptions in the electrical supply, failure of the Internet, strikes, shortages, riots, insurrection, fires, flood, storm, explosions, acts of God, war, terrorism, governmental action, labor conditions, earthquakes, or any other cause which is beyond the reasonable control of such party. This Agreement and the License Documentation set forth all rights for the user of the Software and is the entire agreement between the parties and supersedes any other communications with respect to the Software and License Documentation. The terms and conditions of this Agreement will prevail, notwithstanding any variance with the License Documentation or any purchase order or other written instrument submitted by a party, whether formally rejected by the other party or not. This Agreement may not be modified except by a written addendum issued by a duly authorized representative of IronPort, except that IronPort may modify the IronPort Privacy Statement at any time, in its discretion, via notification to Company of such modification that will be posted at http://www.IronPort.com/privacy.html. No provision hereof shall be deemed waived unless such waiver shall be in writing and signed by IronPort or a duly authorized representative of IronPort. If any provision of this Agreement is held invalid, the remainder of this Agreement shall continue in full force and effect. The parties confirm that it is their wish that this Agreement has been written in the English language only.

10. IRONPORT CONTACT INFORMATION. If Company wants to contact IronPort for any reason, please write to IronPort Systems, Inc., 950 Elm Avenue, San Bruno, California 94066, or call or fax us at tel: 650.989.6500 and fax: 650.989.6543.