Cisco IronPort Email Security Plug-in 7.1 Administrator Guide

December 6, 2010

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

Cisco IronPort Email Security Plug-in 7.1 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 combines two frequently-used email security plug-ins, the Cisco Encryption plug-in-- which allows users to encrypt messages from their email programs and the Cisco Reporting plug-in-- which allows users to report spam, virus, or misclassified email. By combining these plug-ins, Cisco makes it simpler for users to access and modify their email security plug-ins, and it also streamlines the process of installing and updating email security plug-ins. In addition, the Cisco IronPort Email Security Plug-in provides a standard installer based on the Windows Installer. The installer supports standard Windows installer command-line options including silent installation with response file.

Supported Configurations

The following configurations are supported:

Cisco IronPort Email Security Plug-in 7.1.x	Outlook 2003	Outlook 2007	Outlook 2010	Notes 6.x	Notes 7.x	Notes 8.0.x	Notes 8.5.x
XP 32 bit	certified	certified	certified	certified	certified	certified	certified
XP 64 bit	compatible	compatible	compatible	compatible	compatible	compatible	compatible
Vista 32 bit	certified	certified	certified	compatible	compatible	compatible	certified
Vista 64 bit	compatible	certified	certified	compatible	compatible	certified	compatible
Win 7 32 bit	certified	certified	certified	compatible	compatible	certified	certified
Win 7 64 bit	compatible	certified	certified	compatible	compatible	compatible	certified
Citrix	not supported	not supported	not supported	not supported	not supported	not supported	not supported

Note The Cisco IronPort Email Security Plug-in requires Windows Installer 2.0 or higher.

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. To understand how to configure the Cisco IronPort Encryption appliance, you may want to review the following guides:

- *IronPort AsyncOS for Email Encryption User Guide*. This guide provides instructions for configuring email encryption, and it will help you to understand how to configure your encryption appliance settings to work with the plug-in settings you configure.

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.

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 1-4 to determine which chapters are relevant to your particular configuration.

The 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 by clicking the Help button.

How This Book Is Organized

Chapter 1, "Getting Started with the Cisco IronPort Email Security Plug-in" provides an introduction to the 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 creating a response file, running the install, and files you may wish to modify prior to installation.

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 configuring the reporting plug-in and the encryption plug-in.

Chapter 5, "Configuring and Using the Cisco IronPort Email Security Plug-in for Lotus Notes" provides instructions for configuring the Cisco IronPort Email Security Plug-in for Lotus Notes. It includes steps for configuring the reporting plug-in and the encryption plug-in, along with instructions for using the plug-ins from the Lotus Notes Mail program.

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

Typographic Conventions

Typeface	Meaning	Examples
AaBbCc123	The names of commands, files, and directories; on-screen computer output.	`Please choose an IP interface for this Listener.` The `sethostname` command sets the name of the IronPort appliance.
AaBbCc123	User input, in contrast to on-screen computer output.	`mail3.example.com>` **`commit`** `Please enter some comments describing your changes:` `[]>` **`Changed the system hostname`**

AaBbCc123	Book titles, new terms, emphasized words, and command line variables; for command line variables, the italicized text is a placeholder for the actual name or value.	Read the *IronPort Quickstart Guide*.
		
		The IronPort appliance *must* be able to uniquely select an interface to send an outgoing packet.
		
		`Before you begin, please reset your password to a new value.`
		`Old password:` **`ironport`**
		`New password:` *`your_new_password`*
		`Retype new password:`
		`your_new_password`

Where to Find More Information

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

IronPort Technical Training

Cisco IronPort Systems Technical Training Services can help you acquire the knowledge and skills necessary to successfully evaluate, integrate, deploy, maintain, and support Cisco IronPort security products and solutions.

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

Training. For question relating to registration and general training:

- http://training.ironport.com
- training@ironport.com

Certifications. For questions relating to certificates and certification exams:

- http://training.ironport.com/certification.html
- certification@ironport.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`

Note You need a Cisco.com User ID to access the site. If you do not have a Cisco.com User ID, you can register for one here:
`https://tools.cisco.com/RPF/register/register.do`

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 access the Cisco Support Community at the following URL:

`https://supportforums.cisco.com`

Cisco IronPort Customer Support

You can request our support by phone, email, or online 24 hours a day, 7 days a week. Cisco IronPort Customer Support service level agreement details are available on the Support Portal.

To report a critical issue that requires urgent assistance outside of Customer Support hours, contact Cisco IronPort using one of the following methods:

U.S. Toll-free: 1 (877) 646-4766

Support Site: `http://www.cisco.com/web/ironport/index.html`

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

Third Party Contributors

Some software included within IronPort AsyncOS is distributed under the terms, notices, and conditions of software license agreements of FreeBSD, Inc., Stichting Mathematisch Centrum, Corporation for National Research Initiatives, Inc., and other third party contributors, and all such terms and conditions are incorporated in IronPort license agreements.

The full text of these agreements can be found here:

https://support.ironport.com/3rdparty/AsyncOS_User_Guide-1-1.html.

Portions of the software within IronPort AsyncOS is based upon the RRDtool with the express written consent of Tobi Oetiker.

Portions of this document are reproduced with permission of Dell Computer Corporation. Portions of this document are reproduced with permission of McAfee, Inc. Portions of this document are reproduced with permission of Sophos Plc.

Cisco IronPort Welcomes Your Comments

The Cisco IronPort 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:

`docfeedback@ironport.com`

Cisco IronPort Email Security Plug-in Overview

The Cisco IronPort Email Security Plug-in installs reporting and encryption menus onto Outlook or Lotus Notes Email programs. The reporting plug-in enables users to submit feedback about the type of mail they receive (such as reporting spam, phishing, and virus emails), and the encryption plug-in places an "encrypt message" button on the toolbar which enables usesrs to send encrypted email from their email programs.

When the Cisco Security Plug-in is installed, it enables components on either an Outlook mail client or a Lotus Notes mail client. This single interface allows end-users to seamlessly report problem email or send encrypted email from within their email programs. Combining these plug-ins makes installation simple and provides a single interface for users to 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 mark messages to be

encrypted and secured before it leaves the organization.The accurate functionality of the Encryption plug-in depends on the presence and proper configuration of a Cisco IronPort Email Security appliance with an encryption license.

CHAPTER 2

Overview

The Cisco IronPort Email Security Plug-in is a framework that 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 Email Security on Outlook or on Lotus Notes. 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 and Lotus Notes 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 2-12.

- **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 and secured before it leaves the organization. For details, see The Encryption Plug-in, page 2-12.

The Reporting Plug-in

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

You can also report misclassified messages, which are legitimate email messages that are marked as spam, to Cisco IronPort Systems by using the **Not Spam** button. Cisco IronPort Systems uses these reports to adjust its spam filters to improve 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. The Encryption plug-in is designed to work with a functioning and configured Cisco IronPort Encryption appliance and also 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. To perform a silent installation of the Cisco IronPort Email Security Plug-in, you'll need to create a response file (a text file that contains the answers to all of the questions posed during the installation process). You then use the response file to run an installation via Systems Management software, such as Systems Management Server (SMS) or System Center Configuration Manager (SCCM). For instructions on performing the silent installation, see Chapter 3, "Performing a Mass Installation".

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 **Tools > Options > Cisco Email Security** menu in Outlook, and from the **Actions > Cisco Email Security** menu in Lotus Notes.

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 may want to enable logging for both the Encryption and Reporting plug-ins, or you may want to change the method for marking email for Encryption (these 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".

To make configuration changes on a Lotus Notes installation, see Chapter 5, "Configuring and Using the Cisco IronPort Email Security Plug-in for Lotus Notes"

CHAPTER 3

Performing a Mass Installation

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

Overview

To install the Cisco IronPort Email Security Plug-in for groups of users, you will need to prepare by performing a local silent installation to generate the response file you will use during installation. A silent installation allows you to perform an installation without prompting the end user for input. To perform a mass installation of the Cisco IronPort Email Security Plug-in, you'll need to create a response file (a text file that contains the answers to all of the questions posed during the installation process). You then use the response file to run an installation via Systems Management software, such as Systems Management Server (SMS) or System Center Configuration Manager (SCCM).

The basic steps to perform a mass installation include:

1. Uninstall any older versions of the plug-ins that make up the Security plug-in (including Desktop Encrypt Plug-in for Outlook, Desktop Flag Plug-in for Outlook, IronPort Plug-in for Outlook, IronPort Plug-in for Lotus Notes). Or, uninstall any current running version of the Cisco IronPort Email Security Plug-in.
2. Shut down Outlook or Lotus Notes prior to installation.
3. Run a local version of the installation to create a response file, and verify that the response file was properly created. See Creating the Response File, page 3-16.
4. After the response file is created, uninstall the Cisco IronPort Email Security Plug-in that you installed on a local machine. You will re-install the plug-in during the next step to test the response file.
5. Run the installation on your local machine using the response file you created. Verify that the program installed correctly in either Outlook or Lotus Notes.
6. After you verify the installation, run the mass installation on the target computers using Systems Management software, such as System Center Configuration Manager (SCCM). To perform the installation using SCCM, see Performing the Mass Installation Using SCCM, page 3-18.

Creating the Response File

To create the response file, you run the plug-in installation with a special option that records your responses to a file. Once you create the response file with the recorded answers, you can use it during installations to automatically respond to the sequence of installation questions for all the computers where you want to install the Cisco IronPort Email Security Plug-in.

Step 1 To create response file, perform the installation from the Command line with the **/r** key option. The **/r** key option instructs InstallShield to record the results to a response file. By default, InstallShield saves the response file with the following name and location:

c:\windows\setup.iss.

Step 2 To specify a location for the response file, use the **/f1** option. The **/f1** option allows you to specify an alternate response filename and path. For example, running the following command from the command line instructs InstallShield to write the responses to the *install_034.iss* file on the C Drive:

C:\Users\user1\Desktop\CiscoEmailSecurity.7.1.0.34.exe /r /f1"C:\install_034.iss"

where *C:\Users\user1\Desktop\CiscoEmailSecurity.7.1.0.34.exe* is the path to the .exe file.

Ensure that there are spaces between keys (before every slash): */s /v /qn /f1*

The *.exe* file name and *.iss* file name are example file names. If your .exe file name differs from the one listed above, it will not affect the installation performance.

As you perform each installation step, your responses are saved to the response file to be used as the response during the mass installation.

Tip Cisco IronPort recommends you enter an absolute path if you use the **/f1** option to change the path and file name. In addition, if you use the **/f1** option when creating the response file, note that you will need to specify the path to the response file when running the silent installation (using the **/s** option).

Step 3 Verify that the *install_file.iss* was created.

Step 4 After you verify that the *install_file.iss* was created, uninstall the plug-in (without using any command line parameters and keys).

Step 5 Test the response file by running the installer on your local computer. To do this, run the following from the command line:

C:\Users\user1\Desktop\CiscoEmailSecurity.7.1.0.34.exe /s /v /qn /f1"C:\install_034.iss"

where **/s -** causes setup.exe to be silent,

/v - passes parameters to MSI package, and

/qn - causes everything but *setup.exe* to be silent

/f1 - causes the program to use response file located here.

Step 6 Open your email program (Outlook or Lotus Notes), and verify that the Cisco IronPort Email Security Plug-in installed correctly.

Note Once the *install_file.iss* is created, you can also use it when you update the Cisco IronPort Email Security Plug-in.

Performing the Mass Installation Using SCCM

Before you begin, ensure that you have completed the following steps on the client machines where you want to install the Cisco IronPort Email Security Plug-in:

- Install .Net 3.5 on the client machine (the Installation process will download and install missing framework if necessary, but the installation runs more quickly if you have pre-installed .Net 3.5).
- Shut down Outlook or Lotus Notes.
- Uninstall the current version of the Cisco IronPort Email Security Plug-in (if it is installed).
- Uninstall any older versions of the plug-ins that make up the Security plug-in (including Desktop Encrypt Plug-in for Outlook, Desktop Flag Plug-in for Outlook, IronPort Plug-in for Outlook, IronPort Plug-in for Lotus Notes).
- Ensure you have created the *install_file.iss* file. See Creating the Response File, page 3-16.

Before you begin installation, ensure that the following conditions exist on SCCM:

- You created a collection with the list of clients where the Cisco IronPort Email Security Plug-in should be installed.

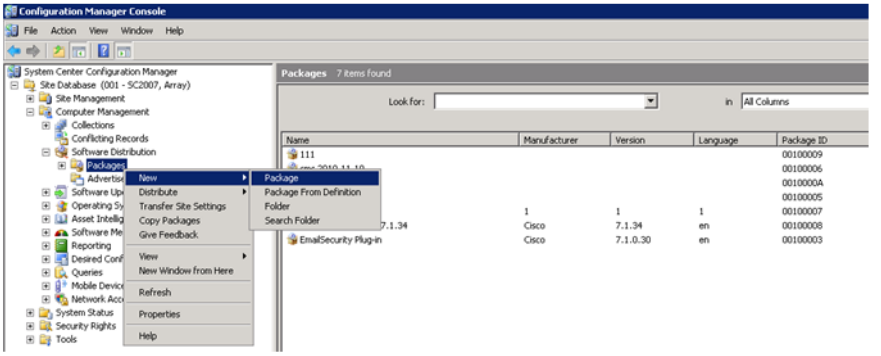
To Perform the Installation:

Step 1 Create a network shared folder and give users access to it.

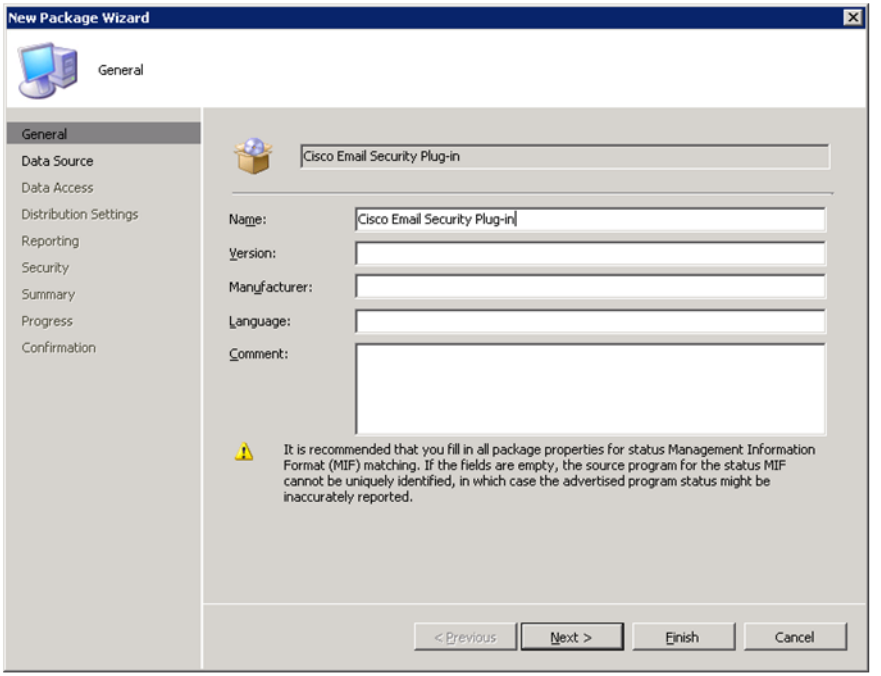
Step 2 Put the installer and the *install_file.iss* file into this folder.

Step 3 Open the SCCM administrative tool.

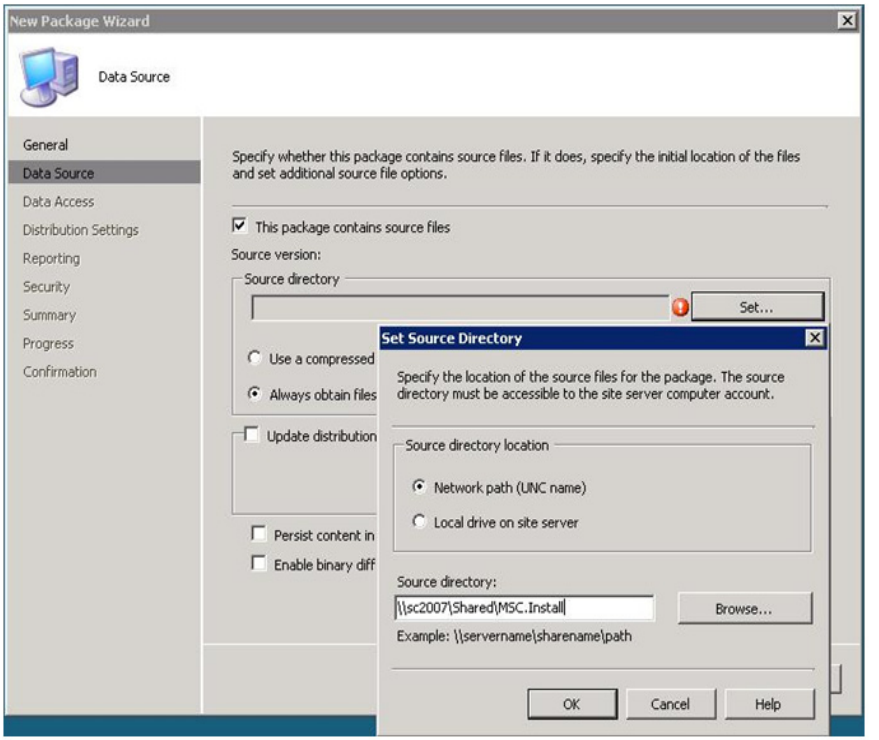
Step 4 Create a new software distribution package.



Step 5 Enter a name for the package, and click **Next**.

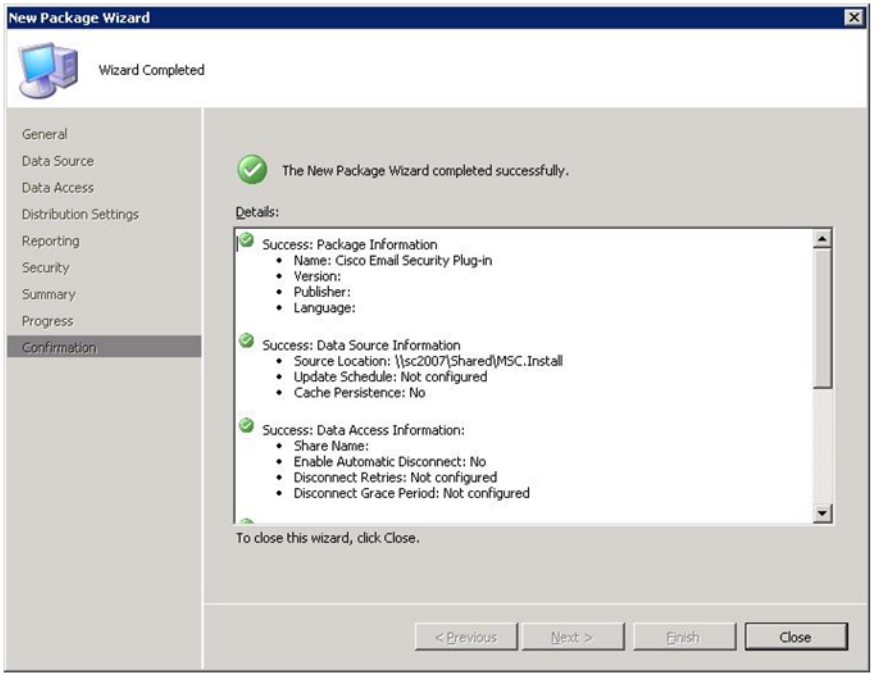


Step 6 Specify the network source directory that you created in Step 1 by entering the path to the network shared folder. You can enter the path or browse to the folder. Click **Next**.

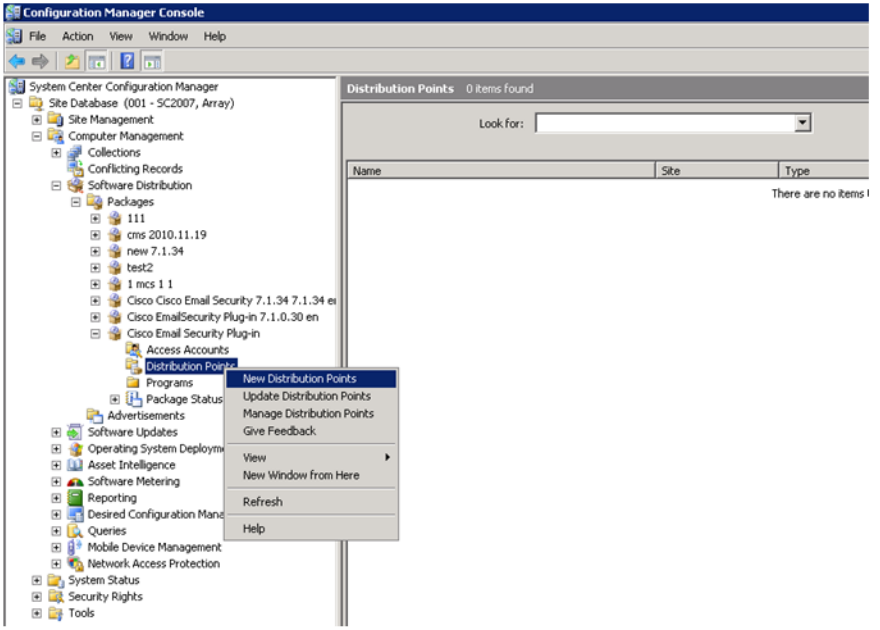


Step 7 Continue to the next step in the New Package wizard, and click **Next**.

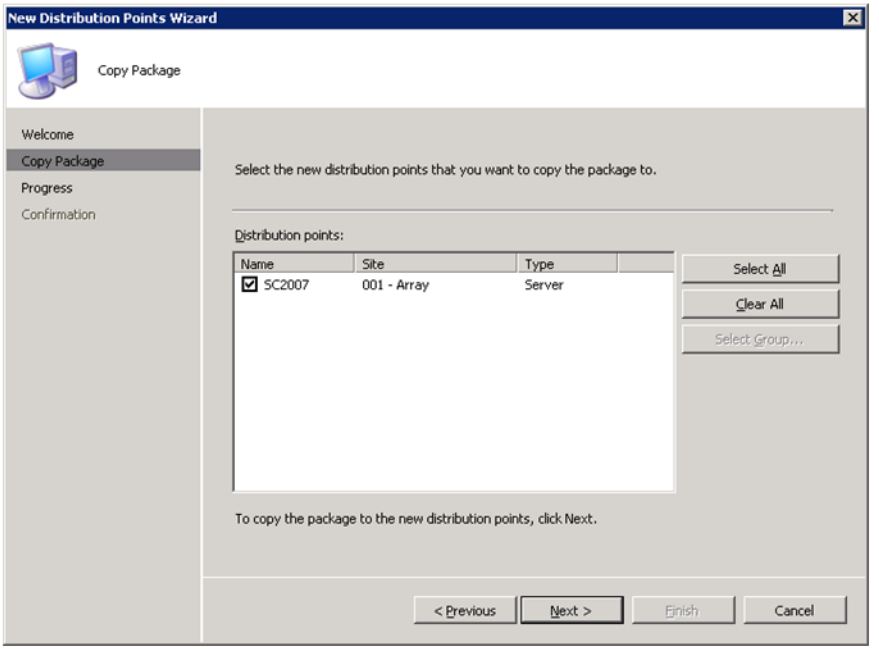
Step 8 View the confirmation that the New Package Wizard completed successfully, and click **Close**.



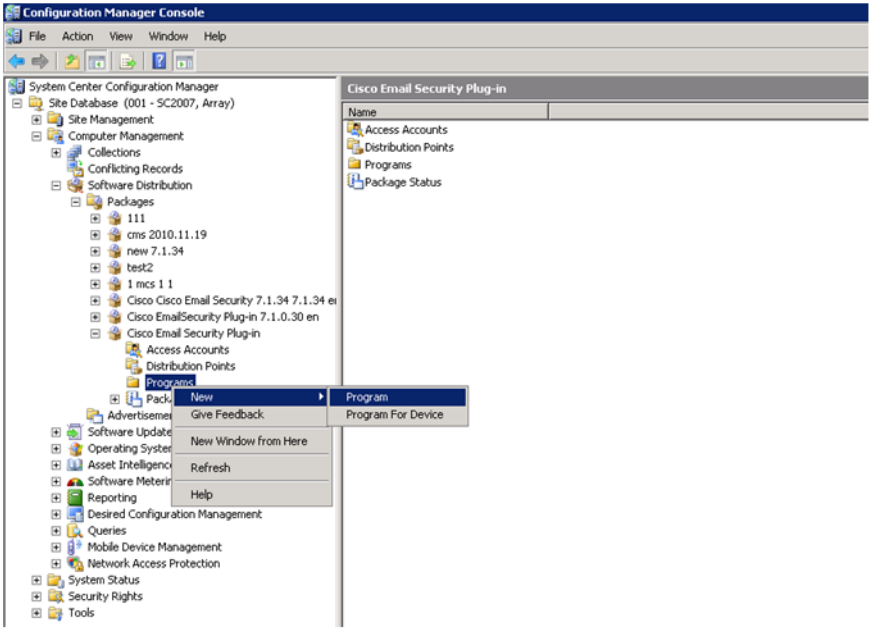
Step 9 Create a new distribution point, and click **Next** on the Welcome page.



Step 10 Select the new distribution point. Click through the next pages on the New Distribution Points Wizard, and click **Close**.

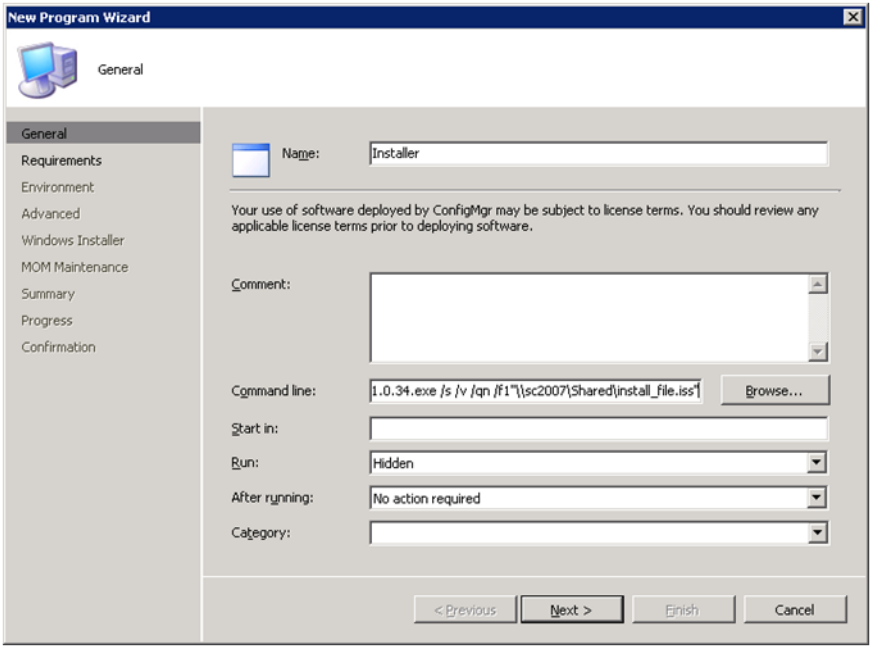


Step 11 Create a new program.



Step 12 In the command line, enter the program name and the following command: *\\sc2007\Shared\CiscoEmailSecurity.7.1.0.34.exe /s /v /qn /f1"\\sc2007\Shared\install_file.iss"*

where *\\sc2007\Shared\CiscoEmailSecurity.7.1.0.34.exe* is the full network path to the .exe file in the network shared folder: "\\sc2007\Shared\install_file.iss".



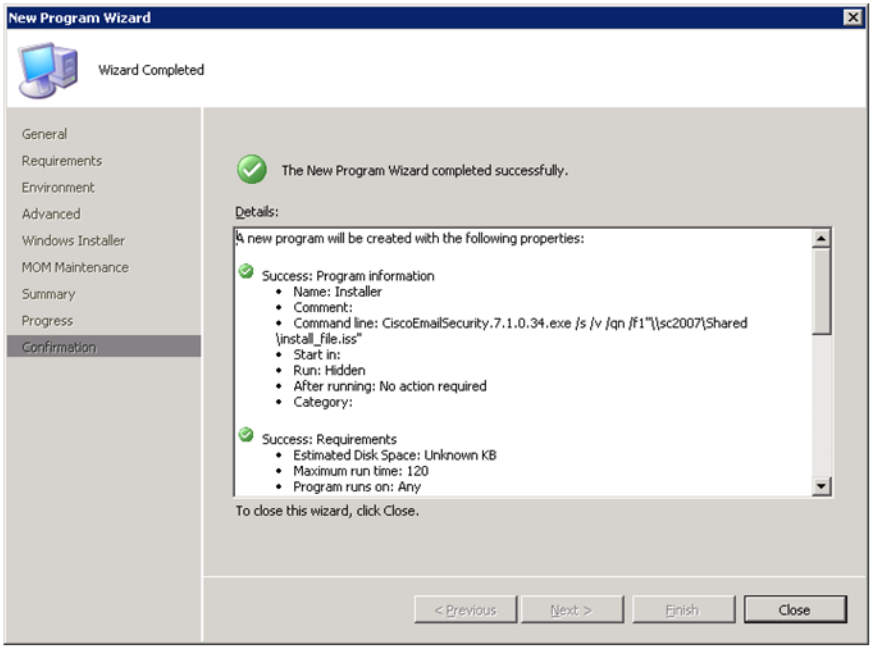
Step 13 In the **Run** field, enter **Hidden**, and then click **Next**.

Step 14 Click through the requirements page, and then click **Next**.

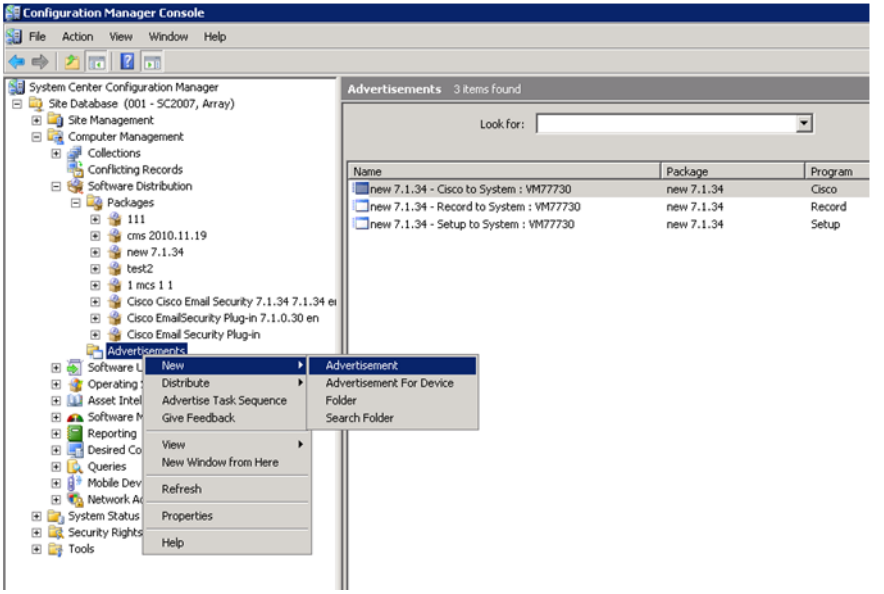
Step 15 Select the following environment options:

- **Program can run**: Only when 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.

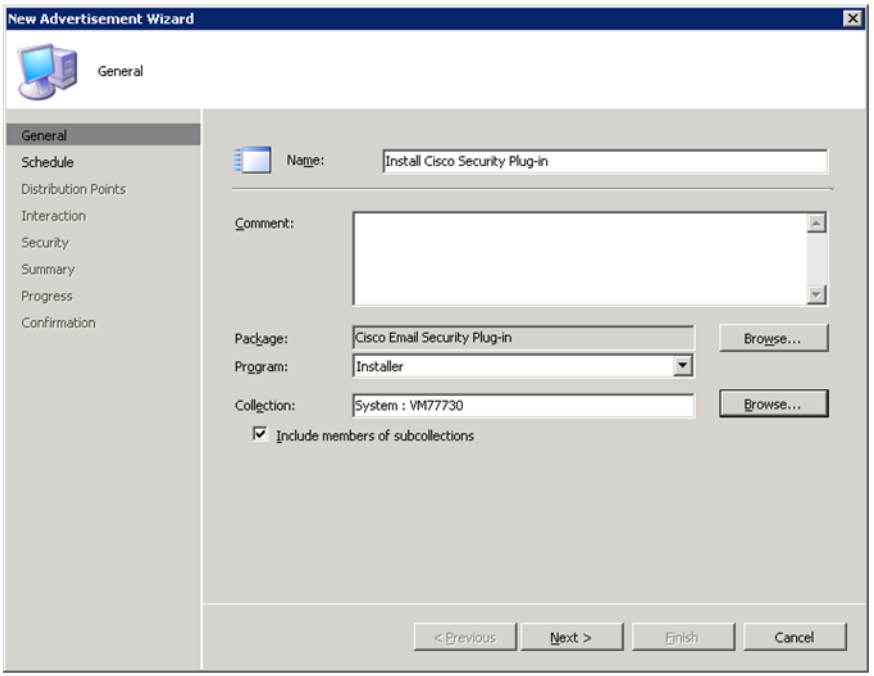
Step 16 Confirm that the New Program Wizard completed successfully, and click **Close**.



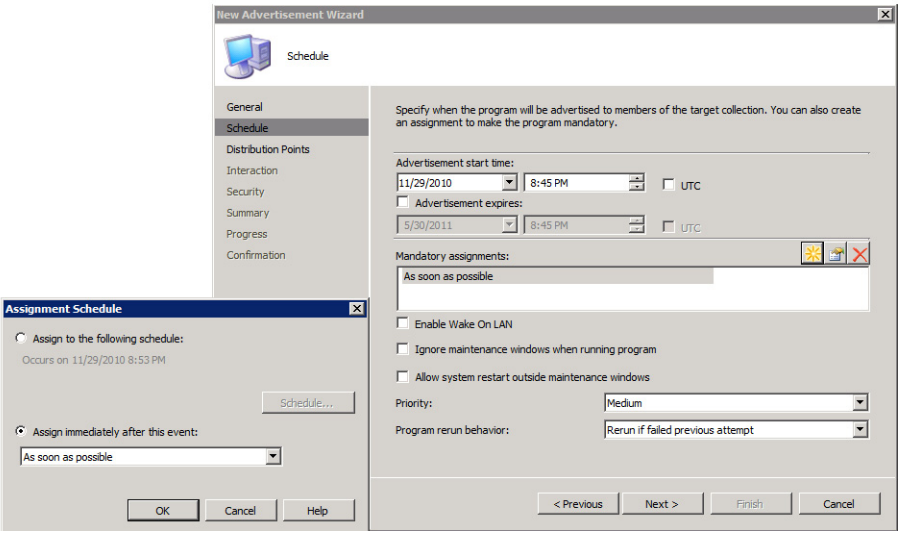
Step 17 Create a new advertisement.



Step 18 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**.



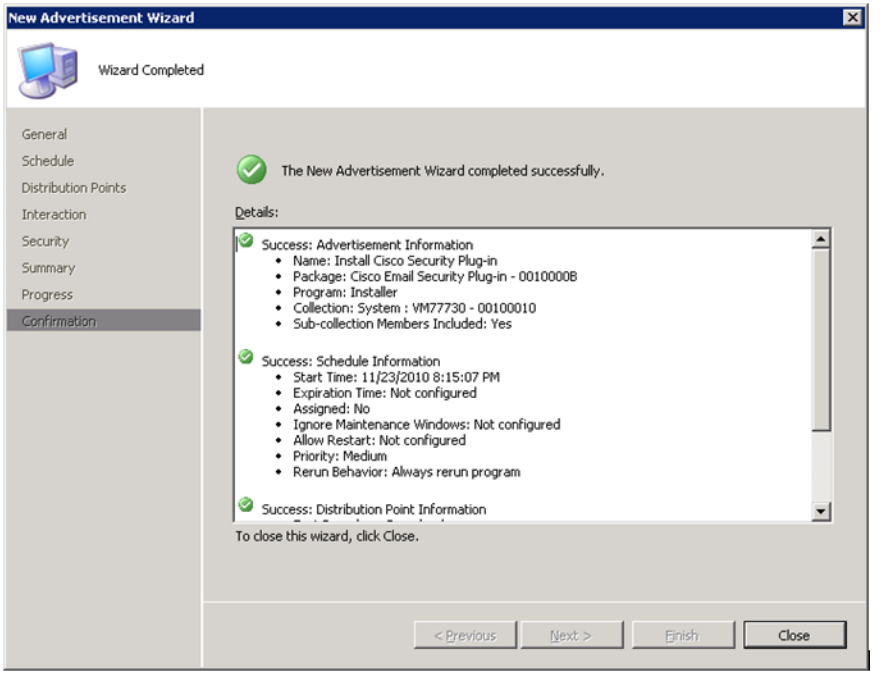
Step 19 Set the assignment as mandatory. Click **Next**.



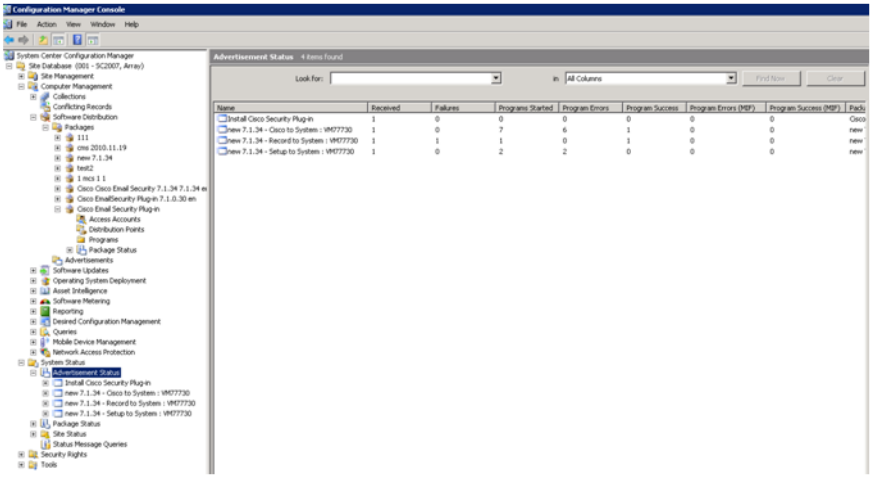
Step 20 Select the switches based on your preferences, but do not select **Do Not Run Program**, as the program will not start if the connection is slow**.** Click **Next**.

Step 21 Click through the New Advertisement Wizard, and click **Next**.

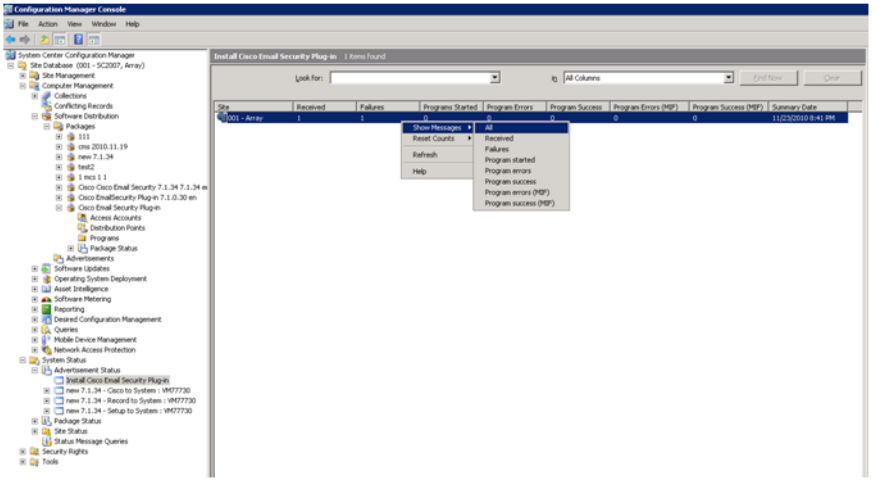
Step 22 View the confirmation that the New Advertisement Wizard completed successfully, and click **Close**.



Step 23 View the Advertisement Status in the Advertisement Status window.



Step 24 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.



Changing the Plug-in Configuration Files

When you install the Cisco IronPort Email Security Plug-in, configuration data is created and saved in the following XML files:

- **CommonConfig.xml**. Contains basic configuration data that is common to both the Reporting and Encryption plug-ins, such as logging information.
- **Reporting.xml**. Contains configuration data related to the Reporting plug-in, such as the maximum mail size that can be reported.
- **Encryption.xml**. Contains configuration data related to the Encryption plug-in, such as the flagging method (subject string or x-header, for example).

The Cisco IronPort Email Security Plug-in installer allows you to change the default configuration files. You might want to use different configuration files to change basic features about 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. And in the main configuration file, you might enable or disable logging or modify the logging levels.

If you want to use custom configuration files, you need to add a special key from the command line using the following syntax:

```
CiscoEmailSecurity-7.0.0.005.exe /s
/v"UseCustomConfigs=\"\\smsarray\SMSClient\config\"" /qn
/"f1CiscoEmailSecurity.7.0.0.005.iss"
```

The **UseCustomConfigs** command line parameter is used to enable the use of custom configuration files and specify the path to the folder containing configuration files which should be used during the installation.

By default, the plug-in installs configuration files in the %appdata% directory in the following locations for Outlook and Lotus Notes:

%appdata%\Cisco\Cisco IronPort Email Security Plug In\Outlook

%appdata%\Cisco\Cisco IronPort Email Security Plug In\LotusNotes

Using the **UseCustomConfigs** command line parameter, you can specify the name and location of your own configuration files for installation. However, you must maintain the structure of the original file to maintain validity. The default configuration files are located in the config.zip file. If you create a folder, make sure that you maintain the file structure and include either Outlook or Lotus Notes subfolders with configuration files (if you install only Outlook plug-ins you can omit LotusNotes folder and vice versa).

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 your Outlook email program. This chapter contains the following sections:

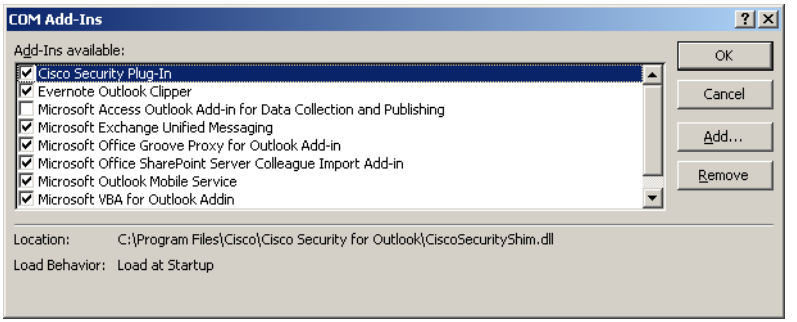
Cisco IronPort Email Security Plug-in For Outlook General Settings

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. You can configure general settings for the Cisco IronPort Email Security Plug-in from the Options page.

Enable/Disable

By default, the Cisco IronPort Email Security Plug-in is enabled upon installation. If you want to disable the Cisco IronPort Email Security Plug-in, you can so do from the following places.

- From Outlook2003/ 2007, go to **Tools > Options > Cisco Email Security**.
- From Outlook 2010, go to **File > Options > Add-ins**. Then select Manage drop-down list to COM Add-ins and click **Go**.



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

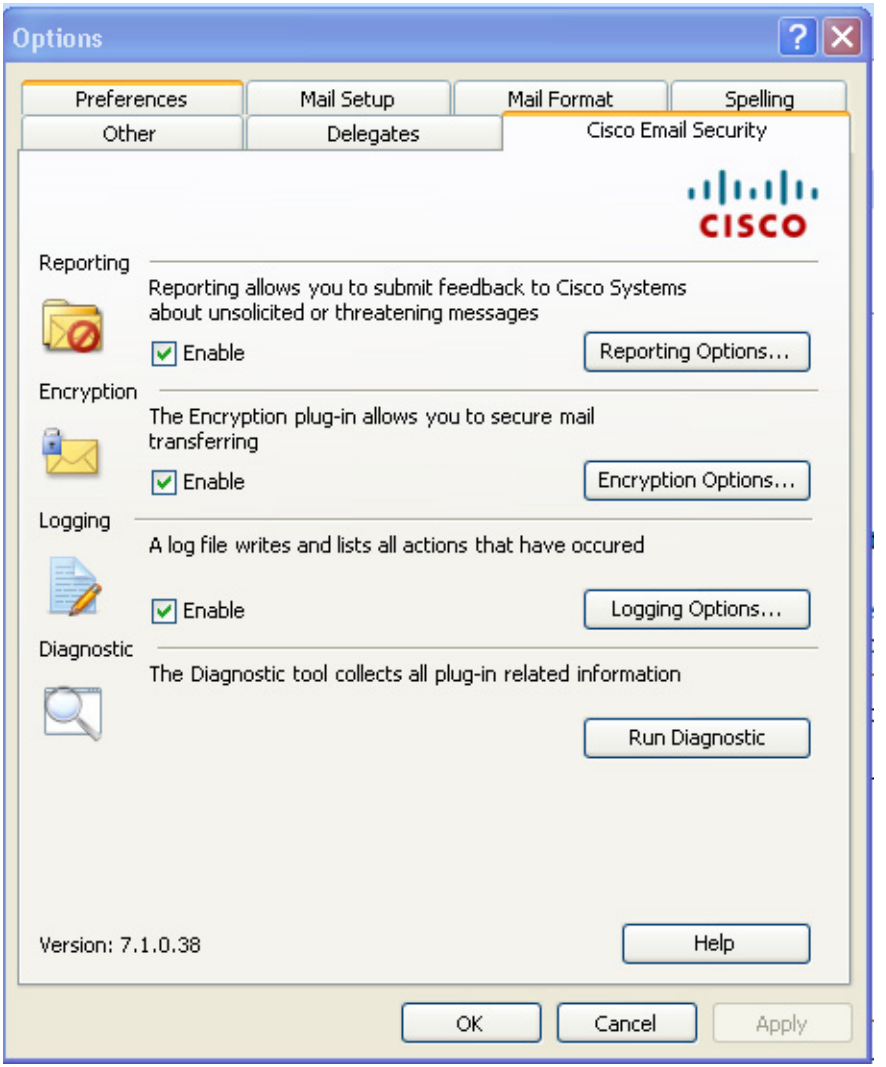
Configuring Basic Settings for the Outlook Plug-in

You can configure basic settings from the Cisco Email Security tab. To open the Cisco Email Security tab in Outlook 2003/2007, go to **Tools > Options > Cisco Email Security**.

-OR-

From Outlook 2010: Go to **File > Options > Add-ins > Add-in Options > Cisco Email Security.**

Cisco Email Security tab:



From this tab, you can enable reporting, encryption, logging by selecting the **Enable** checkbox. To further configure the settings, you click the **Reporting Options...**, **Encryption Options**, or **Logging Options...** buttons. You 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.

The Reporting Plug-in

The Reporting settings allow you to enable or disable the Reporting plug-in. The reporting plug-in allows you to report to Cisco that an email you receive is spam, a phishing attack, a virus, or misclassified as spam (also sometimes called “ham”).

You can configure the Cisco IronPort Email Security Reporting Plug-in for Outlook via the Options page in Outlook.

To enable the Reporting Plug-in for Outlook 2003/2007, go to **Tools > Options > Cisco Email Security** tab and select the **Enable** checkbox in the Reporting field of the Cisco Email Security tab.

-OR-

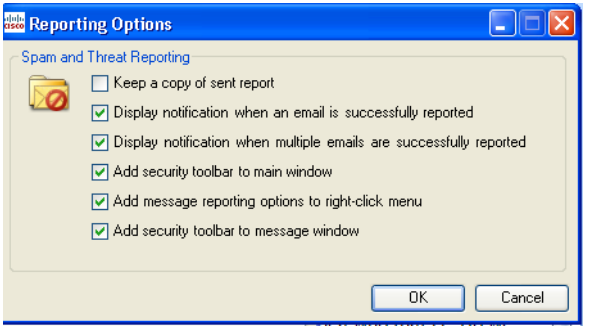
To enable the Reporting Plug-in for Outlook 2010, go to **File > Options > Add-ins > Add-in Options > Cisco Email Security** tab and select the **Enable** checkbox in the Reporting field of the Cisco Email Security tab.

Reporting Options

To access the Reporting options page in Outlook 2003/2007, go to **Tools > Options > Cisco Email Security** tab and click the **Reporting Options** button.

To modify changes to your Encryption settings in Outlook 2010, go to **File > Options > Add-ins > Add-in Options > Cisco Email Security** and click **Reporting Options** button.

Reporting options page:



Options

This section describes the Reporting options you can configure.

- **Keep a copy of sent report**. By default, when you report an email message to Cisco as spam, virus, misclassified spam, or virus, the reporting email you sent is deleted. Selecting this option prevents the email from being deleted.
- **Display notification when an email is successfully reported**. When you successfully report an email as spam or virus, you 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 multiple emails are successfully reported (as spam, virus, phishing or not spam), you can enable Outlook to display a success message in a dialog box. Clearing this option prevents this dialog box from displaying.
- **Add security toolbar to the main window**. By default, when you install 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 you install 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 you install 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 email message window.

Using the Reporting Plug-in for Outlook

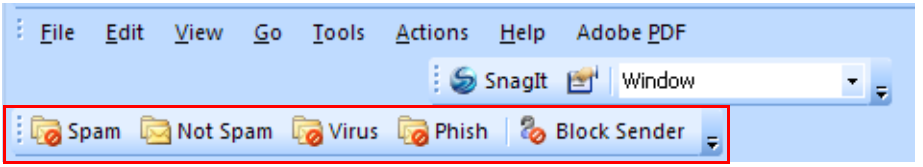
Overview

The Cisco IronPort Email Security Plug-in for Outlook allows you to submit feedback to Cisco about spam, virus, or phishing emails that you receive in your inbox. You 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 your 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 you report are used to improve Cisco's email filters, helping to reduce the overall volume of unsolicited mail to your inbox.

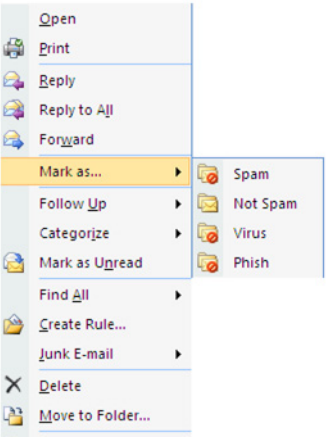
Providing Feedback to Cisco

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 your Junk Email Box).

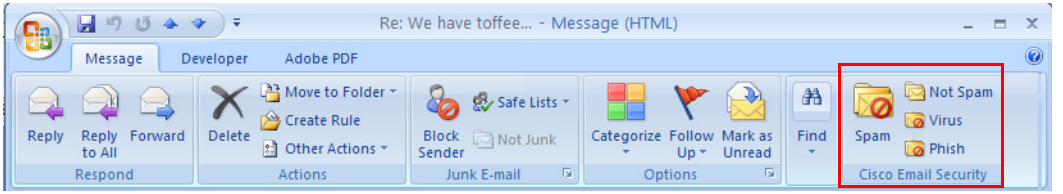


These buttons are used to report spam, virus, and phishing emails (Phishing attacks are emails that link to 'spoofed' and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account user names and passwords, social security numbers. For example, you might receive an email from *infos@paypals.com* that fraudulently requests your personal banking information).

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

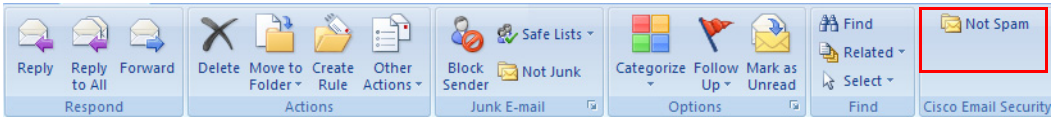


And, you can use the buttons in the message window to report spam, virus, phish and misclassified mail (misclassified mail is mail that was erroneously marked as spam, virus, or phish).

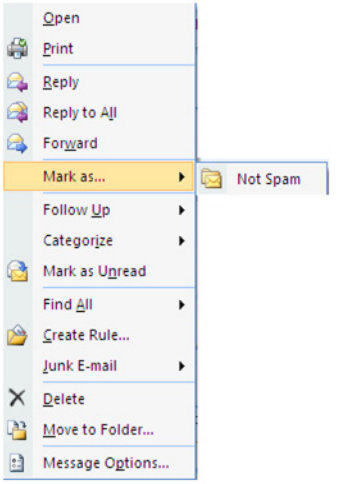


If an email you receive is misclassified as spam (i.e. is filtered and sent to your Spam folder), you can report the email as misclassified by clicking the **Not Spam** button. This ensures that mail from the sender will not be classified as spam in the future.

In addition, from your Junk Email folder, you can mark messages as misclassified by clicking the **Not Spam** button in the message window.



You can also mark misclassified email from the right-click context menu.



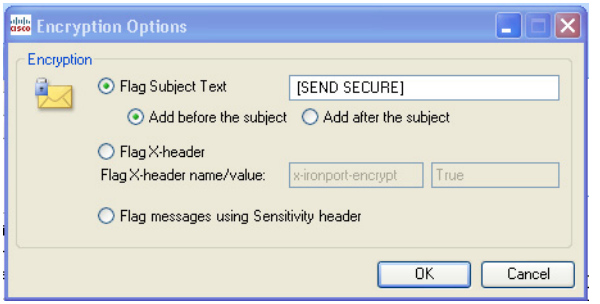
The Encryption Plug-in

Your Encryption settings are located on the Cisco Email Security page. To modify changes to your Encryption settings in Outlook 2003/2007, go to **Tools > Options > Cisco Email Security** and click **Encryption Options**.

To modify changes to your Encryption settings in Outlook 2010, go to **File > Options > Add-ins > Add-in Options > Cisco Email Security** and click the **Encryption Options** button.

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

Encryption Options:



Options

Options for Sending Encrypted Email

When you want to encrypt outgoing email, you need to mark or "flag" the email for encryption. This allows filters created by your System Administrator to identify the messages that need to be encrypted.

Warning **Do not change the method for flagging email for encryption without communicating with your System Administrator. These methods require changes to settings in your Cisco IronPort Encryption appliance to work properly, and only your System Administrator can make these changes.**

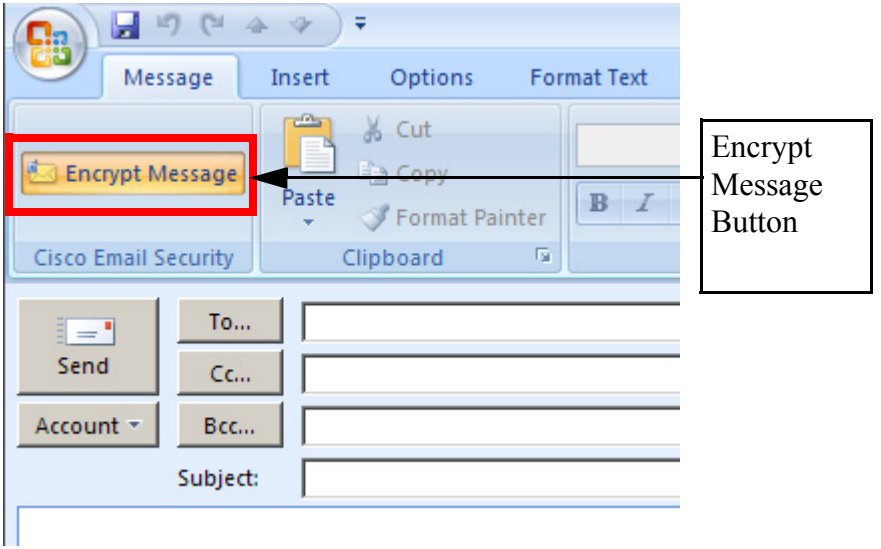
You can mark your emails for encryption using one of the following methods:

- **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 prepend 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*).

- **Outlook 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.

Sending Encrypted Email

You can send secure emails by selecting the “Encrypt Message” button while composing an email. Before you send a secure message, verify that the Encrypt Message button is selected, as shown below:

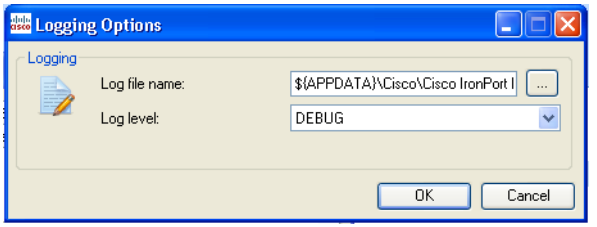


The Encrypt Message button is available when composing emails.

Changing Logging Settings

Click **Logging Options...** to open the Logging Options page.

Logging Options:



Options

You can configure the following options from the Logging menu.

Log file name

Allows you to specify name for the log file that will be stored in %appdata%\Cisco. Log file name should be with .log extension.

Log level

The log level specifies what information will be logged to the log file. You can choose one of the following logging levels:

- **ERROR**. Error messages and exception situations are logged.
- **WARN**. Warning messages are logged as well as ERROR messages.
- **INFO**. Basic information and other status messages are logged. Auto updating process status messages are logged. All WARN and ERROR messages are also logged.
- **DEBUG**. Detailed information about configuration settings are logged. All ERROR, WARN, and INFO error messages are logged, and information that may be helpful for troubleshooting problems is logged.

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

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.

You may want to use the diagnostic tool if you are receiving errors or if you 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.

Note: If you experience errors, review the Diagnostic section 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

Running the Cisco IronPort Email Security Diagnostic Tool

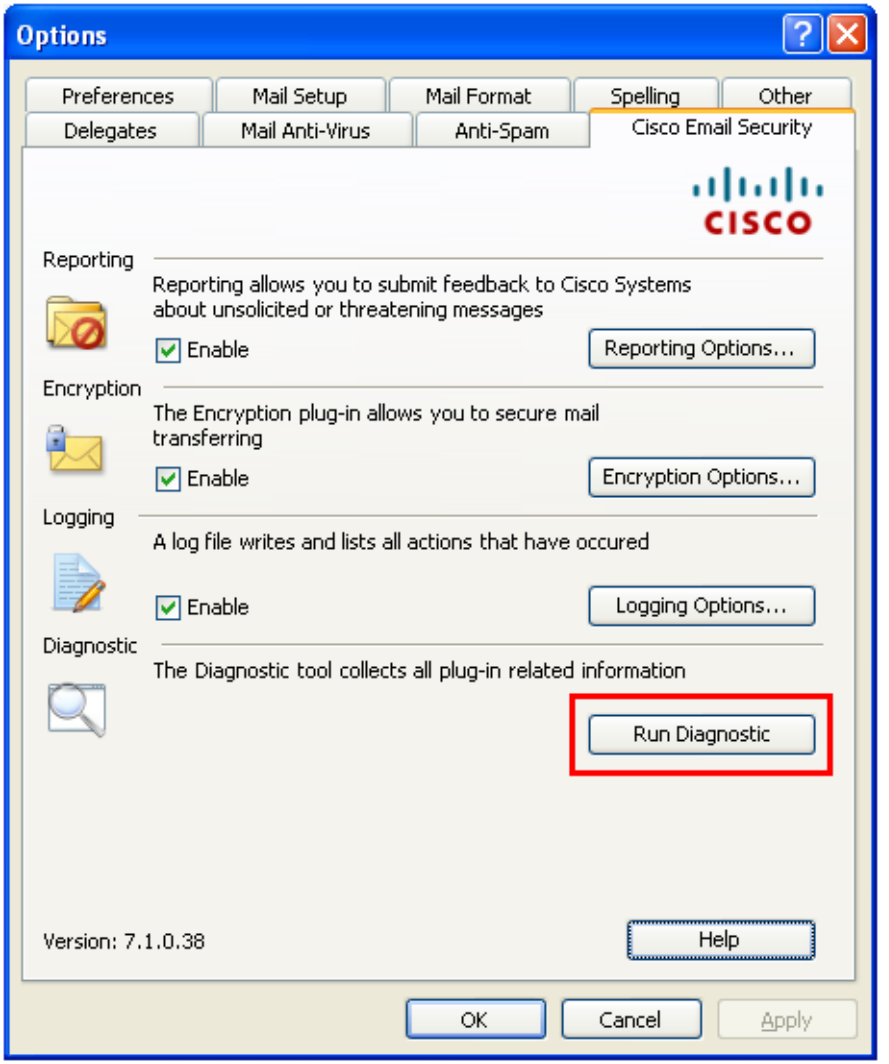
You can run the Cisco Email Security Diagnostic tool from one of the following places:

- **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> Diagnostic Tool.**

Running the Diagnostic Tool from the Outlook Options tab

From Outlook 2003/2007, go to **Tools > Options > Cisco Email Security** tab, and click **Run Diagnostics**. Or, from Outlook 2010, go to **File > Options > Add-ins > Add-in Options > Cisco Email Security** and click **Run Diagnostics**:



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

You may go to *CiscoDiagnosticReport.zip* file and send it manually to your System Administrator or to your Cisco Support representative.

Running the Diagnostic Tool from the Program Files

Navigate to the folder where the 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.

Running the Diagnostic Tool from the Start Menu

Run the Diagnostic tool from **Start > Programs >** Cisco IronPort Email Security Plug-in. Click **Diagnostic Tool**. To view the report, click **Go to Report**. The report is saved i the zip file, *CiscoDiagnosticsReport.zip*.

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 uninstallation, the following items are removed:

- All registry entries made by the plug-in.
- Entry for the plug-in in the Add/Remove programs listing.
- Files related to the plug-in.
- The plug-in toolbar (removed from Outlook).

Note Uninstalling the plug-in does not affect Outlook performance.

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:

- Click **Start > Control Panel >** Add/Remove Programs. Select Cisco IronPort Email Security Plug In, and click **Remove**.

  -OR-

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

CHAPTER 5

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

This chapter introduces the features available in the Cisco IronPort Email Security Plug-in for Lotus Notes. The Cisco IronPort Email Security Plug-in contains several common email security plug-ins. This chapter contains the following sections:

Cisco IronPort Email Security Plug-in For Lotus Notes General Settings

The Cisco IronPort Email Security Plug-in for Lotus Notes is a framework that supports several Cisco IronPort Email Security Plug-ins:

- The Reporting plug-in. Use this plug-in to report email that is spam, virus, a phishing attack, or misclassified as spam.
- The Encryption plug-in. Use this plug-in to send secure encrypted email.

You can configure the Cisco IronPort Email Security Plug-in via the Options page. To access Options page, go to **Actions > Cisco Email Security.**

Cisco Email Security Options page:

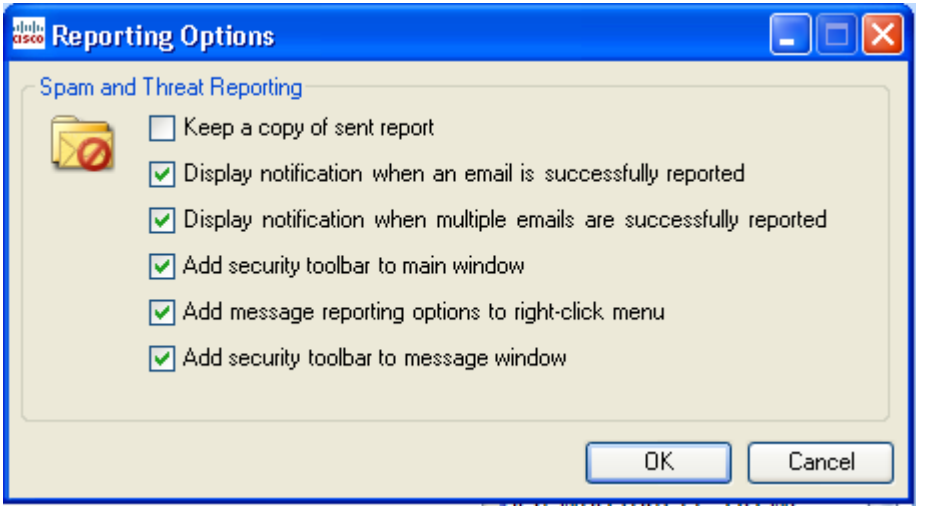
From this tab, you can enable reporting, encryption, and logging by selecting the **Enable** checkbox for these options. To further configure the settings, you click the **Reporting Options...**, **Encryption Options...**, or **Logging Options...** buttons. You can also use the Diagnostic tool to run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

The Reporting Plug-in

Options dialog

The Reporting plug-in allows you to report to Cisco if an email you receive is spam, a phishing attack, a virus, or misclassified as spam.

You can configure the Cisco Email Security Reporting Plug-in for Lotus Notes via the Options dialog. To access the Reporting options page, go to **Actions > Cisco Email Security Options**, and choose the **Reporting** tab in the dialog.



Options

This section describes the Reporting options you can modify.

Keep a copy of sent report

By default, when you report an email message to Cisco as Spam, Virus, Misclassified Spam, or Virus, the reporting email you sent is deleted. Selecting this option prevents the email from being deleted.

Display a notification when an email is successfully reported.

When an email is reported, you can select this option to display a notification alerting you that your email was successfully reported.

Display a notification when multiple emails are successfully reported.

When a group of emails is reported, you can select this option to display a notification alerting you that your emails were successfully reported.

Add a security toolbar to the main window.

Use this option to add a security toolbar to the main window.

Add message reporting options to the right-click window.

Use this option to add message reporting options to the right-click window.

Add security toolbar to message window.

Use this option to add a security toolbar to the message window.

Using the Reporting Plug-in for Lotus Notes

The Cisco Email Security Reporting Plug-in for Lotus Notes allows you to submit feedback to Cisco about spam, virus, or phishing emails that you receive in your inbox. Cisco uses this feedback to update the email filters that prevent unwanted messages from being delivered to your inbox.

You can configure settings via the main menu bar to enable Lotus Notes to report spam, virus, phishing and misclassified emails. After reporting an email, a message appears indicating that the report has been submitted. The messages you report are used to improve Cisco's email filters, helping to reduce the overall volume of unsolicited mail to your inbox.

The Encryption Plug-in

Configuring Encryption Options

You can modify Encryption plug-in settings from the Cisco Email Security Options dialog. To modify your Encryption settings, go to **Actions > Cisco Email Security Options** and click **Encryption Options.**

Options

Options for Sending Encrypted Email

When you want to encrypt outgoing email, you need to mark or "flag" the email for encryption. This allows filters created by your System Administrator to identify the messages that need to be encrypted.

Warning **Do not change the method for flagging email for encryption without communicating with your System Administrator. These methods require changes to be made on the Cisco IronPort Encryption appliance, and only your System Administrator can make these changes.**

You can mark your emails for encryption using one of the following methods:

- **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 prepend 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*).

Using the Encryption Plug-in

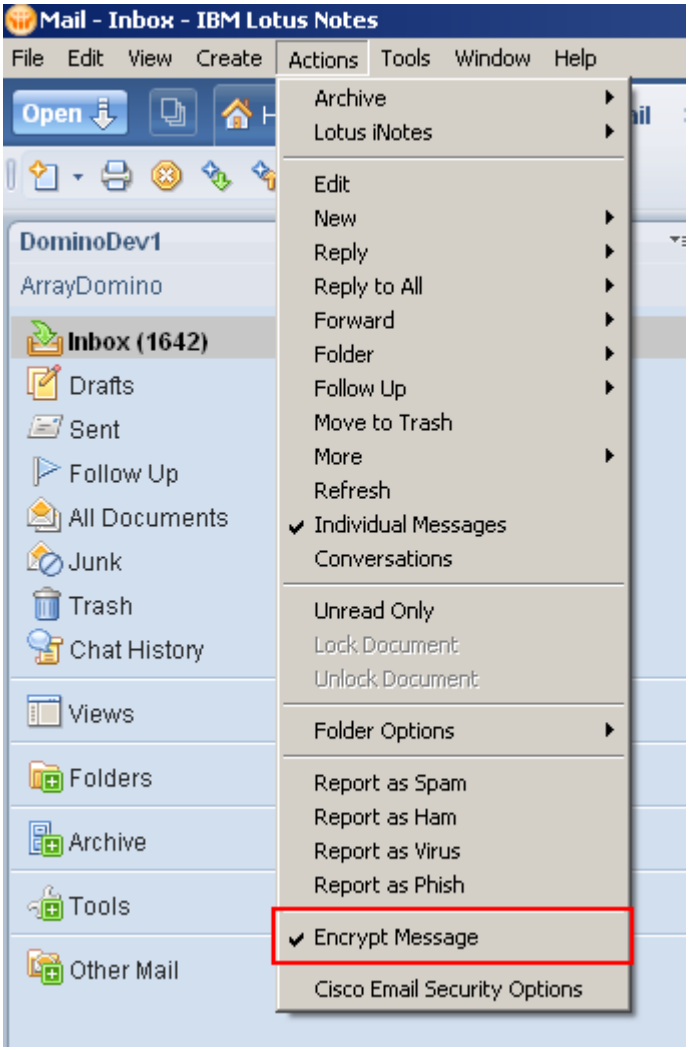
Overview

The Encryption plug-in allows you to send encrypted emails from your Lotus Notes email program. When you send secure emails, the Cisco Email Security Encryption Plug-in will securely send emails that are marked for encryption, ensuring that your mail can be read only by the intended recipient.

Sending Secure Emails

You can enable your mail system to send secure emails by checking the **Encrypt message** button in Actions menu.

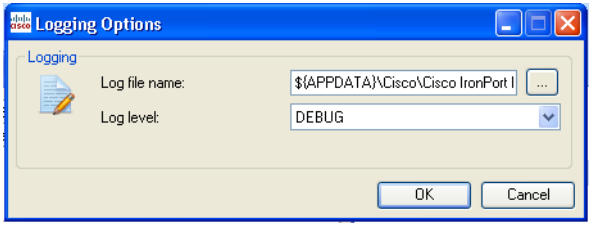
To send a secure message, verify that the **Encrypt message** button is selected, as shown below:



Changing Logging Options

Click **Logging Options...** to open the Logging Options page.

Logging Options:



Options

You can configure the following options from the Logging menu.

Log file name

Allows you to specify name for the log file that will be stored in %appdata%\Cisco. Log file name should be with .log extension.

Log level

The log level specifies what information will be logged to the log file. You can choose one of the following logging levels:

- **ERROR**. Error messages and exception situations are logged.
- **WARN**. Warning messages are logged as well as ERROR messages.
- **INFO**. Basic information and other status messages are logged. Auto updating process status messages are logged. All WARN and ERROR messages are also logged.
- **DEBUG**. Detailed information about configuration settings are logged. All ERROR, WARN, and INFO error messages are logged, and information that may be helpful for troubleshooting problems is logged.

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

Troubleshooting and Diagnostics

This section lists some of the common errors that can occur while using the Cisco IronPort Email Security Plug-in for Lotus Notes and troubleshooting tips for fixing these errors.

Note If you receive the same error message several times and the error disrupts the Cisco IronPort Email Security Plug-in for Lotus Notes functionality, try running the repair process. If you encounter the same error after running the repair process, follow the steps to provide Cisco feedback with the Cisco Email Security Diagnostic tool.

Common Startup Errors

Error occurred during configuration file initialization.

The following messages may appear while Outlook is starting:

- Error occurred during Cisco IronPort Email Security Plug-in configuration file initialization. Some settings set to default values.
- Error during reading configuration for Reporting component. Some settings set to default values.
- Error during reading configuration for Encryption component. Some settings set to default values.

These error messages occur if some values from the configuration file: (*%appdata%\Cisco\Cisco Email Security Plug In\LotusNotes\CommonConfig.xml*) were corrupted.

Solution

The plug-in will restore default values in the corrupted configuration files. However, if you continue to receive the error message, run the repair process to fix the configuration files.

Configuration file not found. Settings set to default values.

One of the following Error messages may display while Outlook is starting:

- Cisco IronPort Email Security Plug-in configuration file not found. Settings set to default values.
- Configuration file for Encryption component was not found. Settings set to default values.
- Configuration file for Reporting component was not found. Settings set to default values.

Solution

The plug-in will restore default values in corrupted configuration files. However, if you continue to receive this error message, run the repair process to fix the configuration files.

Message Reporting Errors

Invalid email address

The following message may appear when you click the **Report as Spam**, **Report as Virus**, **Report as Phish** or **Report as Not Spam** buttons in Lotus Notes:

Invalid address for report type. Please update configuration file.

This error message occurs if you are using the Reporting plug-in and the format of the email you are attempting to report is incorrect. You will need to repair the Reporting plug-in file to ensure that you can report spam and phishing emails (as well as report legitimate mail as “Not Spam”).

Solution

Check the Reporting configuration in the *%appdata%\Cisco\Cisco Email Security Plug In\LotusNotes* folder. Delete it and run the repair process to restore default values.

Repairing Cisco IronPort Email Security Plug-in for Lotus Notes Files

1. Go to **Control Panel > Add** or **Remove Programs**.
2. Find the Cisco IronPort Email Security Plug-in in the list of programs, and click **Change**.
3. Make sure Lotus Notes is closed.
4. Select the Cisco IronPort Email Security Plug-in Installer, and click the **Repair radio** button.
5. Click **Next**. The installer repair process runs.
6. Perform the action that caused the error. If the same error occurs after running the repair process, follow the steps to provide Cisco feedback with the Diagnostic tool.

Cisco Email Security Diagnostic tool

Cisco provides a diagnostic tool for the Cisco IronPort Email Security Plug-in that allows you to send Cisco details required for a full analysis of a problem. You may want to use the diagnostic tool if you are receiving errors or if you 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.

If you experience errors, review the Diagnostic section for troubleshooting tips.

Data Collected by the Cisco Email Security Diagnostic Tool

The Diagnostic tool collects the following information your computer:

- Registration information about some COM components
- Environment variables

- Cisco Email Security output files
- Information about Windows and Lotus Notes
- Your system user name and PC name
- Information about other Lotus Notes plug-ins

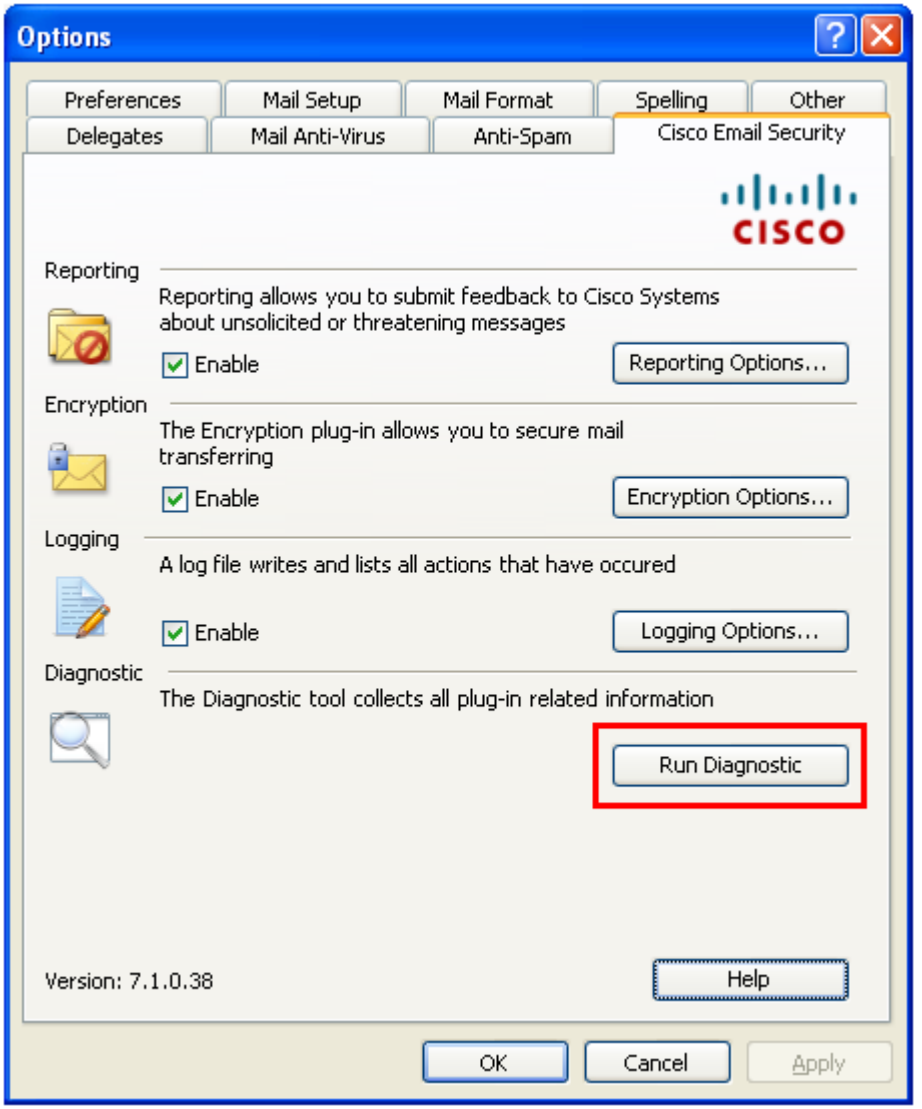
Running the Cisco Email Security Diagnostic Tool

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

- **From the Cisco Email Security options dialog**. Typically, you run the diagnostic tool from the Cisco Email Security options dialog. You can access the diagnostics tool from **Actions > Cisco Options**.
- **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.

Running the Diagnostic Tool from the Options Dialog

Go to **Actions > Cisco Email Security Options**, and click **Run Diagnostics**. 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 tool stores the data in a zip file named *CiscoDiagnosticReport.zip*.

You may access the *CiscoDiagnosticReport.zip* file by clicking **Go to Report** and send it manually to System Administrator or Cisco Security Administrator.

Running the Diagnostic Tool from the Program Files

Run the Diagnostic tool from **Start > Programs > Cisco Email Security for Lotus Notes**. Or, go to the folder where Cisco Email Security was installed (typically C:\Program Files\Cisco\Cisco IronPort Email Security Plug-in) and double-click the *Cisco.EmailSecurity.Framework.Diagnostic.exe* file.

Uninstalling

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

During uninstallation, the following items are removed:

- All registry entries made by the plug-in.
- Entry for the plug-in in the Add/Remove programs listing.
- Files related to the plug-in.

Note uninstalling the plug-in does not affect Lotus Notes performance.

To Uninstall the Plug-in

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

- Click **Start > Control Panel > Add/Remove Programs**. Select Cisco IronPort Email Security Plug-in, and click **Remove**.

  -OR-

- Double-click the plug-in setup file (the file you 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.