Release Notes for Cisco IronPort Email Security Plug-in 7.2

Revised: October 12, 2011

Contents

These release notes contain information critical to installing and running the Cisco IronPort Email Security Plug-in version 7.2, including known issues.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

What's New in the Cisco IronPort Email Security Plug-in 7.2 Release

This release includes the following new features:

- **Support for Cisco IronPort Desktop Encryption**. Desktop encryption uses an SDK to encrypt email from within your email program. You may want to use this feature if you want "end-to-end" encryption (with Flag encryption, the email is encrypted *after* it exits the mail server, so emails routed within your company are not encrypted). This form of encryption is particularly useful if you want to send encrypted email within your organization. For example, a member of the financial services group needs to send a secure financial report to the company CEO, she would choose Desktop Encryption to ensure that the document is secured at her desktop before being sent to the CEO.
- **Support for Multiple Languages**. The Cisco IronPort Email Security Plug-in can now be viewed in the following languages: German, English, Spanish, French, Japanese and Chinese (traditional). The language can be selected from the Cisco IronPort Email Security Plug-in main menu.
- **Saved Desktop Encryption passwords**. End users can configure the plug-in to remember their encryption passwords so that they do not need to re-enter passwords every time they open encrypted messages.
- **Desktop Encryption Secure Envelope Options**. End users can configure multiple options for the encrypted email they send.
  - **Default Expiration dates**. An expiration date for the email. If the mail is not decrypted within a specified period of time, the encrypted message expires and recipients will no longer be allowed to decrypt it.
  - **Default Read-by date**. This option specifies the default duration, in days, by which the recipient is expected to read the message. If the message is not read, the sender is notified. The sender could then choose to lock or expire the message.
  - **Request a Decryption Notification**. When this option is chosen, a notification is sent to the sender once the recipient has decrypted the message.

– **Language Options for Notification Text**. You can select the language to use for the notification text that the recipient will view when he or she receives an encrypted envelope. You can choose from English, German, Spanish French, Japanese and Chinese (traditional).

Supported Configurations

The following configurations are supported:

Cisco IronPort Email Security Plug-in 7.2.x	Outlook 2003 (32 bit)	Outlook 2007 (32 bit)	Outlook 2010 (32 bit)	Outlook 2010 (64 bit)
XP 32 bit	certified	certified	certified	not supported
XP 64 bit	compatible	compatible	compatible	not supported
Vista 32 bit	certified	certified	certified	not supported
Vista 64 bit	compatible	certified	certified	not supported
Win 7 32 bit	certified	certified	certified	not supported
Win 7 64 bit	compatible	certified	certified	not supported
Citrix	not supported	not supported	not supported	not supported

Installation Notes

Installing the 7.2 Release

Cisco Email Security7-2-0-035 is the 7.2 release of the Cisco IronPort Email Security Plug-in. To install the Cisco IronPort Email Security Plug-in, ensure that any previous versions of Cisco IronPort email security plug-ins are uninstalled. This includes:

- Any previous version of the Cisco IronPort Email Security Plug-in
- Any previous version of the Reporting Plug-in (also called the Complaint Plug-in)
- Any previous version of the Encryption Plug-ins (also called Desktop Encrypt, Desktop Flag or Desktop Solutions)

Installing the Plug-in:

Step 1 Double-click on the Cisco Email Security 7-2-0-035.exe file.

Step 2 Click **Run** to start the installation program.

Step 3 The InstallShield opens, and you can choose to perform a full installation or to install only some of the available features. Select from the following components:

- Cisco Email Security Plug-in Core Components
- Cisco IronPort Spam Reporting
- Cisco IronPort Email Encryption

Step 4 Click **Run**. The InstallShield installs your selected components.

Step 5 The InstallShield closes upon completing.

Note If you need to perform a mass installation, see "Performing a Mass Installation" in the *Cisco IronPort Email Security Plug-in Administrator Guide*.

Known Issues

The following list describes known issues in this release of the Cisco IronPort Email Security Plug-in.

Table 1 Cisco IronPort Email Security Plug-in Known Issues

Defect ID	Description
65392	**Encrypt Message Button Absent When Sending an Attachment via Right-click Menu in Windows** When attempting to send an attachment from the Windows right-click menu, some issues may occur, including a missing Encrypt Message button. This occurs because of a defect in a Windows component that uses Simple MAPI. You can track the progress of this issue here: *http://support.microsoft.com/default.aspx?scid=kb;EN-US;916656*
73951	**Errors Occur When Attaching Files Via Microsoft Office 2010** When attaching files to an email message via Microsoft Office 2010, the compose window may become frozen. **Workaround:** Attach the file through Outlook directly by opening a new email and attaching the file.
75976	**Errors Occur When Attempting to Send Mail via the Mail Menu in Microsoft Word** When using the mail menu in Microsoft Word, the mail window may freeze, or the Encrypt Message button may not be present. **Workaround:** Save the document and send the encrypted message via Outlook
77735	**Unable to Disable Cisco IronPort Email Security Plug-in from the COM List in Outlook 2003** When using Outlook 2003, the Cisco IronPort Email Security Plug-in does not appear in the COM-in list as it does in Outlook 2007/2010. **Workaround:** Disable the plug-in via the **Options > Cisco Email Security Plug-in** menu.
78155	**Mass Installation on Windows XP 64 Bit Fails When Using "Typical" Installation** When performing a mass installation on Windows XP 64 bit and selecting the "Typical Installation" option, the files do not get installed into the correct folder, causing the Cisco IronPort Email Security to fail to run. **Workaround:** Choose a custom installation rather than a typical installation when running a mass installation on Windows XP 64 bit.

Table 1 Cisco IronPort Email Security Plug-in Known Issues

Defect ID	Description
78962	**Cisco IronPort Email Security Plug-in Version 6.3.x Does Not Have Forward Compatibility** Because the SDK used in 7.2.x Cisco IronPort Email Security Plug-in was significantly changed from previous versions, messages created in this version cannot be opened using 6.3.x or earlier plug-ins. **Workaround:** Upgrade the Cisco IronPort Email Security Plug-in to version 7.2.x or higher.
79058	**Only the English Version of the Online Help Opens From the Start Menu** When using a translated version of the Cisco IronPort Email Security Plug-in, the online help that opens from the Start menu appears in English rather than the selected language. **Workaround:** Open the online help via the Tools > Options > Cisco Email Security menu.
79111	**Messages Composed in Non-English Language are Corrupted in Certain Email Client Configurations** When sending encrypted email in a non-English language (particularly Asian languages), some email client configurations resulted in corrupted messages. **Workaround for Microsoft Outlook** From the Tools > Options > Mail Format > International Options menu, select the following configuration: • Auto select encoding - False • Preferred encoding - Unicode (UTF-8)
80259	**Desktop Encrypt Does Not Prompt New Users to Register** If a new Encryption user attempts to open an encrypted email from within their email program, they are not prompted to register; rather, they are prompted for a user name and password. **Workaround:** Open the attached HTML file in a browser, which will prompt user registration.

Table 1 Cisco IronPort Email Security Plug-in Known Issues

Defect ID	Description
81125	**Installation stops suddenly when installing the Cisco IronPort Email Security Plug-in 7.1 or 7.2 on Windows 7 64 bit** When installing the Cisco IronPort Email Security Plug-in 7.2 on a Windows 7 64 bit machine, the installation may stop suddenly. This is due to an issue with the installer that does not work with Windows 7 64 bit. For more details, see http://kb.flexerasoftware.com/selfservice/viewContent.do?externalId=Q200150
81326	**If the installation path contains "Program Files" directory, the plugin installation will be split between two directories.** On a Windows 64 bit system, two program files directories exist. Choosing to install in the "Program Files" directory will split the installation between these two directories. Workaround: Always choose "Program Files (x86)" when installing on a Windows 64 bit system.

Related Documentation

For details about configuring and running the Cisco IronPort Email Security Plug-in, see the *Cisco IronPort Email Security Plug-in Administrator Guide*. This guide contains details about performing a mass installation, running the Encryption and Reporting plug-ins on Outlook, and information on running diagnostic tests for troubleshooting as well as uninstalling the plug-in.

In addition, you may need to understand details about how Cisco IronPort Encryption works. 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:

- *Cisco IronPort Email Security Plug-in Administrator 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.

You may also want more details about how Cisco IronPort classifies and handles email that is marked as spam, virus, and 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.

Service and Support

You can request 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 our office hours, please contact Cisco IronPort using one of the following methods:

U.S. toll-free: 1(877) 641- 4766

International: http://cisco.com/web/ironport/contacts.html

Support Portal: http://cisco.com/web/ironport/index.html

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

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.

Printed in the USA on recycled paper containing 10% postconsumer waste.