Release Notes for Cisco IronPort Email Security Plug-in 7.1.1

Revised: September 21, 2011

Contents

These release notes contain information critical to upgrading and running the Cisco IronPort Email Security Plug-in version 7.1.1, including known issues.

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** requires Windows Installer 2.0 or higher.

Installation Notes

Upgrading to the 7.1.1 Release

Follow the instructions below to upgrade to the 7.1.1 release.

Installing the Plug-in:

Step 1 Double-click on the *CiscoEmailSecurity-7-1-1.002.exe* file.

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

The following dialog displays:

```
This setup will perform an upgrade of 'Cisco IronPort Email
Security Plug-In'. Do you want to continue?
```

Step 3 Click **Yes**.

Step 4   Click **Next**.

The installer upgrades the plug-in.

Note   If you need to install the plug-in for multiple users, see "Performing a Mass Installation" in the *Cisco IronPort Email Security Plug-in Administrator Guide*.

Upgrade Paths

The upgrade path for this release is:

7.1.0 --> 7.1.1

Fixed Issues

Table 1 **Cisco IronPort Email Security Plug-in Fixed Issues**

Defect ID	Description
75781	**Fixed: Increased Message Size Due to Encryption Sometimes Causes Message Reporting to Fail** When messages are reported using the Reporting plug-in, the messages are sent to Cisco in an encrypted format, which increases the message size. Occasionally, this causes the message size to increase beyond the size limit for a reported message (1 MB). Now, the size of a reported message is determined by the message size prior to encryption, and messages that do not exceed 1 MB are successfully reported.
75929	**Fixed: Messages Marked for Encryption in Outlook are not Always Sent Encrypted** In some cases, Outlook did not return enough information to determine if the "Encrypt Message" button was pressed, which caused some messages marked for encryption to be sent unencrypted. To resolve this issue, Cisco IronPort has added a secondary check to verify the button's state.

Known Issues

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

Table 2   *Cisco IronPort Email Security Plug-in Known Issues*

Defect ID	Description
76186	**Right-clicking on a Message to Report itMay Report the Wrong Message** When reporting spam, virus or phishing messages, the Reporting tool reports the wrong message if you select a message and then right-click on another message before choosing spam, virus, or phish from the context menu. In this case, the first message you selected is the message that is reported. To work around this issue, first left click on a message before using right-click to report spam, virus, and phishing emails.
75976	**Email Message Window Is Visible But Irresponsive When Using "Send To Mail Recipient" Right-Click Menu or the Mail Menu in Microsoft Word** After sending mail using the "Send to Mail Recipient" option in the right-click menu or using the mail menu in Microsoft Word, the email message window may remain open and visible but irresponsive. Generally, Outlook still sends the mail, but on some occasions the mail may remain in the outbox.
70676	**Encrypt Message Button Disappears or Becomes Disabled in Outlook 2003 when using MS Word as Email Editor** When using Outlook 2003 with Microsoft Word as email editor, if multiple compose windows are open after sending the first encrypted message, the Send Secure button will disappear or become disabled in the remaining open compose windows. **Workaround:** There are two possible workarounds: • Save the remaining open compose messages to the drafts folder, and resend each message separately. -OR- • Disable MS Word as email editor. To do so, go to the Tools menu > options > Mail Format tab. Uncheck "Use Microsoft Office Word 2003 to edit e-mail messages."

Table 2   *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 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*
74324	**"MapiExceptionNamedPropsQuotaExceeded" Error Sometimes Occurs When Sending Encrypted Email** When sending encrypted email using Microsoft Exchange Server, the message is sometimes bounced with the following error "MapiExceptionNamedPropsQuotaExceeded". This error occurs due to quota settings configured in Microsoft Exchange 2003/2007. For more details about how to change these settings, see the following Knowledge Base article: *http://support.microsoft.com/kb/820379/en-us*

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 Lotus Notes and 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 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 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.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

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.