Release Notes for Cisco IronPort Email Security Plug-in 7.1

Revised: December 10, 2010

Contents

These release notes contain information critical to upgrading and running the Cisco IronPort Email Security Plug-in version 7.1, including known issues.

- What's New in the Cisco IronPort Email Security Plug-in 7. 1 Release, page 2
- Supported Configurations, page 2
- Upgrade Paths, page 4
- Known Issues, page 4
- Related Documentation, page 5
- Service and Support, page 6

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. 1 Release

This section describes the new features available in the Cisco IronPort Email Security Plug-in.

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 requires Windows Installer 2.0 or higher.

Installation Notes

Upgrading to the 7.1 Release

CiscoEmailSecurity-7-1-0-039 is the 7.1 release of the Cisco IronPort Email Security Plug-in. To install the Cisco IronPort Email Security Plug-in, you need to uninstall any previous versions of Cisco IronPort Email security plug-ins that you may have installed. 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 (Desktop Encyrpt or Desktop Flag)

Installing the Plug-in:

Step 1 Double-click on the CiscoEmailSecurity-7-1-0-039.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. You can choose to install:

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

Upgrade Paths

There are no upgrade paths for this release.

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
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 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 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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

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.

© 2010 Cisco Systems, Inc. All rights reserved.

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