Release Notes for Cisco IronPort Email Security Plug-in 7.3.1

Revised: September 18, 2013

Contents

These release notes contain information critical to installing and running the Cisco IronPort Email Security Plug-in version 7.3, 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 7.3.1 Release

This release includes the following new features:

- Support for Microsoft Outlook 2013 with Microsoft Windows 7. For more information about which combinations of 32-bit and 64-bit products are supported, see the *Cisco Encryption Compatibility Matrix* at the following URL:

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

What's New in the Cisco IronPort Email Security Plug-in 7.3 Release

This release includes the following new features:

- Ability to configure Cisco Ironport Email Security Plug-in to use a Cisco Ironport Encryption appliance (IEA) or Cisco Registered Envelope Service (CRES) as the hosted key server.
- Support for 64-bit Microsoft Outlook 2010.
- **Automatic Configuration**. The Cisco Ironport Email Security Plug-in is automatically configured by an XML file attachment received from the administrator.
- **Configuration Per Email Account**. The Cisco Ironport Email Security Plug-in is deployed in three modes that determine the configuration per email account as Decrypt Only, Flag, or Encrypt.
- **Desktop Encryption Secure Envelope Options**.
  - **Lock or unlock encrypted email**. The end user is able to lock or unlock encrypted email. They can also set and modify the reason for locking the encrypted email.
  - **Set the expiration date and time for encrypted email**. The end user can set or clear an expiration date and time.

Supported Configurations

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

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

Installation Notes

Installing the 7.3 Release

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_IronPort_Email_Security_Plug-in.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 Administrators who wish to deploy encryption should refer to the "Deploying the Cisco IronPort Email Security Plug-in with the Cisco Registered Envelope Service (CRES) Key Server" and "Deploying the Cisco IronPort Email Security Plug-in with the IronPort Encryption Appliance (IEA) Key Server" sections of the *Cisco IronPort Email Security Plug-in 7.3 Administrator Guide* for more details.

Fixed Defects

The following defect has been fixed in this release:

Table 1 Cisco IronPort Email Security Plug-in Fixed Defects

Defect ID	Description
CSCzv19544 85874	**Fixed: In Office 2010, composing a message directly from Excel causes Outlook to hang.** If the compose message window was launched directly from MS Excel 2010, after the message is composed and the user clicks the send button, Outlook will hang. This issue has been resolved.
SCzv28414 86633	**Fixed: The path for Java should not be hard-coded.** The plug-in searches for a Java installation in C:\Windows\System32 specifically. Instead it should use Windows environment variables such as %WINDIR%. This issue has been resolved.
CSCzv44326 84639	**Fixed: Attachment names containing special characters are not displayed correctly.** When an encrypted message that has attachments with names containing non-ASCII characters is decrypted, the names of the attachments now display correctly.

Table 1 Cisco IronPort Email Security Plug-in Fixed Defects

Defect ID	Description
CSCzv58673 79345	**Fixed: Mobile link in envelopes should be configurable.** The mobile link in envelopes created by the plug-in was previously not configurable. All envelopes pointed users to mobile@res.cisco.com. This can be configured in this release.
CSCzv66130 73951	**Fixed: 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. This issue has been addressed.

Known Limitations

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 Limitations

Defect ID	Description
CSCui96184	**Outlook 2013 plug-in appears in the list of disabled Outlook add-ins** The Cisco Email Security Plug-in is incorrectly included in the list of "Slow and Disabled" add-ins for Outlook 2013. However, the functionality is not impacted and the plug-in works correctly. **Workaround**: No workaround is needed.
CSCuh34033	**BCE configuration validation failure due to email address mismatch** If the email address used to send the signed BCE configuration file is not listed as a CRES account administrator, the verification of the BCE configuration will fail. This can be caused by automatic changes in the mailflow (for example, using the Exchange internal address instead of the SMTP address). **Workaround**: Add the appropriate email address as a CRES account administrator.

Table 2 Cisco IronPort Email Security Plug-in Known Limitations

Defect ID	Description
CSCuh34067	**Improve error message for BCE configuration out-of-range error** Verify that the value you entered is within the minimum and maximum limits set for the value if you receive an error similar to the following message: "Config validation for account <*account*> has failed. Please set the correct configuration values or contact your administrator."
CSCzv13179 85322	**Duplicate Temp Messages Sometimes Appear When Using IMAP** When using encryption with an IMAP email account, sometimes duplicate messages appear. These messages are already marked for deletion and will disappear automatically over time.
CSCzv27779 89439	**Invalid Options are Available for Encrypted Emails in Outlook 2003** When using Microsoft Outlook 2003, some standard Outlook options cannot be used with decrypted emails. For example, once an email is decrypted, the move to folder option will move a blank email to the folder instead of the decrypted email.
CSCzv31994 89252	**Upgrade Option Does Not Work for Non-English Installer** When choosing a language other than English while running the installer, choosing the upgrade option will return the error "Another version of this product is already installed." **Workaround**: Uninstall the previous version before installing the new version.
CSCzv58631 89098	**Encrypt by Default Setting Applies to All Encryption Accounts in Outlook 2003** When using Microsoft Outlook 2003 with multiple email accounts, all email accounts enabled for decryption will share the last configured "Encrypt by Default" setting.

Table 2 Cisco IronPort Email Security Plug-in Known Limitations

Defect ID	Description
CSCzv64207 70676	**Send Secure 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. 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 email messages.
CSCzv98954 91961	**Error occurs when saving CommonEncryptionConfig.xml configuration settings** When upgrading from version 7.2 to 7.3, an error occurs when saving CommonEncryptionConfig.xml configuration settings. **Workaround: The user can uninstall the Plug-in 7.2 and reinstall Plug-in 7.3. This can all be applied to mass installation.** **Note** All Plug-in 7.2 configs will be lost after the uninstall.
CSCuf61810	**Encryption error when using wpad.dat proxy files on workstation** When using wpad.dat files for proxy configuration, and the Plug-in is configured to use system proxy settings, you get an error in the Plug-in “An HTTP error occurred during connection to server: unable to close the socket.”

Related Documentation

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

- *Cisco IronPort Email Security Plug-in 7.3 Administrator Guide*. This guide provides instructions for installing and configuring email encryption, and it may help you to understand how to configure your encryption appliance settings to work with the plug-in settings you configure. See:

http://www.cisco.com/en/US/products/ps10602/prod_installation_guides_list.html

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

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

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

Service and Support

You can request support by phone, email, or online 24 hours a day, 7 days a week. Cisco Customer Support service level agreement details are available on the Support Portal. You can contact Cisco Customer Support using one of the following methods:

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

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