Release Notes for Cisco Email Security Plug-In 7.5

First Published: July 9, 2015
Last Updated: July 9, 2015

Contents

What's New

This release provides the following new features. For more information about these features, see the *Cisco Email Security Plug-in 7.5 Administrator Guide*.

- **Secure Reply and Secure Forward**—Recipients of Registered Envelopes can now forward and reply to encrypted messages using encryption, if it is allowed by the corporate account configuration. Previously, the ability to securely forward and reply was available only for Desktop Encryption accounts. It is now also available for both Decrypt Only accounts and Flag Encryption accounts.
- **Report Marketing Messages**—When providing feedback to Cisco, you can now report Marketing messages, in addition to spam, viruses, and phishing attacks.

Cisco Systems, Inc.
www.cisco.com

- **Localized Envelopes**—The locale selected for the user interface now also determines which language will be used for the contents of registered envelopes. When users send a message to a few recipients in the same locale, they will receive a registered envelope localized according to which of the following locales were selected:
  - English
  - French
  - German
  - Spanish
  - Portuguese
  - Japanese
  - Italian
- **Collection of Usage Data**—You can configure the Cisco Email Security Plug-in to collect anonymous data that will be used to improve the product.

Finding Current Information about Known and Fixed Issues

Use the Cisco Bug Search Tool to find the most current information about known and fixed defects in shipping releases.

Before You Begin

Register for a Cisco account if you do not have one. Go to https://tools.cisco.com/RPF/register/register.do.

Procedure

Step 1 Go to https://tools.cisco.com/bugsearch/.

Step 2 Log in with your Cisco account credentials.

Step 3 Enter search criteria.

For example, the best way to find all issues for this product is to enter Outlook Security Plug-in in the **Search For** field.

Step 4 Optionally filter the search results by status, severity, or other properties.

Step 5 Optionally sort the search results by various criteria

Step 6 If you have questions or problems, click the **Help** or **Feedback** links at the top right side of the tool.

There is also an interactive tour; to view it, click the link in the orange bar above the search fields.

Supported Configurations

The Cisco Email Encryption Compatibility Matrix lists the supported operating systems.

Installation Notes

Installing the 7.5 Release

To install the Cisco Email Security Plug-in, ensure that any previous versions of the plug-in are uninstalled. This includes:

- Any previous version of the Cisco 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 Plug-in.exe* file.

Step 2 Click Run to start the installation program.

Step 3 The AdvancedInstaller 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 Spam Reporting
- Cisco Email Encryption

Step 4 Click Run. The AdvancedInstaller installs your selected components.

Step 5 The AdvancedInstaller closes upon completing.

Note Administrators who wish to deploy encryption should refer to the "Deploying the Cisco Email Security Plug-in with the Cisco Registered Envelope Service (CRES) Key Server" and "Deploying the Cisco Email Security Plug-in with the IronPort Encryption Appliance (IEA) Key Server" sections of the Cisco Email Security Plug-in 7.5 Administrator Guide for more details.

Related Documentation

To use the Encryption plug-in, you need to have a Cisco 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 (IEA), you may want to review the following guides:

- *Cisco Email Security Plug-in 7.5 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.

  To better understand how Cisco 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 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 Email Securty Appliances (ESAs).
- *Cisco Email Security Plug-in 7.5 Open Source Documentation.* This document contains licenses and notices for open source software used in this product.

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What’s New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What’s New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

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