Release Notes for Cisco Email Security Plug-In 7.6

First Published: August 22, 2016
Last Updated: August 22, 2016

Contents

What's New

Simple Registration(*7.6*)—You can now register directly from Email Security Plug-in application in your Outlook. During simple registration, you can register and read your secure messages skipping the Security Questions. Or, you can complete the Advanced Settings form and answer the Security Questions.

Cisco Systems, Inc.
www.cisco.com

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.

Installing the Plug-in

To install the Cisco Email Security Plug-in:

Step 1 Double-click the *Cisco Email Security Plug-in.exe* file.

Step 2 In the **Cisco Email Security Plug-in Setup** window, select a language, and then click **OK**.

Step 3 Click **Next** to start the installation program.

Step 4 Click **Next** to perform a full installation. You can choose to perform a full installation or make one of the features unavailable:

- Reporting Plug-in
- Encryption Plug-in

Step 5 Click **Install**.

Step 6 Wait until the Setup Wizard installs the Plug-in, and click **Finish**.

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” section of the Cisco Email Security Plug-in 7.6 Administrator Guide for more details.

Upgrading the Plug-in

To upgrade the Cisco Email Security Plug-in:

Step 1 Double-click the *Cisco Email Security Plug-in.exe* file.

Step 2 In the **Cisco Email Security Plug-in Setup** window, select a language, and then click **OK**.

Step 3 In the message that appears, click **OK** to start an upgrade. The previous version of Plug-in will be removed.

Step 4 Click **Next** to continue the upgrade.

Step 5 Click **Next** to perform a full installation. You can choose to perform a full installation or make one of the features unavailable:

- Reporting Plug-in
- Encryption Plug-in

Step 6 Click **Install** to start installing the Plug-in 7.6 version.

Step 7 Wait until the Setup Wizard installs the Plug-in, and click **Finish**.

Note In case you cannot perform an upgrade, ensure that any previous versions of the Plug-in are uninstalled and install a new version of Plug-in again.

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 Email Security Appliance (ESA), you may want to review the following guides:

- *Cisco Email Security Plug-in 7.6 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 7.6 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.