Release Notes for Cisco Email Encryption Plug-in 1.2.1

Release Version: 1.2.1-158
Published: July 07, 2020

Contents

Cisco Systems, Inc.
www.cisco.com

What's New

Feature	Description
New Improved User Interface for recipient login	As a recipient, you will now see a new, improved interface when you access a secure message or registered envelope.
Easy Open Feature	The Easy Open feature provides recipients with a simplified method of opening secure messages from any device without the need to install any client-side applications. This is achieved by storing a copy of the encrypted message in CRES, in addition to sending envelope as an attachment to the recipient. When the Easy Open feature is enabled, the new template will have a Read Message button which is active for a maximum of 14 days. After the Read Message link expires, the recipients can retrieve secure messages by opening the attachment in a web browser or forwarding the message to mobile.res.cisco.com.  **Note** The low sensitivity feature is not supported when Easy Open is enabled for your account, If you want to open a message categorized as low sensitivity, click the securedoc HTML attachment or double-click to decrypt your message.
Open Java Runtime Environment (JRE)11	Open JRE version 11 is supported for Cisco Email Encryption Plug-in.

Changes in Behavior

New Date Format for Easy Open Custom Email Notification Template	From this release onwards, in the Administration Console, admins can modify the expiry date format of the Easy Open Custom Email Notification template.
Customizing Template Changes	You can only add one customized template to a notification message. **Note** The customized template now displays the custom logo that you chose for the envelope profile in Account Management > Branding > Images page in the CRES application.
No Support for Mail Encryption using TLS 1.0	Mail encryption with only TLS 1.0 enabled was supported in earlier releases. So you need to migrate to TLS 1.1 or higher.
Secure Message Changes	The Secure Message login page displays the recipient email addresses in a searchable drop-down box. You can use the searchable drop-down box to open a secured message in any one of the following ways: • Select the required recipient email address from the searchable drop-down box. • Search for a recipient email address by entering any character that matches the recipient email address in the searchable drop-down box. **Note** If JavaScript is disabled on your web browser, you will not be able to search for a recipient email address. You can only view and select a recipient email address from the list of recipient email addresses available in the searchable drop-down box. **Note** If you receive the secure message as a BCC recipient, you need to select the 'Address Not listed' option from the searchable drop-down box and enter the recipient email address manually.
Security questions and personal passphrase are removed for new user registration	Security questions and personal passphrase are no longer required when a new user registers for Cisco Registered Envelope Service.
Users must agree to the Terms of Service during registration	New users must agree to the Terms of Service by clicking the **I agree to CRES's Terms of Service** check box to register their account in Cisco Registered Envelope Service.
Change in password reset workflow	Users will receive an email with the subject "Your CRES password reset link" containing a password reset hyperlink to change their password. They will receive another confirmation email saying "Your CRES password has been changed" after changing the password.
Cisco logo is no longer shown in the securedoc HTML attachment	Registered Envelopes do not display Cisco logo and the text Cisco Registered Envelope Service at the bottom of the securedoc.

Supported Configurations

The following configurations are supported for the Cisco Email Encryption Plug-in 1.2.1.

Cisco Email Encryption Plug-in 1.2.0	Outlook 2016 (32 bit)	Outlook 2016 (64 bit)	Outlook 2019 (64 bit)	Office 365
Win 10 32 bit	compatible	—	compatible	—
Win 10 64 bit	compatible	certified	certified	certified

Note When you upgrade to Office 365, Cisco Email Encryption Plug-in may be disabled in your Outlook. In that case, you must enable it manually.

Note Support for Microsoft Windows 7 and 8.1 versions was available till the Cisco Email Encryption Plug-in version 1.2.1-151. From this release onwards, there is only support for Microsoft Windows 10.

Upgrading to Cisco Email Encryption Plug-in 1.2.1

Upgrade Paths

You can upgrade to Cisco Email Encryption Plug-in 1.2.1-158 from the following component versions:

- Cisco Email Security Plug-in 7.6.2.033
- Cisco Email Encryption Plug-in 1.2.1-151

Note After you update the Cisco Email Security Plug-in 7.6.2.033, the Cisco Email Security Plug-in will be removed and the Cisco Email Encryption Plug-in will be available instead.

Upgrading the Cisco Email Encryption Plug-in

To upgrade the Cisco Email Encryption Plug-in:

Step 1 Download the Email Encryption Plug-in installer from the Cisco Software Download Center.

Step 2 Double-click the *Cisco Email Encryption Plug-in.exe* file.

Step 3 In the **Cisco Email Encryption Plug-in Setup** window, select a language, and then click **OK**.

Step 4 In the message that appears, click **OK** to start an upgrade. The previous version of the Cisco Email Encryption Plug-in will be removed.

Step 5 Click **Next** to continue upgrading the Cisco Email Encryption Plug-in.

Step 6 Click **Install** to start installing the latest version.

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

Note If you cannot upgrade the Cisco Email Encryption Plug-in, uninstall all previous versions of the plug-in and then perform a fresh install.

Upgrading from the Cisco Email Security Plug-in to the Cisco Email Encryption Plug-in

To upgrade from the Cisco Email Security Plug-in to the Cisco Email Encryption Plug-in:

Step 1 Download the Email Encryption Plug-in installer from the Cisco Software Download Center.

Step 2 Double-click the *Cisco Email Encryption Plug-in.exe* file.

Step 3 In the **Cisco Email Encryption Plug-in Setup** window, select a language, and then click **OK**.

Step 4 In the message that appears, click **OK** to start an upgrade. The Cisco Email Security Plug-in will be removed and the Cisco Email Encryption Plug-in will be installed.

Step 5 Click **Next** to continue upgrading the Cisco Email Encryption Plug-in.

Step 6 Click **Install** to start installing the latest version.

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

Note The Cisco Email Security Plug-in will be removed from the Outlook toolbar, and the Cisco Email Encryption Plug-in will be available instead.

Installing Cisco Email Encryption Plug-in 1.2.1

Installing the Cisco Email Encryption Plug-in

Note Do not use or install the Cisco Email Encryption Plug-in 1.2.1 with the Cisco Email Security Plug-in 7.6.0 or later. If you need the reporting functionality, install both the Cisco Email Encryption Plug-in 1.x and the Cisco Email Reporting Plug-in 1.x.

To install the Cisco Email Encryption Plug-in:

Step 1 Download the Email Encryption Plug-in installer from the Cisco Software Download Center.

Step 2 Double-click the *Cisco Email Encryption Plug-in.exe* file.

Step 3 In the **Cisco Email Encryption Plug-in Setup** window, select a language, and then click **OK**.

Step 4 Click **Next** to start the installation program.

Step 5 Click **Install**.

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

Performing Mass Installation of Cisco Email Encryption Plug-in

See *Cisco Email Encryption Plug-in 1.2.1 Administrator Guide* for instructions on how to perform mass installation of Cisco Email Encryption Plug-in.

Known and Fixed Issues

Use the Cisco Bug Search Tool to find information about known and fixed defects in this release.

List of Known and Fixed Issues

Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283137618&rls=1.2.1-158&sb=afr&bt=custV
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283137618&rls=1.2.1-158&sb=fr&bt=custV

Finding Information about Known and Fixed Issues

Use the Cisco Bug Search Tool to find information about known and fixed defects in this release.

Before You Begin

Register for a Cisco account if you do not have one. Go to https://identity.cisco.com/ui/tenants/global/v1.0/enrollment-ui.

Procedure

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

Step 2 Log in with your Cisco account credentials.

Step 3 Enter the search criteria.

For example, the easiest way to find all issues for this product is to enter *Cisco Email Encryption* in the **Product** field.

Step 4 In the text entry field for **Releases**, enter the version of the release, for example, 1.2.1-158.

Step 5 Depending on your requirements, do one of the following:

- To view the list of resolved issues, select **Fixed in these Releases** from the drop down for **Releases**.
- To view the list of known issues, select **Affecting these Releases** from the drop down list for **Releases** and select **Open** from the **Status** drop down.

Step 6 Optionally, filter the search results by status, severity, or other properties.

Step 7 Optionally, sort the search results by various criteria.

Note 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

Related Documentation

For more information about the Cisco Email Encryption Plug-in, see:

- *Cisco Email Encryption Plug-in 1.2.1 Administrator Guide*. This guide provides instructions for installing and configuring the Cisco Email Encryption Plug-in, and it may help you to understand how to configure your encryption settings to work with the plug-in settings you configure.
- *Cisco Email Encryption Plug-in 1.0 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: https://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.

To have a list of all new and revised Cisco technical documentation delivered directly to your desktop using a reader application, subscribe to *What's New in Cisco Product Documentation* as an RSS feed by clicking the RSS icon on the What's New page. The RSS feeds are a free service.

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