



Release Notes for Cisco Email Security Plug-In 7.6

Release Version: 7.6.2-037


Published: July 14, 2020

Contents


- [What's New, page 2](#)
- [Changes in Behavior, page 2](#)
- [Supported Configurations, page 3](#)
- [Upgrade Paths, page 4](#)
- [Installing Cisco Email Security Plug-in 7.6, page 4](#)
- [Fixed Issues, page 4](#)
- [Related Documentation, page 5](#)
- [Service and Support, page 5](#)
- [Obtaining Documentation and Submitting a Service Request, page 5](#)





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	<p>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.</p> <p> 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.</p>
Open Java Runtime Environment (JRE)11	This release supports Open JRE version 11 for Cisco Email Security 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	<p>From this release onwards, you can only add one customized template to a notification message.</p> <p> 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.</p>
No Support for Mail Encryption using TLS 1.0	<p>Prior to this release, mail encryption with only TLS 1.0 enabled was supported.</p> <p>From this release onwards, you need to migrate to TLS 1.1 or higher.</p>

Secure Message Changes	<p>From this release onwards, the Secure Message login page displays the recipient email addresses in a searchable drop-down box.</p> <p>You can use the searchable drop-down box to open a secured message in any one of the following ways:</p> <ul style="list-style-type: none"> • 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. <p> 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.</p> <p> 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.</p>
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 checkbox 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 Security Plug-in 7.6.x:

Cisco Email Security Plug-in 7.6.2.	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

Support for Microsoft Windows 7 and 8.1 versions was available till the Cisco Email Security Plug-in version 7.6.2-033. From this release onwards, there is only support for Microsoft Windows 10.

Upgrade Paths

You can upgrade to Cisco Email Security Plug-in 7.6.2-037 release from Cisco Email Security Plug-in 7.6.2-033 version.



Note If you plan to upgrade to Cisco Email Security Plug-in 7.6.2-037 release from Cisco Email Security Plug-in 7.6.2-033 version, it is a silent installation process.

Installing Cisco Email Security Plug-in 7.6

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)

-
- Step 1** Double-click 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 Email Reporting
 - Cisco Email Encryption
- Step 4** Click **Run**. The AdvancedInstaller installs your selected components.
- Step 5** The AdvancedInstaller closes upon completing.



Note The administrators who want to deploy encryption should see 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.

Fixed Issues

The following table lists the bug that is fixed in this release:

Defect ID	Description
CSCvr55889	Cisco Email Encryption installers can't be verified.
CSCvt97767	Outlook 2019 as a supported client for Encryption and Reporting Plugin.

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, 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 the Cisco Email Security Plug-in, and it may help you to understand how to configure your security settings to work with the plug-in settings you configure..
- [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 Security appliances.
- [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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned 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. (1110R)

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.

© 2011—2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.