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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Improved User Interface for recipient login</td>
<td>As a recipient, you will now see a new, improved interface when you access a secure message or registered envelope.</td>
</tr>
<tr>
<td>Easy Open Feature</td>
<td>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.</td>
</tr>
<tr>
<td>Note</td>
<td>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.</td>
</tr>
<tr>
<td>Open Java Runtime Environment (JRE)11</td>
<td>This release supports Open JRE version 11 for Cisco Email Security Plug-in.</td>
</tr>
</tbody>
</table>

Changes in Behavior

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Date Format for Easy Open Custom Email</td>
<td>From this release onwards, in the Administration Console, admins can modify the expiry date format of the Easy Open Custom Email Notification template.</td>
</tr>
<tr>
<td>Notification Template</td>
<td></td>
</tr>
<tr>
<td>Customizing Template Changes</td>
<td>From this release onwards, you can only add one customized template to a notification message.</td>
</tr>
<tr>
<td>Note</td>
<td>The customized template now displays the custom logo that you chose for the envelope profile in Account Management &gt; Branding &gt; Images page in the CRES application.</td>
</tr>
<tr>
<td>No Support for Mail Encryption using TLS 1.0</td>
<td>Prior to this release, mail encryption with only TLS 1.0 enabled was supported.</td>
</tr>
<tr>
<td></td>
<td>From this release onwards, you need to migrate to TLS 1.1 or higher.</td>
</tr>
</tbody>
</table>
Release Notes for Cisco Email Security Plug-In 7.6

**Supported Configurations**

The following configurations are supported for the Cisco Email Security Plug-in 7.6.x:

<table>
<thead>
<tr>
<th>Cisco Email Security Plug-in 7.6.x</th>
<th>Outlook 2016 (32 bit)</th>
<th>Outlook 2016 (64 bit)</th>
<th>Outlook 2019 (64 bit)</th>
<th>Office 365</th>
</tr>
</thead>
<tbody>
<tr>
<td>Win 10 32 bit</td>
<td>compatible</td>
<td>—</td>
<td>compatible</td>
<td>—</td>
</tr>
<tr>
<td>Win 10 64 bit</td>
<td>compatible certified</td>
<td>certified certified</td>
<td>certified certified</td>
<td></td>
</tr>
</tbody>
</table>

**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.

**Secure Message Changes**

From this release onwards, 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 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.
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:

<table>
<thead>
<tr>
<th>Defect ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCvr55889</td>
<td>Cisco Email Encryption installers can't be verified.</td>
</tr>
<tr>
<td>CSCvt97767</td>
<td>Outlook 2019 as a supported client for Encryption and Reporting Plugin.</td>
</tr>
</tbody>
</table>
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:

- 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.