User Guide for Cisco Secure Email Encryption Service Add-In

Revised: September 14, 2024

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Contents

Chapter 1: Getting Started

The Cisco Secure Email Encryption Service add-in allows you to encrypt your messages directly from Microsoft Outlook with a single click. You can install this add-in on Microsoft Outlook (for Windows and macOS) and Outlook Web App.

In addition to encrypting your messages, you can use the add-in to:

- Identify if the recipient has read your message
- Revoke the encryption keys
- Set expiration dates for encrypted messages
- Lock and unlock encrypted messages
- Manage and search your encrypted messages

Supported Configurations

Microsoft Office Variant	
Certified	Microsoft 365 Apps for Enterprise
	Outlook Web App (on the latest version of Google Chrome, Mozilla Firefox, Microsoft Edge, and Apple Safari.)

Note: You can install the Cisco Secure Email Encryption Service add-in only if you are using an Office 365/Microsoft 365 subscription.

Note: Only Microsoft Office 365 and Exchange Online are supported for Secure Email Encryption Add-In. Exchange Server (on-premises) is not supported.

Related Documents

If you are an account administrator for Cisco Secure Email Encryption Service, we recommend that you review the following documents:

Product	Guide	Location
Cisco Secure Email Gateway	Release Notes	http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html
	User Guide	http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html
Cisco Secure Email Encryption Service	Release Notes	https://www.cisco.com/c/en/us/support/security/email-encryption/products-release-notes-list.html
	User Guide	https://www.cisco.com/c/en/us/support/security/email-encryption/products-user-guide-list.html
Microsoft 365 Admin Center	Publish Office Add-Ins Using Centralized Deployment via the Microsoft 365 Admin Center	https://docs.microsoft.com/en-us/office/dev/add-ins/publish/centralized-deployment

Cisco End User License Agreement

For information about the Cisco End User License Agreement, see https://www.cisco.com/c/en/us/about/legal/cloud-and-software/end_user_license_agreement.html.

Chapter 2: Installing and Configuring the Cisco Secure Email Encryption Service Add-In

To encrypt your messages, install and configure the Cisco Secure Email Encryption Service add-in on your Microsoft Outlook.

Note: If your administrator uses Centralized Deployment to publish the Cisco Secure Email Encryption Service add-in, you may already have the add-in in your Outlook. In this scenario, skip the installation process.

Installing the Cisco Secure Email Encryption Service Add-In

Before You Begin

- Review the Supported Configurations topic.
- Contact your administrator to obtain the add-in manifest file or URL.
- Ensure that you are a registered Cisco Secure Email Encryption Service user and that your account is activated.

  Note: SAML and Google-based authentications are not supported on the Cisco Secure Email Encryption Service add-in. For further assistance, contact your administrator.

- Check whether your Outlook client is installed using the Microsoft Store. If you have installed the Outlook client using Microsoft Store, you may not find an option to install custom add-ins. In this scenario, install the Cisco Secure Email Encryption Service add-in using the Outlook Web App.

Procedure

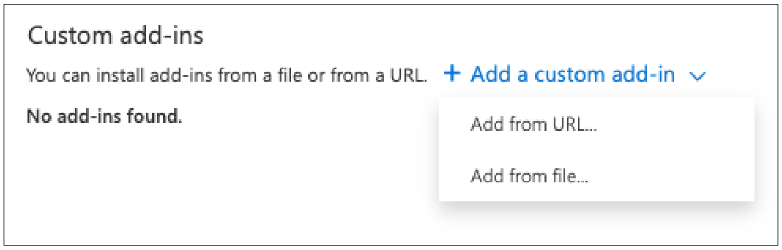
Note: To install the Secure Email Encryption Service Add-in, you have two options. If you are using Outlook for Windows or macOS, click the **Get Add-ins** button located on the Ribbon or Toolbar. However, if you do not see this button in your Outlook app, you can follow these steps to install the add-in via your web browser.

Step 1. Open your web browser and go to https://aka.ms/olksideload and log in with your credentials.

Step 2. On the pop-up that appears, click **My Add-ins**.

Step 3. Under **Custom Addins**, click **Add a custom add-in** > **Add from File**.

Step 4. install the Cisco Secure Email Encryption Service add-in from the manifest file.



Custom add-ins

You can install add-ins from a file or from a URL.

No add-ins found.

Step 5. Follow the on-screen instructions to complete the installation process.

Step 6. After installation, restart your Outlook app to see the encryption add-in.

For detailed instructions about installing add-ins, see the Microsoft Office documentation.

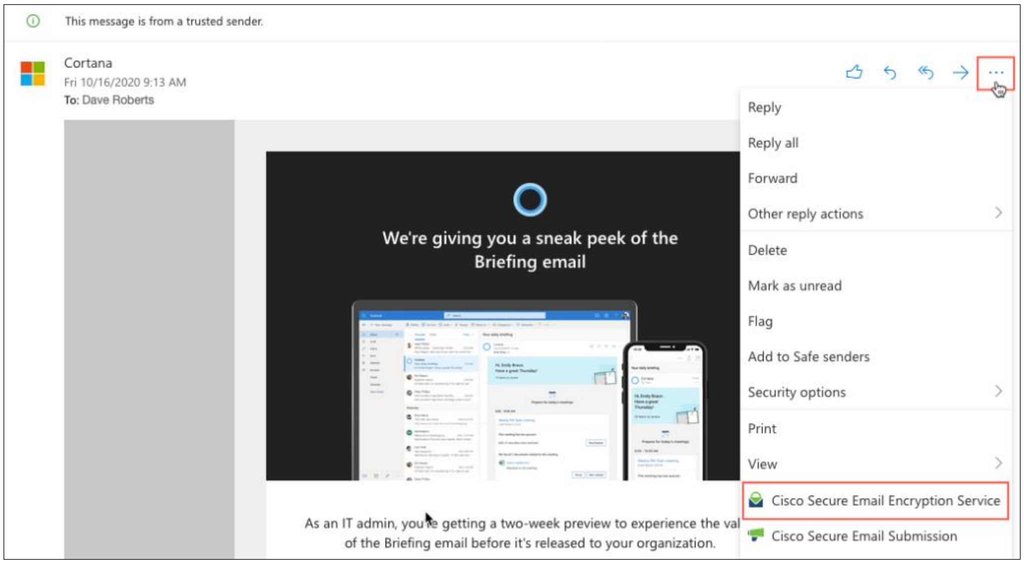
Accessing Cisco Secure Email Encryption Service Add-In

Procedure

Step 1. Open the Cisco Secure Email Encryption Service add-in from your Outlook for Office 365/Microsoft 365 or Outlook Web App.

Do one of the following:

- On Outlook Web App, after you select a message, click the ellipsis icon in the Reading pane, and click **Cisco Secure Email Encryption Service**.



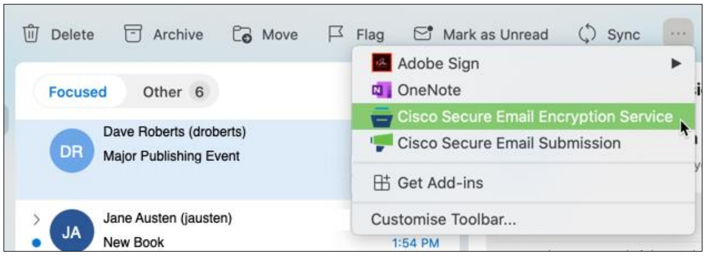
This message is from a trusted sender.

Cortana
Fri 10/16/2020 9:13 AM
To: Dave Roberts

We're giving you a sneak peek of the Briefing email

As an IT admin, you're getting a two-week preview to experience the val of the Briefing email before it's released to your organization.

- On Outlook for Windows or macOS, click **Manage Encrypted Messages** from the Ribbon or Toolbar.



Note: If you are on Outlook for macOS version 16.42 or later and using the New Outlook interface, click **Cisco Secure Email Encryption Service** from the Toolbar.

Registering for Cisco Secure Email Encryption Service

If you do not have a Secure Email Encryption Service account, you must register before you can start using the encryption service.

Procedure

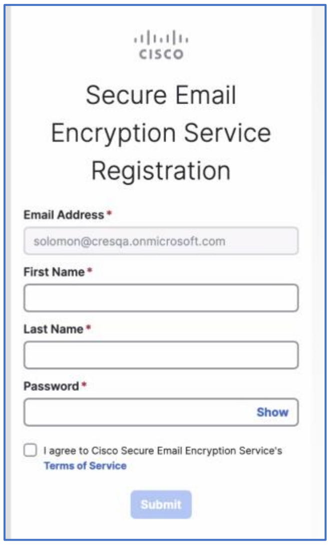
Step 1. Click the **Register** button.

Step 2. Enter your **First Name**, and **Last Name** in the specified fields.

Step 3. Enter a Password of your choice.

Step 4. Select the **Terms of Service** check box.

Step 5. Click **Submit**.



Secure Email Encryption Service Registration

Email Address * solomon@cresqa.onmicrosoft.com

First Name *

Last Name *

Password *

□ I agree to Cisco Secure Email Encryption Service's Terms of Service

You will receive an email with the account activation link. Check your email and click the link to activate your Secure Email Encryption Service account.

Note: When you click the account activation link, you might see an *invalid link* error. This is because of the Safelink protection action from Microsoft. Microsoft Defender is enabled in Office 365 by default and checks link safety by clicking them in the background. As a result, users may see an "Invalid link" error since Microsoft has already verified the link before user interaction. You can either ignore this error, or disable the safelink protection for res.cisco.com domain and add an exception.
To exclude Secure Email Encryption Service from safelink protection:

Step 1. Go to https://security.microsoft.com/

Step 2. In the left pane, go to Email & collaboration > Policies & rules > Threat policies > Preset security policies.

Step 3. Click the toggle to turn OFF (disable) *Standard Protection* and *Strict Protection*.

Step 4. Under **Built-in protection**, click **Add Exclusions (not recommended)**.

Step 5. Click the + icon to add a new exclusion for the domain *res.cisco.com*.

Note: The changes will take effect in 6 hours.

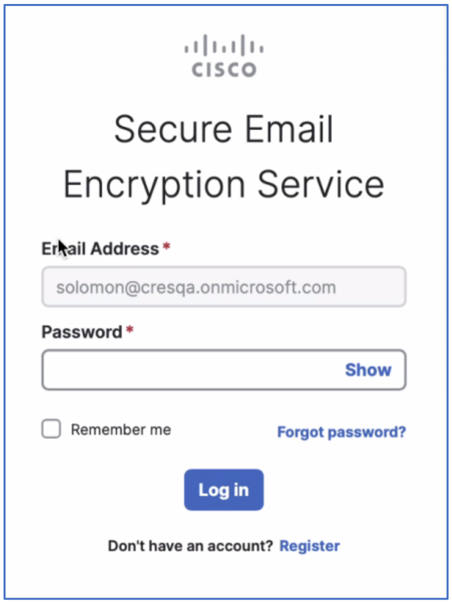
Logging in to Cisco Secure Email Encryption Service

Procedure

Step 1. If you are logging in to the add-in for the first time, click **Get Started**.

Step 2. In the Cisco Secure Email Encryption Service add-in pane, enter your credentials.

Step 3. Select **Remeber Me** and click **Sign in**.



Email Address *

solomon@cresqa.onmicrosoft.com

Password *

If you select *Remember me*, you need not enter the password every time you open the Secure Eamil Encryption Service Add-In client. The Secure Email Encryption Service administrator needs to configure this feature in the admin portal for it to take effect.

Note: SAML and Google-based authentications are not supported on the Cisco Secure Email Encryption Service add-in. For further assistance, contact your administrator

When you log in to the Cisco Secure Email Encryption Service add-in for the first time, the add-in downloads your organization-specific configuration. Wait for this process to complete.

After the process is complete, you can send encrypted messages and manage them. For more information, see Encrypting Messages Using the Cisco Secure Email Encryption Service and Managing Messages Using the Cisco Secure Email Encryption Service Add-In.

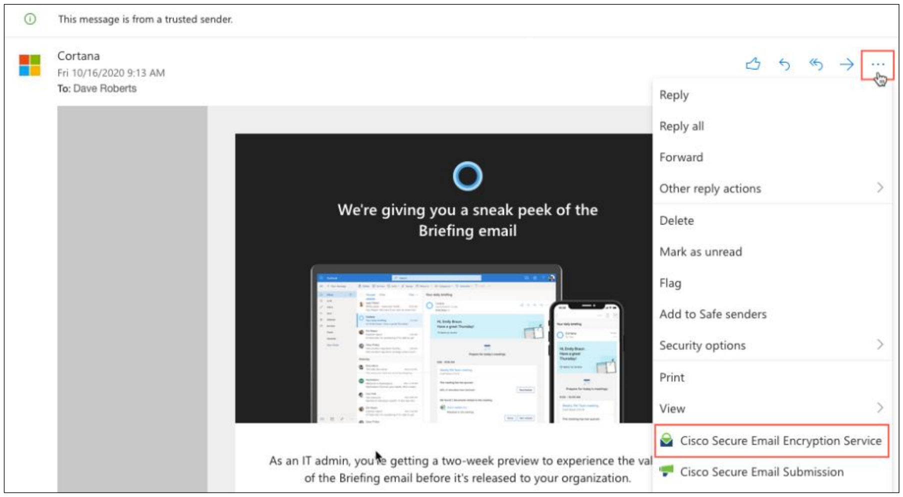
Modifying the Cisco Secure Email Encryption Service Add-In Settings

Procedure

Step 1. Open the Cisco Secure Email Encryption Service add-in from your Outlook for Office 365/Microsoft 365 or Outlook Web App.

Do one of the following:

- On the Outlook Web App, after you select a message, click the ellipsis icon in the Reading pane, and click **Cisco Secure Email Encryption Service**.



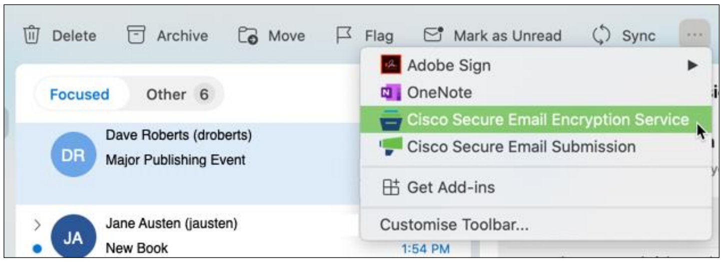
This message is from a trusted sender.

Cortana
Fri 10/16/2020 9:13 AM
To: Dave Roberts

We're giving you a sneak peek of the Briefing email

As an IT admin, you're getting a two-week preview to experience the val… of the Briefing email before it's released to your organization.

- On Outlook for Windows or macOS, click **Manage Encrypted Messages** from the Ribbon or Toolbar.



Note: If you are on Outlook for macOS version 16.42 or later and using the New Outlook interface, click **Cisco Secure Email Encryption Service** from the Toolbar.

Step 2. Enter your credentials, and click **Sign in**.

Step 3. Click the settings (⚙) icon.

Step 4. Adjust the following options as needed:

Option	Description
Add-in Configuration	
Update Configuration	Click this button to download the latest version of the configuration.
General Settings	
Email Address	The email address associated with your Outlook account. This field is auto-populated and cannot be edited.
Encryption Type	The encryption type set by your Cisco Secure Email Encryption Service administrator. This field is auto-populated and cannot be edited. Cisco Secure Email Encryption Service add-in supports the following encryption types: • **Flag** - Allows you to flag the message for encryption, and the Cisco Email Security appliance encrypts the message before the message is sent out of the network. For more information, contact your administrator. • **Encrypt** - Allows you to encrypt and send the message from within Outlook.
Security Level	Select the security level for the encrypted message: • **High**. The recipient must authenticate whenever the messages are decrypted. • **Medium**. If the password of the recipient is cached, the recipient does not need to authenticate whenever the messages are decrypted. • **Low**. Transmitted securely, but the recipient does not need to authenticate whenever the messages are decrypted.
Request Decryption Notification	Select this option to request return receipt when the recipient decrypts the message you sent.
Reply Options	• **Allow Reply**. Select this option to allow the recipient to reply to an encrypted message. • **Allow Reply All**. Select this option to allow the recipient to reply to all the users in an encrypted message. • **Allow Forward**. Select this option to allow the recipient to forward an encrypted message. In these scenarios, the messages are encrypted automatically.

Step 5. Click **Apply**.

Note: You cannot edit the **Email Address** and **Encryption Type** fields under the **Profile Details** section. The email address is auto-populated from your Outlook profile, and the encryption type is set by your Cisco Secure Email Encryption Service administrator.

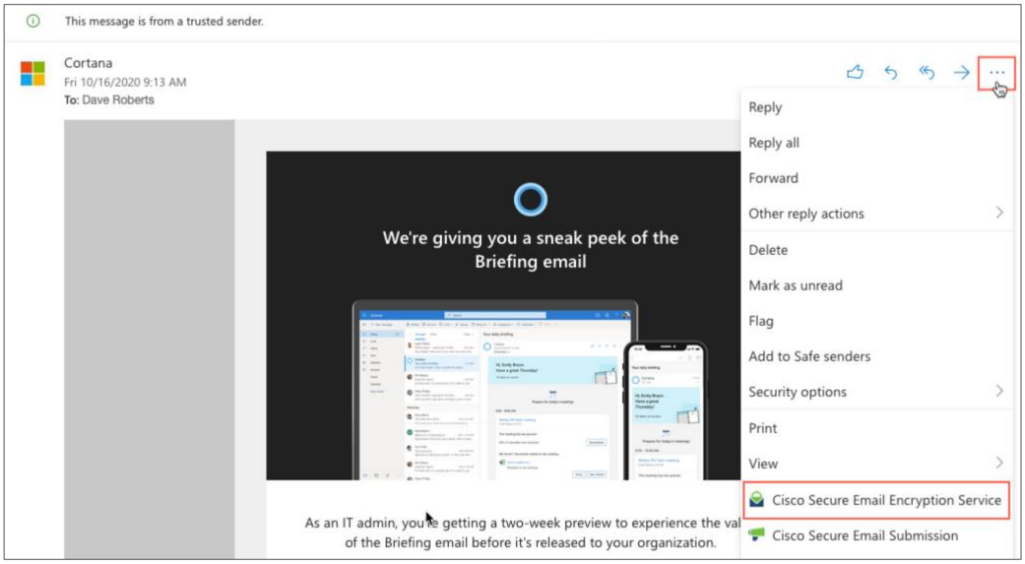
Updating the Cisco Secure Email Encryption Service Add-In Configuration

If your administrator has updated the add-in configuration, you must download and apply the new configuration manually. You can either perform this activity periodically or after you receive a configuration update notification from your administrator.

Procedure

Step 1. Open the Cisco Secure Email Encryption Service add-in from your Outlook for Office 365/Microsoft 365 or Outlook Web App.

Do one of the following:



This message is from a trusted sender.

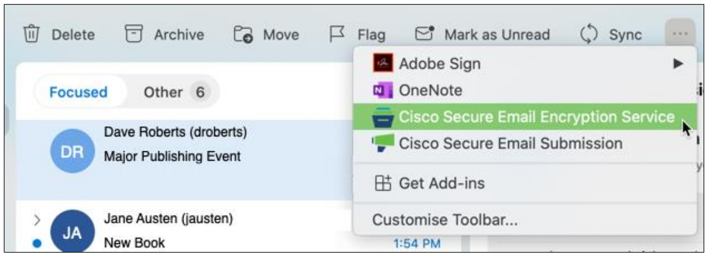
Cortana
Fri 10/16/2020 9:13 AM
To: Dave Roberts

We're giving you a sneak peek of the Briefing email

As an IT admin, you're getting a two-week preview to experience the val of the Briefing email before it's released to your organization.

- On Outlook Web App, after you select a message, click the ellipsis icon in the Reading pane, and click **Cisco Secure Email Encryption Service**.
- On Outlook for Windows or macOS, click **Manage Encrypted Messages** from the Ribbon or Toolbar.

Note: If you are on Outlook for macOS version 16.42 or later and using the New Outlook interface, click **Cisco Secure Email Encryption Service** from the Toolbar.



Step 2. Enter your credentials, and click **Sign in**.

Step 3. Click the settings (⚙) icon.

Step 4. Click **Update Configuration**.

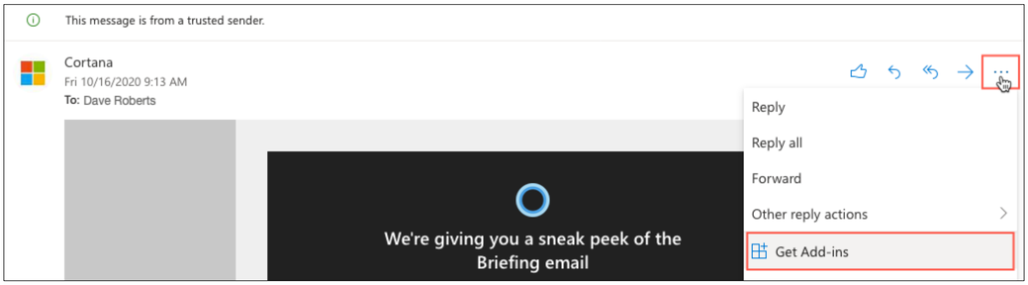
The latest add-in configuration is downloaded and applied.

Uninstalling the Cisco Secure Email Encryption Service Add-In

Procedure

Step 1. Open the Add-ins for Outlook page from your Outlook for Office 365/Microsoft 365 or Outlook Web App.

Do one of the following:



This message is from a trusted sender.

Cortana
Fri 10/16/2020 9:13 AM
To: Dave Roberts

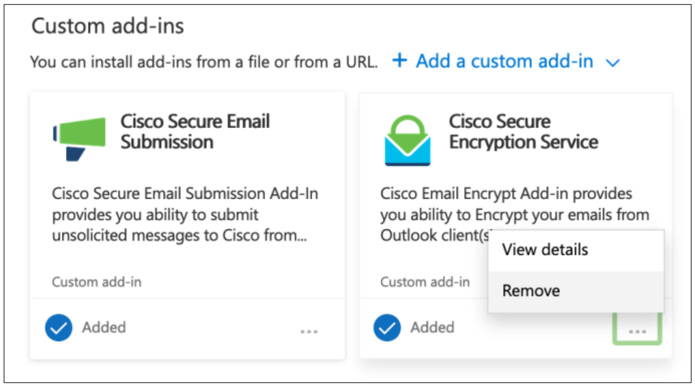
We're giving you a sneak peek of the Briefing email

- On Outlook Web App, after you select a message, click the ellipsis icon in the Reading pane, and click **Get Add-ins**.
- On Outlook for Windows or macOS, click **Get Add-ins** from the Ribbon or Toolbar.

Note: If the **Get Add-ins** button is not available on your Outlook for macOS, log in to the Outlook Web App to complete this task.

Step 2. Click **My add-ins**.

Step 3. Under **Custom add-ins**, click the ellipsis icon in the Cisco Secure Email Encryption Service add-in, and click **Remove**.



Custom add-ins

You can install add-ins from a file or from a URL.

Cisco Secure Email Submission

Cisco Secure Email Submission Add-In provides you ability to submit unsolicited messages to Cisco from...

Custom add-in

Cisco Secure Encryption Service

Cisco Email Encrypt Add-in provides you ability to Encrypt your emails from Outlook client(s

Custom add-in

For detailed instructions about uninstalling add-ins, see the Microsoft Office documentation.

Note: The Cisco Secure Email Encryption Service add-in settings are stored in your Office 365/Microsoft 365 account and are retained for as long as your account is active. These settings are not deleted when you uninstall the add-in. As a result, when you reinstall the Cisco Secure Email Encryption Service add-in for the same Office 365/Microsoft 365 account, the old settings are applied again.

Chapter 3: Encrypting and Managing Messages Using the Cisco Secure Email Encryption Service Add-In

This chapter describes how to encrypt and manage messages using the Cisco Secure Email Encryption Service add-in.

Encrypting Messages Using the Cisco Secure Email Encryption Service Add-In

Procedure

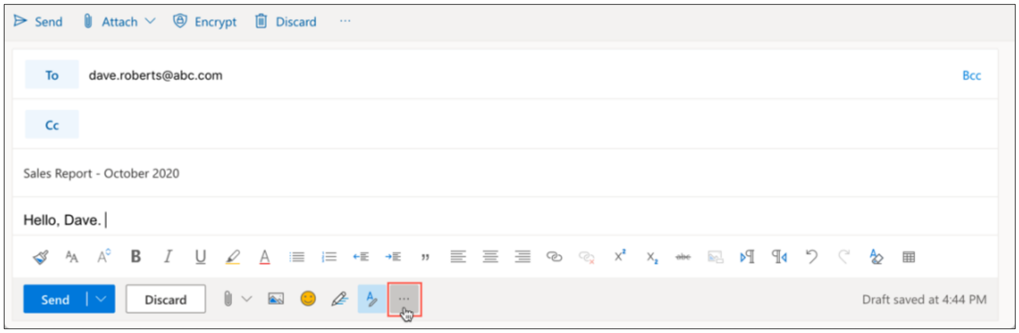
Step 1. On your Outlook for Office 365/Microsoft 365 or Outlook Web App, compose the message that you want to encrypt, and add at least one valid recipient to it.

Note: If the encryption type (set by your administrator) is Encrypt, ensure that you have completed your message and added valid recipients before proceeding to the next step. After Step 3, the message is encrypted and sent immediately.

Step 2. Open the Cisco Secure Email Encryption Service add-in.

Do one of the following:

- On the Outlook Web App, click the ellipsis icon (located near the **Send** and **Discard** buttons), and click **Cisco Secure Email Encryption Service**.



To: dave.roberts@abc.com

Cc:

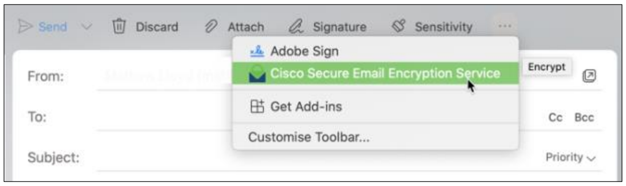
Sales Report - October 2020

Hello, Dave.

Draft saved at 4:44 PM

- On Outlook for Windows or macOS, click **Encrypt** from the Ribbon or Toolbar.

Note: If you are on Outlook for macOS version 16.42 or later and using the New Outlook interface, click **Cisco Secure Email Encryption Service** from the Toolbar.



Step 3. Enter your credentials, and click **Sign in**.

Depending on the encryption type set by your administrator, one of the following events happens:

- If the encryption type is *Encrypt*, the message is encrypted and sent after authentication.
- If the encryption type is *Flag*, the message is flagged for encryption. Proceed to the next step.

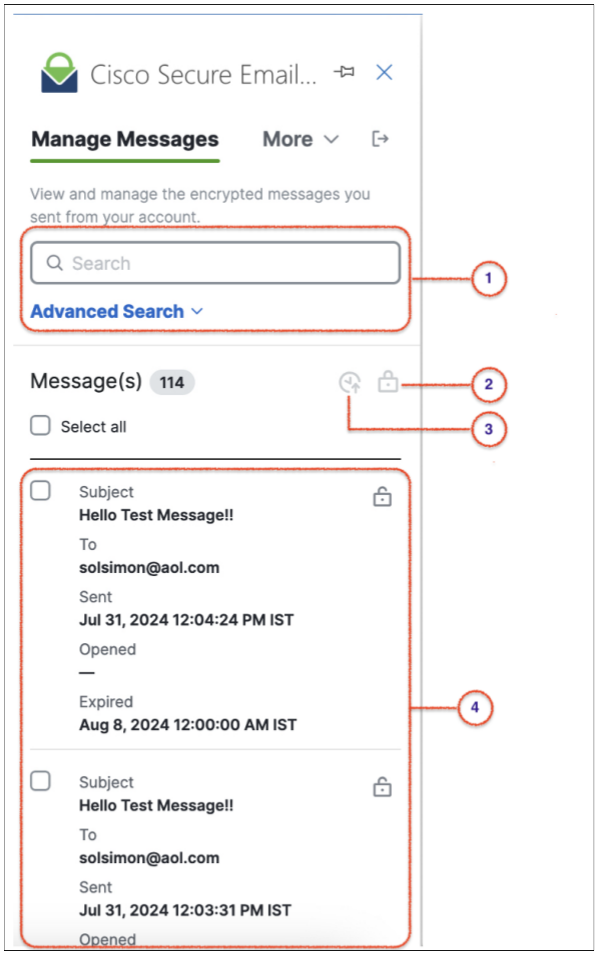
Note: When composing a message, if the encryption type is Flag, you do not need to enter your password.

Step 4. (Only if the Encryption Type is *Flag*) Click **Send**.

You can view the encryption status under the **Encryption Flow Summary** section of the Cisco Secure Email Encryption Service add-in pane. For troubleshooting encryption issues, see the *Troubleshooting Cisco Secure Email Encryption Service Add-in* chapter.

Managing Messages Using the Cisco Secure Email Encryption Service Add-In

You can manage the encrypted messages you have sent using the **Manage Messages** tab. The following illustration shows various actions that you can perform on this tab:



View and manage the encrypted messages you sent from your account.

Subject
Hello Test Message!!
To
solsimon@aol.com
Sent
Jul 31, 2024 12:04:24 PM IST
Opened
—
Expired
Aug 8, 2024 12:00:00 AM IST

Subject
Hello Test Message!!
To
solsimon@aol.com
Sent
Jul 31, 2024 12:03:31 PM IST
Opened

#	Action	More Info
1	Basic and advanced searches	Finding Encrypted Messages
2	Set lock status	Locking Encrypted Messages
3	Set expiration date	Setting Expiration Date for Encrypted Messages
4	View encrypted messages	Viewing the List of Encrypted Messages

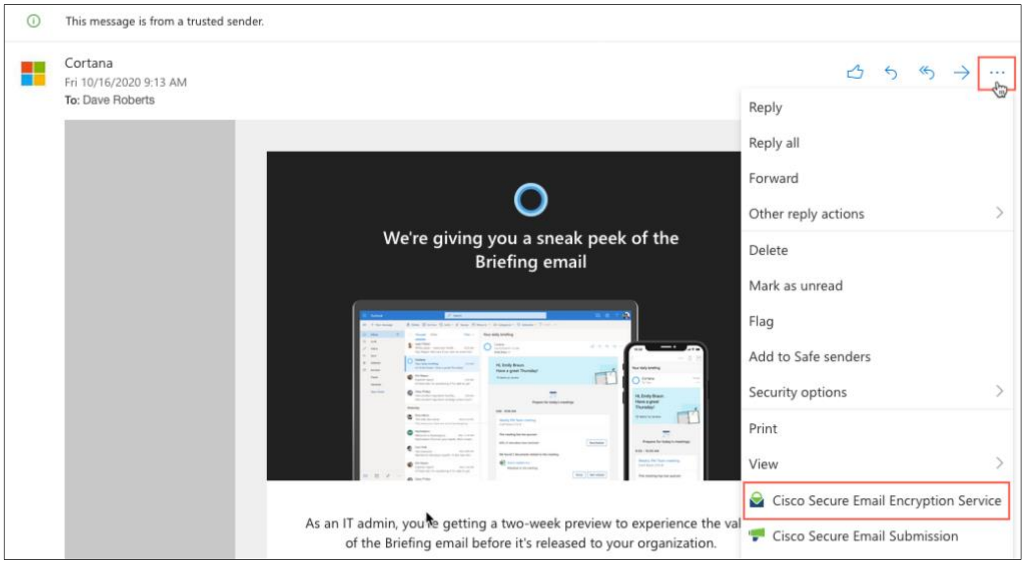
Viewing the List of Encrypted Messages

Procedure

Step 1. Open the Cisco Secure Email Encryption Service add-in from your Outlook for Office 365/Microsoft 365 or Outlook Web App.

Do one of the following:

- On Outlook Web App, after you select a message, click the ellipsis icon in the Reading pane, and click **Cisco Secure Email Encryption Service**.



This message is from a trusted sender.

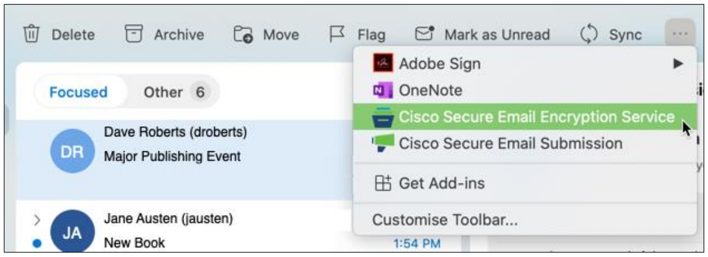
Cortana
Fri 10/16/2020 9:13 AM
To: Dave Roberts

We're giving you a sneak peek of the Briefing email

As an IT admin, you're getting a two-week preview to experience the val
of the Briefing email before it's released to your organization.

- On Outlook for Windows or macOS, click **Manage Encrypted Messages** from the Ribbon or Toolbar.

  Note: If you are on Outlook for macOS version 16.42 or later and using the New Outlook interface, click **Cisco Secure Email Encryption Service** from the Toolbar.



Dave Roberts (droberts)
Major Publishing Event

Jane Austen (jausten)
New Book
1:54 PM

Step 2. Enter your credentials, and click **Sign in**.

Step 3. Under the **Manage Messages** (✉) tab, view all the encrypted messages that you sent.

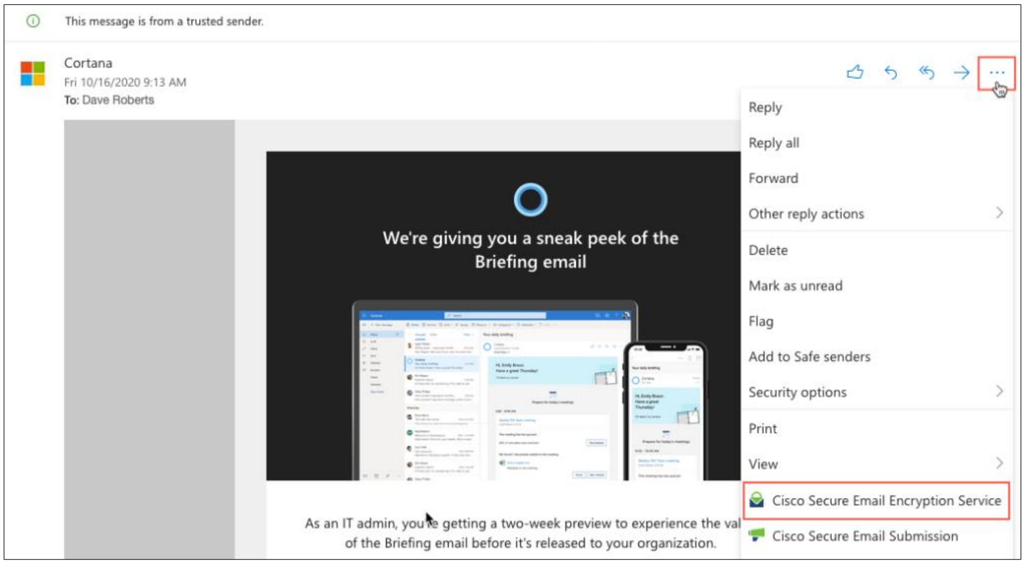
Finding Encrypted Messages

Procedure

Step 1. Open the Cisco Secure Email Encryption Service add-in from your Outlook for Office 365/Microsoft 365 or Outlook Web App.

Do one of the following:

- On the Outlook Web App, after you select a message, click the ellipsis icon in the Reading pane, and click **Cisco Secure Email Encryption Service**.



This message is from a trusted sender.

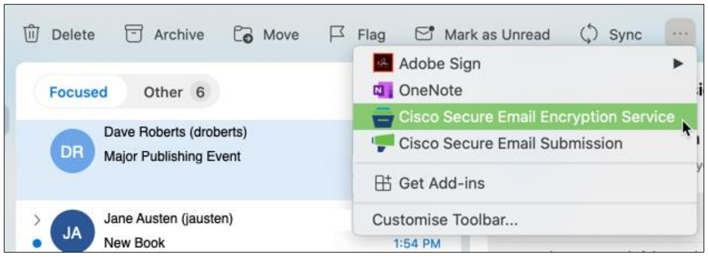
Cortana
Fri 10/16/2020 9:13 AM
To: Dave Roberts

We're giving you a sneak peek of the Briefing email

As an IT admin, you're getting a two-week preview to experience the val
of the Briefing email before it's released to your organization.

- On Outlook for Windows or macOS, click **Manage Encrypted Messages** from the Ribbon or Toolbar.

Note: If you are on Outlook for macOS version 16.42 or later and using the New Outlook interface, click **Cisco Secure Email Encryption Service** from the Toolbar.



Dave Roberts (droberts)
Major Publishing Event

Jane Austen (jausten)
New Book
1:54 PM

Step 2. Enter your credentials, and click **Sign in**.

Step 3. Under the **Manage Messages** (✉) tab, enter your search word(s) in the search box.

To find encrypted messages using the advanced search, click **Advanced Search** under the search box. You can find encrypted messages based on the following criteria:

Option	Description
Search box	Enter your search word or words
In	Specify whether the search words are present in the To or Subject fields. Select **Failed Attempts** to find messages that were not sent because of encryption errors.
Status	Select the status of the message – expired, locked, opened, unopened, or all.
Date From	• Set only the **Date From** option to find any messages sent, opened, or expired after the selected date. • Set only the **Date To** option to find any messages sent, opened, or expired before the selected date. • Set both options to find any messages sent, opened, or expired between the selected dates. Use these options along with the **In** option (see the next row).
Date To	
In	Select the criteria (Sent, Opened, or Expired) for the date-related searches.

Setting Expiration Date for Encrypted Messages

You can specify how long the encrypted messages remain valid. After the specified date, the messages expire, and the recipient cannot open these messages.

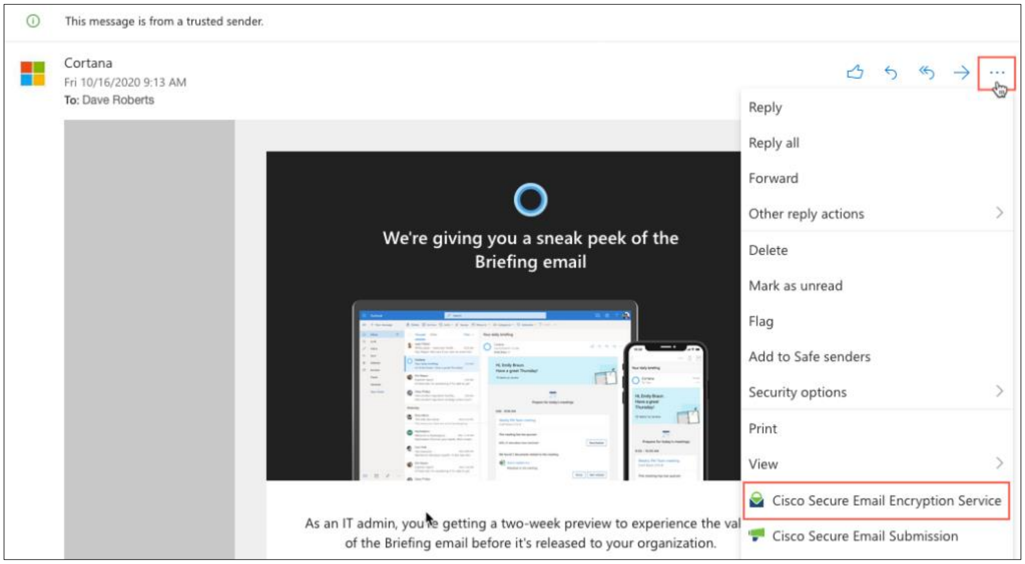
Note: You cannot select an expiry date that exceeds the key retention period set by the admin.

Procedure

Step 1. Open the Cisco Secure Email Encryption Service add-in from your Outlook for Office 365/Microsoft 365 or Outlook Web App.

Do one of the following:

- On Outlook Web App, after you select a message, click the ellipsis icon in the Reading pane, and click **Cisco Secure Email Encryption Service**.



This message is from a trusted sender.

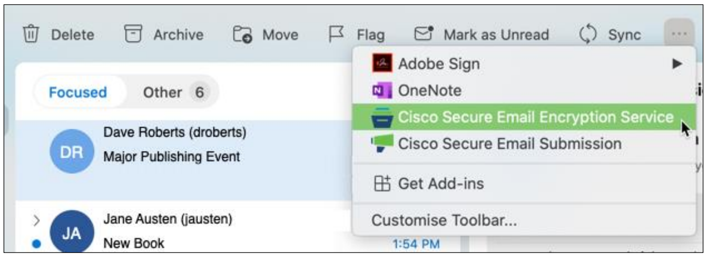
Cortana
Fri 10/16/2020 9:13 AM
To: Dave Roberts

We're giving you a sneak peek of the Briefing email

As an IT admin, you're getting a two-week preview to experience the val of the Briefing email before it's released to your organization.

- On Outlook for Windows or macOS, click **Manage Encrypted Messages** from the Ribbon or Toolbar.

Note: If you are on Outlook for macOS version 16.42 or later and using the New Outlook interface, click **Cisco Secure Email Encryption Service** from the Toolbar.



Step 2. Enter your credentials, and click **Sign in**.

Step 3. Under the **Manage Messages** (✉) tab, select the encrypted messages that you want to expire.

Note: You can perform a basic or advanced search to find specific encrypted messages.

Step 4. Click the expire (🕓) icon.

Step 5. Set an expiration date. The selected messages expire at 00:00:00 hours on the specified date.

Step 6. Click **Update**.

Locking Encrypted Messages

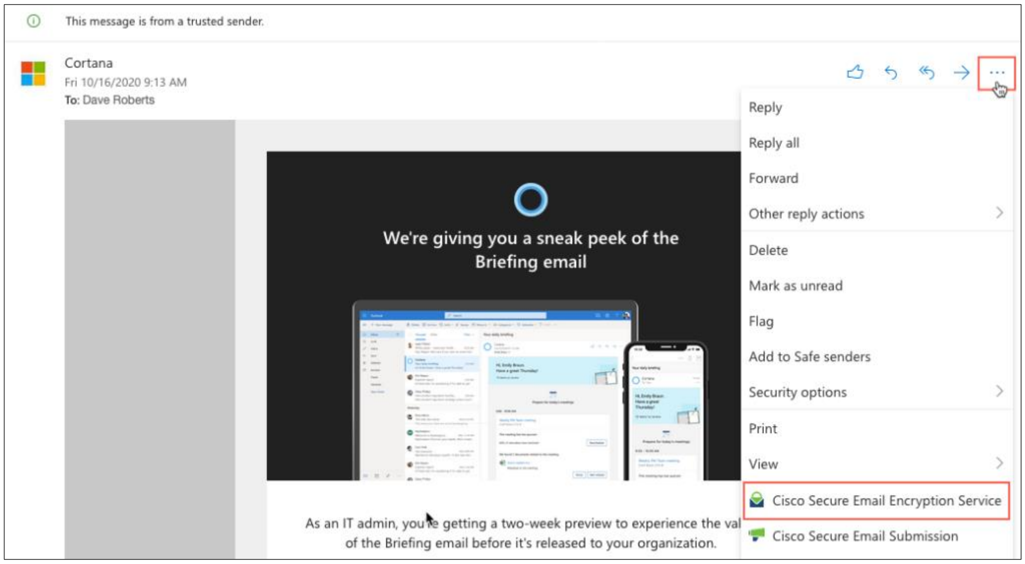
You can lock encrypted messages to prevent the recipient from opening them.

Procedure

Step 1. Open the Cisco Secure Email Encryption Service add-in from your Outlook for Office 365/Microsoft 365 or Outlook Web App.

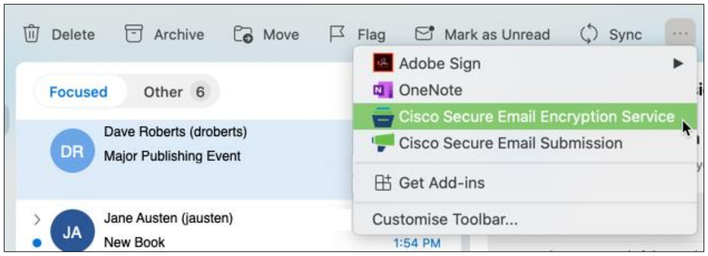
Do one of the following:

- On Outlook Web App, after you select a message, click the ellipsis icon in the Reading pane, and click **Cisco Secure Email Encryption Service**.


This message is from a trusted sender.
Cortana
Fri 10/16/2020 9:13 AM
To: Dave Roberts
We're giving you a sneak peek of the Briefing email
As an IT admin, you're getting a two-week preview to experience the val
of the Briefing email before it's released to your organization.
Reply
Reply all
Forward
Other reply actions
Delete
Mark as unread
Flag
Add to Safe senders
Security options
Print
View
Cisco Secure Email Encryption Service
Cisco Secure Email Submission

- On Outlook for Windows or macOS, click **Manage Encrypted Messages** from the Ribbon or Toolbar.

  Note: If you are on Outlook for macOS version 16.42 or later and using the New Outlook interface, click **Cisco Secure Email Encryption Service** from the Toolbar.



Step 2. Enter your credentials, and click **Sign in**.

Step 3. Under the **Manage Messages** (✉) tab, select the encrypted messages that you want to lock.

Note: You can perform a basic or advanced search to find specific encrypted messages.

Step 4. Click the lock (🔒) icon.

Step 5. To lock the messages, slide the toggle button from left to right, and enter the reason for locking the messages.

Note: To unlock a locked message, slide the toggle button from right to left.

Step 6. Click **Update**.

Chapter 4: Customizing the Secure Email Service Encryption Add-In Branding

You can customize the Add-In Name, Description, Tooltip, and icons using the Manifest XML file downloaded from the Secure Email Encryption Service Admin portal.

Note: Do not make any additional changes in the manifest XML file other than the ones mentioned in the section. Making additional changes will affect the deployment of the add-in and its functionality.

To customize the add-in properties:

1. Login to the admin portal and navigate to the **Addin Config** tab.
2. Click **Download Manifest**.
   The manifest.xml file gets downloaded to your system.
3. Open the *manifest.xml* file on your system using any text editor.
   You can customize the following items:

Item	**Parameter Name**	**Default Value**
Add-In Name	DisplayName DefaultValue	Cisco Secure Email Encryption Service
Description	Description DefaultValue	Cisco Secure Email Encryption Add-in provides you the ability to Encrypt your emails from Outlook client(s).
Encryption Add-In Icon (Image)	IconUrl DefaultValue	https://static.cres-aws.com/add-in/email-encrypt-80x80.png
Icon (Image, High-Resolution)	HighResolutionIconUrl DefaultValue	https://static.cres-aws.com/add-in/email-encrypt-80x80.png
Encryption Add-In icons in Different resolutions	bt:Image id="Icon.16x16" bt:Image id="Icon.32x32" bt:Image id="Icon.80x80"	https://static.cres-aws.com/add-in/email-encrypt-16x16.png https://static.cres-aws.com/add-in/email-encrypt-32x32.png https://static.cres-aws.com/add-in/email-encrypt-80x80.png

Manage Messages Icons in different resolutions	bt:Image id="MMIcon.16x16" bt:Image id="MMIcon.32x32" bt:Image id="MMIcon.80x80"	https://static.cres-aws.com/add-in/manage-message-16x16.png https://static.cres-aws.com/add-in/manage-message-32x32.png https://static.cres-aws.com/add-in/manage-message-80x80.png
Tooltip text for Encryption Add-In	bt:String id="ComposePaneButton.Tooltip"	Cisco Secure Encryption Service add-in provides a convenient interface that enables you to send encrypted messages by using toolbar buttons in the compose pane.
Tooltip text for Manage Messages button on Compose Mode	bt:String id="ReadpaneButton.Tooltip"	Use Manage Messages dialog to manage all messages sent from a chosen account. Use this dialog to search for a specific message.

After making the required changes, install the updated manifest file as described in Installing the Cisco Secure Email Encryption Service Add-In.

Chapter 5: Troubleshooting Cisco Secure Email Encryption Service Add-In

Sign-In Errors

Unable to Log In to the Add-In

You are unable to log in to the add-in.

Reason

You may have entered an incorrect password or are using your SSO or Google account to log in. Currently, SAML and Google-based authentication are not supported on the add-in.

Solution

Depending on the error message you are seeing, do one of the following:

- If you have forgotten your Cisco Secure Email Encryption Service account password, go back to the login screen, and use the **Forgot Password** link to reset your password.
- If you have an SSO or Google account and need to use the add-in, contact your administrator to set up a Cisco Secure Email Encryption Service account. Ensure that you activate your account before logging in to the add-in.

Encryption Errors

Unable to Encrypt Messages

When you are encrypting a message, you see a warning message.

Reason and Solution

Depending on the warning message you see, do one of the following:

Warning Message	Reason	Recommended Solution
`There are no recipients specified in the To, CC, or Bcc fields. Please add at least one recipient and try again.`	There are no recipients specified in the To, CC, or Bcc fields.	Add at least one recipient and try again.
`The size of the attachment(s) in the message is more than 10 MB.`	The size of the attachments in the message is more than 10 MB.	Consider compressing the attachment or upload the attachment in a shared location and add the link in the message instead.

`Unable to send the message. The add-in configuration is missing or incorrect on your Cisco Secure Email Encryption Service account.`	The add-in configuration is missing or incorrect on your Cisco Secure Email Encryption Service account.	Contact your administrator to validate your add-in configuration.
`Unable to connect to the Cisco Secure Email Encryption Service server. Ensure that you have network connectivity and try again.`	The add-in is unable to connect to the Cisco Secure Email Encryption Service key server.	Verify the connectivity between your host and the Cisco Secure Email Encryption Service key server (res.cisco.com). If the problem persists, contact your administrator.

Unable to Encrypt Messages – Microsoft Errors

When you are encrypting a message, you see the following warning message:

```
Unable to send your encrypted message because of a Microsoft error. Contact your
administrator and provide the following error code:<error-code>.
```

Reason and Solution

Depending on the error code displayed on the warning message, do one of the following:

Error Code	Reason	Recommended Solution
`401`	None of the required permissions for Microsoft Graph API* access are not granted for your domain.	Contact your Office 365/Microsoft 365 administrator and ensure that the following Microsoft Graph API access permissions are granted on the Azure Management Portal: • Mail.Read • Mail.ReadWrite • Mail.Send • User.Read.All
`403`	One or more of the required permissions (Mail.ReadWrite, Mail.Send) for Microsoft Graph API access are not granted for your domain.	Contact your Office 365/Microsoft 365 administrator and ensure that the following Microsoft Graph API access permissions are granted on the Azure Management Portal: • Mail.ReadWrite • Mail.Send
`404`	Cached Exchange Mode is enabled on your Outlook client.	Disable Cached Exchange Mode, and try encrypting the message again.
	The *Mail.Read* and *User.Read.All* permission for Microsoft Graph API access are not granted for your domain.	Contact your Office 365/Microsoft 365 administrator and ensure that the Microsoft Graph API access permission: *Mail.Read* and *User.Read.All* are granted on the Azure Management Portal.

*The Cisco Secure Email Encryption Service add-in uses Microsoft Graph APIs to communicate with Microsoft Azure.

Recipients Receive Plaintext Messages Instead of Encrypted Messages

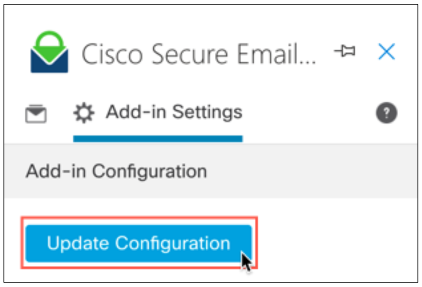
When you use the add-in to send encrypted messages, your recipients receive plaintext messages instead of encrypted messages.

Reason

Your add-in may not have the latest add-in configuration. Though your administrator pushes the updated configuration, you must manually download it.

Solution

Download the latest configuration by clicking **Update Configuration** under your add-in's **Settings** (⚙) tab.



Known Caveats

Defect ID	**Description**
CSCvw04459	Rendering of envelopes has discrepancies when the add-in encryption security level is set to Low.
CSCvw04485	

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**