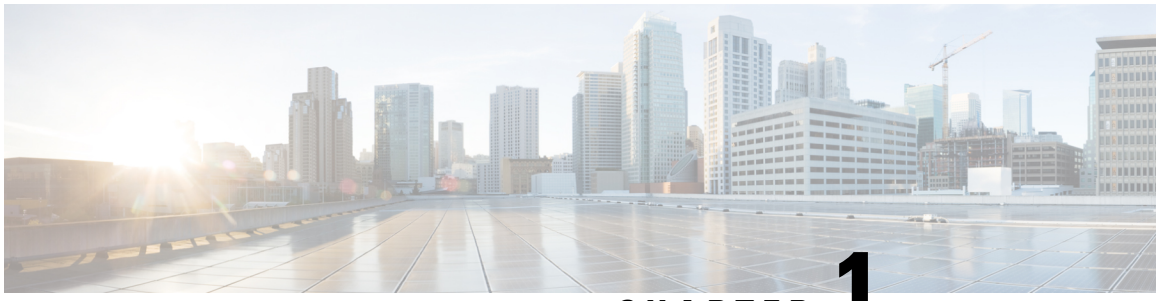
Recipient Guide for Cisco Secure Email Encryption Service 10.0

First Published: 2024-09-27

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

CONTENTS



CHAPTER 1

Opening Your First Secure Message

This chapter provides step-by-step instructions for first-time recipients of password-protected secure messages. It explains how to enroll with Cisco Secure Email Encryption Service and open secure messages.

This chapter discusses the following topics:

Note The latest version of this guide and other Secure Email Encryption Service documentation is available on this https://www.cisco.com/c/en/us/support/security/email-encryption/products-user-guide-list.html.

Important If JavaScript is disabled on your web browser, the functionality of some of the web pages will not work.

Important If you are using Internet Explorer to access the web pages, it might cause alignment issues. It is recommended to switch to any one of the following supported browsers:

- Google Chrome
- Mozilla Firefox
- Safari (for MAC operating system)

Overview of Secure Messages

A Secure Message is a type of encrypted email message. Some Secure Messages are password-protected, whereas others are encrypted but do not require a password.

If you receive a password-protected Secure Message, you need to set up a free user account with Cisco Secure Message Service to open your encrypted message.

After you enroll with the service, you can use your account password to open all Secure Messages that you receive—from any sender. You can also use the service to send and manage your own Secure Messages.

Why Use Secure Messages?

Secure Messages enable you to easily send and receive encrypted email. Typically, senders encrypt messages to prevent important or confidential information from getting into the wrong hands. Encryption protects against accidental breaches of security, as well as intentional illegal and malicious security breaches. Often, when individuals or organizations send Secure Messages, they want to protect confidential information for the benefit of the recipient. In some cases, senders are required to maintain confidentiality because of government regulations or statutes. For example, a health care provider might use a Secure Message to convey confidential information about a patient's medical history, and a financial institution might send protected information about a personal bank account.

Secure Message Notification

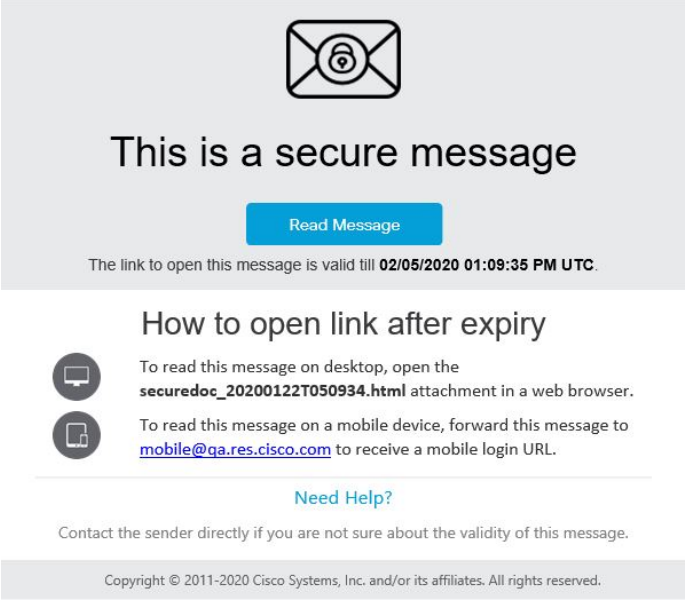
When someone sends you a Secure Message, you receive the following files:

- **Notification email message.** The notification message indicates that someone has sent you a secure, encrypted message in the form of a Secure Message. The notification also includes links to information about Secure Messages and Encryption Service.
- **Encrypted message file attachment.** The notification message includes an encrypted message file attachment. The file attachment uses the naming convention of securedoc_*date* T*time* .html where *date* and *time* are represented as a numerical date and time stamp that are added to the file. For example, you might receive a file called securedoc_20100615T193043.html, where the year, month, and day are represented as 20100615 and time is represented as 193043. This file contains both the Secure Message and the encrypted content. To view the Secure Message, save the file attachment to your hard drive. Then, double-click the file to display the Secure Message in a web browser. Typically, a computer must have an Internet connection to properly display the Secure Message and decrypt the message.

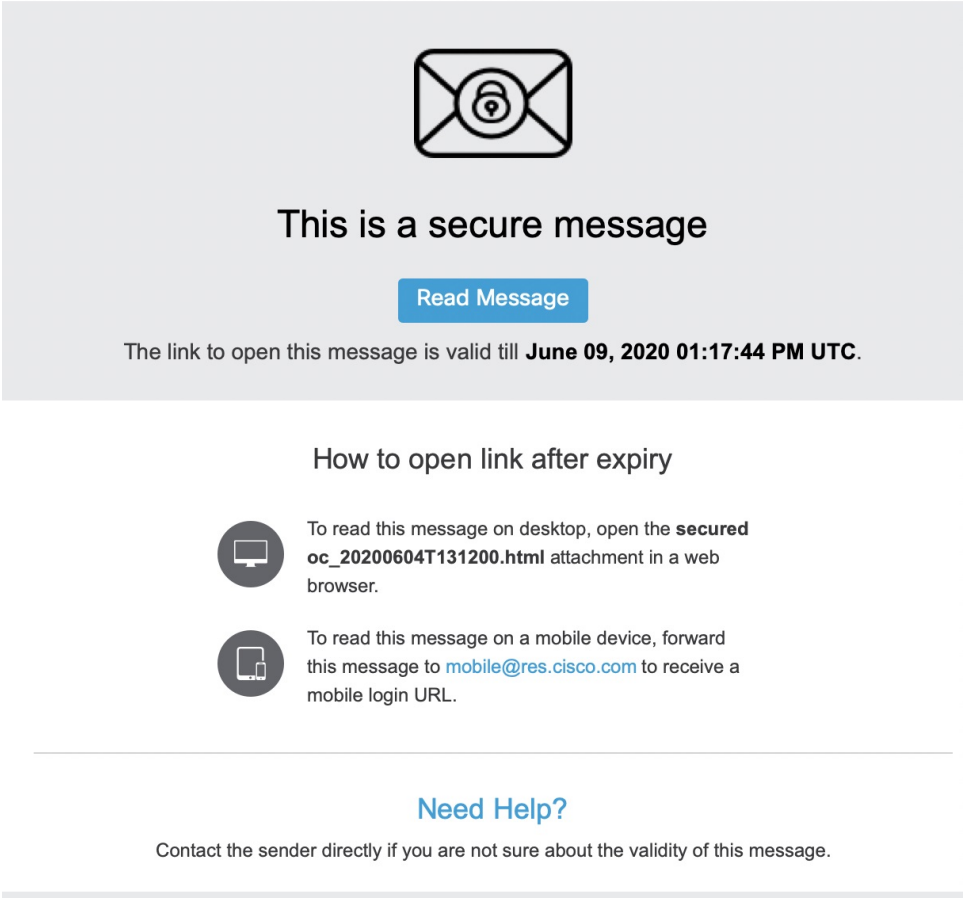
Note If the email administrator has enabled the support for large file attachments, and the secure message contains a file attachment of size greater than 25 MB, then the securedoc html attachment is not present in the secure message.

The notification message that you receive will look in one of the following ways:

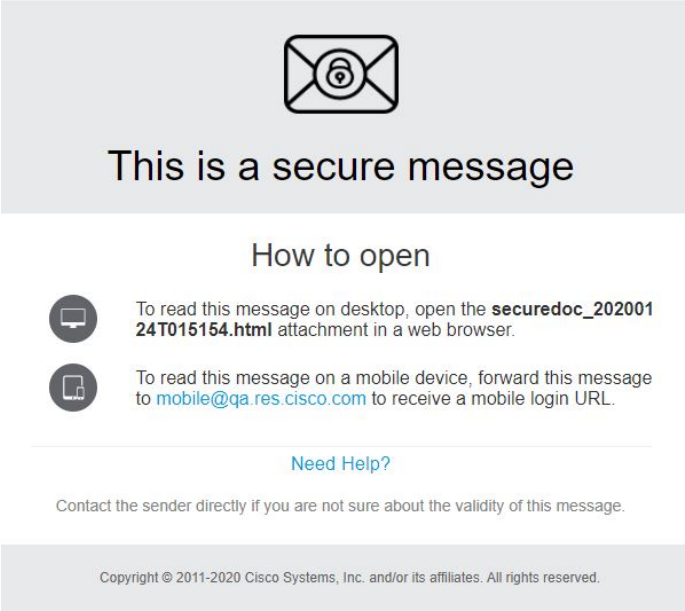
- The following figure shows a notification email message with the **Read Message** button. To read a secure message, click the **Read Message** button. By default, the **Read Message** link is valid for a maximum of 14 days. After the link expires, you can read messages by opening the attachment in a web browser or forwarding the message to mobile.res.cisco.com.



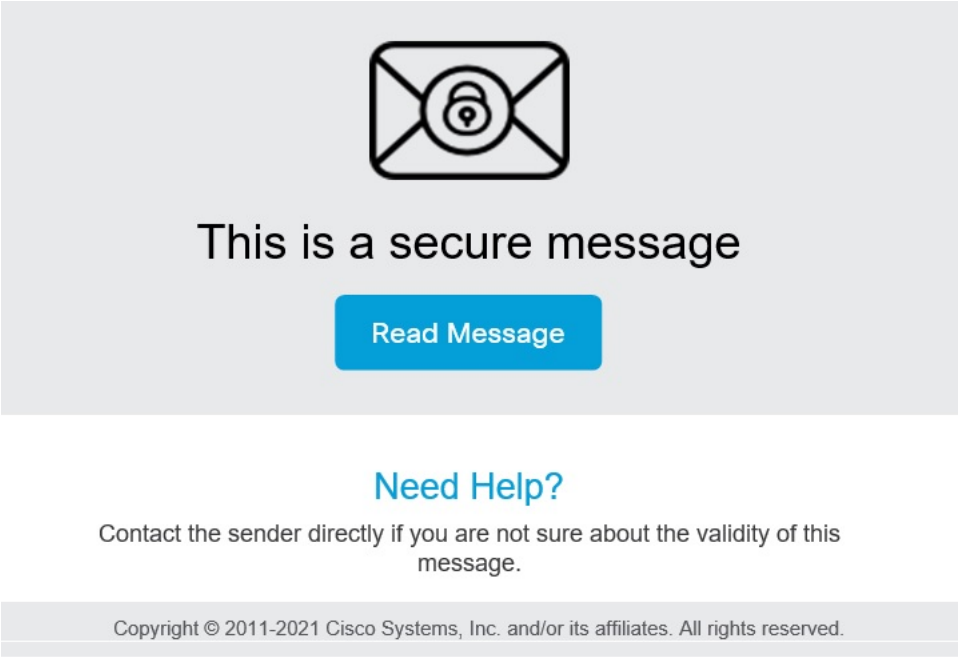
- The following figure shows a notification email message with the **Read Message** button. The email expiration month is in text format and the day of month with timestamp. This new date format is applicable for custom templates only.



- The next figure shows a notification email message without the **Read Message** button. To read a secure message, open the **securedoc_dateTtime.html** file attachment in a web browser or forward the message to mobile.res.cisco.com. For more information, see Steps to Opening Your First Secure Message, on page 8.



- The following figure shows a notification email without the securedoc html attachment and the expiry date. This notification type appears when the secure message contains a file attachment of size greater than 25 MB. Click the **Read Message** button to open the secure message.



Note The file attachment includes software to decrypt the encrypted message when you enter the password for your user account. In some cases, the included software cannot decrypt the message, and you must use one of the alternative decryption methods. For more information about alternative methods for opening secure messages, see Troubleshooting Secure Message Issues, on page 25

Note Some encrypted messages may be sent to the Spam folder. Please check your Spam folder for secure messages. Additionally, you may notice a yellow or red warning banner on secure messages. You can click the "Looks safe" button.

Note You cannot open a secure message if its encryption key has expired. Your email administrator configures the validity of the encryption key. If the encryption key has expired, you will see the error message: "Cannot open this secure message. This secure message has expired due to the security setting configured by the administrator."

Components of a Secure Message

When you click on the **Read message** button in the received secure message, it directs you to the web browser and the message is displayed.

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 the list of recipient email addresses in the searchable drop-down box.

If you send a Secure Message to a single recipient, the “Your Address” field is auto-populated with the recipient's email address. If there are multiple recipients in the 'To' and 'CC' address fields of the Secure Message, the “Your Address” field is auto-populated when you enter any character that matches the recipient email address in the searchable drop-down box.

Note If you have received 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.

If you have already enrolled with the service, the **Open** button appears. Click the **Open** button to decrypt the content and view your message.

If you have not enrolled with the service, you will be directed to enroll and create a user account before you can enter your password. If your email address is not associated with a user account, the message may display a **Register** button. In that case, click the **Register** button to enroll with the service.

When you open the securedoc attachment in the received mail, the Secure Message is displayed in a web browser.

The following table describes the important features of a Secure Message highlighted in above figure.

Feature	Description
Address fields and subject line	The address fields identify the sender in the From: field and intended recipient in the To: field.
Password field	If the secure message is password-protected, enter your Encryption Service password to open the message. If you have not enrolled with the service, you will be directed to enroll before you can enter your password.
Open button	If you receive a password-protected message and you have already enrolled with the service, the Open button appears. Click the Open button to decrypt the content and view your message. The Open button appears only after you enroll with the service and create a user account. If your email address is not associated with a user account, the message may display a Register button in place of the Open button. In that case, click the Register button to enroll with the service. If the Secure Message was sent to you with low security, you will see an Acknowledge button instead of an Open button. **Note** Your company may have configured a single-sign-on (SAML) login for you to use with the Cisco Secure Message Service. In this case, a pop-up will appear that allows you to log in using your company's credentials.
Sign in with Google button	If you have a Google account, you need to register by clicking the **Google Sig-up** button. After registering, you can **sign in with Google** and read your secure messages. In this case, you do not have to enroll with Encryption Service or enter the Encryption Service password.
Help link	Click the Help link to access the online help for Secure Messages. The online help describes the standard and alternative methods for opening Secure Messages. It also provides a link to frequently asked questions (FAQs).
Message security level	The message security level can be low, medium, or high. The default is medium. When a message is sent with low security, you do not need to enter a password to open it. Medium security enables standard password features. When a message is sent with high security, you must always enter a password to open it, even if you previously chose the "Remember me on this computer" option.
Remember Me checkbox	Select the "Remember me on this computer" check box to have your settings remembered on your computer. These settings vary depending on the encryption profile. For example, when receiving a medium security message, you may not have to enter a password to open it, but when receiving a high security message, you will always have to enter your password.

Feature	Description
Language	Select the language that will be used to translate incoming Secure Messages. This selection will override the language that is determined by the System Default Locale set in the BCE configuration file.
Logo	Displays the image that you chose as the custom logo for the envelope profile in Account Management > Branding > Images page in the Encryption Service application.

For information about other Secure Message features, see the frequently asked questions (FAQs) at:

https://res.cisco.com/websafe/help?topic=FAQ

Many Secure Message components vary from each other, depending on several factors, including:

- The sender's account configuration.
- The software available on the recipient's computer.
- Modifications that email gateways sometimes make to the encrypted message file attachment.
- The status of the recipient as either enrolled or unenrolled with the service.

Secure Messages are dynamic, and the components of a particular message can vary over time.

Steps to Opening Your First Secure Message

This section provides step-by-step instructions for opening a password-protected Secure Message for the first time. The steps demonstrate a typical scenario for a first-time recipient. Some of the steps may vary, depending on the particular circumstances. If you have a Google account, you can open the secure messages using Google authentication. For more information, see the Opening Secure Messages Through Google Sign-in, on page 12.

Note These steps apply to first-time recipients opening a password-protected message only. After you enroll with Encryption Service and activate your account, you can use your password to open secure messages from any sender. If you receive a Secure Message that is not password-protected, you do not need to register to open the message. For more information, see the Opening Secure Messages After You Activate Your Encryption Service Account, on page 11.

To open your first secure message, you must perform the following steps.

Note If the secure message contains a file attachment size of more than 25 MB, the securedoc html attachment is not present in the secure message. In such cases, click the **Read Message** button on the secure message and start from step 3 below.

Procedure

Save the Encrypted Message File Attachment to Your Hard Drive

When you receive a secure message notification, you need to download the file attachment (securedoc_*date* T*time* .html where *date* and *time* represent the time stamp appended at the time the mail is sent), and save it to your hard drive before opening it.

Note The dialog box for saving an attachment may look different, depending on your email program, and whether you use a web mail site, such as Yahoo! Mail, Gmail, or Hotmail.

For more information about the notification message, see the Secure Message Notification, on page 2.

Open the File in a Web Browser

Open the securedoc_*date* T*time* .html file (from the downloaded location on your system) in a web browser.

Note Do not open the file directly from the email attachment. You must first download the file to your system and then open the html file from the downloaded location in your system.

The Secure Message displays the registartion page.

Click the Register Button to Enroll with the Service

You need to register your account with Cisco Secure Email Encryption Service to open a Secure Message.

Note Your company may have configured single-sign-on (SAML) authentication for you to use with Encryption Service. In this case, the new user registration is a shortened registration and only requests that you enter the portal language and the name for the Encryption Service user account. The below figure shows the new user registration with SAML authentication.

The **New User Registration** page is displayed.

Note You will not be able to view the customized logo and footer links in the New User Registration page until you register your account with Cisco Secure Message Service.

Note Security questions and personal security phrases are no longer required during new account registration.

Enter the information in the following fields:

Table 1: Fields on the Encryption Service Registration Page

Field	Value
First Name	Required. Enter the first name of the Encryption Service user account.
Last Name	Required. Enter the last name of the Encryption Service user account.
Password and Confirm Password	Required. Enter and confirm a password for the account. Password must be alphanumeric and case-sensitive. The following password requirements can be additionally set by your Account Administrator: • Password must contain characters from at least three of the available character types: lowercase letters, uppercase letters, digits, and special characters. • Password must not contain a character repeated more than three times consecutively. • Password must not contain the username or the reversed username. • Password must not be “Cisco”, “ocsic” or any similar words by changing the capitalization of letters, or replacing “i” with “1”, “|”, “!”, “o” with “0”, or “s” with “$”. **Note** If you forget your password, click the **Forgot password?** button on a Secure Message to reset your password. If your company has configured a single-sign-on (SAML) login for you to use with the Cisco Secure Message Service, you will need to contact your company’s support group to obtain or reset your password.
I agree to Encryption Service's Terms of Service	You must click this checkbox to register your account on Encryption Service.

Note Dynamic password validation does not perform a check on any additional password rules configured for your Encryption Service account by your account administrator.

Upon registering, the following account activation page is displayed. You need to follow the instructions in the account activation mail to activate your Encryption Service account.

Note You may need to set up more than one user account, if you receive Secure Messages at multiple email addresses. You need a separate user account for each email address.

Activate Your Encryption Service Account

Check your email inbox for an activation message from the service. If the email is not in your inbox, check the spam or junk email folder in case the activation message was filtered.

In the activation email message, click the link to activate your user account.

View the Secure Message Again and Enter Your Password

Procedure

Step 1 Return to the Secure Message. The **Register** button is no longer displayed on the message. The **Open** button appears in its place.

Step 2 Enter the password for your Cisco Secure Message Service user account, and click **Open**.

Note Your company might have configured a single-sign-on (SAML) login for you to use with the Cisco Secure Message Service. In this case, a pop-up will appear that allows you to log in using your company's credentials (username and password) to authenticate and open the encrypted email. If you sign in through your Google account, then you do not need to enter your Encryption Service username and password to read the secure message.

The decrypted message is displayed in the browser window.

Step 3 Click **Reply** to send a Secure Reply message or click **Forward** to send a Secure Forward message, after you open a Secure Message. When you send a Secure Reply or Secure Forward message, the recipient receives a Secure Message containing the encrypted message.

Note Depending on the original sender's preferences, some features may not be available. For example, it might not be possible to send a Secure Reply or Secure Forward message.

Opening Secure Messages After You Activate Your Encryption Service Account

After you enroll with the Cisco Secure Message Service and activate your account, you can use your Encryption Service password to open secure messages from any sender.

While opening the secure message, if you forget your Encryption Service password, click the **Forgot password?** button on a Secure Message to reset your password. You will receive a *New Password* message to the email address associated with your account.

The *New Password* message contains a link to the *Create New Password* page. When you click on this link, you will be re-directed to a browser, where you can create a new password and use that password to log in to your account and open the secure message. Whenever you reset your password, a notification mail is sent to the e-mail address that is associated with your Encryption Service account. Security questions are no longer required to reset your password.

Note If your company has configured a single-sign-on (SAML) login for you to use with the Cisco Secure Message Service, you will need to contact your company's support group to obtain or reset your password.

Note The password reset link is valid for 60 minutes only. You must change your password before the link expires.

Opening Secure Messages Through Google Sign-in

If you have a Google account, you can open the secure messages using Google authentication. In this case, you do not need enroll with Encryption Service or enter Encryption Service password to open secure messages.

To open your first secure message through Google authentication:

Procedure

Step 1 Download the attached **securedoc.html** file to your system.

Step 2 Navigate to the location where the file is saved, and open the file in a web browser.

Note If the secure message contains a file attachment size of more than 25 MB, the securedoc html attachment is not present in the secure message. In such cases, click the **Read Message** button on the secure message.

Step 3 Click the **Google Sign-up** button to register.

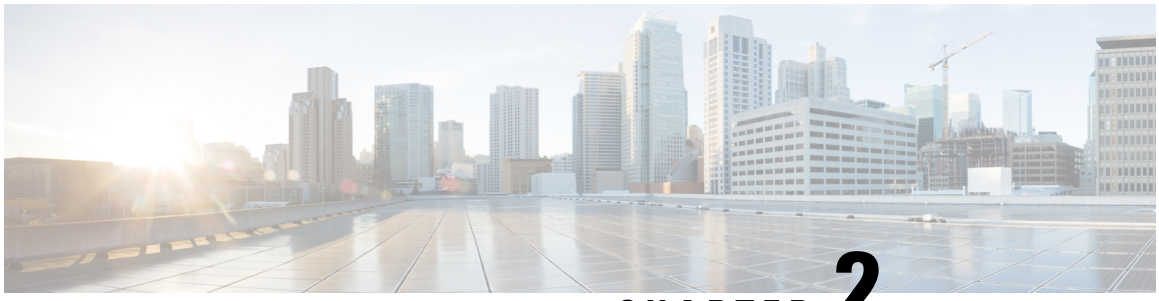
Step 4 Choose your Google account.

Step 5 In the **New Google User Registration** page, enter your first name and last name, and then click **Register**.

The confirmation message appears. You will receive the confirmation letter on your email.

Step 6 Return to the Secure Messages and click the **Sign in with Google** button and read your secure message.

Note The **Password** field is required only with Encryption Service authentication. If you open the secure message through Google Sign-in, the **Password** field is not applicable. Skip this field and click **Sign in with Google**.



CHAPTER 2

Overview of Sending Email

You can send encrypted messages from your Cisco Secure Email Encryption Service account. When you sign up for an Encryption Service account, you can receive as well as send encrypted messages. When you send encrypted messages using Secure Email Encryption Service, the encryption server encrypts the outbound email and routes it to its intended destination. You can also save the frequently contacted email addresses in the Encryption Service address book, and choose from those addresses when you compose emails.

Note Account administrators can disable access to Secure Compose. If your account administrator has disabled this functionality, you will not see the Compose Message link in the left-hand navigation menu and will not be able to send a secure message from the Encryption Service website.

Important If JavaScript is disabled on your web browser, the functionality of some of the web pages will not work.

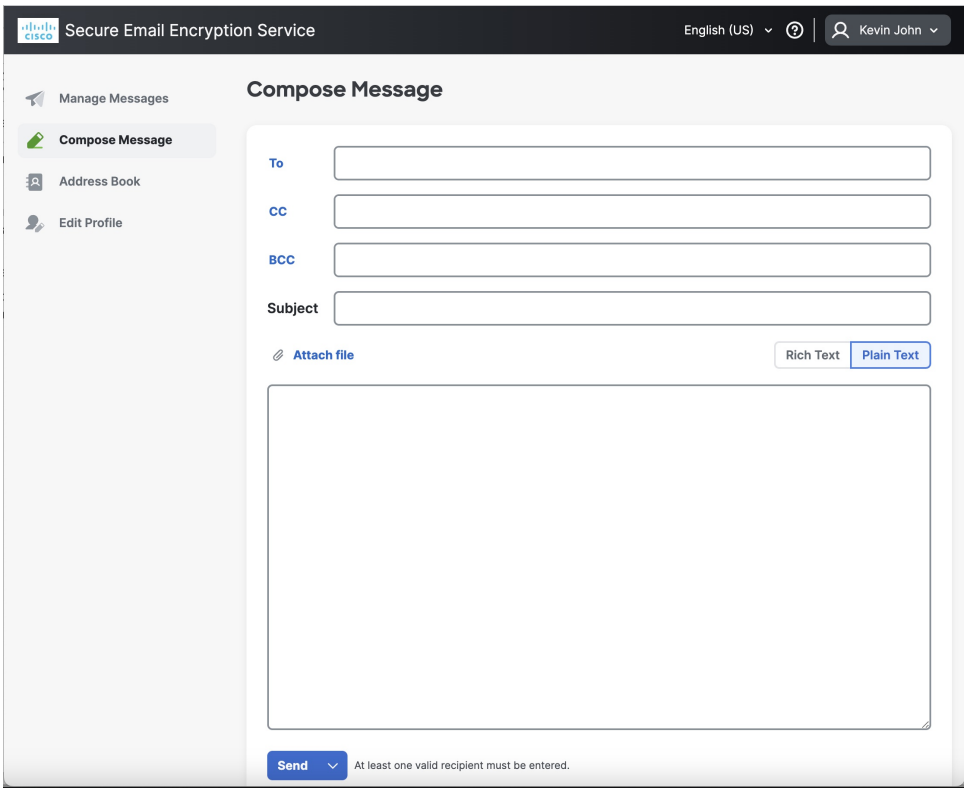
Important If you are using Internet Explorer to access the web pages, it might cause alignment issues. It is recommended to switch to any one of the following supported browsers:

- Google Chrome
- Mozilla Firefox
- Safari (for MAC operating system)

- Composing and Sending an Email, on page 13
- Using the Address Book, on page 15
- Managing Messages, on page 17
- Editing Your Profile, on page 22

Composing and Sending an Email

To compose and send a secure message from the Encryption Service website, click **Compose Message** in the left-hand navigation menu.



When you send a secure message through the Encryption Service, the recipient receives a Secure Message containing the encrypted content. If the recipient does not already have an Encryption Service user account, they will need to enroll and set up a free account to open the message.

Note If you have logged in using a non-corporate email address:

- You cannot send new secure messages to other non-corporate accounts.
- You cannot forward a secure message to other non-corporate accounts if the Forward functionality is enabled in the secure email gateway or Secure Email Encryption Add-In.

Procedure

Step 1 Begin creating a message from the Compose Message page. Enter an email address, click the To: field, or click the Address Book icon in the left pane to open the Address Book.

For more information about using the Address Book, see the Using the Address Book, on page 15

Step 2 Complete the appropriate address fields (To, CC, and BCC) on the Compose Message page.

For more information about the BCC option, see the Using the Automatically BCC me on this Email Option, on page 15

Step 3 Optionally, complete the **Subject** field.

Step 4 Optionally, click the **Attachments** button to include file attachments.

The maximum file size of all attachments is 25 MB. If your email administrator has enabled the support for large file attachments, you can attach up to 100 MB.

Step 5 Enter the body of your encrypted message in the **Message** field. To format your message, click the **Rich Text** link. Use the formatting options to format your text as needed.

Step 6 Optionally, select the check box to send yourself a copy of the message as a BCC recipient.

Step 7 Optionally, select the check box to receive a read receipt the first time each recipient opens the message.

For more information about read receipts, see the Requesting Read Receipts, on page 15

Step 8 Click **Send**

A notice appears at the top of the Compose Message page indicating that the message has been sent.

Note While you are composing a secure message, your web browser session might expire if you stop typing for a period of 20 minutes or longer. If the browser session times out, an error is displayed when you click Send. To send your message, you must log in to the Encryption Service website again.

Using the Automatically BCC me on this Email Option

When you send a secure message, you can select the **Automatically BCC me on this email** check box to receive a copy of this message on your email account.

Note You can set the default value for this option by selecting the **Bcc me on messages that I send** check box on the **Edit Profile** page in the **Preferences** section.

Requesting Read Receipts

When you send a secure message, you can select a check box to request a read receipt. A read receipt is a notification email message that alerts you when a recipient first opens a secure message that you have sent.

Note Because the configuration of some recipients' email systems can prevent read receipts from reaching you, read receipts are not guaranteed. To verify the date and time when a recipient first opened your message, use the Manage Messages feature of the Encryption Service website to view the message details.

Using the Address Book

When you send a secure message, you may want to store frequently used email addresses in your address book so that you can access them easily. You can perform the following using the address book:

- Adding an Address to the Address Book, on page 16

Adding an Address to the Address Book

Procedure

Step 1 Click the Address Book icon in the left pane to open the address book.
Step 2 Enter a first name, last name, and email address for the contact.
Step 3 Click **Save**.
Step 4 The new address is added to your address book.

Deleting an Address from the Address Book

Procedure

Step 1 Click the **Address Book** icon in the left pane to open the address book.
Step 2 Click the trash icon next to the address that you want to remove.
Step 3 Or, select the check box next to the address that you want to remove and click **Delete Contact**.

Editing an Address

Procedure

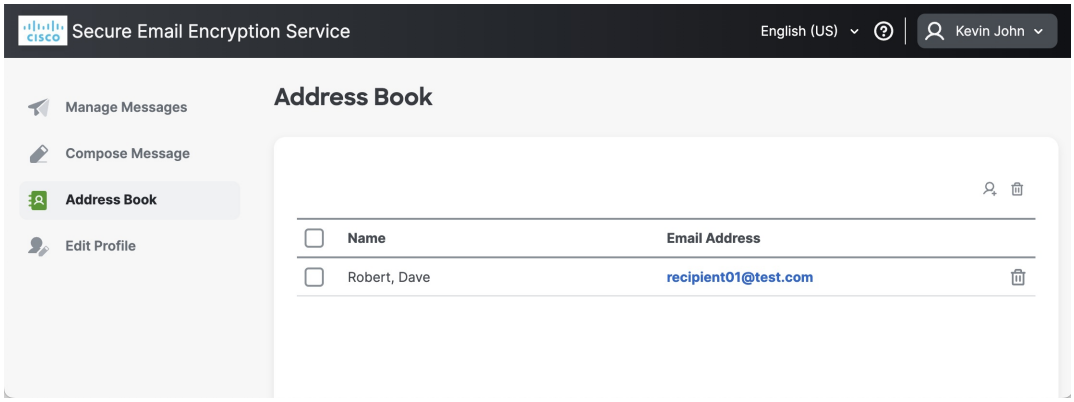
Step 1 Click the **Address Book** icon in the left pane to open the address book.
Step 2 Click the **Edit** icon next to the address you want to edit.
Step 3 Modify the first name, last name, or email address of the contact, and click **Save**.

Adding an Email Address to a Message from the Address Book

Procedure

Step 1 Click the To: field or click the **Address Book** icon in the left pane to open the address book.

When you click the To field, the Address Book opens, where you can add an email address to a message.



Note You can also click the CC and BCC fields to display the Address book and add an email address to a message.

Step 2 Click the email address for the contact you want to send an email. The **Compose Message** page opens and populates the To: field with your selected address.

Step 3 Enter your message (and complete any other desired fields), and click **Send**.

Managing Messages

You can select Manage Messages in the left-hand navigation menu to manage the encrypted messages that you have sent. When you manage messages, you first run a search to retrieve your sent messages.Then, you use the search results to view message details, lock and unlock messages, or specify message expiration dates. You can:

- Retrieve All Sent Messages, on page 17
- Retrieve Specific Messages, on page 18

Note When you manage messages, you can view message details and control access to sent messages. You cannot view the content of sent messages.

Retrieve All Sent Messages

To retrieve a list of all the secure messages that you have sent:

Procedure

Step 1 Select **Manage Messages** in the left-hand navigation menu. The **Search Sent Messages** page opens.

Step 2 Leave the **Keyword** field blank.

Step 3 Click the **Search** button.

The results list at the bottom of the page displays the sent messages. Click the column headings to change the sort order. The results list displays up to 25 sent messages on a page. To view more messages, click the link for additional messages.

Retrieve Specific Messages

You can run a basic or advanced search to retrieve a subset of secure messages that you have sent.

Basic Search

When you run a basic search, you enter a keyword text string to find messages with that text string in the **To** or **Subject** fields. The keyword text string is not case-sensitive, and it can be any combination of characters, such as a partial word, a word, or a phrase.

To run a basic search:

Procedure

Step 1 Select **Manage Messages** in the left-hand navigation menu.

Step 2 Enter a text string in the **Keyword** field.

Step 3 Click the **Search** button.

The results list displays the messages that match the search criteria. A message matches the search

criteria if the keyword text string appears anywhere in the **To** or **Subject** field. For example, if you search for the keyword test, the results list could include messages with the following text strings in the **To** or **Subject** field:

- test
- TESTS
- testing
- smartest

Advanced Search

When you run an advanced search, you can narrow the search results in several ways using keywords, date ranges, and message status.

To run an advanced search:

Procedure

Step 1 Select **Manage Messages** in the left-hand navigation menu.

Step 2 Click the **Advanced Search** link.

Step 3 Complete the fields for the search criteria you want to specify.

Step 4 Click the **Search** button.

The following table describes the criteria that you can use in an advanced search.

Table 2:

Field	Description
Keyword 1	Enter a keyword text string, similar to the text string for a basic search. Use the corresponding drop-down list to specify theMessage data to search. You can search the To field, the Subject field, the Locked Reason text, or the Failed Attempts data forMessages. For example, enter Confidential and select Subject to search for sentMessages with the word "Confidential" in the Subject field.
Keyword 2	Enter a keyword text string and use the corresponding drop-down list to specify theMessage data to search. You can search the To field, the Subject field, the Locked Reason text, or the Failed Attempts data. For example, enter 3 and select Failed Attempts to search for lockedMessages with recipients who made three unsuccessful attempts to open them.
Date From *and* Date To	To specify a date range for the search criteria, enter dates in the Date From and Date To fields, and then select the message status in the corresponding drop-down list. You can search for messages that were sent, opened, or expired in the specified date range. By default, an advanced search returns messages that were sent during the preceding month.
Status	Select a message status to limit the search results based on status. Options are All, Opened, Unopened, Locked, and Expired. The default is All.

You can use a combination of advanced search criteria to narrow your search results. Leave fields blank to exclude them from the search criteria. Only the Status field is required.

An advanced search uses an AND operator rather than an OR operator to join search criteria. For example, if you use the Keyword 1 and the Keyword 2 fields together, the search returns Messages that meet both criteria, not one or the other.

Viewing Message Details

After you run a search, the results list displays details about the messages that match the search criteria.The details include recipient email addresses, subject lines, and the dates and times when messages weresent and first opened. The details also indicate message locking status and expiration dates. All times are displayed in Greenwich Mean Time (GMT).

The results list contains a separate row for each recipient of a secure message. For example, if you sent an encrypted message to three recipients, the results list contains three rows for the message.

You can use the results list to control message locking and expiration. For more information about locking, see Locking Messages, on page 20 and Unlocking Messages, on page 21. For more information about expiration, see Setting Message Expiration Dates, on page 21

Viewing Message Details in Single-Message View

To view details for an individual message, click the subject line in the results list. The Update Sent Message page is displayed. It includes much of the same information about the message as the results list, plus additional information about message locking.

The Update Sent Message page displays the first-opened time for the particular recipient listed in the To field. If the recipient has not opened the message, the Opened Date field is blank.

In single-message view, you can click the padlock icon to change the lock status for the recipient in the To field. You can also click the calendar icon to set an expiration date for that recipient. After you update the lock status or expiration date, click Save to save your changes.

Locking and Unlocking Messages

This topic provides information on the following:

Locking Messages

You can lock sent messages to prevent recipients from opening them. After you lock a message, the recipient cannot open the message to access the encrypted content. When you lock messages, you lock them for individual message recipients. You can lock a message for some recipients and leave it unlocked for others.

To lock one or more messages:

Procedure

Step 1 Select **Manage Messages** in the left-hand navigation menu.

Step 2 Click **Search** to retrieve all sent Message, or else run a basic or advanced search to retrieve specific messages.

Step 3 In the results list, select the check boxes for the messages you want to lock.

Note If you sent a message to multiple recipients, the same message might appear in several rows. Select the check box for each recipient you want to prevent from opening the message.

Step 4 Click the **Lock/Unlock Message** icon above the results list. The Update Sent Messages page opens.

Step 5 Verify that the **Lock all selected messages** option is selected.

Step 6 Optionally, enter your reason for locking the messages.

The lock reason is displayed to recipients when they view the secure message.

Step 7 Click **Update**.

Note If you specify a reason for the lock, the reason is displayed to recipients when they view the Secure Message. To change the lock reason notification, follow the steps to lock the message, and enter a new reason before you click **Update**.

When a secure message is locked, a padlock icon appears in the **Locked** column of the results list.

Unlocking Messages

To unlock messages:

Procedure

Step 1 Select **Manage Messages** in the left-hand navigation menu.

Step 2 Click **Search** to retrieve all sent Messages, or else run a basic or advanced search to retrieve specific messages.

Step 3 In the results list, select the check boxes for the messages you want to unlock.

Step 4 If you sent a message to multiple recipients, select the check box for each recipient's row, as appropriate.

Step 5 Click the **Lock/Unlock Message** icon above the results list. The **Update Sent Messages** page opens.

Step 6 Select the **Unlock selected messages** option.

Step 7 Click **Update**.

Note You can also change the lock status of a message when you view details in the single-message view. After you update the lock status, click Save to save your changes. For more information about using the single-message view, see Viewing Message Details in Single-Message View, on page 20.

Setting Message Expiration Dates

You can set a message expiration date to prevent recipients from opening a message after the specified date. You typically set expiration dates for a future time. After a message expires, the recipient cannot open the message to access the encrypted content. When the recipient views the message, a notification displays indicating that the message has expired.

When you manage messages, you can set, modify, and remove message expiration dates. When you view message information in the results list, expiration dates for expired messages appear in red text. All times are displayed in Greenwich Mean Time (GMT).

To set or modify a message expiration date:

Procedure

Step 1 Select **Manage Messages** in the left-hand navigation menu.

Step 2 Click **Search** to retrieve all sent Messages, or else run a basic or advanced search to retrieve specific messages.

Step 3 In the results list, select the check boxes for the messages you want to update. If you sent a message to multiple recipients, select the check box for each recipient's row, as appropriate.

Step 4 Click the **Update Expiration For Messages** icon above the results list. The **Update Sent Messages** page opens.

Step 5 Enter an expiration date and time for the messages, or click the calendar icon and select the expiration date.

Step 6 Remember, the time you enter is GMT, not local time.

Step 7 Click **Update**. The message expiration date appears in the **Expires** column of the results list.

Removing a message expiration date:

To remove a message expiration date:

Procedure

Step 1 Select **Manage Messages** in the left-hand navigation menu.

Step 2 Click **Search** to retrieve all sent Messages, or else run a basic or advanced search to retrieve specific messages.

Step 3 In the results list, select the check boxes for the messages you want to update.

Step 4 If you sent a message to multiple recipients, select the check box for each recipient's row, as appropriate.

Step 5 Click the **Update Expiration For Messages** icon above the results list. The **Update Sent Messages** page opens.

Step 6 Delete the text in the **New expiration date** field.

Step 7 Click **Update**.

Note NoteYou can also set or remove the expiration date of a message when you view details in the single-message view. After you enter or delete the expiration date, click Save to save your changes. For more information about using the single-message view, see Viewing Message Details in Single-Message View, on page 20.

Editing Your Profile

You can select Edit Profile in the left-hand navigation menu to update your user account information with Cisco Secure Email Encryption Service (Encryption Service). After you update the Edit Profile page, enter the password for your user account and click **Save Profile** to save your changes.

Task you can perform include:

- Setting Your Local Time Zone, on page 23
- Editing Personal Details and Preferences, on page 23

Setting Your Local Time Zone

The time zone is set automatically based on your current location. If you set the time zone previously, the autodetection is not enabled. You can also change it by choosing the preferred time zone from the **Time Zone** drop-down menu.

You can set the time stamp to your local time zone and to your desired format (12 hours or 24 hours) for all messages that you send.

To set your local time zone:

Procedure

Step 1 Click the **Edit Profile** icon in the left pane. The **Edit Profile** page opens.

Step 2 Choose the appropriate value from the **Time Zone** drop-down menu.

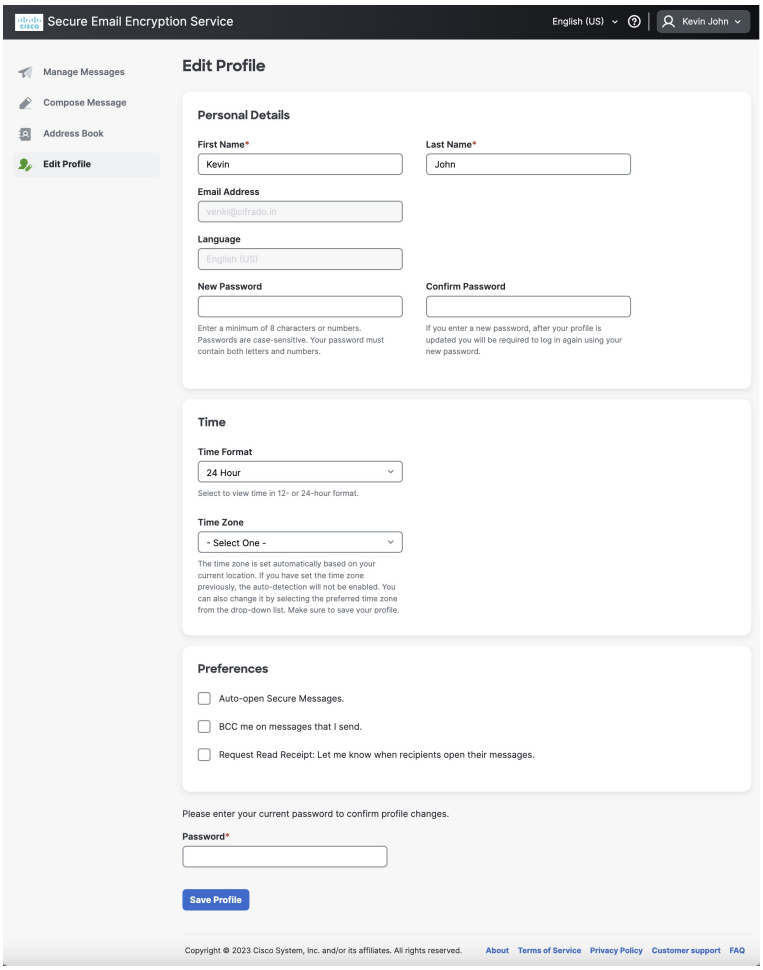
Step 3 Choose 12 hours or 24 hours from the **Time Format** drop-down menu.

Step 4 Enter your password to confirm changes.

Step 5 Click **Save Profile** .

Editing Personal Details and Preferences

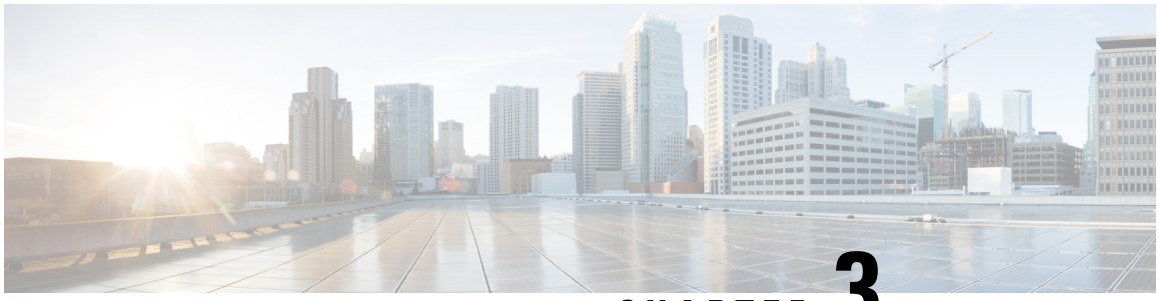
You can edit your personal details in the following fields, as shown in the below figure.



Note By default, your first name and last name is taken from your Encryption Service account.

In case, you reset your Encryption Service password and click **Save Profile**, your Encryption Service account will be logged out. In that case, you need to re-login to your Encryption Service account using your new password.

You can also set the below preferences, enter your Encryption Service **Password** and click **Save Profile**.



CHAPTER 3

Troubleshooting Secure Message Issues

This chapter provides information on the following topics:

Troubleshooting Tips

This section provides troubleshooting tips for issues that you might encounter when opening Secure Messages.

Issue: Open Button Is Missing from the Message or Does Not Work

The Open button might be missing or inoperable for several reasons. For example, if your email address is not associated with a Cisco Secure Email Encryption Service user account, the Message might display a Register button instead of an Open button. Also, the Open button might not function properly if your computer is not configured to run Java or JavaScript or if the Message was modified during transmission.

Tip If a Register button is displayed on the Message, click **Register** and create a new user account for the email address where you received the Message.

Tip If you have already created a user account for the email address, enter your password and click the **Open Online** link to use an alternative method to open the Message.

Tip If the Open Online method does not work, forward the Message to mobile@res.cisco.com. The service will send you an email message with a temporary link that you can click to securely retrieve the message by using a web browser on your computer or personal digital assistant (PDA). For more information about using the Open Online method and the Open by Forwarding method, see the Secure Message online help at the following URL: https://res.cisco.com/websafe/help?topic=RegEnvelope

Issue: Email Address Does Not Appear in the To: Field

If the Secure Message was sent to multiple recipients, your email address might not immediately appear in the To: field.

Tip Click the arrow in the To: field, and choose your email address in the drop-down menu.

Tip If you received the secure message as a BCC recipient, your email address does not appear in the drop-down menu for the To: field. In that case, choose the "Address not listed" option. Then, enter your email address and click **Submit** to include your email address in the To: field.

Issue: Secure Message Is Not Displayed Properly

Occasionally, the Secure Message may not be displayed properly when you open the attached encrypted file. For example, the file might contain garbage text or HTML markup (such as <!-- or -->).

Tip If you have a problem viewing the Secure Message, forward it to mobile@res.cisco.com. Cisco Secure Email Encryption Service will send you a message with a link that you can click to view the encrypted message.

Issue: Message Processing Slows Down or Stops

When you view or open a Secure Message, the message processing might be interrupted because of connection problems or other issues. In that case, a notification below the secure message might indicate that the tools are loading or that the message decryption in progress. If a message does not open within several minutes, it is possible that the processing has slowed down or stopped, or that the message contains an unusually large attachment.

Tip If the secure message processing slows down or stops, re-enter your password and click **Open** again.

Tip If clicking **Open** again does not work, forward the secure message to mobile@res.cisco.com. Cisco Secure Email Encryption Service will send you a message with a link that you can click to view the encrypted message.

Issue: Password Is Forgotten or Does Not Work

If you cannot remember your password, or if your password does not seem to work, you might need to reset your password.

Tip If you forget your password, click the **Forgot Password?** button on a Secure Message to reset your password. Cisco Secure Message Service will send a *New Password* message to the email address associated with your account. The *New Password* message contains a link to the *Create New Password* page. When you click on this link, you will be re-directed to a browser, where you can create a new password and use that password to log in to your account or open the Secure Message. Whenever you reset your password, a notification mail is sent to the e-mail address that is associated with your Encryption Service account. Security questions will no longer required during password reset.

If your company has configured a single-sign-on (SAML) login, and you forget or lose your password, you will need to contact your company's support group to obtain or reset your password.

Note The password reset link is valid for 60 minutes only. You must change your password before the link expires.

Tip Cisco Secure Email Encryption Service passwords are case-sensitive. If your password does not work, verify that you did not accidentally press the Caps Lock key on your keyboard. If the password still does not work, click the **Forgot Password?** button on a Secure Message to reset your password. Cisco Secure Email Encryption Service will send a *New Password* message to the email address associated with your account.

Issue: Microsoft OWA 2007 Compatibility

To ensure compatibility, install the Microsoft Patch for OWA 2007 Encryption Service Secure Mail Recipients.

Secure Email Encryption Service Secure Message recipients attempting to open the Encryption Service Secure Message through Microsoft OWA 2007 will need to enable the server side administrative option to disable the HTML/XML filter. Though this HTML filter option will be officially released in the yet-to-be-released Microsoft Exchange 2007 SP1 Rollup 8, Microsoft customers can request an interim patch from Microsoft. How and when to contact Microsoft Customer Service and Support:

https://support.microsoft.com/en-us/help/295539

Issue: Compose Message Link is Not Visible in the Left-Hand Navigation Menu

Account administrators can disable access to Secure Compose. If your account administrator has disabled this functionality, you will not see the Compose Message link in the left-hand navigation menu and will not be able to send a secure message from the Encryption Service website.

Issue: Accented Characters Not Rendering Correctly for Secure Emails (Plain Text or HTML)

Problem: The secure emails in plain text or HTML format are not rendering correctly if accented characters of certain foreign languages are used in the message content. Currently, the accented characters are displayed as black diamonds or question marks (?) in the message content.

Solution: You need to switch the encoding option for outgoing messages from 'Western European (Windows)' to 'Unicode (UTF-8)' on Microsoft Outlook.

Steps:

1. Go to **File** > **Outlook Options** > **Advanced** > **International Options** section on Microsoft Outlook.
2. Choose **Unicode (UTF-8)** as the preferred encoding option for outgoing messages.
3. Uncheck the **Automatically select encoding for outgoing messages** check box.

Issue: Secure Message Not Opening Properly on Firefox

Problem: Occasionally, the Secure Message may not open properly when you open the attached encrypted file using the Firefox browser. After you enter the password to open the message, it stays on the same page and doesn't proceed further.

Solution: Perform the following steps on your Firefox browser.

1. Click the hamburger icon (3 lines) on the top right of the Firefox browser and click **Settings**.
2. Select the **Privacy & Security** tab from the left pane.
3. Under **Enhanced Tracking Protection**, select **Custom**.
4. Select the **Cross-site tracking cookies** option from the **Cookies** dropdown.

Note The changes are auto-saved.

5. Reload all tabs.

Additional Resources

For more information about Cisco Secure Email Encryption Service and Secure Messages, you can refer to the following additional resources.

Cookies Used in Secure Email Encryption Service

The following cookies are used while accessing the secure message and the websafe portal.

- **Password Reset Cookie**: Cookie name: *cabstsrpr*. This is used for the password reset functionality. The cookie-related data are: cookie validity, cookie token alias, cookie key, cookie encryption algorithm, cookie status, and cookie secure status.
- **Session ID Cookie**: Cookie name: *JSESSIONID*. This is used as an anti-CSRF token to prevent possible CSRF attacks.
- **Remember Me Cookie**: Cookie name: *PostXAuth*. This is used for the 'Remember Me' functionality.
- **Secure Cookies**: Separate secure cookies for admin and websafe - *secureCookieWebsafe* and *secureCookieAdmin* respectively.

- Locale set in the websafe portal - *WebSafe.current-locale*. This is used for deciding the application display language.
- PostX userAlert - *Name*. This is used for remembering the **Do not show this message again** checkbox on the 'Cisco Secure Email Encryption Service: Important Update!' pop-up.
- On the admin portal - *PostXConfig.CurrentView*. This cookie is used to decide whether to display the Configuration tab in Standard mode or Expert mode.

Note You must allow cookies on your browser settings and your email administrator must not block cookies for the secure message to work as expected.

Secure Message Help

For an overview of the service and the various methods of opening Secure Messages, access the Secure Message help page at the following URL:

https://res.cisco.com/websafe/help?topic=RegEnvelope

Frequently Asked Questions

For answers to common questions about opening encrypted email, enrolling with Cisco Secure Email Encryption Service, and configuring optimal browser settings, view the frequently asked questions (FAQs) at the following URL:

https://res.cisco.com/websafe/help?topic=FAQ

Customer Support

To contact Customer Support for Secure Email Encryption Service, you can send an email message to the following address:

support@res.cisco.com

See the following URL for complete Customer Support information:

https://res.cisco.com/websafe/help?topic=ContactSupport

Note You can also access Instant Message Chat Support from this URL.

Note The Email and Web Chat Support is now available in English and French. The French Support will be available between the hours of 8:00 AM to 5:00 PM, Eastern Time, on weekdays.

Using the Web Chat

You can use the instant messaging web chat to raise a support ticket or contact the customer support.

1. Click the chat icon on the **Contacting Customer Support** page.
2. Enter your first name, last name and email address in the chat window that pops up.
3. If you are facing any issues in opening a secure message, click **Unable to Open the Secure Message** button.

Note You can use this option if you are facing any issues related to opening a secure message. Click the **More Information** button to see the different types of issues for which you can use this option and raise a support ticket. A new tab opens in your web browser displaying the different types of issues.

4. For any other issues, click the **I have Other Issues** button.

INDEX