CHAPTER 1

Configuring and Using Cisco Business Class Email for iOS

- Overview, page 1-2
- What’s New, page 1-2
- Licensing Versions and Configuration Modes, page 1-2
- Supported Operating Systems, page 1-2
- Downloading and Installing the Cisco BCE Application, page 1-3
- Opening Cisco BCE Application for iOS, page 1-3
- Opening a Secure Message in the Cisco BCE Application, page 1-11
- Configuring Settings for Cisco BCE Application, page 1-14
- Email Encryption Options Available by Configuration Mode, page 1-17
- Message Security, page 1-24
- Cache Management, page 1-24
- Troubleshooting Tips, page 1-25
- Upgrading the Cisco BCE Application, page 1-26
- Uninstalling the Cisco BCE Application, page 1-27
- Customer Support, page 1-27
Overview

The Cisco Business Class Email (BCE) mobile application provides you the ability to receive and send encrypted email messages directly from your Apple iOS devices. Depending on the configuration mode of the Cisco BCE mobile application, the following tasks can be performed:

- Add an account to the Cisco BCE application
- Synchronize secure messages in the Inbox and Sent folders
- Open an encrypted email on the iOS device using Cisco BCE
- Send an encrypted email from the iOS device using Cisco BCE
- Manage the secure emails sent from the iOS device using Cisco BCE
- Lock and unlock an encrypted email sent from the iOS device using Cisco BCE
- Set or modify an expiration date for an encrypted email sent from the iOS device using Cisco BCE
- Receive a read receipt for encrypted email sent from the iOS device using Cisco BCE
- Check or modify encrypted email options from the iOS device

What’s New

With this release, you can add an account to the Cisco BCE application. After adding your account, the messages will be synchronized in the Inbox and Sent folders. For more information, see the “Adding an Account” section on page 1-3.

Licensing Versions and Configuration Modes

The Cisco BCE application is deployed in two separate licensing versions that determine the configuration mode for the application. The default configuration mode for the Cisco BCE application is Decrypt Only.

The two licensing versions and configuration modes are:

- **Decrypt Only**: Allows you to decrypt the received secure email messages and to forward and reply to the received messages. To create a Decrypt account, open a secure message. The account will appear in the BCE settings.

- **Decrypt and Encrypt**: Allows you to encrypt and decrypt secure email messages. To create an Encrypted account, apply the configuration file that you received from Administrator, as described in the “Opening a Secure Message in the Cisco BCE Application” section on page 1-11.

Supported Operating Systems

For information about operating systems supported for release 3.0, see the Cisco Email Encryption Compatibility Matrix.
Downloading and Installing the Cisco BCE Application

To install the Cisco BCE application, go to the Apple App Store from your Apple iOS device and search for the Cisco BCE application. Download the application and start the installation on the device. To create an Encrypted account, you must also apply the configuration file that you received from Administrator, as described in the “Opening a Secure Message in the Cisco BCE Application” section on page 1-11. For more information about the types of BCE accounts, see Licensing Versions and Configuration Modes, page 1-2.

Opening Cisco BCE Application for iOS

After the Cisco BCE application is successfully installed on the iOS device, you will see a new Cisco BCE application icon. To open the application, tap the Cisco BCE icon on the iOS home screen.

Note

You can use multiple CRES accounts to open BCE email on the same device. To create multiple accounts, configure your account to be associated with different servers. Each account will have its own account settings.

Adding an Account

To more easily decrypt and read the secure messages, you can add your account to the Cisco BCE application. After setting up your account, the secure messages will be synchronized in the Inbox and Sent folders.

There are two ways of adding an account to the Cisco BCE application:

- Adding Your Account Automatically
- Adding Your Account Manually

The first way is an automated process that guides you through the set-up procedure. The second one is manual, where you enter all account information by yourself. If the automated set-up process does not work, or if the BCE application does not contain information about your email provider, you can set up your account manually. You can find the information that you need to set up an account on your email provider’s web site or by contacting their technical support department.
Adding Your Account Automatically

To add your account automatically:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>On the <strong>Home</strong> screen, tap <strong>Add Account</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><img src="image" alt="Home screen with Add Account option" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Tap your email account provider in the list of available providers.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><img src="image" alt="Account options" /></td>
</tr>
</tbody>
</table>

**Note**  
If there is no email account in the list, tap **Other** and proceed with configuring your account.
Step 3  (Optionally) In the Name field, enter your name that will be displayed for the users who receive the encrypted messages from you.

Step 4  In the Email field, enter your email address.

Step 5  In the Password field, enter the password of your email account.

Step 6  (Optionally) In the Description field, enter the name of the email that will be displayed in the application.
Step 7  (Applicable only if you have selected the Other email account) Complete the information in the Incoming and Outgoing Server Settings.

Adding Your Account Manually

To add your account manually:

Step 1  On the Home screen, tap Add Account.
Step 2  In the list of available email account providers, tap Other.
Step 3  Enter your email address and password.
Step 4  In the Incoming Server Settings, enter a Hostname.

Note Each Internet service provider has a different configuration for connecting to their email servers. The ISP websites are the best source of connection information.

Step 5  In the Username field, enter your full email address.
Step 6  In the Password field, enter the password to your email address.
Step 7  In the Connection Type field, enter the security setting for connection with the server.
Step 8  In the Port field, enter the default port.
Setting Up Your Account and Synchronizing Secure Messages

If you are still using the previous version of the BCE application (for example, 2.0, 2.1, or 2.1.1), you can set up your account and synchronize the secure messages in the Inbox and Sent folders. If you have already set up an account, the messages should be synchronized in the application.

To synchronize your secure messages and set up an account, use one of the following ways:

- Setting Up Your Account From the Home Screen
- Setting Up Your Account From the Settings screen
- Setting Up Your Account From the Inbox or Sent Folders

Setting Up Your Account From the Home Screen

To set up your account from the Home screen:

**Step 1**

On the Home screen, tap the Information icon near your account.

**Note**

This icon appears only after the BCE application upgrade to version 3.0.
Step 2
In the message that appears, tap Set Up.

Step 3
Enter the password to your email. Your account will be set up, and the messages will be synchronized in the Inbox and Sent folders.
Setting Up Your Account From the Settings screen

To set up your account from the Settings screen:

Step 1  On the Home screen, tap Settings.
Step 2  On the Settings screen, tap your account or the icon near your account.
Step 3  On the next Settings screen, tap Set Up Account.
Step 4  Enter your email address and password. Your account will be set up, and the messages will be synchronized in the Inbox and Sent folders.

Setting Up Your Account From the Inbox or Sent Folders

To set up your account from the Inbox or Sent folders:

Step 1  In the Inbox or Sent folder, pull down to refresh.
Step 2  In the message that appears, tap Set Up.

Step 3  In the Password field, enter your email password. Your account will be set up, and the messages will be synchronized.

Application Home Screen

Tap the Cisco BCE icon to open the application home screen.
The following table describes the application home screen options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>account name &gt; Inbox</td>
<td>Displays a list of decrypted emails opened for the selected account.</td>
</tr>
<tr>
<td>account name &gt; Sent</td>
<td>Displays a list of encrypted emails sent from the selected account.</td>
</tr>
<tr>
<td>account name &gt;</td>
<td>Manage email messages sent from your device and other devices. You can load</td>
</tr>
<tr>
<td>Manage Messages</td>
<td>messages from the server for the selected account that were not sent from the</td>
</tr>
<tr>
<td></td>
<td>current device. Tap the individual email account to display a list of emails</td>
</tr>
<tr>
<td></td>
<td>encrypted and sent from the selected account.</td>
</tr>
<tr>
<td>Secure Compose</td>
<td>Launches screen to compose a secure message. Composing secure messages is</td>
</tr>
<tr>
<td></td>
<td>available only if you apply the BCE configuration file that you have received</td>
</tr>
<tr>
<td></td>
<td>from your administrator. See Opening a Secure Message in the Cisco BCE</td>
</tr>
<tr>
<td></td>
<td>Application, page 1-11.</td>
</tr>
<tr>
<td>Settings</td>
<td>Launches the configuration screen for general settings for the application.</td>
</tr>
<tr>
<td></td>
<td>See Configuring Settings for Cisco BCE Application, page 1-14.</td>
</tr>
<tr>
<td>Tutorial</td>
<td>Brief description how to enable the Cisco BCE application.</td>
</tr>
</tbody>
</table>
Opening a Secure Message in the Cisco BCE Application

There are two ways how you can open and read your secure messages using the Cisco BCE application:

- **Opening a Secure Message after Adding Your Account**
- **Opening a Secure Message Using the Native Mail Application**

### Opening a Secure Message after Adding Your Account

To open a secure message after adding your account:

1. **Step 1**
   - Add your account to the Cisco BCE application. For more information about adding an account, see the “Adding an Account” section on page 1-3.
   - **Note** After adding your account, your secure messages will be synchronized in the **Inbox** and **Sent** folders.

2. **Step 2**
   - Go to the **Inbox** or **Sent** folder.

3. **Step 3**
   - Tap a secure message and wait until the download process completes.

4. **Step 4**
   - Tap **Submit** on the screen that appears.

5. **Step 5**
   - Enter your CRES password and read the secure message.

### Opening a Secure Message Using the Native Mail Application

To open a secure message using the **Native Mail** application:

1. **Step 1**
   - Open the secure message in the **Native Mail** application.
   - **Note** There are other mail applications that can be used on the iOS device. Currently, the Cisco BCE application integrates only with the **Native Mail** application that is provided with a mobile device.
Step 2  Scroll down to the attached securedoc.html file.

Step 3  Press and hold the attachment until a menu appears, and then tap Open in Cisco BCE.
Step 4  Select your email address from the **Open As** drop-down menu.

![Open As drop-down menu](image)

Step 5  Enter your password in the **Password** field and read the secure message.

## Registering with the Cisco BCE Application

If you do not have a CRES account, you will need to register with the Cisco BCE application. Only secure messages will be synchronized in the Cisco BCE application. The insecure messages, for example, activation letters, read receipts, and other messages will be sent to your email provider account.

To register with the Cisco BCE application:

---

**Step 1**  Complete the **New User Registration** form and click **Register**. Then check your inbox for the account activation email.

**Step 2**  In the account activation email, click the **Click here to activate this account** link. A message indicates that the account activation is confirmed and you can now view encrypted emails sent to the registered email address.

**Step 3**  Return to the original email with the HTML attachment. Press and hold the attachment until a menu appears. Depending on the screen display, you will tap either **Open in Cisco BCE** or tap **Open In > Open in Cisco BCE**.

---

**Note**  The registration confirmation letter will be sent to your email provider account. The confirmation letter will not appear in the BCE Inbox folder. All other notification letters that do not require entering a password will be also sent to your email provider account.
Launching the Cisco Business Class Email Configuration File

To create an Encrypted account, you must apply the configuration file that you received from Administrator after the Cisco BCE application is installed, as described below.

To enable and configure the BCE application for an Encrypted account:

---

**Step 1**  Add your account to the Cisco BCE application. For more information about adding an account, see the “Adding an Account” section on page 1-3.

**Step 2**  After messages are loaded in the Inbox folder, search for the configuration file from Administrator.

**Step 3**  Open the configuration file you need to enter your CRES password.

**Step 4**  When prompted, accept the configuration to complete this procedure.

---

Configuring Settings for Cisco BCE Application

The following tables list the two types of settings that you can configure for Cisco BCE:

- General Settings
- Mail Account Settings
- Envelope Cache Settings
- Secure Account Settings

### General Settings

To configure the General Settings, tap **Settings > General Settings**. Depending on your configuration mode, some of the options are not available for configuration. See **Licensing Versions and Configuration Modes**, page 1-2.

The following email security options are available on the General Settings screen.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Account</td>
<td>Specifies the address of the email account that will be used as the default Cisco BCE registered account. Available only after you apply the BCE configuration file that you have received from Administrator.</td>
</tr>
<tr>
<td>Save Draft</td>
<td>By default, this option is disabled. Enabling Save Draft preserves data entered in secure compose until you send the message. The data is stored in the clear and may be recoverable if your device is lost or stolen.</td>
</tr>
<tr>
<td>Send Usage Data</td>
<td>Determines whether anonymous usage data will be sent to Cisco to help improve the BCE application.</td>
</tr>
<tr>
<td>Reset Identifier</td>
<td>Determines whether to reset identifier used to send the usage data.</td>
</tr>
<tr>
<td>Detailed Logging</td>
<td>Turn on to diagnose issues and improve the BCE application.</td>
</tr>
</tbody>
</table>
In the Advanced Settings, you can manage the messages that you have sent and the Trash folder. The Advanced Settings contain the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name that will be displayed for the users who receive the secure messages from you.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter the description of the mail that will be displayed in the Cisco BCE application.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Enter the hostname. Each Internet Service Provider has a different configuration for connecting to their email servers. The ISP websites are the best source of connection information.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter your full email address.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password to your email address.</td>
</tr>
<tr>
<td>Connection Type</td>
<td>Enter the connection type that is a security setting for connection with the server (for example, &quot;STARTTLS&quot; or &quot;SSL/TLS&quot;).</td>
</tr>
<tr>
<td>Port</td>
<td>For IMAP Server (Incoming Messages), the default port and connection type are SSL/TLS 993. For SMTP Server (Outgoing Messages), the default ports and connection types are SSL/TLS 465 or StartTLS 587.</td>
</tr>
<tr>
<td>Sent Folder</td>
<td>The default Sent folder where all messages that you have sent from the Cisco BCE application are stored.</td>
</tr>
<tr>
<td>Save Sent Mail</td>
<td>This option is enabled by default so that the messages sent from the Cisco BCE application could be stored in the Sent folder.</td>
</tr>
<tr>
<td>Move Mail to Trash Folder</td>
<td>The messages deleted from the Cisco BCE application are stored in the Trash folder of your email provider server. If you disable this option, the messages will not be stored in the Trash folder and will not be accessible anymore.</td>
</tr>
<tr>
<td>Trash Folder</td>
<td>The messages deleted from the Cisco BCE application are stored in the Trash folder.</td>
</tr>
</tbody>
</table>
Chapter 1  Configuring and Using Cisco Business Class Email for iOS

Configuring Settings for Cisco BCE Application

Envelope Cache Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cache Size</td>
<td>Defines the size of the cache in MB for downloaded secure messages after they are opened for the first time. By default, this number is 100 MB.</td>
</tr>
<tr>
<td>Cache Duration</td>
<td>Specifies the amount of time before the cache is cleared. The downloaded secure messages are cached on the device after they are opened for the first time. The default time is 30 days.</td>
</tr>
</tbody>
</table>

Secure Account Settings

To configure the Account Settings, tap Settings > account name. Depending on your configuration mode, some options may not be available for configuration. See Licensing Versions and Configuration Modes, page 1-2.

The following email security options are available on the Account Settings screen:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login</td>
<td>Login name submitted for the Cisco BCE registered account.</td>
</tr>
<tr>
<td>Server</td>
<td>Server name submitted for the Cisco BCE registered account.</td>
</tr>
<tr>
<td>Password Cache Duration</td>
<td>Enter the cache duration in days, hours, and minutes. The default is 1 day.</td>
</tr>
<tr>
<td>Clear Password Cache</td>
<td>Tap to immediately clear the cache. The cache is automatically cleared when the password cache time duration has elapsed.</td>
</tr>
<tr>
<td>Expiration</td>
<td>Sets the default expiration date, which specifies how long encrypted email messages remain valid. After the specified date, messages expire, and cannot be opened by the recipient after this period. See Set an Email Expiration Time, page 1-19.</td>
</tr>
<tr>
<td>Request Read Receipt</td>
<td>Determines whether to request a default read-receipt notification to the sender when the recipient opens the encrypted message. By default, it is enabled. See Manage Sent Secure Messages, page 1-21.</td>
</tr>
<tr>
<td>Message Security</td>
<td>Determines whether the message security level is set to Low, Medium, or High. By default, the message security level is set to High. See Message Security, page 1-24.</td>
</tr>
<tr>
<td>Allow Reply</td>
<td>Determines whether you can send an encrypted reply to a received encrypted message if the message setting also allows it. By default, it is enabled. See Reply/Reply All/Forward an Email, page 1-18.</td>
</tr>
<tr>
<td>Allow Reply All</td>
<td>Determines whether you can send an encrypted reply to all recipients of a received encrypted message if the message setting also allows it. By default, this option is enabled.</td>
</tr>
<tr>
<td>Allow Forward</td>
<td>Determines whether you can forward a received encrypted message if the message setting also allows it. By default, this option is enabled.</td>
</tr>
</tbody>
</table>
Email Encryption Options Available by Configuration Mode

The Cisco BCE application is deployed in two separate licensing versions that determine the email encryption options available and the configuration mode for the application. For more information about deploying the different configuration modes, see Licensing Versions and Configuration Modes, page 1-2. The option of opening an encrypted email is available in both configuration modes.

The following sections describe the email encryption options in each of the configuration modes:

- **Options Available in Both the Decrypt and Encrypt Modes, page 1-17**
  - Reply/Reply All/Forward an Email, page 1-18
  - Lock or Unlock an Encrypted Email, page 1-18
  - Set an Email Expiration Time, page 1-19
  - Manage Sent Secure Messages, page 1-21

- **Options Available in Only the Encrypt Mode, page 1-22**
  - Sending an Encrypted Email, page 1-22
  - Request a Read-Receipt, page 1-22
  - Envelope Settings, page 1-23

**Options Available in Both the Decrypt and Encrypt Modes**

The default configuration mode for the Cisco BCE application is Decrypt Only. In Decrypt Only mode, you can receive and open encrypted messages, but you cannot send them.

---

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recipient Language</td>
<td>Enables application to determine which language is used for the message body, according to the locale set for recipients. Use this option when you want to send encrypted messages to recipients who have the same locale. If the recipients have different locales, the message body will always use the default language you select from the following options.</td>
</tr>
<tr>
<td></td>
<td>• Server Default</td>
</tr>
<tr>
<td></td>
<td>• English</td>
</tr>
<tr>
<td></td>
<td>• French</td>
</tr>
<tr>
<td></td>
<td>• German</td>
</tr>
<tr>
<td></td>
<td>• Spanish</td>
</tr>
<tr>
<td></td>
<td>• Portuguese</td>
</tr>
<tr>
<td></td>
<td>• Japanese</td>
</tr>
<tr>
<td></td>
<td>• Italian</td>
</tr>
<tr>
<td>Submit Diagnostic Information</td>
<td>Allows you to specify the recipient, subject, and content of diagnostic emails sent for troubleshooting purposes. To set the type of logs being maintained by the application, as defined by the log level, see Upgrading the Cisco BCE Application, page 1-26.</td>
</tr>
</tbody>
</table>
Email Encryption Options Available by Configuration Mode

The combined Decrypt and Encrypt mode allows encrypting and decrypting the secure email messages. For more information about how to enable either mode, see Licensing Versions and Configuration Modes, page 1-2.

Reply/Reply All/Forward an Email

An encrypted email that is replied or forwarded is automatically encrypted by default. The secure message will allow zero or more of the following:

- Secure Reply
- Secure Reply All
- Secure Forward

Based on the permissions defined on the Settings screen for the encrypted email, applicable menu options are added to the iOS device. For example, if the encrypted email has permissions to Forward only, then only the Forward menu option would be available. See Configuring Settings for Cisco BCE Application, page 1-14.

Note

To maintain the security of your replies, you cannot change the list of recipients.

To reply to or forward an encrypted email:

Step 1

Follow the steps for “Opening a Secure Message in the Cisco BCE Application” section on page 1-11.

Step 2

Tap the Settings icon. Tap Secure Reply or Secure Reply All, or Secure Forward.

The original message is added to a new message compose screen. Add a response and delete or modify the content from the original message.

Step 3

When the message is complete, tap Encrypt to open the iOS email system and complete the action.

Step 4

Tap Send.

The message is encrypted, attached as an HTML file to the outgoing email, and sent.

Lock or Unlock an Encrypted Email

After sending an encrypted email, the email can be locked to prevent the recipient from opening the email. This option can be used if the email was sent to the wrong recipient or if there is updated information since the email was sent.

Note

The Lock/Unlock Email Messages and Edit Lock Reason menu options will not be available for key servers that do not support these features.
To lock an encrypted email:

**Step 1**  
Tap *account name > Manage Messages*.  
To display a list of the encrypted email messages sent from the selected account, perform a pull-down gesture.

**Step 2**  
Check the encrypted email messages that you want to lock in the email list.  
This will enable the lock and expire icons.

**Step 3**  
Tap **Lock**.

**Step 4**  
While the selected email messages are still checked, you can optionally enter a reason for locking the message and tap **Update**.  
The lock reason is displayed to recipients when they view the envelope.

**Step 5**  
Tap **Lock**. Successful locking of the email message is confirmed. Locked emails are displayed with an icon of a padlock.

**Note**  
After an email is locked, the lock reason can be edited by selecting the locked email. Tap the selected email to display the menu options and tap **Edit Lock Reason**.

To unlock an encrypted email:

**Step 1**  
Tap *account name > Manage Messages*.  
To display a list of the encrypted email messages sent from the selected account, perform a pull-down gesture.

**Step 2**  
Check the encrypted email messages that you want to unlock in the email list.

**Step 3**  
Tap **Unlock**.

### Set an Email Expiration Time

An expiration time can be set for encrypted email. You can specify how long the encrypted email remains valid. After the expiration time is met, the message expires, and cannot be opened by the recipient. When setting an expiration time, the following options are available:

- A default expiration interval can be set for all secure email.
- The default expiration can be overridden for a specific email.
- The expiration time can be changed after the email is sent.

#### Default Settings

To set the default expiration interval:

**Step 1**  
Tap **Settings > account name** to open the settings screen for your email account.

**Step 2**  
Tap **Expiration** and specify the number of days after which the email will expire.

**Step 3**  
Tap < *account name* to exit and save the changes.
Per Message Settings

To set expiration time for a specific email:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Tap the Secure Compose icon to open the Secure Compose screen.</td>
</tr>
<tr>
<td>2</td>
<td>Tap Encrypt with to select the registered email account that will be used to send the encrypted message.</td>
</tr>
<tr>
<td>3</td>
<td>When you have completed writing the message, tap the Settings icon located on the bottom left of the screen for iPhones and on top right of the screen for tablets.</td>
</tr>
<tr>
<td>4</td>
<td>Tap Expiration. The New Expiry Date screen displays.</td>
</tr>
<tr>
<td>5</td>
<td>Select the expiration date and time that the email will expire.</td>
</tr>
<tr>
<td>6</td>
<td>Tap Message Settings to save the changes.</td>
</tr>
<tr>
<td>7</td>
<td>Tap Set to exit the Envelope Settings screen and return to the secure email.</td>
</tr>
<tr>
<td>8</td>
<td>When the message is complete, tap Encrypt to open the iOS email system and complete the action.</td>
</tr>
<tr>
<td>9</td>
<td>Tap Send. The message is encrypted, attached as an HTML file to the outgoing email, and sent.</td>
</tr>
</tbody>
</table>

After Sending Message

To set expiration time after sending an email:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Tap account name &gt; Manage Messages. To display a list of the encrypted email messages sent from the selected account, perform a pull-down gesture.</td>
</tr>
<tr>
<td>2</td>
<td>Select the encrypted email messages that you want to set the expiration time for in the email list. This will enable the lock and expire icons.</td>
</tr>
<tr>
<td>3</td>
<td>Tap the Expiration icon.</td>
</tr>
<tr>
<td>4</td>
<td>Select the expiration date and time that the email will expire.</td>
</tr>
<tr>
<td>5</td>
<td>Tap Set to save the changes. A message confirms the date and time that the message will expire.</td>
</tr>
</tbody>
</table>

Clear Expiration Date and Time

To clear the expiration date and time after sending an email:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Tap account name &gt; Manage Messages. A list of the encrypted emails sent from the selected account is displayed.</td>
</tr>
<tr>
<td>2</td>
<td>Select the encrypted email messages that you want to clear the expiration time for in the email list. This will enable the lock and expire icons.</td>
</tr>
<tr>
<td>3</td>
<td>Tap the Expiration icon.</td>
</tr>
<tr>
<td>4</td>
<td>Tap Never.</td>
</tr>
<tr>
<td>5</td>
<td>Tap Update to save the changes.</td>
</tr>
</tbody>
</table>
Manage Sent Secure Messages

You can use the Manage Messages screen to read and manage messages sent from both your device and other devices. Messages sent from your device are marked with a “Sent from this device” icon. The Manage Messages also enables you to delete, lock, or expire a message, or view its details.

You can view only those messages that were sent from your device by tapping on the Filter button and selecting “sent from device.” To remove the filter, tap the Filter button and selecting “show all.” All filtered messages are sorted by date they were sent.

If you delete a message that was sent from your device, the message will no longer be marked as “Sent from this device.” However, when a sent message is deleted, some message information is still visible (such as the subject, recipients, and sent date). After a message is deleted, it will be opened as if it was sent from another device or by using the web interface. You can lock, expire, and browse message details for deleted messages, but you cannot see the message body and attachment.

To view a list of the encrypted emails sent from your mobile device, tap account name > Manage Messages. Select an email address and the email from the list of sent encrypted messages for which you want to set or view the lock reason or expiration date.

Tap the selected email to display the following menu options that you can use with the sent encrypted emails:

- **Lock.** After sending an encrypted email, the email can be locked to prevent the recipient from opening the email. After the email is locked, the Edit Lock Reason and Unlock options are available from this screen. See Lock or Unlock an Encrypted Email, page 1-18.
- **Set Expiry.** An expiration time can be set for encrypted email. See Set an Email Expiration Time, page 1-19.
- **View Details.** View details of the encrypted email sent from the device.
- **Remove.**

For iPhones, you can view the appropriate icons to determine whether the messages are locked, expired, or opened.

On iPads, you can view the following information about the messages in the Manage Messages table.

- **Open Date.** Date on which the secure message was opened by the respective recipient.
- **Expiration Date.** Expiration date for the encrypted email.
- **Locked Status.** If the encrypted email has been locked a lock icon is displayed. Otherwise, an unlocked icon is displayed.
- **Locked Reason.** Displays comments entered when locking the encrypted email.

You can also view details of the encrypted emails sent from the device. Depending on the security settings of a message, you may have to enter your password when you tap the message and view its details. The following information is displayed:

- **Subject.** Subject of the message.
- **Date.** Date the message was sent.
- **To.** Email address of the recipient.
- **From.** Email address of the sender.
- **Body text**
- **Attachments**
Options Available in Only the Encrypt Mode

The combined Decrypt and Encrypt mode allows encrypting and decrypting of secure email messages. For more information about how to enable this mode, see Licensing Versions and Configuration Modes, page 1-2.

Sending an Encrypted Email

When sending an encrypted message, the message will be encrypted for all recipients.

To send an encrypted email:

Step 1 Tap the Secure Compose icon to open the Secure Compose screen. The Secure Compose icon is available only if the “encrypt” type edition has been applied in the BCE Configuration file.

Step 2 Complete the appropriate fields:
- Address (To, CC, and BCC)
- Subject

If there is only one configured email account, that account is added in the “Encrypt with” field for new messages. If there are multiple configured email accounts, you can select an account as the default account that will appear on Compose screen in the Encrypt with field. To set the default account, select General Settings > Default Account.

Step 3 Enter the message text.

Step 4 Optionally, when composing the secure message, the message settings for the outgoing message can be changed from the Envelope Settings screen. To access Envelope Settings, tap the Settings icon located at top right screen on iPads and at the bottom of the screen on iPhones.

Note When composing a secure message on the iPhone, you can add attachments as large as 3MB.

Note You can save a draft of the message if the Save Draft option enabled on the Settings screen. The contents of the message are displayed when the application is restarted or returns from the background.

Step 5 When the message is complete, tap Encrypt to open the iOS email system and complete the action.

Step 6 Tap Send. The message is encrypted, attached as an HTML file to the outgoing email, and sent.

Request a Read-Receipt

A read-receipt can be requested directly on the iOS device when the sent email is opened by the recipient.

Default Settings

To request a read-receipt (the default settings):

Step 1 Tap Settings > account name to open the settings screen for your email account.

Step 2 Enable the Request Read Receipt option. It is enabled by default.
Per Message Settings

This option applies if the default setting is not enabled and you are requesting a read-receipt for an individual email.

To request a read-receipt for a specific email:

---

**Step 1** Tap the Secure Compose icon to open the Secure Compose screen.

**Step 2** Tap Encrypt with to select the registered email account that will be used to send the encrypted message.

**Step 3** When you have completed writing the message, tap the Settings icon located on the bottom left of the screen for iPhones and on top right of the screen for tablets.

**Step 4** Enable the Request Read Receipt option. It is enabled by default.

**Step 5** Tap Set to save the changes and exit.

---

Envelope Settings

When composing a secure email, the message settings for the email you are composing can be changed.

To change the envelope settings:

---

**Step 1** Tap account name > Secure Compose to open the Secure Compose screen.

**Step 2** Tap Encrypt with to select the registered email account that will be used to send the encrypted message.

**Step 3** Complete the appropriate fields:

- Address (To, CC, and BCC)
- Subject

**Step 4** Enter the message text.

**Step 5** When you have completed writing the message, tap the Settings icon located on the bottom left of the screen for iPhones and on top right of the screen for tablets.

**Step 6** Set the applicable message options:

- Expiration
- Request Read Receipt
- Message Security
- Allow Reply
- Allow Reply All
- Allow Forward

**Step 7** Tap Set to save the changes and exit.
Message Security

The sender can specify the security level for the encrypted email by tapping Settings > account name > Message Security. The following message security options can be set:

- **High.** A high security message requires a password for authentication every time an encrypted message is decrypted.
- **Medium.** If the recipient password is cached, a medium security message does not require a password when an encrypted message is decrypted.
- **Low.** A low security message is transmitted securely but does not require a password to decrypt an encrypted message.

A default security of high is set for all messages. The default security can be overridden for a specific message by modifying the value in Envelope Settings.

Cache Management

Cache Passwords

The Cisco BCE registered account password is cached for a time period that you can configure by tapping Settings > account name > Password Cache Duration. The default cache time is 1440 minutes (24 hours). Password caching is Off by default but it can be turned On by using the Remember Password switch located on the Medium Security messages screen or the Manage Messages screen.

The password cache can be cleared from the Account Settings screen by tapping Settings > account name > Clear Password Cache. For Encrypt accounts, you can also set the Password Cache Duration.

Secure Envelope Caching

The downloaded secure envelopes are cached on the device after they are opened for the first time. This avoids re-downloading of a secure envelope when you open the same secure envelope for the second time.

The caching is based on a combination of time and size. The maximum size of cached envelopes is configurable by the administrator. The default is 100 MB. Envelopes are deleted from Inbox and Manage messages folders if they exceed allowable envelope cache size (MB) and duration (time), when the Inbox or Manage Messages folders are reopened.
Troubleshooting Tips

This section provides the troubleshooting tips for issues that you may encounter when using the Cisco BCE application.

Issue: Cannot Add an Account

If you use a Google account, you may encounter a problem with adding an account. In this case, you will see a notification massage: "Incorrect email address or password. Try again". This happens when you have the Allow less secure apps option disabled.

To enable the Allow less secure apps option:

- Step 1: Log in to your Google account.
- Step 2: Tap the Information icon in the right upper corner.
- Step 3: Tap My Account and then Sign-in & security.
- Step 4: Scroll down to the bottom and make sure that the Allow less secure apps option is ON.

Issue: Cannot Add an Account

If you cannot add an account, the following notification massage appears: "To add an account to the BCE app, log in to your Google account, generate a password on the App passwords page, and then enter the App password on your device." In this case, you need to follow the procedure on generating the App password described in the Google help by the following link: https://support.google.com/accounts/answer/185833?hl=en.

If you use any another email service provider then Google, you may get the following error message: "The email address or password is incorrect. Please try again." In this case, you need to generate a password and enter this password on your device.

Issue: Cannot Add an Account

If you use a Google account, you may encounter a problem with adding an account. In this case you will see a notification massage: "To add an account to the BCE app, log in to your Google account and enable the "IMAP" option in Settings > Forwarding and POP/IMAP". You can find the procedure on how to enable the IMAP option is by the following link: https://support.google.com/mail/troubleshooter/1668960?rd=1.

Issue: Messages are Duplicated in the Sent Folder

The messages you send from the Cisco BCE application can be duplicated in the Sent folder of your email service provider. To fix this issue, in the Cisco BCE application go to Settings > your account > Mail Account Settings > Advanced Settings > Sent Mailbox Behavior on the server and turn off the Save Sent Message option.
Troubleshooting Using the Diagnostic Tool

The Cisco BCE application includes a diagnostic tool to help with troubleshooting problems. You can use the diagnostic tool if receiving errors or if there are issues with the Cisco BCE application.

The diagnostic tool attaches the data collected to an email. The diagnostic email contains data information that is generated on the device during your interaction with the encryption application.

Note
This functionality is available if you have decrypted at least one secure message.

To report a problem using the Diagnostic Tool:

Step 1  Go to Settings > Account Name > Key Server Name > Submit Diagnostic Information.
Step 2  In the Subject field, enter the subject of the issue that will appear in the diagnostic email.
Step 3  In the To field, enter the Cisco support email.
Step 4  Tap Send Diagnostic Email.

Reporting a Problem

To help us fix the issues you encounter when using the Cisco BCE application, you can turn on the Detailed Logging in General Settings.

Note
In your email, it is recommended to include the errors you receive or issues you encounter with the Cisco BCE application. This information will help with troubleshooting and resolving issues.

To report a problem:

Step 1  Go to Settings > General Settings > Report a Problem.
Step 2  Enter the Cisco support email.
Step 3  Send the report.

Upgrading the Cisco BCE Application

To upgrade the Cisco BCE application:

Step 1  On your mobile device, go to Google Play (on Android) or Apple App Store (on iOS).
Step 2  Search for the Cisco BCE application.
Step 3  Tap Update, if a new version of the Cisco BCE application is available. The application will be updated automatically.

Note
The previous configuration settings are retained after the upgrade.
Uninstalling the Cisco BCE Application

To uninstall Cisco BCE:

**Step 1** Go to the iOS home screen.
**Step 2** Press and hold the **Cisco BCE** icon until a delete (X) icon appears above it.
**Step 3** Tap the delete (X) icon. The application is removed.

Customer Support

Please contact your system administrator to provide assistance with Cisco Business Class Email.