CHAPTER 1

Configuring and Using Cisco Business Class Email for Android

- Overview, page 1-2
- What’s New, page 1-2
- Licensing Versions and Configuration Modes, page 1-2
- Supported Operating Systems, page 1-2
- Hardening Recommendations, page 1-3
- Downloading and Installing the Cisco BCE Application, page 1-4
- Registering with the Cisco BCE Application, page 1-10
- Opening a Secure Message in the Cisco BCE Application, page 1-11
- Launching the Cisco BCE Configuration File, page 1-13
- Configuring Settings for Cisco BCE Application, page 1-13
- Email Encryption Options Available by Configuration Mode, page 1-16
- Message Security, page 1-23
- Cache Management, page 1-23
- Troubleshooting Tips, page 1-24
- Upgrading the Cisco Business Class Email Application, page 1-25
- Uninstalling the Cisco Business Class Email Application, page 1-26
- Customer Support, page 1-26
Overview

With the Cisco Business Class Email (BCE) mobile application you can receive and send encrypted email messages directly from your Android devices. Depending on the configuration mode of the Cisco BCE 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 Android device using Cisco BCE
- Send an encrypted email from the Android device using Cisco BCE
- Manage the secure emails sent from the Android device using Cisco BCE
- Lock or unlock an encrypted email sent from the Android device using Cisco BCE
- Set or modify an expiration date for an encrypted email sent from the Android device using Cisco BCE
- Receive a read receipt for encrypted email sent from the Android device using Cisco BCE
- Check or modify encrypted email options from the Android device

What’s New

In this release, the encryption methods are improved and comply with the world standards so that the message encryption is now more secure.

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 received secure email messages and to forward and reply to received messages. To create a Decrypt account, open a secure email using the Native email system.

- **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 “Registering with the Cisco BCE Application” section on page 1-10.

Supported Operating Systems

For information about operating systems supported for release 3.1, see the Cisco Email Encryption Compatibility Matrix.
Hardening Recommendations

For security reasons, follow *The Center for Internet Security (CIS)* hardening recommendations. The checklist of hardening items is intended for system and application administrators, security specialists, help desks, end users, and platform deployment personnel who plan to use, access, or secure the Cisco BCE application on Android.

The following table provides the hardening checklist.

<table>
<thead>
<tr>
<th>Step</th>
<th>To Do</th>
<th>CIS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Basic Security</strong></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Update operating system to the latest version</td>
<td>1.1.1</td>
</tr>
<tr>
<td>2</td>
<td>Do not Root the device</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Do not install applications from third party app stores</td>
<td>1.1.17</td>
</tr>
<tr>
<td>4</td>
<td>Enable the device encryption</td>
<td>1.1.15</td>
</tr>
<tr>
<td>5</td>
<td>Disable Developer Actions</td>
<td>1.1.16</td>
</tr>
<tr>
<td>6</td>
<td>Use an application or service to provide remote wipe functionality</td>
<td>3.2</td>
</tr>
<tr>
<td>7</td>
<td>Enable Android Device Manager</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Erase all data before return, repair, or recycle</td>
<td>1.1.11</td>
</tr>
<tr>
<td></td>
<td><strong>Authentication Security</strong></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Set a PIN and automatically lock the device when it sleeps</td>
<td>1.1.2</td>
</tr>
<tr>
<td>10</td>
<td>Set an alphanumeric password</td>
<td>1.1.3</td>
</tr>
<tr>
<td>11</td>
<td>Set Auto-Lock Timeout</td>
<td>1.1.4</td>
</tr>
<tr>
<td>12</td>
<td>Disable Make Passwords Visible</td>
<td>1.1.14</td>
</tr>
<tr>
<td>13</td>
<td>Erase data upon excessive passcode failures</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Browser Security</strong></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Show security warnings for visited sites</td>
<td>1.2.2</td>
</tr>
<tr>
<td>15</td>
<td>Disable Form Auto-Fill</td>
<td>1.2.3</td>
</tr>
<tr>
<td>16</td>
<td>Do not automatically remember passwords</td>
<td>1.2.7</td>
</tr>
<tr>
<td>17</td>
<td>Disable browser plug-ins</td>
<td>1.2.6</td>
</tr>
<tr>
<td>18</td>
<td>Turn on Do Not Track</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Network Security</strong></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Turn off Bluetooth when not in use</td>
<td>1.1.9</td>
</tr>
<tr>
<td>20</td>
<td>Disable network notification</td>
<td>1.1.6</td>
</tr>
<tr>
<td>21</td>
<td>Forget Wi-Fi networks to prevent automatic rejoin</td>
<td>1.1.15</td>
</tr>
<tr>
<td></td>
<td><strong>Additional Security Settings</strong></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Turn off Location Services</td>
<td>1.1.8</td>
</tr>
<tr>
<td>23</td>
<td>Use a third party application to password protect applications with sensitive data</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>Limit the number of text (SMS) and multimedia messages (MMS) saved</td>
<td>1.1.18 - 1.1.19</td>
</tr>
<tr>
<td>25</td>
<td>Disallow cookies in Chrome browser</td>
<td>1.2.4</td>
</tr>
</tbody>
</table>
To install the Cisco BCE application, go to Google Play from your Android 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 “Registering with the Cisco BCE Application” section on page 1-10. For more information about the types of BCE accounts, see Licensing Versions and Configuration Modes, page 1-2.

Opening the Cisco BCE Application for Android

After the Cisco BCE application is successfully installed on your Android device, you will see a new Cisco BCE application icon. To open the application, tap the Cisco BCE icon from the Android 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 of these 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>To Do</th>
<th>CIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>Disable JavaScript in Chrome browser</td>
<td>1.2.1</td>
</tr>
<tr>
<td>27</td>
<td>Use TextSecure to encrypt SMS messages</td>
<td></td>
</tr>
</tbody>
</table>
Adding Your Account Automatically

To add your account automatically:

**Step 1**  On the **Home** screen, tap **Add account**.

**Step 2**  Tap your email account provider in the list of available providers.

*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 in the application.

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**  
(Applicable only if you have selected the Other email account) Complete the information in the Incoming and Outgoing server settings.

![Cisco BCE Application for Android](image)

**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), after upgrade 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 Settings Screen
- Setting Up Your Account From the Inbox or 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.
- **Step 3**: On the next Settings screen, tap Set up account.
- **Step 4**: Enter your 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**.

![Set up account screen](image)

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

---

### Application Landing Screen for Phones

Tap the **Cisco BCE** icon to open the application landing screen.

The following table describes the application landing screen options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>account name &gt; account name</strong> (account settings)</td>
<td>Launches the configuration screen for account settings. See <a href="#">Configuring Settings for Cisco BCE Application, page 1-13</a>.</td>
</tr>
<tr>
<td><strong>account name &gt; Inbox</strong></td>
<td>Displays a list of encrypted secure messages opened for the selected account.</td>
</tr>
<tr>
<td><strong>account name &gt; Sent</strong></td>
<td>Displays a list of encrypted secure messages sent from the selected account.</td>
</tr>
<tr>
<td><strong>account name &gt; Manage Messages</strong></td>
<td>Manage secure messages sent from your device and other devices. You can load messages from the server for the selected account that were not send from the current device. You can display a list of emails encrypted and sent from each of your individual email accounts.</td>
</tr>
<tr>
<td><strong>Search icon</strong></td>
<td>Search your inbox or sent messages.</td>
</tr>
</tbody>
</table>
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 Cisco BCE.
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 Gmail Application

Opening a Secure Message after Adding Your Account

To open a secure message after adding your account:

1. Add your account to the Cisco BCE application. For more information about adding an account, see the “Adding an Account” section on page 1-4.

   **Note** After adding your account, your secure messages will be synchronized in the Inbox and Sent folders.

2. Go to the Inbox or Sent folder.
3. Tap a secure message and wait until the download process completes.
4. Tap Submit on the screen that appears.
5. Enter your CRES password and read the secure message.

Opening a Secure Message Using the Gmail Application

To open a secure message using the Gmail application:

1. Open the secure message in the Gmail application.
2. Scroll down to the attached securedoc.html file.
Chapter 1      Configuring and Using Cisco Business Class Email for Android

Opening a Secure Message in the Cisco BCE Application

Step 3  Tap the attachment, and then tap Cisco BCE to decrypt the secure message.

Step 4  Select your email address from the Open As drop-down menu.
Step 5 Enter your password in the **Password** field and read the secure message.

### Launching the Cisco BCE 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:

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.
2. **Step 2** After messages are loaded in the **Inbox** folder, search for the configuration file from Administrator.
3. **Step 3** Open the configuration file you need to enter your CRES password.
4. **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 from the General Settings screen:

<table>
<thead>
<tr>
<th>General Configuration 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>Detailed Logging</td>
<td>Turn on to diagnose issues and improve the Cisco BCE application.</td>
</tr>
<tr>
<td>Report a Problem</td>
<td>Report an issue with troubleshooting purposes.</td>
</tr>
<tr>
<td>Show Tutorial</td>
<td>Determines whether the tutorial can be launched from General Settings.</td>
</tr>
<tr>
<td>About</td>
<td>Shows information about the BCE application, such as the application version number, third-party licenses and notices, usage data details, terms of service, and the User Guide.</td>
</tr>
</tbody>
</table>
### Configuring Settings for Cisco BCE Application

**Mail Account Settings**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the mail that will be displayed 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>
</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>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 to Trash</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 Android

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 of the options are not available for configuration. See Licensing Versions and Configuration Modes, page 1-2.

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

<table>
<thead>
<tr>
<th>Account Configuration Option/Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login</td>
<td>Sets the email address of the account that is being used.</td>
</tr>
<tr>
<td>Server</td>
<td>Sets the name of the mail server for the email account.</td>
</tr>
<tr>
<td>Remember Password</td>
<td>Sets the amount of time that the encryption password is cached. If you clear the cache, you must re-enter the password the next time you log in.</td>
</tr>
<tr>
<td>Clear Password</td>
<td>Tap to immediately clear the password in 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 time in days. This option specifies how long the encrypted email message remains valid. Once a message expires, it cannot be opened by the recipient. See Set an Email Expiration Time, page 1-18.</td>
</tr>
<tr>
<td>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 1-20.</td>
</tr>
<tr>
<td>Reply</td>
<td>Determines whether an encrypted message that is replied to is automatically encrypted, if the message setting also allows it. By default, it is enabled. See Reply/Reply All/Forward an Email, page 1-17.</td>
</tr>
<tr>
<td>Reply All</td>
<td>Determines whether an encrypted message is automatically encrypted when you reply to all of the recipients, if the message setting also allows it. This option is enabled by default.</td>
</tr>
<tr>
<td>Forward</td>
<td>Determines whether an encrypted message that is forwarded is automatically encrypted, if the message setting allows it. This option is enabled by default.</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. You can open an encrypted email 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 1-17
  - Lock or Unlock an Encrypted Email, page 1-17
  - Set an Email Expiration Time, page 1-18
  - Manage Sent Secure Messages, page 1-20
- Options Available Only in Encrypt Mode, page 1-21
  - Sending an Encrypted Email, page 1-21
  - Request a Read-Receipt, page 1-21
  - Message Settings, page 1-22

### Account Configuration Option/Action

<table>
<thead>
<tr>
<th>Option/Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 1-23.</td>
</tr>
</tbody>
</table>
| Recipient Language     | 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.  
  - Server Default  
  - English  
  - French  
  - German  
  - Spanish  
  - Portuguese  
  - Japanese  
  - Italian |
| Diagnostic Subject     | Displays the text used in the subject line of diagnostic emails. |
| Send Diagnostic Message| 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 Setting Log Levels, 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.

The combined Decrypt and Encrypt mode allows encrypting and decrypting of secure email messages.

For more information about how to enable either mode, see Licensing Versions and Configuration Modes, page 1-2.

The decrypted message is displayed.

Reply/Reply All/Forward an Email

An encrypted email that is replied or forwarded is automatically encrypted by default. The settings of the secure message will determine whether you can perform zero or more of the following:

- Secure Reply
- Secure Reply All
- Secure Forward

Based on the permissions defined in the Settings screen for the encrypted email, applicable menu options are added to the Android 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 1-13.

Replying to or forwarding an encrypted email:

Step 1 Follow the steps for The decrypted message is displayed., page 1-17 or Opening an Encrypted Email - Previously Opened Message, page 1-9.

Step 2 To see if you can perform a secure reply, reply all, or forward, view the settings for this message by tapping the Android Menu button > Message Settings.

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 Send Secure. From the menu options, select the third-party email system to complete the action. For example, select Android email.

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 in the email list that you want to lock.
This will enable the lock and expire icons.

Step 3  Tap the padlock icon.

Step 4  Optionally, enter a reason for locking the message. 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 an envelope with a lock.

Note  After an email is locked, the lock reason can be edited by checking the locked email, tapping the padlock icon, edit the lock reason, and tap Update.

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 in the email list that you want to unlock.
This will enable the lock and expire icons.

Step 3  Tap the padlock icon.

Step 4  Tap on the recipient.

Step 5  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** On smartphones, tap **Settings > account name**; or on tablets, tap **account name > account name**.

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

**Step 3** Tap **Done** to exit and save the changes.

## Per Message Settings

To set expiration time for a specific email:

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

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

**Step 3** Enter the message text.

**Step 4** Tap the Android Menu button, then tap **Message Settings**.

**Step 5** Tap **Expiration**. The New Expiry Date screen displays.

**Step 6** Set the **Set Expiration** switch to On.

**Step 7** Select the expiration date and time that the email will expire.

**Step 8** Tap **Done** to save the changes.

**Step 9** Tap the back button to exit the Message Settings screen and return to the secure email.

**Step 10** When the message is complete, tap **Send Secure**. From the menu options, select the third-party email system to complete the action. For example, select Android email.

**Step 11** Tap **Send**. The message is encrypted, attached as an HTML file to the outgoing email, and sent.

## After Sending Message

To set expiration time after sending an 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 in the email list for which you want to set the expiration time. This will enable the lock and expire icons.

**Step 3** Tap the Android Menu button, then tap **Message Settings**.

**Step 4** Tap **Expiration**. The New Expiry Date screen displays. If the message is already set to expire, the current expiry date is displayed.

**Step 5** Select the expiration date and time that the email will expire.

**Step 6** Tap **Set** to save the changes. A message displays confirming the date and time that the message will expire.
Clear Expiration Date and Time

To clear the expiration date and time after sending an 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 in the email list for which you want to clear the expiration time.
This will enable the lock and expire icons.

**Step 3** Tap the Android Menu button, then tap **Message Settings**.

**Step 4** Tap **Expiration**. The New Expiry Date screen displays and shows the current expiry date.

**Step 5** Set the **Set Expiration** switch to **On**.

**Step 6** Tap **Done** to save the changes.

Manage Sent Secure Messages

To view a list of the encrypted emails sent from your Android device, tap *account name* > **Manage Messages**. Check the email messages you want to view from the list of sent encrypted emails. Tap the selected messages to display the following information:

- **Subject**. Subject of the message.
- **Date**. Date the message was sent.
- **To**. Email address of the recipient.
- **From**. Email address of the sender.

You can update all messages and recipients from the server by making a pull-down gesture.

You can use the Manage Massages 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 Massages also enables you to delete, lock, or expire a message, or view its details.

You can perform the following actions on 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 1-17.

- **Set Expiration**. An expiration time can be set for encrypted email. See Set an Email Expiration Time, page 1-18.

To set the following information, tap the Lock or Expire icon:

- **Open Date**. Date on which the secure message was opened by the respective recipient. This is displayed only on Android tablets.

- **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.
Options Available Only in 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 from the drop-down list. To set the account that will be used as the default account in the **Encrypt with** field, tap the Android Menu button > Settings > 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 Message Settings screen. To access Message Settings, tap the Android Menu button. Then tap **Message Settings**.

**Note** When composing a secure message on Android devices, you can add attachments.

**Step 5** When the message is complete, tap **Send Secure**. From the menu options, select the third-party email system to complete the action. For example, select Android email.

**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 Android device when the sent email is opened by the recipient.

**Default Settings**

To request a read-receipt (default settings):

**Step 1** On smartphones, tap **Settings > account name**; or on tablets, tap **account name > account name**.

**Step 2** Set the **Read Receipt** switch to On. This is enabled by default.
Email Encryption Options Available by Configuration Mode

Chapter 1      Configuring and Using Cisco Business Class Email for Android

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  Complete the appropriate fields:
  - Address (To, CC, and BCC)
  - Subject
Step 3  Enter the message text.
Step 4  Tap the Android Menu button, then tap Message Settings.
Step 5  Set the Read Receipt switch to On.
Step 6  Tap the back button to exit the Message Settings screen and return to the secure email.

Message Settings

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

To change the Message Settings:

Step 1  Tap the Secure Compose icon to open the Secure Compose screen.
Step 2  Complete the appropriate fields:
  - Address (To, CC, and BCC)
  - Subject
Step 3  Enter the message text.
Step 4  To access Message Settings, tap the Android Menu button, then tap Message Settings.
Step 5  Tap to enable or disable the applicable message options:
  - Expiration
  - Read Receipt
  - Reply
  - Reply All
  - Forward
  - Message Security
Step 6  Your changes are saved automatically.
Message Security

To specify the security level for sent encrypted message, tap **Settings > account name** on Android devices; or tap **account name > account name** on tablets.

The following message security levels 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 level of high is set for all messages. The default can be overridden for a specific message by modifying the value in Message Settings. See Options Available Only in Encrypt Mode, page 1-21.

Cache Management

Cache Passwords

The Cisco BCE registered account password is cached for a time period that can be configured by tapping **Settings > account name > Remember Password**. 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 by tapping **Settings > account name > Clear Password**. 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 message when you open the same secure message 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. By default, the cache envelope size is 6 MB. Envelopes are deleted from the 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 message 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 or Yahoo 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 Settings and turn off the Save sent message option.
Troubleshooting Using the Diagnostic Tool

This functionality is available if you have decrypted at least one secure message. The Cisco BCE application has a diagnostic tool to help with troubleshooting problems. You can use the diagnostic tool when 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 generates on the device when you work with the encryption application.

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 Business Class Email 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 Business Class Email Application

To uninstall Cisco BCE on the Android:

**Step 1**  Go to the Android home screen.
**Step 2**  Tap Settings.
**Step 3**  Tap Apps > Cisco BCE.
**Step 4**  Tap Uninstall, then tap OK.

The application is removed.

Customer Support

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