



Cisco Business Class Email 1.0 Administrator Guide - For Mobile Devices

Revised: November 09, 2012

Published: June 2012

Americas Headquarters

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

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

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

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

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

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

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)



CONTENTS

CHAPTER 1

Getting Started with Cisco Business Class Email 1-1

- Related Documents 1-2
- How to Use This Guide 1-2
 - How This Book is Organized 1-3
 - Where to Find More Information 1-3
 - Cisco Support Community 1-3
 - Cisco IronPort Customer Support 1-3
 - Third Party Contributors 1-4
 - Cisco IronPort Welcomes Your Comments 1-4

CHAPTER 2

Overview 2-1

- Downloading the Cisco Business Class Email Application 2-1
- Supported Operating Systems 2-2
- Licensing Versions and Configuration Modes 2-2
- Administrator Configuration Settings for the BCE Application 2-3
 - Creating a Configuration File for Each End User 2-3
 - Sending the Configuration File to the End User 2-4

CHAPTER 3

Configuring and Using Cisco Business Class Email for iOS 3-1

- Installing the Cisco Business Class Email Application 3-1
- Opening Cisco Business Class Email for iOS 3-1
 - Application Landing Screen 3-2
- Launching the Cisco Business Class Email Configuration File 3-3
- Configuring Settings for Cisco Business Class Email 3-3
- Email Encryption Options Available by Configuration Mode 3-5
 - Options Available in Decrypt Only Mode 3-6
 - Opening an Encrypted Email - New Message 3-6
 - Opening an Encrypted Email - Previously Opened Message 3-8
 - Options Available in Decrypt and Flag Mode 3-8
 - Opening an Encrypted Email - New Message 3-8
 - Opening an Encrypted Email - Previously Opened Message 3-10
 - Flagging an Email for Encryption 3-10
 - Options Available in Decrypt and Encrypt Mode 3-12
 - Opening an Encrypted Email - New Message 3-12

Opening an Encrypted Email - Previously Opened Message	3-14
Sending an Encrypted Email	3-14
Reply/Reply All/Forward an Email	3-15
Lock or Unlock an Encrypted Email	3-16
Set an Email Expiration Time	3-17
Receive a Read-Receipt	3-19
Manage Sent Secure Messages	3-19
Envelope Settings	3-21
Message Sensitivity	3-22
Cache Management	3-22
Cache Passwords	3-22
Secure Envelope Caching	3-22
Troubleshooting Using the Diagnostic Tool	3-23
Data Collected by the Diagnostic Tool	3-23
BCE.txt Content	3-23
Device.txt Content	3-24
Config.txt Content	3-24
Running the Diagnostic Tool	3-24
Setting Log Levels	3-25
Upgrading the Cisco Business Class Email Application	3-26
Uninstalling the Cisco Business Class Email Application	3-26

CHAPTER 4

Configuring and Using Cisco Business Class Email for Android 4-1

Installing the Cisco Business Class Email Application	4-1
Opening Cisco Business Class Email for Android Application	4-1
Application Landing Screen	4-1
Launching the Cisco Business Class Email Configuration File	4-3
Configuring Settings for Cisco Business Class Email	4-4
Email Encryption Options Available by Configuration Mode	4-6
Options Available in Decrypt Only Mode	4-7
Opening an Encrypted Email - New Message	4-7
Opening an Encrypted Email - Previously Opened Message	4-9
Options Available in Decrypt and Flag Mode	4-9
Opening an Encrypted Email - New Message	4-9
Opening an Encrypted Email - Previously Opened Message	4-11
Flagging an Email for Encryption	4-11
Options Available in Decrypt and Encrypt Mode	4-13
Opening an Encrypted Email - New Message	4-13

Opening an Encrypted Email - Previously Opened Message	4-15
Sending an Encrypted Email	4-15
Reply/Reply All/Forward an Email	4-16
Lock or Unlock an Encrypted Email	4-17
Set an Email Expiration Time	4-18
Receive a Read-Receipt	4-19
Manage Sent Secure Messages	4-20
Envelope Settings	4-22
Message Sensitivity	4-23
Cache Management	4-23
Cache Passwords	4-23
Secure Envelope Caching	4-23
Troubleshooting Using the Diagnostic Tool	4-24
Data Collected by the Diagnostic Tool	4-24
BCE.txt Content	4-24
Device.txt Content	4-25
Config.txt Content	4-25
Running the Diagnostic Tool	4-25
Setting Log Levels	4-25
Upgrading the Cisco Business Class Email Application	4-26
Uninstalling the Cisco Business Class Email Application	4-26

APPENDIX A

IronPort End User License Agreement A-27

Cisco IronPort Systems, LLC Software License Agreement	A-27
--	------



CHAPTER 1

Getting Started with Cisco Business Class Email

The Cisco Business Class Email (BCE) plug-in mobile application provides the ability to encrypt and decrypt messages directly from your Apple iOS® and Google Android™.

With the proliferation of smartphone devices, end users are always connected to their business and personal networks. Enterprise mobile workers are constantly “on the go” and need to stay connected and on top of their work obligations. Furthermore, mobile workers utilize their free time to access and respond to email.

Due to compliance reasons and corporate policies, increasing numbers of important email messages are encrypted. Recipients do not want to wait until they are on a laptop to access their email messages. End users want a seamless experience between their laptop and mobile devices. As a result, many organizations are demanding a consistent experience across all the devices, computer and smartphones, used by their end users for encrypted messages. To meet this demand, Cisco introduces Business Class email, a solution for sending encrypted email from smartphones.

Cisco Business Class Email provides enhanced security and reliable controls for traditional email tools. It is fully integrated in the most common email technologies and into a end user's daily email routine. The three components of Business Class Email are confidentiality, seamless end user authentication, and enhanced email controls.

- **Confidentiality**—The Cisco Business Class Email solution is based on robust email encryption technology that uses the most reliable encryption algorithms available. Our solution not only encrypts the data to protect its confidentiality while it travels through the network but also applies the latest authentication mechanism to make the access to the encryption key easy and secure.
- **Enhanced email controls**—Secure messaging enables Cisco to provide new email controls for end users. Encrypted emails not only ensure that the information sent remains confidential but also enable the sender to expire or recall an email and know exactly when it was opened. The specific features are described below.
 - **Read receipt**—When a recipient opens a message (successfully authenticated and received the encryption key), Cisco ensures that the information was read and delivers a read receipt to the sender within seconds.
 - **Message expiration**—Enables the sender to set an expiration date to the message. After the expiration date has passed, the encryption key will be disposed of, making the information inaccessible.
 - **Control over forward/reply**—Provides advanced controls over what can be done to an email message once it has been received. Forward/Reply/Reply All can be disabled or enabled only if the sender's company or administrator authorizes it.

In addition, the Business Class Email solution removes the complexity of encryption and key management, enabling end users to send and received secure messages as easily as unencrypted emails.

Related Documents

To use BCE, you need a key server, which can be the Cisco Registered Envelope Service (CRES), or a Cisco IronPort Email Security appliance (ESA) when using flag encryption. If you use a Cisco IronPort Encryption appliance (IEA) as your key server, you'll need to have a CRES administrator account created for you before you begin. See [Administrator Configuration Settings for the BCE Application, page 2-3](#).

To understand how to configure the Cisco IronPort Encryption appliance, you may want to review the following guides:

- *Cisco IronPort Cisco Registered Envelope Service 4.1 Account Administrator Guide*. This guide provides information about Cisco Registered Envelope Service (CRES) that provides support for Cisco IronPort Encryption technology. It also contains information about deploying the Cisco Business Class Email plug-ins, or mobile application, by sending a signed configuration file. This guide can be accessed from a link within the CRES software.
- *IronPort Encryption Appliance Installation Guide*. This guide provides instructions for installing and configuring email encryption, and it may help you to understand how to configure your encryption appliance settings to work with the plug-in settings you configure. This guide can be accessed from the following URL:

http://www.cisco.com/en/US/docs/security/iea/iea6.5/IEA_Configuration_Manual_v6.5.pdf

How to Use This Guide

Use this guide as a resource to learn about the features in your Cisco BCE application. The topics are organized in a logical order, but you might not need to read every chapter in the book. Review the Table of Contents and the section called [How This Book is Organized, page 1-3](#) to determine which chapters are relevant to your smartphone and particular configuration.

How This Book is Organized

[Chapter 1, “Getting Started with Cisco Business Class Email”](#) provides an introduction to the Cisco BCE application.

[Chapter 2, “Overview”](#) is an overview of the Cisco BCE application, supported smartphone devices, and the administrator configuration settings for the Cisco BCE end user accounts.

[Chapter 3, “Configuring and Using Cisco Business Class Email for iOS”](#) provides instructions for installing the Cisco BCE application on the Apple iOS and describes the email encryption options available in the configuration modes. It includes steps for configuring the application settings and features such as sending encrypted emails, locking or expiring emails, and receiving a read-receipt notification.

[Chapter 4, “Configuring and Using Cisco Business Class Email for Android”](#) provides instructions for installing the Cisco BCE application on the Google Android and describes the email encryption options available in the configuration modes. It includes steps for configuring the application settings and features such as sending encrypted emails, locking or expiring emails, and receiving a read-receipt notification.

[Appendix A, “Cisco IronPort Systems, LLC Software License Agreement”](#) contains detailed information about the licensing agreements for Cisco IronPort products.

Where to Find More Information

Cisco IronPort offers the following resources to learn more about Cisco Business Class Email and Cisco security products.

Cisco Support Community

Cisco Support Community is an online forum for Cisco customers, partners, and employees. It provides a place to discuss general email and web security issues, as well as technical information about specific Cisco products. You can post topics to the forum to ask questions and share information with other Cisco and Cisco IronPort end users.

You access the Cisco Support Community at the following URL:

<https://supportforums.cisco.com>

Cisco IronPort Customer Support

You can request our support by phone, email, or online 24 hours a day, 7 days a week.

**Note**

The level of support available to you depends upon your service level agreement. Cisco IronPort Customer Support service level agreement details are available on the Support Portal. Check this website for details about your level of support.

To report a critical issue that requires urgent assistance outside of Customer Support hours, contact Cisco IronPort using one of the following methods:

U.S. Toll-free: 1 (877) 646-4766

Support Site: <http://www.cisco.com/web/ironport/index.html>

If you purchased support through a reseller or another supplier, please contact that supplier directly with your product support issues.

Third Party Contributors

Some software included with Cisco BCE is distributed under the terms, notices, and conditions of software license agreements of Apple iOS and Google Android. All such terms and conditions are incorporated in IronPort license agreements.

Cisco IronPort Welcomes Your Comments

The Cisco IronPort Technical Publications team is interested in improving the product documentation. Your comments and suggestions are always welcome. You can send comments to the following email address:

docfeedback@ironport.com



CHAPTER 2

Overview

The Cisco Business Class Email (BCE) mobile application provides the end user the ability to receive and send encrypted email messages directly from their iOS and Android smartphone devices.

Depending on the configuration mode of the Cisco BCE mobile application, the following tasks can be performed:

- Open an encrypted email on the smartphone using Cisco BCE
- Send an encrypted email from the smartphone using Cisco BCE
- Manage the secure emails sent from the smartphone using Cisco BCE
- Lock/unlock an encrypted email sent from the smartphone using Cisco BCE
- Set or modify an expiration date for an encrypted email sent from the smartphone using Cisco BCE
- Receive a read receipt for encrypted email sent from the smartphone using Cisco BCE
- Check or modify encrypted email options from the smartphone

This chapter includes the following sections:

- [Downloading the Cisco Business Class Email Application, page 2-1](#)
- [Supported Operating Systems, page 2-2](#)
- [Licensing Versions and Configuration Modes, page 2-2](#)
- [Administrator Configuration Settings for the BCE Application, page 2-3](#)

Downloading the Cisco Business Class Email Application

The Cisco Business Class Email application, *Cisco BCE*, can be downloaded directly to the smartphone from the Apple App Store and from Google Play.

Supported Operating Systems

The *Cisco Encryption Compatibility Matrix* lists the supported operating systems for Cisco BCE and can be accessed from the following URL:

http://www.cisco.com/en/US/docs/security/iea/Compatibility_Matrix/IEA_Compatibility_Matrix.pdf

Licensing Versions and Configuration Modes

The Cisco Business Class Email application is deployed in three separate licensing versions that determine the configuration mode for the application. The default configuration mode for the Cisco BCE application is Decrypt Only and can be downloaded from the Apple App Store and from Google Play.

In order to enable the other versions and configuration modes, the smartphone device is configured by an updated attachment file received from the administrator. The administrator sends a *BCE_Config_signed.xml* file attachment to the end user's email account. The end user will receive this file as a *securedoc.html* file. When the end user clicks the *securedoc.html* attachment, the currently installed application detects the configuration information attached to the message and applies the updated configuration.

The three licensing versions and configuration modes are:

- **Decrypt Only**—Allows decrypting of secure email messages received.
- **Decrypt and Flag**—Allows decrypting and flagging of secure emails messages. The flag option allows the end user to flag the email for encryption, and the email is encrypted by the Cisco IronPort Encryption appliance or Email Security appliance before the email is sent out of the network. The server must be configured to detect the flagged messages and encrypt them at the server.
- **Decrypt and Encrypt**—Allows encrypting and decrypting of secure email messages.

The following table specifies which features are supported in each configuration mode.

Feature	Decrypt Only	Decrypt and Flag	Decrypt and Encrypt
Send encrypted message			X
Flag message for encryption		X	
Open encrypted email	X	X	X
Reply/Reply All/Forward Message			X
Email lock and unlock			X
Email expiration			X
Email diagnostic (Error/Log reporting)	X	X	X
Read-receipt			X
Envelope settings			X
Settings	X	X	X
Sent items			X

Administrator Configuration Settings for the BCE Application

To deploy the Cisco BCE plug-in mobile application, you will need to create a configuration file for each end user, using the provided configuration template. Then send the signed configuration file to the end user.

The default configuration mode, Decrypt Only, does not require a signed configuration file. But in order to enable the other two configuration modes, Flag mode and Encrypt, the end user must receive and launch the signed configuration file for the BCE application to be reconfigured.

Cisco Registered Envelope Service (CRES) is a hosted service that provides support for Cisco IronPort Encryption technology. Recipients of encrypted messages authenticate themselves with the service to receive decryption keys. You must be a CRES account administrator to complete the following steps.

Creating a Configuration File for Each End User

**Note**

If you use a Cisco IronPort appliance as your key server, you'll need to have a CRES administrator account created for you before you begin. Contact Cisco IronPort Customer Support at a t: <http://www.cisco.com/web/ironport/index.html>

To create a signed configuration file for each end user:

-
- Step 1** Log into your CRES account: <https://res.cisco.com/admin>. The Administration Console displays.
- Step 2** To sign and deploy the BCE Configuration file, go to the **Accounts** tab and select the account from which you want to enable the BCE mobile application. Then, go to the **BCE Config** tab.
- Step 3** Choose the token to use with the configuration template. There are two Token Types:
- **CRES**—Select if your key server is CRES.
 - **SecureCompose**—Do not choose this option as your CRES token.
 - **Token <Account number>**—Choose this option as your CRES token.
 - **IEA**—Select if your key server is a Cisco IronPort Encryption appliance.
 - **Browse**—Click to browse to locate and upload your IEA token file.
- Step 4** Click **Download Template** to download the template file in order to edit it. The filename is *BCE_Config.xml*.
- Step 5** Edit the configuration file.
- The *BCE_Config.xml* file contains detailed instructions for the fields you will need to edit based on your particular environment. Open the file in a text editor and follow the instructions included in the comments to make the necessary modifications.
- Step 6** Click **Browse** to navigate to the edited *BCE_Config.xml* file, and click **Upload and Sign** after you have located the file.
- Once the configuration file is signed, the signed version will be downloaded as *BCE_Config_signed.xml*. Save this file to your local machine.
-

Sending the Configuration File to the End User

-
- Step 1** As a CRES admin, logged into CRES, use the Secure Compose page to compose an encrypted email.
- Step 2** Browse your local machine and locate the *BCE_Config_signed.xml* file that you created in the previous procedure.
- Step 3** Attach the *BCE_Config_signed.xml* file to the encrypted email. The end user will receive this file as a *securedoc.html* file.
- Step 4** Send the encrypted email to the end user's email account for which you want to enable BCE.
- When the end user opens the attachment from their email on their device, this automatically configures the Cisco BCE application.

**Note**

The sender email must be same as the account administrator who signed the *BCE_Config.xml* file.

**Note**

Do not send the *BCE_Config_signed.xml* file to a mailing list. CRES does not support mailing lists.



CHAPTER 3

Configuring and Using Cisco Business Class Email for iOS

- [Installing the Cisco Business Class Email Application, page 3-1](#)
- [Opening Cisco Business Class Email for iOS, page 3-1](#)
- [Launching the Cisco Business Class Email Configuration File, page 3-3](#)
- [Configuring Settings for Cisco Business Class Email, page 3-3](#)
- [Email Encryption Options Available by Configuration Mode, page 3-5](#)
- [Message Sensitivity, page 3-22](#)
- [Cache Management, page 3-22](#)
- [Troubleshooting Using the Diagnostic Tool, page 3-23](#)
- [Upgrading the Cisco Business Class Email Application, page 3-26](#)
- [Uninstalling the Cisco Business Class Email Application, page 3-26](#)

Installing the Cisco Business Class Email 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. See [Supported Operating Systems, page 2-2](#).

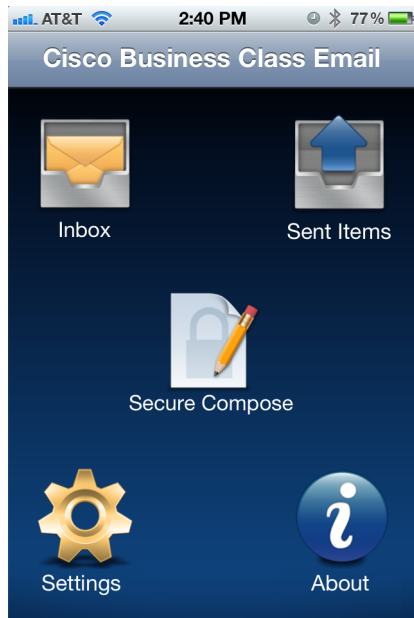
Opening Cisco Business Class Email for iOS

After the Cisco BCE application is successfully installed on the iOS, you will see a new *Cisco BCE* application icon. To open the application, tap the **Cisco BCE** icon from the iOS home screen. Starting the application adds the necessary menus to the device that allow end users to send and receive encrypted emails.

Application Landing Screen

Tap the **Cisco BCE** icon to open the application landing screen. Depending on the configuration mode, some of the icons on this screen are dimmed, indicating unavailable. See [Licensing Versions and Configuration Modes, page 2-2](#).

Cisco BCE landing screen:



The following options are available:

Option	Description
Inbox	Lists email accounts for which encrypted emails were opened on the device. Tap the individual email account or All Email Accounts to display a list of decrypted emails opened for the selected account. The list of email accounts is not shown if encrypted messages have been opened for a single email address.
Sent Items	Lists email accounts from which encrypted emails were sent from the device. Tap the individual email account or All Email Accounts to display a list of emails encrypted and sent from the selected account. The list of email accounts is not shown if encrypted messages have been sent from a single email address.
Secure Compose	Launches screen to compose a secure message. See Sending an Encrypted Email, page 3-14 .
Settings	Launches the configuration screen for general settings for the application. See Configuring Settings for Cisco Business Class Email, page 3-3 .
About	View the About information for the Cisco BCE application.

Launching the Cisco Business Class Email Configuration File

The Cisco BCE application must be open and running prior to opening the *BCE_Config_signed.xml* attachment from the end user's email account.

To enable and configure the BCE application:

-
- Step 1** As a CRES administrator, logged into CRES, the administrator uses the Secure Compose screen to compose and send the *BCE_Config_signed.xml* file to the end user's email account. The end user will receive this file as a *securedoc.html* file.
- Step 2** The end user receiving the *securedoc.html* file opens the attachment from their email on their iPhone device. This automatically configures the Cisco BCE application installed in the previous procedure [Installing the Cisco Business Class Email Application, page 3-1](#).

**Note**

If the end user does not see the encrypted email in their inbox, check the spam or junk folder.

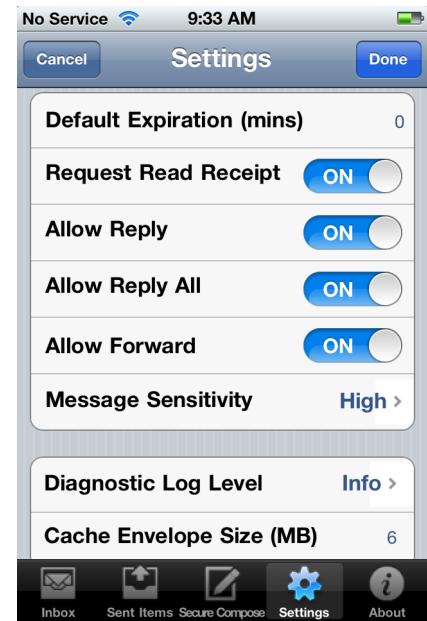
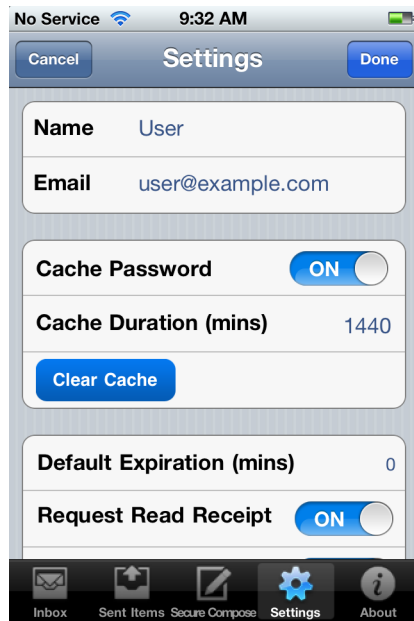
- If the end user does not have a Cisco CRES registered account, they are prompted to register.
 - Complete the **New User Registration** form and click **Register**. Then the end user checks their inbox for the account activation email.
 - From the account activation email, the end user clicks the **Click here to activate this account** link. A message indicates that the account activation is confirmed and the end user can now view encrypted emails sent to the registered email address.
 - Return to the original email with the HTML attachment. Tap and hold the attachment. Depending on the screen display, the end user will tap either **Open in “Cisco BCE”** or tap **Open In...> Open in “Cisco BCE.”**

- Step 3** When prompted, the end user accepts the configuration to complete this procedure.
-

Configuring Settings for Cisco Business Class Email

General email security options can be configured from the Settings screen. To access these settings, tap **Cisco BCE > Settings**. Depending on the end user's configuration mode, some of the options are not available for configuration by the end user. See [Licensing Versions and Configuration Modes, page 2-2](#).

Settings screen:



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

Option	Description
Name	Name submitted for Cisco BCE registered account.
Email	Email submitted for Cisco BCE registered account.
Cache Password	By default, this option is enabled to ensure that the encryption password is cached. If you clear the cache, you need to re-enter the password at the next login.
Cache Duration (mins)	Enter the cache duration in minutes. The default is 1440 minutes.
Clear Cache	Tap to immediately clear the cache. The cache is automatically cleared when the device is shut down or restarted.
Default Expiration (mins)	Enter the default expiration time in minutes. This option specifies how long the encrypted email message remains valid. After the number of expiry minutes is met, the message expires, and it cannot be opened by the recipient after this period.
Request Read Receipt	By default, this option is enabled to request a default read-receipt notification to the sender when the recipient opens the encrypted message.
Allow Reply	By default, this option is enabled to specify that an encrypted message that is replied to is automatically encrypted.
Allow Reply All	By default, this option is enabled to specify that an encrypted message is automatically encrypted when you reply to all of the recipients.
Allow Forward	By default, this option is enabled to specify that an encrypted message that is forwarded is automatically encrypted.

Option	Description
Message Sensitivity	By default, the message sensitivity is set to High. The other options from the drop-down list are Medium and Low.
Diagnostic Log Level	Set the type of logs being maintained by the application by defining the log level. See Setting Log Levels, page 3-25 .
Cache Envelope Size (MB)	The downloaded secure envelopes are cached on the device after they are opened for the first time. By default, this number is set to 6 MB.
Save Draft	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.

Email Encryption Options Available by Configuration Mode

The Cisco BCE application is deployed in three 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 2-2](#). The option of opening an encrypted email is available in all three configuration modes.

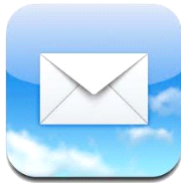
The following sections describe the email encryption options in each of the three configuration modes:

- [Options Available in Decrypt Only Mode, page 3-6](#)
 - [Opening an Encrypted Email - New Message, page 3-6](#)
 - [Opening an Encrypted Email - Previously Opened Message, page 3-8](#)
- [Options Available in Decrypt and Flag Mode, page 3-8](#)
 - [Opening an Encrypted Email - New Message, page 3-8](#)
 - [Opening an Encrypted Email - Previously Opened Message, page 3-10](#)
 - [Flagging an Email for Encryption, page 3-10](#)
- [Options Available in Decrypt and Encrypt Mode, page 3-12](#)
 - [Opening an Encrypted Email - New Message, page 3-12](#)
 - [Opening an Encrypted Email - Previously Opened Message, page 3-14](#)
 - [Sending an Encrypted Email, page 3-14](#)
 - [Reply/Reply All/Forward an Email, page 3-15](#)
 - [Lock or Unlock an Encrypted Email, page 3-16](#)
 - [Set an Email Expiration Time, page 3-17](#)
 - [Receive a Read-Receipt, page 3-19](#)
 - [Manage Sent Secure Messages, page 3-19](#)
 - [Manage Sent Secure Messages, page 3-19](#)
 - [Envelope Settings, page 3-21](#)

**Note**

There are numerous mail applications that can be used with the iPhone, such as the Google Gmail mail application but currently Cisco BCE only integrates with the native mail application that is provided with the phone. An example of the iPhone mail icon follows and the icon usually appears on the first screen of the iPhone.

Example of iPhone mail icon:



Options Available in Decrypt Only Mode

The default configuration mode for the Cisco BCE application is Decrypt Only and this version can be downloaded from the Apple App Store. In Decrypt Only mode, end users can receive and open encrypted messages, but they cannot send them.

Opening an Encrypted Email - New Message

The Cisco BCE application enables you to open an encrypted email message directly from your iOS email client.

- Cisco BCE detects that the message is encrypted and requests the end user to enter the Cisco BCE registered account credentials to decrypt the message.
- After the end user enters the correct username and password, Cisco BCE downloads the envelope and displays the decrypted message on the smartphone device.

To open a new encrypted message:

Step 1 Start the email client on the iOS device.

Step 2 Tap the encrypted email from the email list view and open it.

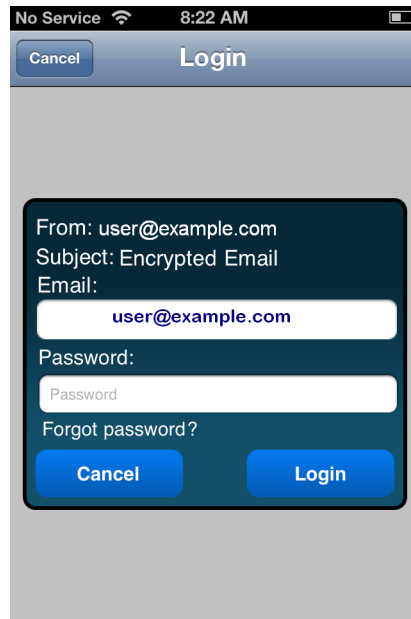
**Note**

If you do not see the encrypted email in their inbox, check the spam or junk folder.

Step 3 Browse to the HTML attachment in the email. Tap and hold the HTML attachment until menu options appear.

Step 4 Depending on the screen display, tap either **Open in “Cisco BCE”** or tap **Open In...> Open in “Cisco BCE.”** The Login screen displays.

Login screen:



- If the end user does not have a Cisco CRES registered account, they are prompted to register.
 - Complete the **New User Registration** form and click **Register**. Then the end user checks their inbox for the account activation email.
 - From the account activation email, the end user clicks the **Click here to activate this account** link. A message indicates that the account activation is confirmed and the end user can now view encrypted emails sent to the registered email address.
 - Return to the original email with the HTML attachment. Tap and hold the attachment. Depending on the screen display, the end user will tap either **Open in “Cisco BCE”** or tap **Open In...> Open in “Cisco BCE.”**
- If multiple email addresses exist for the end user:
 - From the drop-down list, select the applicable email address and enter the password from your Cisco BCE registered account.
- If the email address and password were entered earlier to open encrypted email, then this information is cached and the Login screen is not displayed.

Step 5 Tap **Login**. The secure email is decrypted and the message is displayed.



Note

The default maximum file size of attachments that can be download to the iPhone device is dependent on their mail server and device hardware.

Opening an Encrypted Email - Previously Opened Message

After a message has been opened, the email will be in the inbox of the Cisco BCE application, and can be opened again from the Cisco BCE inbox.

To reopen an encrypted message:

-
- Step 1** Tap **Cisco BCE > Inbox** to open the inbox email accounts screen.
- Step 2** Tap **All Email Accounts** or a specific email address. A list of the decrypted emails for the selected account displays.
- Step 3** Tap the encrypted email from the email list to open it.
- If the email address and password are not cached, the Login screen displays. Select the email address, enter the password from the Cisco BCE registered account, and tap **Login**.
 - If the email address and password are cached, the Login screen is not displayed.

The decrypted message is displayed.

Options Available in Decrypt and Flag Mode

The Decrypt and Flag mode allows decrypting and flagging of secure email messages. The flag option allows the end user to flag the email for encryption, and the email is encrypted by the Cisco IronPort Encryption appliance or Email Security appliance before the email is sent out of the network. The server must be configured to detect the flagged messages and encrypt them at the server.

In order to enable the Decrypt and Flag mode, the smartphone device is configured by an updated *BCE_Config_signed.xml* file received from the administrator. These options are available after the end user receives and launches the *BCE_Config_signed.xml* file in their smartphone email account.

Opening an Encrypted Email - New Message

The Cisco BCE application enables you to open an encrypted email message directly from your iOS email client.

- Cisco BCE detects that the message is encrypted and requests the end user to enter the Cisco BCE registered account credentials to decrypt the message.
- After the end user enters the correct username and password, Cisco BCE downloads the envelope and displays the decrypted message on the smartphone device.

To open a new encrypted message:

-
- Step 1** Start the email client on the iOS device.
- Step 2** Tap the encrypted email from the email list view to open it.



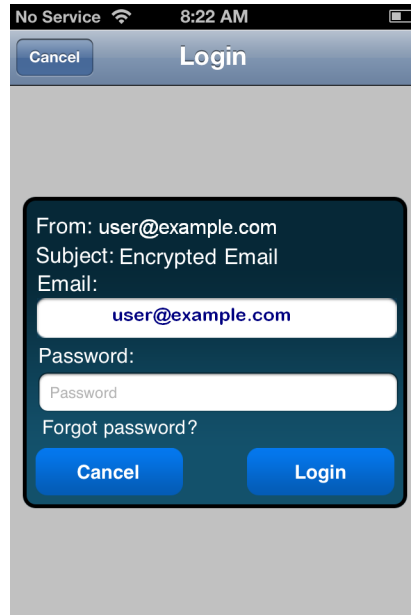
Note

If you do not see the encrypted email in their inbox, check the spam or junk folder.

- Step 3** Browse to the HTML attachment in the email. Tap and hold the HTML attachment until menu options appear.

- Step 4** Depending on the screen display, tap either **Open in “Cisco BCE”** or tap **Open In...> Open in “Cisco BCE.”** The Login screen displays.

Login screen:



- If the end user does not have a Cisco CRES registered account, they are prompted to register.
 - Complete the **New User Registration** form and click **Register**. Then the end user checks their inbox for the account activation email.
 - From the account activation email, the end user clicks the **Click here to activate this account** link. A message indicates that the account activation is confirmed and the end user can now view encrypted emails sent to the registered email address.
- If multiple email addresses exist for the end user:
 - From the drop-down list, select the applicable email address and enter the password from your Cisco BCE registered account.
- If the email address and password were entered earlier to open encrypted email, then this information is cached and the Login screen is not displayed.

- Step 5** Tap **Login**. The secure email is decrypted and the message is displayed.



Note

The default maximum file size of attachments that end users can download to their iPhone device is dependent on their mail server and their device hardware.

Opening an Encrypted Email - Previously Opened Message

After a message has been opened, the email will be in the inbox of the Cisco BCE application, and can be opened again from the Cisco BCE inbox.

To reopen an encrypted message:

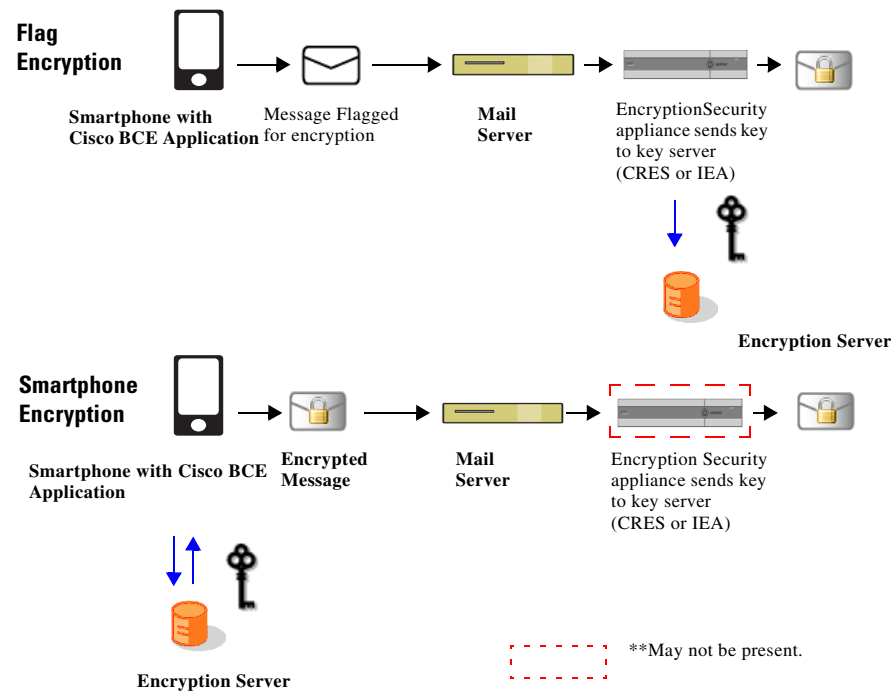
-
- Step 1** Tap **Cisco BCE > Inbox** to open the inbox email accounts screen.
- Step 2** Tap **All Email Accounts** or a specific email address. A list of the decrypted emails for the selected account displays.
- Step 3** Tap the encrypted email from the email list to open it.
- If the email address and password are not cached, the Login screen displays. Select the email address, enter the password from the Cisco BCE registered account, and tap **Login**.
 - If the email address and password are cached, the Login screen is not displayed.

The decrypted message is displayed.

Flagging an Email for Encryption

The Flag Encryption option allows the end user to flag the email for encryption, and the email is encrypted by the Cisco IronPort Encryption appliance (IEA) or Email Security appliance (ESA) before the email is sent out of the network. The server must be configured to detect the flagged messages and encrypt them at the server. All of the encryption options, such as requesting a read receipt or enabling secure forward, are set at the server.

The following figure illustrates how the secure email flows from the smartphone device to the internal mail server, flagged, then sent out of the network. It also compares the flag encryption workflow with encryption directly on the smartphone device.

Figure 3-1 Workflows for Flag Encryption versus Smartphone Encryption

To flag an email for encryption:

-
- Step 1** Tap **Cisco BCE > Secure Compose** to open the Secure Compose screen.
- Step 2** By default, the email address for the registered email account is added in the From field.
- Complete the appropriate fields:
- Address (To, CC, and BCC)
 - Subject
- 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 **Options** icon located at top right of screen, then tap **Envelope Settings**.

**Note**

When composing a secure message on the iPhone, you cannot add attachments.

-
- Step 5** When the message is complete, tap the **Options** icon in the upper-right corner and tap **Send Secure**.
- The subject of the email is modified before the message is sent. The new subject is one of the configuration options in the *BCE_Config.xml* file. For example, the subject can be modified to read “SECURE.”
-

Options Available in Decrypt and Encrypt Mode

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

In order to enable the Decrypt and Encrypt mode, the smartphone device is configured by an updated *BCE_Config_signed.xml* file received from the administrator. These options are available after the end user receives and launches the *BCE_Config_signed.xml* file in their smartphone email account.

Opening an Encrypted Email - New Message

The Cisco BCE application enables you to open an encrypted email message directly from your iOS email client.

- Cisco BCE detects that the message is encrypted and requests the end user to enter the Cisco BCE registered account credentials to decrypt the message.
- After the end user enters the correct username and password, Cisco BCE downloads the envelope and displays the decrypted message on the smartphone device.

To open a new encrypted message:

Step 1 Start the email client on the iOS device.

Step 2 Tap the encrypted email from the email list view to open it.

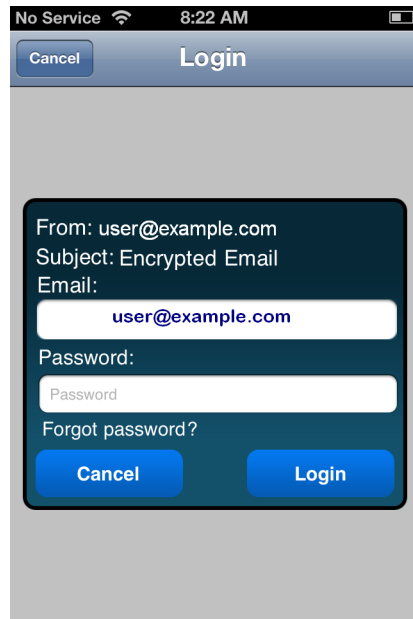


Note If you do not see the encrypted email in their inbox, check the spam or junk folder.

Step 3 Browse to the HTML attachment in the email. Tap and hold the HTML attachment until menu options appear.

Step 4 Depending on the screen display, tap either **Open in “Cisco BCE”** or tap **Open In...> Open in “Cisco BCE.”** The Login screen displays.

Login screen:



- If the end user does not have a Cisco CRES registered account, they are prompted to register.
 - Complete the **New User Registration** form and click **Register**. Then the end user checks their inbox for the account activation email.
 - From the account activation email, the end user clicks the **Click here to activate this account** link. A message indicates that the account activation is confirmed and the end user can now view encrypted emails sent to the registered email address.
- If multiple email addresses exist for the end user:
 - From the drop-down list, select the applicable email address and enter the password from your Cisco BCE registered account.
- If the email address and password were entered earlier to open encrypted email, then this information is cached and the Login screen is not displayed.

Step 5 Tap **Login**. The secure email is decrypted and the message is displayed.



Note

The default maximum file size of attachments that end users can download to their iPhone device is dependent on their mail server and their device hardware.

Opening an Encrypted Email - Previously Opened Message

After a message has been opened, the email will be in the inbox of the Cisco BCE application, and can be opened again from the Cisco BCE inbox.

To reopen an encrypted message:

-
- Step 1** Tap **Cisco BCE > Inbox** to open the inbox email accounts screen.
 - Step 2** Tap **All Email Accounts** or a specific email address. A list of the decrypted emails for the selected account displays.
 - Step 3** Tap the encrypted email from the email list to open it.
 - If the email address and password are not cached, the Login screen displays. Select the email address, enter the password from the Cisco BCE registered account, and tap **Login**.
 - If the email address and password are cached, the Login screen is not displayed.

The decrypted message is displayed.

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 **Cisco BCE > Secure Compose** to open the Secure Compose screen.
 - Step 2** By default, the email address for the registered email account is added in the From field.
Complete the appropriate fields:
 - Address (To, CC, and BCC)
 - Subject
 - 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 **Options** icon located at top right of screen, then tap **Envelope Settings**.

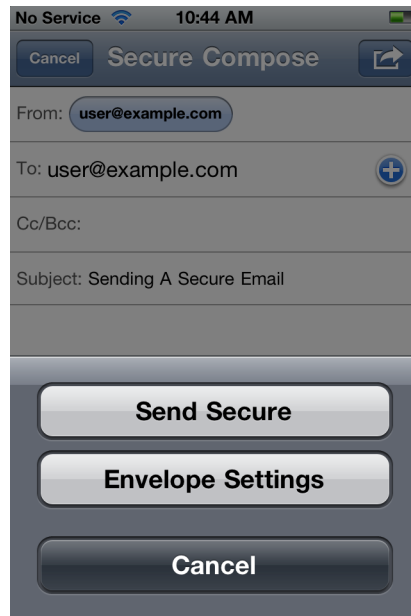


Note

When composing a secure message on the iPhone, you cannot add attachments.

- Step 5** When the message is complete, tap the **Options** icon located at top right of screen, then tap **Send Secure**. The email is encrypted, attached as an HTML to the outgoing email, and sent.

Secure Compose Options screen:



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 in the Settings screen for the encrypted email, applicable menu options are added to the smartphone 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 Business Class Email, page 3-3](#).



Note

To respond with a secure reply/reply all/forward, the smartphone device has to be able to send an encrypted message. These options are not available in the Decrypt Only mode. Also, the smartphone device needs to be able to send the encrypted email using the same server as the original message. For example:

- If you use the Cisco BCE application, encrypting email with CRES and receive a CRES secure message, you can reply to that message.
- If you use the Cisco BCE application, encrypting email with CRES and receive an IEA secure message, you cannot reply to that message because the plug-in mobile application would not have a token to communicate with the key server. In this instance, the menu options will not be available.

Replying to or forwarding an encrypted email:

-
- Step 1** Follow the steps for [Opening an Encrypted Email - Previously Opened Message, page 3-14](#) or [Sending an Encrypted Email, page 3-14](#).
- Step 2** Tap the **Options** icon located at top right of screen. 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** Tap **Send**.
-

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 **Cisco BCE > Sent Items**. The Cisco BCE Mailbox screen displays a list of email accounts from which encrypted emails were sent from the device. This screen is not displayed if encrypted emails have been sent from one email account.
- Step 2** Tap **All Email Accounts** or a specific email address. A list of the decrypted emails sent from the selected account is displayed.
- Step 3** Select the encrypted email that you want to lock from the email list. Tap the selected email to display the menu options.
- Step 4** Tap **Lock**. The login screen is displayed if the cache duration has expired.
- Step 5** Optionally, enter a reason for locking the message. The lock reason is displayed to recipients when they view the envelope. You may be asked to enter your Cisco BCE registered account email address and password.
- Step 6** 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 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 Cisco BCE > Sent Items . The Cisco BCE Mailbox screen displays a list of email accounts from which encrypted emails were sent from the device. This screen is not displayed if encrypted emails have been sent from one email account. |
| Step 2 | Tap All Email Accounts or a specific email address. A list of the decrypted emails sent from the selected account is displayed. |
| Step 3 | Select the encrypted email that you want to unlock from the email list. Tap the selected email to display the menu options. |
| Step 4 | 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 Setting

To set the default expiration interval:

-
- | | |
|---------------|--|
| Step 1 | Tap Cisco BCE > Settings to open the Settings screen. |
| Step 2 | In Default expiration (mins) , specify the number of minutes after which the email will expire. |
| Step 3 | Tap Done to exit and save the changes. |
-

Per Message Setting

To set expiration time for a specific email:

-
- | | |
|---------------|--|
| Step 1 | Tap Cisco BCE > Secure Compose to open the Secure Compose screen. |
| Step 2 | Enter the name and email address for the registered email account sending the encrypted message. Tap Apply . |
| Step 3 | When you have completed writing the message, tap the Options icon located at top right of screen, then tap Envelope Settings . |
| Step 4 | Tap Set Expiry . The New Expiry Date screen displays. |
| Step 5 | Select the expiration date and time that the email will expire. |
| Step 6 | Tap Set Expiry to save the changes. |
| Step 7 | Tap Done to exit the Envelope Settings screen and return to the secure email. |

- Step 8** Tap **Send** in the upper-right corner to display the menu options, then tap **Send Secure**.
- Step 9** The email is encrypted and displayed with the HTML attachment. Tap **Send**.
-

After Sending Message

To set expiration time after sending an email:

-
- Step 1** Tap **Cisco BCE > Sent Items**. The Cisco BCE Mailbox screen displays a list of email accounts from which encrypted emails were sent from the device. This screen is not displayed if encrypted emails have been sent from one email account.
- Step 2** Tap **All Email Accounts** or a specific email address. A list of the decrypted emails sent from the selected account is displayed.
- Step 3** Select the encrypted email that you want to set the expiration time from the email list. Tap the selected email to display the menu options. If the message is already set to expire, the current expiry date is displayed.
- Step 4** Tap **Set Expiry**. The New Expiry Date screen displays.
- Step 5** Select the expiration date and time that the email will expire.
- Step 6** Tap **Set Expiry** 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 **Cisco BCE > Sent Items**. The Cisco BCE Mailbox screen displays a list of email accounts from which encrypted emails were sent from the device. This screen is not displayed if encrypted emails have been sent from one email account.
- Step 2** Tap **All Email Accounts** or a specific email address. A list of the decrypted emails sent from the selected account is displayed.
- Step 3** Select the encrypted email that you want to clear the expiration from the email list. Tap the selected email to display the menu options.
- Step 4** Tap **Set Expiry**. The New Expiry Date screen displays and shows the current expiry date.
- Step 5** Tap **Clear Expiry**.
-

Receive a Read-Receipt

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

Default Setting

To request a read-receipt (default setting):

-
- Step 1** Tap **Cisco BCE > Settings** to open the Settings screen.
 - Step 2** Tap **Request Read Receipt**. This is enabled by default.
 - Step 3** Tap **Done** to exit and save the changes.
-

Per Message Setting

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

To request a read-receipt for a specific email:

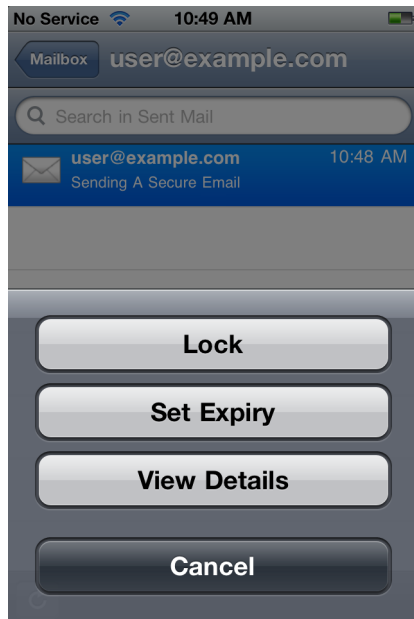
-
- Step 1** Tap **Cisco BCE > Secure Compose** to open the Secure Compose screen.
 - Step 2** Enter the name and email address for the registered email account sending the encrypted message. Tap **Apply**.
 - Step 3** When you have completed writing the message, tap the **Options** icon located at top right of screen, then tap **Envelope Settings**.
 - Step 4** Tap **Request Read Receipt** to enable this option.
 - Step 5** Tap **Done**.
-

Manage Sent Secure Messages

The Sent Items screen lists the encrypted emails sent from the smartphone.

To access, tap **Cisco BCE > Sent Items**. Select an email address and the email you want to modify or view from the list of sent encrypted emails. Tap the selected email to display the menu options.

Sent Items screen:



From Cisco BCE Mailbox, the following can be performed 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 3-16](#).
- **Set Expiry**—An expiration time can be set for encrypted email. See [Set an Email Expiration Time, page 3-17](#).
- **View Details**—View details of the encrypted email sent from the device.

Sent Email Message Details

From the Cisco BCE Mailbox, details of the encrypted emails sent from the device can be viewed. To access the Cisco BCE Mailbox, tap **Cisco BCE > Sent Items**. Select an email address and the email you want to view from the list of sent encrypted emails. Tap the selected email to display the menu options. Tap **View Details**.

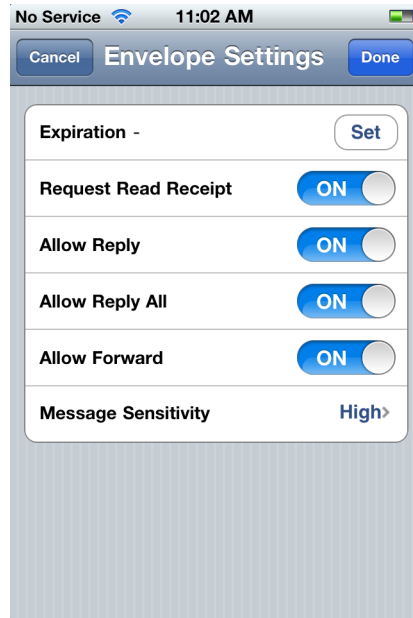
The following information is displayed:

- **Subject**—Subject of the message.
- **To**—Email address of the recipient.
- **Open Date**—Date on which the secure message was opened by the respective recipient.
- **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.
- **Expiration Date**—Expiration date for the encrypted email.

Envelope Settings

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

Envelope Settings screen:



To change the envelope settings:

-
- Step 1** Tap **Cisco BCE > Secure Compose** to open the Secure Compose screen.
 - Step 2** By default, the email address for the registered email account is added in the From field.
Complete the appropriate fields:
 - Address (To, CC, and BCC)
 - Subject
 - Step 3** Enter the message text.
 - Step 4** To access Envelope Settings, tap the **Options** icon located at top right of screen, then tap **Envelope Settings**.
 - Step 5** Tap to enable or disable the applicable message options:
 - Expiration
 - Request Read Receipt
 - Allow Reply
 - Allow Reply All
 - Allow Forward
 - Message Sensitivity
 - Step 6** Tap **Done** to save the changes.
-

Message Sensitivity

The sender can specify the sensitivity for the encrypted email from the **Cisco BCE > Settings** screen. The following message sensitivity options can be set:

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

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

**Note**

The administrator can define the minimum message sensitivity for the end user in the *BCE_Config.xml* file using the sensitivity options of high, medium, or low. After this is defined, the end user cannot set the message sensitivity below the minimum defined message sensitivity in the *BCE_Config.xml* file.

Cache Management

Cache Passwords

The Cisco BCE registered account password is cached for a time period that is configurable from the **Cisco BCE > Settings** screen. Password caching is On by default and the default cache time is 1440 minutes (24 hours). Caching of the password can be turned off from the Settings screen. Tap **Cache Password** to turn on or off, then and tap **Done** to save changes.

The password cache can be cleared from the **Cisco BCE > Settings** screen by tapping **Clear Cache**. The password cache is automatically cleared when the device is shut down or restarted.

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 the end user opens 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 6 MB. A task runs every 24 hours on the device and deletes any cached envelopes that are more than two weeks old.

Troubleshooting Using the Diagnostic Tool

The Cisco BCE application includes a diagnostic tool to help Cisco Support in troubleshooting problems. The administrator or the end user can use the diagnostic tool if receiving errors or if there are issues with the Cisco BCE application. The diagnostic tool can also be used to share critical information with Cisco engineers when reporting a bug.

The diagnostic tool is available from the About screen. See [Running the Diagnostic Tool, page 3-24](#).

Data Collected by the Diagnostic Tool

The diagnostic tool attaches the data collected to an email. The diagnostic email contains data information that is generated on the device during the end user's interaction with the encryption application. The diagnostic tool output includes the three files; *BCE.txt*, *device.txt*, and *config.txt*.



Note

A task runs every 24 hours on the device and deletes any logs that are more than one week old.

BCE.txt Content

The BCE.txt diagnostic tool file contains error, warning, information, and debug messages. When saving to the *BCE.txt* file, messages are prefixed with the following:

- **I**—Information messages
- **W**—Warning messages
- **E**—Error messages
- **D**—Debug log messages



Note

The level of log information collected is determined by the log level set in the configuration. See [Setting Log Levels, page 3-25](#).

The log content format is:

```
<Source> TAB <Log Category> TAB <Date Timestamp GMT> TAB <Log Message>
```

The table shows sample log content:

Sample Log Content			
BB	I	2011-05-13 12:31:24	Cisco BCE service started on device
BB	W	2011-05-13 12:32:37	Configuration for DecryptionNotification not defined
BB	E	2011-05-13 12:45:17	Timeout occurred
SDK	E	2011-09-07 16:38:48	EnvelopeBuilder :: finish setAlgorithm

Device.txt Content

The device.txt diagnostic tool file includes the following device information:

- **Device info**—Device ID, device name, platform version, software version, SD card size, mobile country code, and mobile network code.
- **List of email accounts configured on device**—Account name and email address.
- **Plug-in application details**—Application version.
- **Details of applications running on the device**—Application name and version.
- **Details of installed application on the device**—Application name, version, and vendor.

Config.txt Content

The config.txt diagnostic tool file includes the application configuration settings details stored on the end user's device.

Running the Diagnostic Tool



Note

In your email, it is important to include any errors you are receiving or an explanation of any issues with the Cisco BCE application. This information will help with troubleshooting and resolving issues.

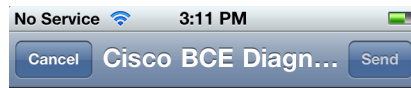
To run the diagnostic tool and send a diagnostic email:

Step 1 Tap **Cisco BCE > About** to open the Cisco BCE About screen.

Step 2 Tap the **Options** icon located at top right of screen, and tap **Diagnostic**.

The Email Compose screen displays with the diagnostic output attached. The diagnostic output includes the three files: *device.txt*, *BCE.txt*, and *config.txt*.

Example of diagnostic email:



Subject: Cisco BCE Diagnostic Information

Contains Cisco BCE diagnostic log.



Step 3 Enter the To address and complete the message content. The Subject and To address may be prefilled but editable, depending on the configuration of these fields by the administrator.

Step 4 Tap **Send**.

Setting Log Levels

The end user can set the type of logs being maintained in the application by defining the log level from the Advanced Settings screen. Tap **Cisco BCE > Settings**. From the Settings screen, tap **Diagnostic Log Level** to view or set log levels. Depending on your configuration mode, this option might not be available for configuration.

The following log levels can be set:

- **Error**—Logs error messages generated by Cisco BCE. This is the default option.
- **Warning**—Logs warning and error messages generated by the application.
- **Info**—Logs errors, warnings, and information messages generated by the application. Logs content that can be used to observe the flow of the application. This option slows down the smartphone device.
- **Debug**—Logs errors, warnings, information, and debug information generated by the application. Logs maximum content which may be used to resolve any issues that the end user might experience. This option slows down the smartphone device.

Upgrading the Cisco Business Class Email Application

Cisco BCE application upgrades are available from the Apple App Store. If the application was originally installed using the Apple App Store, the end user will automatically be notified when an updated version is available.

The previous configuration settings are retained after the upgrade.

Uninstalling the Cisco Business Class Email Application

To uninstall Cisco BCE on the iOS:

-
- Step 1** Go to the iOS home screen.
 - Step 2** Tap 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.
-



CHAPTER 4

Configuring and Using Cisco Business Class Email for Android

- [Installing the Cisco Business Class Email Application, page 4-1](#)
- [Opening Cisco Business Class Email for Android Application, page 4-1](#)
- [Launching the Cisco Business Class Email Configuration File, page 4-3](#)
- [Configuring Settings for Cisco Business Class Email, page 4-4](#)
- [Email Encryption Options Available by Configuration Mode, page 4-6](#)
- [Message Sensitivity, page 4-23](#)
- [Cache Management, page 4-23](#)
- [Troubleshooting Using the Diagnostic Tool, page 4-24](#)
- [Upgrading the Cisco Business Class Email Application, page 4-26](#)
- [Uninstalling the Cisco Business Class Email Application, page 4-26](#)

Installing the Cisco Business Class Email Application

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. See [Supported Operating Systems, page 2-2](#).

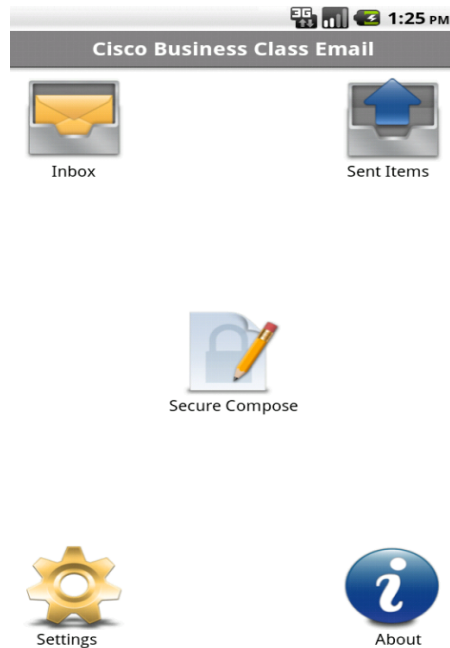
Opening Cisco Business Class Email for Android Application

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. Starting the application adds the necessary menus to the device that allow end users to send and receive encrypted emails.

Application Landing Screen

Tap the **Cisco BCE** icon to open the application landing screen. Depending on the configuration mode, some of the icons on this screen are dimmed, indicating unavailable. See [Licensing Versions and Configuration Modes, page 2-2](#).

Cisco BCE landing screen:



The following options are available:

Option	Description
Inbox	Lists email accounts for which encrypted emails were opened on the device. Tap the individual email account or All Email Accounts to display a list of decrypted emails opened for the selected account. The list of email accounts is not shown if encrypted messages have been opened for a single email address.
Sent Items	Lists email accounts from which encrypted emails were sent from the device. Tap the individual email account or All Email Accounts to display a list of emails encrypted and sent from the selected account. The list of email accounts is not shown if encrypted messages have been sent from a single email address.
Secure Compose	Launches screen to compose a secure message. See Sending an Encrypted Email, page 4-15 .
Settings	Launches the configuration screen for general settings for the application. See Configuring Settings for Cisco Business Class Email, page 4-4 .
About	View the About information for the Cisco BCE application.

Launching the Cisco Business Class Email Configuration File

The Cisco BCE application must be open and running prior to opening the *BCE_Config_signed.xml* attachment from the end user's email account.

To enable and configure the BCE application:

-
- Step 1** As a CRES administrator, logged into CRES, the administrator uses the Secure Compose screen to compose and send the *BCE_Config_signed.xml* file to the end user's email account. The end user will receive this file as a *securedoc.html* file.
- Step 2** The end user receiving the *securedoc.html* file opens the attachment from their email on their Android device. This automatically configures the Cisco BCE application installed in the previous procedure [Installing the Cisco Business Class Email Application, page 4-1](#).



Note

If the end user does not see the encrypted email in their inbox, check the spam or junk folder.

- If the end user does not have a Cisco CRES registered account, they are prompted to register.
 - Complete the **New User Registration** form and click **Register**. Then the end user checks their inbox for the account activation email.
 - From the account activation email, the end user clicks the **Click here to activate this account** link. A message indicates that the account activation is confirmed and the end user can now view encrypted emails sent to the registered email address.
 - Return to the original email with the HTML attachment. Tap **Open** on the *securedoc.html* file attachment. Then tap **Cisco BCE**.

- Step 3** When prompted, the end user accepts the configuration to complete this procedure.
-

Configuring Settings for Cisco Business Class Email

General email security options can be configured from the Settings screen. To access these settings, tap **Cisco BCE > Settings**. Depending on the end user's configuration mode, some of the options are not available for configuration by the end user. See [Licensing Versions and Configuration Modes, page 2-2](#).

Settings screen:



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

Option	Description
Cache Password	By default, this option is enabled to ensure that the encryption password is cached. If you clear the cache, you need to re-enter the password at the next login.
Cache Duration (mins)	Enter the cache duration in minutes. The default is 1440 minutes.
Clear Cache	Tap to immediately clear the cache. The cache is automatically cleared when the device is shut down or restarted.
Set Expiration	Check this option to specify how long the encrypted email message remains valid. After the number of expiry minutes is met, the message expires, and it cannot be opened by the recipient after this period. See Set an Email Expiration Time, page 4-18 .
Default Expiration (mins)	Enter the default expiration time in minutes. This option specifies how long the encrypted email message remains valid. After the number of expiry minutes is met, the message expires, and it cannot be opened by the recipient after this period.

Option	Description
Request Read Receipt	By default, this option is enabled to request a default read-receipt notification to the sender when the recipient opens the encrypted message. See Receive a Read-Receipt, page 4-19 .
Allow Reply	By default, this option is enabled to specify that an encrypted message that is replied to is automatically encrypted. See Reply/Reply All/Forward an Email, page 4-16 .
Allow Reply All	By default, this option is enabled to specify that an encrypted message is automatically encrypted when you reply to all of the recipients.
Allow Forward	By default, this option is enabled to specify that an encrypted message that is forwarded is automatically encrypted.
Message Sensitivity	By default, the message sensitivity is set to High. The other options from the drop-down list are Medium and Low. See Message Sensitivity, page 4-23 .
Diagnostic Log Level	Set the type of logs being maintained by the application by defining the log level. See Setting Log Levels, page 4-25 .
Diagnostic Email	Define the email address that will receive the diagnostic emails for troubleshooting.
Diagnostic Subject	Define the text that appears in the subject line for diagnostic emails.
Cache Envelope Size (MB)	The downloaded secure envelopes are cached on the device after they are opened for the first time. By default, this number is 6 MB.

Email Encryption Options Available by Configuration Mode

The Cisco BCE application is deployed in three 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 2-2](#). The option of opening an encrypted email is available in all three configuration modes.

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

- [Options Available in Decrypt Only Mode, page 4-7](#)
 - [Opening an Encrypted Email - New Message, page 4-7](#)
 - [Opening an Encrypted Email - Previously Opened Message, page 4-9](#)
- [Options Available in Decrypt and Flag Mode, page 4-9](#)
 - [Opening an Encrypted Email - New Message, page 4-9](#)
 - [Opening an Encrypted Email - Previously Opened Message, page 4-11](#)
 - [Flagging an Email for Encryption, page 4-11](#)
- [Options Available in Decrypt and Encrypt Mode, page 4-13](#)
 - [Opening an Encrypted Email - New Message, page 4-13](#)
 - [Opening an Encrypted Email - Previously Opened Message, page 4-15](#)
 - [Sending an Encrypted Email, page 4-15](#)
 - [Reply/Reply All/Forward an Email, page 4-16](#)
 - [Lock or Unlock an Encrypted Email, page 4-17](#)
 - [Set an Email Expiration Time, page 4-18](#)
 - [Receive a Read-Receipt, page 4-19](#)
 - [Manage Sent Secure Messages, page 4-20](#)
 - [Envelope Settings, page 4-22](#)

**Note**

There are numerous mail applications that can be used with the Android but currently Cisco BCE only integrates with the native mail application that is provided with the phone. An example of the Android mail icon follows and the icon usually appears on the first screen of the Android.

Example of Android mail icon:



Options Available in Decrypt Only Mode

The default configuration mode for the Cisco BCE application is Decrypt Only and this version can be downloaded from Google Play. In Decrypt Only mode, end users can receive and open encrypted messages, but they cannot send them.

Opening an Encrypted Email - New Message

The Cisco BCE application enables you to open an encrypted email message directly from your Android email client.

- Cisco BCE detects that the message is encrypted and requests the end user to enter the Cisco BCE registered account credentials to decrypt the message.
- After the end user enters the correct username and password, Cisco BCE downloads the envelope and displays the decrypted message on the smartphone device.

To open a new encrypted message:

Step 1 Start the email client on the Android device.

Step 2 Tap the encrypted email from the email list view and open it.

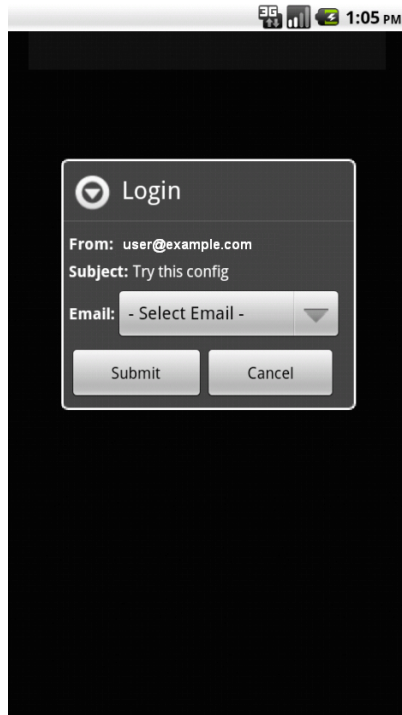


Note If you do not see the encrypted email in their inbox, check the spam or junk folder.

Step 3 Browse to the HTML attachment in the email. Tap and hold the HTML attachment until menu options appear.

Step 4 Browse to the HTML attachment in the email. Tap **Open** on the *securedoc.html* file attachment. Then tap **Cisco BCE**.

Login screen:



- If the end user does not have a Cisco CRES registered account, they are prompted to register.
 - Complete the **New User Registration** form and click **Register**. Then the end user checks their inbox for the account activation email.
 - From the account activation email, the end user clicks the **Click here to activate this account** link. A message indicates that the account activation is confirmed and the end user can now view encrypted emails sent to the registered email address.
 - Return to the original email with the HTML attachment. Tap **Open** on the *securedoc.html* file attachment. Then tap **Cisco BCE**.
- If multiple email addresses exist for the end user:
 - From the drop-down list, select the applicable email address and tap **Submit**. Enter the password from your Cisco BCE registered account and tap **Open**.
- If the email address and password were entered earlier to open encrypted email, then this information is cached and the Login screen is not displayed.

The secure email is decrypted and the message is displayed.



Note

The default maximum file size of attachments that can be download to the Android device is dependent on their mail server and device hardware.

Opening an Encrypted Email - Previously Opened Message

After a message has been opened, the email will be in the inbox of the Cisco BCE application, and can be opened again from the Cisco BCE inbox.

To reopen an encrypted message:

-
- Step 1** Tap **Cisco BCE > Inbox** to open the inbox email accounts screen.
- Step 2** Tap **All Email Accounts** or a specific email address. A list of the decrypted emails for the selected account displays.
- Step 3** Tap the encrypted email from the email list to open it.
- If the email address and password are not cached, the Login screen displays. Select the email address and tap **Submit**. Enter the password from the Cisco BCE registered account, and tap **Open**.
 - If the email address and password are cached, the Login screen is not displayed.

The decrypted message is displayed.

Options Available in Decrypt and Flag Mode

The Decrypt and Flag mode allows decrypting and flagging of secure email messages. The flag option allows the end user to flag the email for encryption, and the email is encrypted by the Cisco IronPort Encryption appliance or Email Security appliance before the email is sent out of the network. The server must be configured to detect the flagged messages and encrypt them at the server.

In order to enable the Decrypt and Flag mode, the smartphone device is configured by an updated *BCE_Config_signed.xml* file received from the administrator. These options are available after the end user receives and launches the *BCE_Config_signed.xml* file in their smartphone email account.

Opening an Encrypted Email - New Message

The Cisco BCE application enables you to open an encrypted email message directly from your Android email client.

- Cisco BCE detects that the message is encrypted and requests the end user to enter the Cisco BCE registered account credentials to decrypt the message.
- After the end user enters the correct username and password, Cisco BCE downloads the envelope and displays the decrypted message on the smartphone device.

To open a new encrypted message:

-
- Step 1** Start the email client on the Android device.
- Step 2** Tap the encrypted email from the email list view and open it.

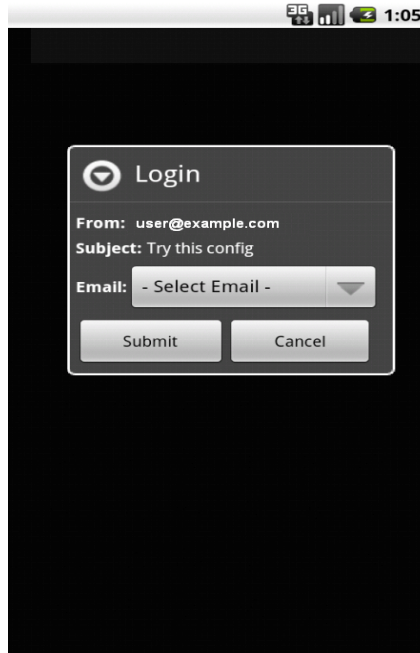


Note If you do not see the encrypted email in their inbox, check the spam or junk folder.

- Step 3** Browse to the HTML attachment in the email. Tap and hold the HTML attachment until menu options appear.

- Step 4** Browse to the HTML attachment in the email. Tap **Open** on the *securedoc.html* file attachment. Then tap **Cisco BCE**.

Login screen:



- If the end user does not have a Cisco CRES registered account, they are prompted to register.
 - Complete the **New User Registration** form and click **Register**. Then the end user checks their inbox for the account activation email.
 - From the account activation email, the end user clicks the **Click here to activate this account** link. A message indicates that the account activation is confirmed and the end user can now view encrypted emails sent to the registered email address.
 - Return to the original email with the HTML attachment. Tap **Open** on the *securedoc.html* file attachment. Then tap **Cisco BCE**.
- If multiple email addresses exist for the end user:
 - From the drop-down list, select the applicable email address and tap **Submit**. Enter the password from your Cisco BCE registered account and tap **Open**.
- If the email address and password were entered earlier to open encrypted email, then this information is cached and the Login screen is not displayed.

The secure email is decrypted and the message is displayed.



Note

The default maximum file size of attachments that can be download to the Android device is dependent on their mail server and device hardware.

Opening an Encrypted Email - Previously Opened Message

After a message has been opened, the email will be in the inbox of the Cisco BCE application, and can be opened again from the Cisco BCE inbox.

To reopen an encrypted message:

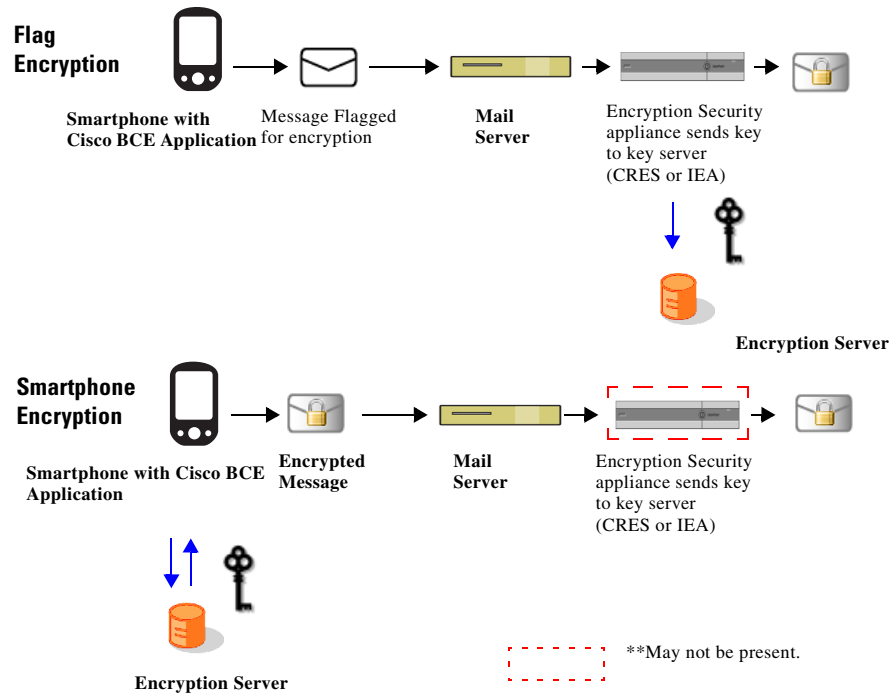
-
- | | |
|---------------|--|
| Step 1 | Tap Cisco BCE > Inbox to open the inbox email accounts screen. |
| Step 2 | Tap All Email Accounts or a specific email address. A list of the decrypted emails for the selected account displays. |
| Step 3 | Tap the encrypted email from the email list to open it. <ul style="list-style-type: none">• If the email address and password are not cached, the Login screen displays. Select the email address and tap Submit. Enter the password from the Cisco BCE registered account, and tap Open.• If the email address and password are cached, the Login screen is not displayed. |

The decrypted message is displayed.

Flagging an Email for Encryption

The Flag Encryption option allows the end user to flag the email for encryption, and the email is encrypted by the Cisco IronPort Encryption appliance (IEA) or Email Security appliance (ESA) before the email is sent out of the network. The server must be configured to detect the flagged messages and encrypt them at the server. All of the encryption options, such as requesting a read receipt or enabling secure forward, are set at the server.

The following figure illustrates how the secure email flows from the smartphone device to the internal mail server, flagged, then sent out of the network. It also compares the flag encryption workflow with encryption directly on the smartphone device.

Figure 4-1 Workflows for Flag Encryption versus Smartphone Encryption

To flag an email for encryption:

-
- Step 1** Tap **Cisco BCE > Secure Compose** to open the Secure Compose screen.
- Step 2** By default, the email address for the registered email account is added in the From field. Complete the appropriate fields:
- Address (To, CC, and BCC)
 - Subject
- 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 Android **Menu** key, then tap **Envelope Settings**.
- Step 5** When the message is complete, tap **Send Secure**. From the menu options, select option 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. The subject of the email is modified before the message is sent. The new subject is one of the configuration options in **Cisco BCE > Settings**. For example, the subject can be modified to read "SECURE."
-

Options Available in Decrypt and Encrypt Mode

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

In order to enable the Decrypt and Encrypt mode, the smartphone device is configured by an updated *BCE_Config_signed.xml* file received from the administrator. These options are available after the end user receives and launches the *BCE_Config_signed.xml* file in their smartphone email account.

Opening an Encrypted Email - New Message

The Cisco BCE application enables you to open an encrypted email message directly from your Android email client.

- Cisco BCE detects that the message is encrypted and requests the end user to enter the Cisco BCE registered account credentials to decrypt the message.
- After the end user enters the correct username and password, Cisco BCE downloads the envelope and displays the decrypted message on the smartphone device.

To open a new encrypted message:

Step 1 Start the email client on the Android device.

Step 2 Tap the encrypted email from the email list view and open it.

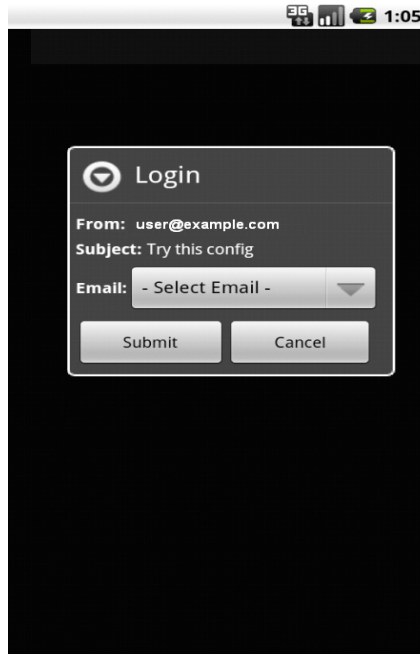


Note If you do not see the encrypted email in their inbox, check the spam or junk folder.

Step 3 Browse to the HTML attachment in the email. Tap and hold the HTML attachment until menu options appear.

Step 4 Browse to the HTML attachment in the email. Tap **Open** on the *securedoc.html* file attachment. Then tap **Cisco BCE**.

Login screen:



- If the end user does not have a Cisco CRES registered account, they are prompted to register.
 - Complete the **New User Registration** form and click **Register**. Then the end user checks their inbox for the account activation email.
 - From the account activation email, the end user clicks the **Click here to activate this account** link. A message indicates that the account activation is confirmed and the end user can now view encrypted emails sent to the registered email address.
 - Return to the original email with the HTML attachment. Tap **Open** on the *securedoc.html* file attachment. Then tap **Cisco BCE**.
- If multiple email addresses exist for the end user:
 - From the drop-down list, select the applicable email address and tap **Submit**. Enter the password from your Cisco BCE registered account and tap **Open**.
- If the email address and password were entered earlier to open encrypted email, then this information is cached and the Login screen is not displayed.

The secure email is decrypted and the message is displayed.



Note

The default maximum file size of attachments that can be download to the Android device is dependent on their mail server and device hardware.

Opening an Encrypted Email - Previously Opened Message

After a message has been opened, the email will be in the inbox of the Cisco BCE application, and can be opened again from the Cisco BCE inbox.

To reopen an encrypted message:

-
- Step 1** Tap **Cisco BCE > Inbox** to open the inbox email accounts screen.
- Step 2** Tap **All Email Accounts** or a specific email address. A list of the decrypted emails for the selected account displays.
- Step 3** Tap the encrypted email from the email list to open it.
- If the email address and password are not cached, the Login screen displays. Select the email address and tap **Submit**. Enter the password from the Cisco BCE registered account, and tap **Open**.
 - If the email address and password are cached, the Login screen is not displayed.

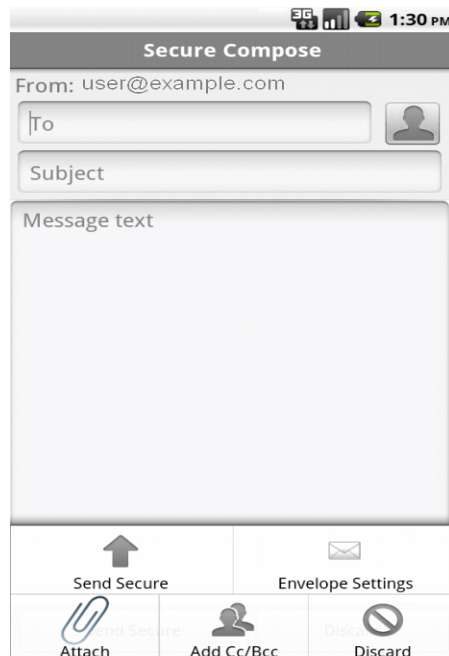
The decrypted message is displayed.

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 **Cisco BCE > Secure Compose** to open the Secure Compose screen.
- Secure Compose Options screen:



- Step 2** By default, the email address for the registered email account is added in the From field. Complete the appropriate fields:
- Address (To, CC, and BCC)
 - Subject
- 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 Android **Menu** key, then tap **Envelope Settings**.
- Step 5** When the message is complete, tap **Send Secure**. From the menu options, select option 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.
-

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 in the Settings screen for the encrypted email, applicable menu options are added to the smartphone 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 Business Class Email, page 4-4](#).



Note

To respond with a secure reply/reply all/forward, the smartphone device has to be able to send an encrypted message. These options are not available in the Decrypt Only mode. Also, the smartphone device needs to be able to send the encrypted email using the same server as the original message. For example:

- If you use the Cisco BCE application, encrypting email with CRES and receive a CRES secure message, you can reply to that message.
 - If you use the Cisco BCE application, encrypting email with CRES and receive an IEA secure message, you cannot reply to that message because the plug-in mobile application would not have a token to communicate with the key server. In this instance, the menu options will not be available.
-

Replying to or forwarding an encrypted email:

- Step 1** Follow the steps for [Opening an Encrypted Email - New Message, page 4-13](#) or [Opening an Encrypted Email - Previously Opened Message, page 4-15](#).
- Step 2** Tap the Android **Menu** key. 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 **Send Secure**. From the menu options, select option 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 **Cisco BCE > Sent Items**. The Cisco BCE Mailbox screen displays a list of email accounts from which encrypted emails were sent from the device. This screen is not displayed if encrypted emails have been sent from one email account.
- Step 2** Tap **All Email Accounts** or a specific email address. A list of the decrypted emails sent from the selected account is displayed.
- Step 3** Tap the encrypted email that you want to lock from the email list. The menu options display.
- Step 4** Tap **Lock**. The login screen is displayed if the cache duration has expired.
- Step 5** Optionally, enter a reason for locking the message. The lock reason is displayed to recipients when they view the envelope. You may be asked to enter your Cisco BCE registered account email address and password.
- Step 6** 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 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 **Cisco BCE > Sent Items**. The Cisco BCE Mailbox screen displays a list of email accounts from which encrypted emails were sent from the device. This screen is not displayed if encrypted emails have been sent from one email account.
- Step 2** Tap **All Email Accounts** or a specific email address. A list of the decrypted emails sent from the selected account is displayed.
- Step 3** Tap the encrypted email that you want to unlock from the email list. The menu options display.
- Step 4** Tap **Unlock**. Successful unlocking of the email message is confirmed.
-

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 Setting

To set the default expiration interval:

-
- Step 1** Tap **Cisco BCE > Settings** to open the Settings screen.
 - Step 2** Select **Set Expiration** and in **Default expiration (mins)**, specify the number of minutes after which the email will expire.
 - Step 3** Tap **Apply** to exit and save the changes.
-

Per Message Setting

To set expiration time for a specific email:

-
- Step 1** Tap **Cisco BCE > Secure Compose** to open the Secure Compose screen.
 - Step 2** By default, the email address for the registered account is added in the From field.
Complete the appropriate fields:
 - Address (To, CC, and BCC)
 - Subject
 - Step 3** Enter the message text.
 - Step 4** Tap the Android **Menu** key, then tap **Envelope Settings**.
 - Step 5** Tap **Set Expiration > Set Expiry**. The New Expiry Date screen displays.
 - Step 6** Select the expiration date and time that the email will expire.
 - Step 7** Tap **Set Expiry** to save the changes.
 - Step 8** Tap **Apply** to exit the Envelope Settings screen and return to the secure email.
 - Step 9** When the message is complete, tap **Send Secure**. From the menu options, select option to complete the action. For example, select Android email.
 - Step 10** 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 **Cisco BCE > Sent Items**. The Cisco BCE Mailbox screen displays a list of email accounts from which encrypted emails were sent from the device. This screen is not displayed if encrypted emails have been sent from one email account.
 - Step 2** Tap **All Email Accounts** or a specific email address. A list of the decrypted emails sent from the selected account is displayed.
 - Step 3** Tap the encrypted email that you want to set the expiration time from the email list. The menu options display.
 - Step 4** Tap **Set Expiry**. 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 **Apply** 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 **Cisco BCE > Sent Items**. The Cisco BCE Mailbox screen displays a list of email accounts from which encrypted emails were sent from the device. This screen is not displayed if encrypted emails have been sent from one email account.
 - Step 2** Tap **All Email Accounts** or a specific email address. A list of the decrypted emails sent from the selected account is displayed.
 - Step 3** Tap the encrypted email that you want to clear the expiration from the email list. The menu options display.
 - Step 4** Tap **Set Expiry**. The New Expiry Date screen displays and shows the current expiry date.
 - Step 5** Tap **Clear Expiry**.
-

Receive a Read-Receipt

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

Default Setting

To request a read-receipt (default setting):

-
- Step 1** Tap **Cisco BCE > Settings** to open the Settings screen.
 - Step 2** Tap **Request Read Receipt**. This is enabled by default.

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

Per Message Setting

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

To request a read-receipt for a specific email:

Step 1 Tap **Cisco BCE > Secure Compose** to open the Secure Compose screen.

Step 2 By default, the email address for the registered account is added in the From field.

Complete the appropriate fields:

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

Step 3 Enter the message text.

Step 4 Tap the Android **Menu** key, then tap **Envelope Settings**.

Step 5 Tap **Request Read Receipt** to enable this option.

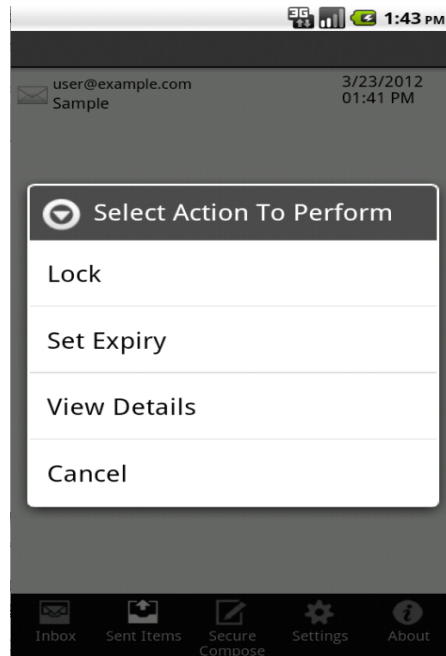
Step 6 Tap **Apply**.

Manage Sent Secure Messages

The Sent Items screen lists the encrypted emails sent from the smartphone.

To access, tap **Cisco BCE > Sent Items**. Select an email address and the email you want to modify or view from the list of sent encrypted emails. Tap the selected email to display the menu options.

Cisco BCE Mailbox screen options:



From Cisco BCE Mailbox, the following can be performed 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 4-17](#).
- **Set Expiry**—An expiration time can be set for encrypted email. See [Set an Email Expiration Time, page 4-18](#).
- **View Details**—View details of the encrypted email sent from the device.

Sent Email Message Details

From the Cisco BCE Mailbox, details of the encrypted emails sent from the device can be viewed. To access the Cisco BCE Mailbox, tap **Cisco BCE > Sent Items**. Select an email address and the email you want to view from the list of sent encrypted emails. Tap the selected email to display the menu options. Tap **View Details**.

The following information is displayed:

- **From**—Email address of the sender.
- **Subject**—Subject of the message.
- **Sent Date**—Date and time message was sent.
- **To**—Email addresses of the recipients.
- **Open Date**—Date on which the secure message was opened by the respective recipient.
- **Expiration Date**—Expiration date and time 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.

Envelope Settings

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

Envelope Settings screen:



To change the envelope settings:

-
- Step 1** Tap **Cisco BCE > Secure Compose** to open the Secure Compose screen.
- Step 2** By default, the email address for the registered email account is added in the From field. Complete the appropriate fields:
- Address (To, CC, and BCC)
 - Subject
- Step 3** Enter the message text.
- Step 4** To access Envelope Settings, tap the Android **Menu** key, then tap **Envelope Settings**.
- Step 5** Tap to enable or disable the applicable message options:
- Set Expiration
 - Request Read Receipt
 - Allow Reply
 - Allow Reply All
 - Allow Forward
 - Message Sensitivity
- Step 6** Tap **Apply** to save the changes.
-

Message Sensitivity

The sender can specify the sensitivity for the encrypted email from the **Cisco BCE > Settings** screen or from the Envelope Settings screen.

The following message sensitivity options can be set:

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

A default sensitivity of high is set for all messages. The default can be overridden for a specific message by modifying the value in Envelope Settings. See [Envelope Settings, page 4-22](#).

**Note**

The administrator can define the minimum message sensitivity for the end user in the *BCE_Config.xml* file using the sensitivity options of high, medium, or low. After this is defined, the end user cannot set the message sensitivity below the minimum defined message sensitivity in the *BCE_Config.xml* file.

Cache Management

Cache Passwords

The Cisco BCE registered account password is cached for a time period that is configurable from the **Cisco BCE > Settings** screen. Password caching is On by default and the default cache time is 1440 minutes (24 hours). Caching of the password can be turned off from the Settings screen. Tap **Cache Password** to turn on or off, then and tap **Apply** to save changes.

The password cache can be cleared from the **Cisco BCE > Settings** screen by tapping **Clear Cache**. The password cache is automatically cleared when the device is shut down or restarted.

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 the end user opens 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 6 MB. A task runs every 24 hours on the device and deletes any cached envelopes that are more than two weeks old.


Troubleshooting Using the Diagnostic Tool

The Cisco BCE application includes a diagnostic tool to help Cisco Support in troubleshooting problems. The administrator or the end user can use the diagnostic tool if receiving errors or if there are issues with the Cisco BCE application. The diagnostic tool can also be used to share critical information with Cisco engineers when reporting a bug.

The diagnostic tool is available from the About screen. See [Running the Diagnostic Tool, page 4-25](#).

Data Collected by the Diagnostic Tool

The diagnostic tool attaches the data collected to an email. The diagnostic email contains data information that is generated on the device during the end user's interaction with the encryption application. The diagnostic tool output includes the three files; *BCE.txt*, *device.txt*, and *config.txt*.




Note

A task runs every 24 hours on the device and deletes any logs that are more than one week old.

BCE.txt Content

The BCE.txt diagnostic tool file contains error, warning, information, and debug messages. When saving to the *BCE.txt* file, messages are prefixed with the following:

- **I**—Information messages
- **W**—Warning messages
- **E**—Error messages
- **D**—Debug log messages



Note

The level of log information collected is determined by the log level set in the configuration. See [Setting Log Levels, page 4-25](#).

The log content format is:

<Source> TAB <Log Category> TAB <Date Timestamp GMT> TAB <Log Message>

The table shows sample log content:

Sample Log Content			
BB	I	2011-05-13 12:31:24	Cisco BCE service started on device
BB	W	2011-05-13 12:32:37	Configuration for DecryptionNotification not defined
BB	E	2011-05-13 12:45:17	Timeout occurred
SDK	E	2011-09-07 16:38:48	EnvelopeBuilder :: finish setAlgorithm

Device.txt Content

The device.txt diagnostic tool file includes the following device information:

- **Device info**—Device ID, device name, platform version, software version, SD card size, mobile country code, and mobile network code.
- **List of email accounts configured on device**—Account name and email address.
- **Plug-in application details**—Application version.
- **Details of applications running on the device**—Application name and version.
- **Details of installed application on the device**—Application name, version, and vendor.

Config.txt Content

The config.txt diagnostic tool file includes the application configuration settings details stored on the end user's device.

Running the Diagnostic Tool



Note

In your email, it is important to include any errors you are receiving or an explanation of any issues with the Cisco BCE application. This information will help with troubleshooting and resolving issues.

To run the diagnostic tool and send a diagnostic email:

-
- Step 1** Tap **Cisco BCE > About** to open the Cisco BCE About screen. If you are in Decrypt Only mode, you need to press and hold the **About** button in order to send diagnostic mail.
 - Step 2** Tap the Android **Menu** key and tap **Diagnostic**.
 - Step 3** Enter the message content and click **OK** to confirm.
 - Step 4** From the menu options, select option to complete the action. For example, select Android email.
The Email Compose screen displays with the diagnostic output attached. The diagnostic output includes the three files: *device.txt*, *BCE.txt*, and *config.txt*.
 - Step 5** Enter the To address. The Subject and To address may be prefilled but editable, depending on the configuration of these fields by the administrator.
 - Step 6** Tap **Send**.
-

Setting Log Levels

The end user can set the type of logs being maintained in the application by defining the log level from the Advanced Settings screen. Tap **Cisco BCE > Settings**. From the Settings screen, tap **Diagnostic Log Level** to view or set log levels. Depending on your configuration mode, this option might not be available for configuration.

The following log levels can be set:

- **Error**—Logs error messages generated by Cisco BCE. This is the default option.
- **Warning**—Logs warning and error messages generated by the application.
- **Info**—Logs errors, warnings, and information messages generated by the application. Logs content that can be used to observe the flow of the application. This option slows down the smartphone device.
- **Debug**—Logs errors, warnings, information, and debug information generated by the application. Logs maximum content which may be used to resolve any issues that the end user might experience. This option slows down the smartphone device.

Upgrading the Cisco Business Class Email Application

Cisco BCE application upgrades are available from Google Play. If the application was originally installed using Google Play, the end user will automatically be notified when an updated version is available.

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 the Android **Menu** key, then tap **Settings**.
 - Step 3** Tap **Applications > Manage Applications**.
 - Step 4** From the list, tap **Cisco BCE > Uninstall**, then tap **OK**.

The application is removed.



APPENDIX **A**

IronPort End User License Agreement

This appendix contains the following section:

- [Cisco IronPort Systems, LLC Software License Agreement, page A-27](#)

Cisco IronPort Systems, LLC Software License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT (“AGREEMENT”) FOR THE LICENSE OF THE SOFTWARE (AS DEFINED BELOW). BY tapING THE ACCEPT BUTTON OR ENTERING “Y” WHEN PROMPTED, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY, COLLECTIVELY, THE “COMPANY”) CONSENT TO BE BOUND BY AND BECOME A PARTY TO THE FOLLOWING AGREEMENT BETWEEN CISCO IRONPORT SYSTEMS, LLC, A DELAWARE CORPORATION (“IRONPORT”) AND COMPANY (COLLECTIVELY, THE “PARTIES”). BY tapING THE ACCEPT BUTTON OR ENTERING “Y” WHEN PROMPTED, YOU REPRESENT THAT (A) YOU ARE DULY AUTHORIZED TO REPRESENT YOUR COMPANY AND (B) YOU ACCEPT THE TERMS AND CONDITIONS OF THIS AGREEMENT ON BEHALF OF YOUR COMPANY, AND AS SUCH, AN AGREEMENT IS THEN FORMED. IF YOU OR THE COMPANY YOU REPRESENT (COLLECTIVELY, “COMPANY”) DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, tap THE CANCEL BUTTON OR ENTER “N” WHEN PROMPTED AND PROMPTLY (BUT NO LATER THAT THIRTY (30) DAYS OF THE DELIVERY DATE, AS DEFINED BELOW) NOTIFY IRONPORT, OR THE RESELLER FROM WHOM YOU RECEIVED THE SOFTWARE, FOR A FULL REFUND OF THE PRICE PAID FOR THE SOFTWARE.

1. DEFINITIONS

1.1 “Company Service” means the Company’s email or internet services provided to End Users for the purposes of conducting Company’s internal business and which are enabled via Company’s products as described in the purchase agreement, evaluation agreement, beta or pre-release agreement, purchase order, sales quote or other similar agreement between the Company and IronPort or its reseller (“Agreement”) and the applicable user interface and IronPort’s standard system guide documentation that outlines the system architecture and its interfaces (collectively, the “License Documentation”).

1.2 “End User” means the employee, contractor or other agent authorized by Company to access to the Internet or use email services via the Company Service.

1.3 “Service(s)” means (i) the provision of the Software functionality, including Updates and Upgrades, and (ii) the provision of support by IronPort or its reseller, as the case may be.

1.4 “Software” means: (i) IronPort’s proprietary software licensed by IronPort to Company along with IronPort’s hardware products; (ii) any software provided by IronPort’s third-party licensors that is licensed to Company to be implemented for use with IronPort’s hardware products; (iii) any other IronPort software module(s) licensed by IronPort to Company along with IronPort’s hardware products; and (iv) any and all Updates and Upgrades thereto.

1.5 “Updates” means minor updates, error corrections and bug fixes that do not add significant new functions to the Software, and that are released by IronPort or its third party licensors. Updates are designated by an increase to the Software’s release number to the right of the decimal point (e.g., Software 1.0 to Software 1.1). The term Updates specifically excludes Upgrades or new software versions marketed and licensed by IronPort or its third party licensors as a separate product.

1.6 “Upgrade(s)” means revisions to the Software, which add new enhancements to existing functionality, if and when it is released by IronPort or its third party licensors, in their sole discretion. Upgrades are designated by an increase in the Software’s release number, located to the left of the decimal point (e.g., Software 1.x to Software 2.0). In no event shall Upgrades include any new versions of the Software marketed and licensed by IronPort or its third party licensors as a separate product.

2. LICENSE GRANTS AND CONSENT TO TERMS OF DATA COLLECTION

2.1 License of Software. By using the Software and the License Documentation, Company agrees to be bound by the terms of this Agreement, and so long as Company is in compliance with this Agreement, IronPort hereby grants to Company a non-exclusive, non-sublicensable, non-transferable, worldwide license during the Term to use the Software only on IronPort’s hardware products, solely in connection with the provision of the Company Service to End Users. The duration and scope of this license(s) is further defined in the License Documentation. Except as expressly provided herein, no right, title or interest in any Software is granted to the Company by IronPort, IronPort’s resellers or their respective licensors. This license and any Services are co-terminus.

2.2 Consent and License to Use Data. Subject to Section 8 hereof, and subject to the IronPort Privacy Statement at <http://www.IronPort.com/privacy.html>, as the same may be amended from time to time by IronPort with notice to Company, Company hereby consents and grants to IronPort a license to collect and use the data from the Company as described in the License Documentation, as the same may be updated from time to time by IronPort (“Data”). To the extent that reports or statistics are generated using the Data, they shall be disclosed only in the aggregate and no End User identifying information may be surmised from the Data, including without limitation, user names, phone numbers, unobfuscated file names, email addresses, physical addresses and file content. Notwithstanding the foregoing, Company may terminate IronPort’s right to collect and use Data at any time upon prior written or electronic notification, provided that the Software or components of the Software may not be available to Company if such right is terminated.

3. CONFIDENTIALITY. Each Party agrees to hold in confidence all Confidential Information of the other Party to the same extent that it protects its own similar Confidential Information (and in no event using less than a reasonable degree of care) and to use such Confidential Information only as permitted under this Agreement. For purposes of this Agreement “Confidential Information” means information of a party marked “Confidential” or information reasonably considered by the disclosing Party to be of a proprietary or confidential nature; provided that the Data, the Software, information disclosed in design reviews and any pre-production releases of the Software provided by IronPort is expressly designated Confidential Information whether or not marked as such.

4. PROPRIETARY RIGHTS; OWNERSHIP. Title to and ownership of the Software and other materials and all associated Intellectual Property Rights (as defined below) related to the foregoing provided by IronPort or its reseller to Company will remain the exclusive property of IronPort and/or its superior licensors. Company and its employees and agents will not remove or alter any trademarks, or other proprietary notices, legends, symbols, or labels appearing on or in copies of the Software or other materials delivered to Company by IronPort or its reseller. Company will not modify, transfer, resell for

profit, distribute, copy, enhance, adapt, translate, decompile, reverse engineer, disassemble, or otherwise determine, or attempt to derive source code for any Software or any internal data files generated by the Software or to create any derivative works based on the Software or the License Documentation, and agrees not to permit or authorize anyone else to do so. Unless otherwise agreed in writing, any programs, inventions, concepts, documentation, specifications or other written or graphical materials and media created or developed by IronPort or its superior licensors during the course of its performance of this Agreement, or any related consulting or professional service agreements, including all copyrights, database rights, patents, trade secrets, trademark, moral rights, or other intellectual property rights (“Intellectual Property Right(s)”) associated with the performance of such work shall belong exclusively to IronPort or its superior licensors and shall, in no way be considered a work made for hire for Company within the meaning of Title 17 of the United States Code (Copyright Act of 1976).

5. LIMITED WARRANTY AND WARRANTY DISCLAIMERS

5.1 Limited Warranty. IronPort warrants to Company that the Software, when properly installed and properly used, will substantially conform to the specifications in the License Documentation for a period of ninety (90) days from the delivery date or the period set forth in the License Documentation, whichever is longer (“Warranty Period”). FOR ANY BREACH OF THE WARRANTY CONTAINED IN THIS SECTION, COMPANY’S EXCLUSIVE REMEDY AND IRONPORT’S ENTIRE LIABILITY, WILL BE PROMPT CORRECTION OF ANY ERROR OR NONCONFORMITY, PROVIDED THAT THE NONCONFORMITY HAS BEEN REPORTED TO IRONPORT AND/OR ITS RESELLER BY COMPANY WITHIN THE WARRANTY PERIOD. THIS WARRANTY IS MADE SOLELY TO COMPANY AND IS NOT TRANSFERABLE TO ANY END USER OR OTHER THIRD PARTY. IronPort shall have no liability for breach of warranty under this Section or otherwise for breach of this Agreement if such breach arises directly or indirectly out of or in connection with the following: (i) any unauthorized, improper, incomplete or inadequate maintenance or calibration of the Software by Company or any third party; (ii) any third party hardware software, services or system(s); (iii) any unauthorized modification or alteration of the Software or Services; (iv) any unauthorized or improper use or operation of the Software or Company’s failure to comply with any applicable environmental specification; or (v) a failure to install and/or use Updates, Upgrades, fixes or revisions provided by IronPort or its resellers from time to time.

5.2 WARRANTY DISCLAIMER. THE EXPRESS WARRANTIES SET FORTH IN SECTION 5.1 OF THIS AGREEMENT CONSTITUTE THE ONLY PERFORMANCE WARRANTIES WITH RESPECT TO THE SOFTWARE OR SERVICES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IRONPORT LICENSES THE SOFTWARE AND SERVICES HEREUNDER ON AN “AS IS” BASIS. EXCEPT AS SPECIFICALLY SET FORTH HEREIN, IRONPORT AND ITS SUPERIOR LICENSORS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, OR STATUTORY (EITHER IN FACT OR BY OPERATION OF LAW), AND EXPRESSLY DISCLAIM ALL OTHER WARRANTIES, INCLUDING WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. NEITHER IRONPORT NOR ITS THIRD PARTY LICENSORS WARRANT THAT THE SOFTWARE OR SERVICES (1) IS FREE FROM DEFECTS, ERRORS OR BUGS, (2) THAT OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED, OR (3) THAT ANY RESULTS OR INFORMATION THAT IS OR MAY BE DERIVED FROM THE USE OF THE SOFTWARE WILL BE ACCURATE, COMPLETE, RELIABLE AND/OR SECURE.

6. LIMITATION OF LIABILITY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER FOR ANY LOSS OF PROFITS, COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF BUSINESS, LOSS OF USE OR DATA, INTERRUPTION OF BUSINESS, OR FOR INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES OF ANY KIND, EVEN IF SUCH PARTY RECEIVED ADVANCE NOTICE OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF EITHER PARTY ARISING UNDER ANY PROVISION OF THIS AGREEMENT, REGARDLESS OF WHETHER THE CLAIM FOR SUCH DAMAGES IS

BASED IN CONTRACT, TORT, OR OTHER LEGAL THEORY, EXCEED THE TOTAL AMOUNT PAID FOR THE SOFTWARE OR SERVICES DURING THE TWELVE (12) MONTHS PRIOR TO THE EVENT GIVING RISE TO SUCH LIABILITY.

7. **TERM AND TERMINATION.** The term of this Agreement shall be as set forth in the License Documentation (the “Term”). If IronPort defaults in the performance of any material provision of this Agreement or the License Documentation, then Company may terminate this Agreement upon thirty (30) days written notice if the default is not cured during such thirty (30) day period. If Company defaults in the performance of any material provision of this Agreement or the License Documentation, IronPort may terminate this Agreement upon thirty (30) days written notice if the default is not cured during such thirty (30) day notice and without a refund. This Agreement may be terminated by one Party immediately at any time, without notice, upon (i) the institution by or against the other Party of insolvency, receivership or bankruptcy proceedings or any other proceedings for the settlement of such Party’s debts, (ii) such other Party making a general assignment for the benefit of creditors, or (iii) such other Party’s dissolution. The license granted in Section 2 will immediately terminate upon this Agreement’s termination or expiration. Within thirty (30) calendar days after termination or expiration of this Agreement, Company will deliver to IronPort or its reseller or destroy all copies of the Software and any other materials or documentation provided to Company by IronPort or its reseller under this Agreement.

8. **U.S. GOVERNMENT RESTRICTED RIGHTS; EXPORT CONTROL.** The Software and accompanying License Documentation are deemed to be “commercial computer software” and “commercial computer software documentation,” respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying License Documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement. Company acknowledges that the Software and License Documentation must be exported in accordance with U.S. Export Administration Regulations and diversion contrary to U.S. laws is prohibited. Company represents that neither the United States Bureau of Export Administration nor any other federal agency has suspended, revoked or denied Company export privileges. Company represents that Company will not use or transfer the Software for end use relating to any nuclear, chemical or biological weapons, or missile technology unless authorized by the U.S. Government by regulation or specific license. Company acknowledges it is Company’s ultimate responsibility to comply with any and all import and export restrictions, and other applicable laws, in the U.S. or elsewhere, and that IronPort or its reseller has no further responsibility after the initial sale to Company within the original country of sale.

9. **MISCELLANEOUS.** This Agreement is governed by the laws of the United States and the State of California, without reference to conflict of laws principles. The application of the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded. Nothing contained herein shall be construed as creating any agency, partnership, or other form of joint enterprise between the parties. Neither party shall be liable hereunder by reason of any failure or delay in the performance of its obligations hereunder (except for the payment of money) on account of (i) any provision of any present or future law or regulation of the United States or any applicable law that applies to the subject hereof, and (ii) interruptions in the electrical supply, failure of the Internet, strikes, shortages, riots, insurrection, fires, flood, storm, explosions, acts of God, war, terrorism, governmental action, labor conditions, earthquakes, or any other cause which is beyond the reasonable control of such party. This Agreement and the License Documentation set forth all rights for the user of the Software and is the entire agreement between the parties and supersedes any other communications with respect to the Software and License Documentation. The terms and conditions of this Agreement will prevail, notwithstanding any variance with the License Documentation or any purchase order or other written instrument submitted by a party, whether formally rejected by the other party or not. This Agreement may not be modified except by a written addendum issued by a duly authorized representative of IronPort, except that IronPort may modify the IronPort Privacy Statement at any time, in its discretion, via notification to Company of such modification that will be posted at <http://www.IronPort.com/privacy.html>. No provision hereof shall be deemed waived unless such waiver

shall be in writing and signed by IronPort or a duly authorized representative of IronPort. If any provision of this Agreement is held invalid, the remainder of this Agreement shall continue in full force and effect. The parties confirm that it is their wish that this Agreement has been written in the English language only.

10. IRONPORT CONTACT INFORMATION. If Company wants to contact IronPort for any reason, please write to IronPort Systems, Inc., 950 Elm Avenue, San Bruno, California 94066, or call or fax us at tel: 650.989.6500 and fax: 650.989.6543.

