CHAPTER 1

Cisco Business Class Email 3.0 Administrator's Guide

This guide includes the following sections:

Overview

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™ smartphone or tablet.

With the proliferation of mobile 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.

TCP Services Required for the Cisco Business Class Email Application

The Cisco BCE application requires the use of an available port for HTTPS or HTTP. The Cisco BCE application is typically configured to use HTTPS on port 443 and is unlikely to be configured otherwise. However, the application can be configured to use either HTTPS or HTTP on any available port. All other TCP protocols can be disabled without affecting the operation of the Cisco BCE application.

Downloading the Cisco Business Class Email Application

The Cisco Business Class Email application, *Cisco BCE*, can be downloaded directly to the smartphone or tablet from the Apple App Store and from Google Play. After the user downloads the Cisco BCE application from the Apple App Store and from Google Play, they must create an account, as described in the "Licensing Versions and Configuration Modes" section on page 1-3.

Supported Operating Systems

For information about operating systems supported for release 3.0, see the *Cisco Email Encryption Compatibility Matrix*.

Licensing Versions and Configuration Modes

The Cisco Business Class Email application is deployed in two separate licensing versions that determine the configuration mode for the application. The two licensing versions and configuration modes are:

- **Decrypt Only**—Allows decrypting of secure email messages received and to forward and reply to received messages.
- **Decrypt and Encrypt**—Allows encrypting and decrypting of secure email messages.

Note **Flag** mode is not supported

The default configuration mode for the Cisco BCE application is Decrypt Only.

After the user downloads the Cisco BCE application from the Apple App Store and from Google Play, they must create an account, as describe below.

- To create a Decrypt account, the user can just open a secure email using the Native email system.
- To create an Encrypted account, the user must apply the configuration file that they receive from Administrator, as described below.

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 presses and holds on the *securedoc.html* attachment, the currently installed application detects the configuration information attached to the message and applies the updated configuration.

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

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

Note The availability of reply options depends on the settings of the received message.

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 Encrypt configuration mode, 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 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

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:

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.

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.

Related Documents

The BCE User Guides, Compatibility Matrix, and Release Notes are located at:
http://www.cisco.com/c/en/us/support/security/email-encryption/products-user-guide-list.html

To use BCE, you need a key server, which can be the Cisco Registered Envelope Service (CRES), or a Cisco IronPort Encryption appliance (IEA). If you use an 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 1-4.

To understand how to configure the Cisco IEA, you may want to review the following guides:

- *Cisco Registered Envelope Service 5.0 Account Administrator Guide*. This guide provides information about Cisco Registered Envelope Service (CRES) that provides support for Cisco 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.

Where to Find More Information

Cisco 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 end users.

You access the Cisco Support Community at the following URL:

https://supportforums.cisco.com

Cisco 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 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 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. For more information about these license agreements, see:

- http://www.cisco.com/web/mobile/terms.html
- Cisco BCE Open Source Documentation

Cisco Welcomes Your Comments

The Cisco Content Security 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:

contentsecuritydocs@cisco.com