Cisco Email Encryption Plug-in 1.2
Administrator Guide

February 28, 2018

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
Preparing the Mass Installation Package and Script  3-3
Performing the Installation  3-12
Using Custom Configuration Files  3-27
   Overview  3-28
   Editing the XML Configuration Files  3-28
Mass Installation Using the BCE_Config.xml File  3-29
Deploying the Custom Configuration Files  3-31

Configuring and Using the Cisco Email Encryption Plug-in for Outlook  4-1
   Enabling the Cisco Email Encryption Plug-in  4-2
   Configuring the Sending of Usage Data  4-2
      General Information  4-2
      Account-Specific Information  4-3
   Cisco Email Encryption Plug-in For Outlook General Settings  4-4
      Enable or Disable  4-4
   Configuring Basic Settings for the Outlook Plug-in  4-5
   Configuring the Outlook Plug-in to Check for Updates  4-6
      Update Notifications  4-6
   Configuring Common Options Using the BCE_Config File  4-8
   Encrypting Email  4-9
   Flag and Desktop Encryption Configuration  4-11
      Launching the Email Encryption Plug-in Configuration File  4-11
   Flag Encryption  4-13
      Flag Encryption Options  4-15
   Desktop Encryption  4-18
      Desktop Encryption Options  4-18
   Sending Encrypted Email  4-24
   Manage Secure Messages  4-31
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receiving and Replying To Secure Emails</td>
<td>4-36</td>
</tr>
<tr>
<td>Changing Additional Settings</td>
<td>4-40</td>
</tr>
<tr>
<td>Logging Tab</td>
<td>4-41</td>
</tr>
<tr>
<td>Sending Usage Data Tab</td>
<td>4-42</td>
</tr>
<tr>
<td>Privacy Tab</td>
<td>4-42</td>
</tr>
<tr>
<td>Errors and Troubleshooting</td>
<td>4-42</td>
</tr>
<tr>
<td>Outlook Startup Errors</td>
<td>4-43</td>
</tr>
<tr>
<td>Decryption and Encryption Errors</td>
<td>4-44</td>
</tr>
<tr>
<td>Repairing Cisco Email Encryption Plug-in for Outlook Files</td>
<td>4-46</td>
</tr>
<tr>
<td>Troubleshooting Using the Diagnostic Tool</td>
<td>4-47</td>
</tr>
<tr>
<td>Data Collected by the Cisco Email Encryption Diagnostic Tool</td>
<td>4-47</td>
</tr>
<tr>
<td>Running the Cisco Email Encryption Diagnostic Tool</td>
<td>4-47</td>
</tr>
<tr>
<td>Disabling JavaScript in Envelopes</td>
<td>4-50</td>
</tr>
<tr>
<td>Uninstalling the Cisco Email Encryption Plug-in</td>
<td>4-50</td>
</tr>
<tr>
<td>Cisco End User License Agreement</td>
<td>A-1</td>
</tr>
</tbody>
</table>
CHAPTER 1

Getting Started with the Cisco Email Encryption Plug-in

This chapter contains the following sections:

- Supported Configurations, page 1-2
- Compliance With Security Configuration Guidelines, page 1-2
- Related Documents, page 1-2
- How to Use This Guide, page 1-3
- Cisco Email Encryption Plug-in Overview, page 1-5
Supported Configurations

For information about operating systems supported for release 1.2, see the Cisco Email Encryption Compatibility Matrix.

Compliance With Security Configuration Guidelines

The Cisco Email Encryption Plug-in 1.2 has been tested to confirm that it can operate in the configurations and environments described in the following hardening guides:

- NSA Security Configuration Guides, located at: https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml#microsoft

Related Documents

To use the Encryption plug-in, you need to have a Cisco Email Security Appliance (ESA) running and properly configured to work with the Encryption plug-in or have a Cisco Registered Envelope Service (CRES) account. To understand how to configure the Cisco Email Security Appliance (ESA), you may want to review the following guides:

- Cisco Email Security Appliance 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. To find the guide for your release, see: http://www.cisco.com/en/US/products/ps10154/prod_installation_guides_list.html
How to Use This Guide

Use this guide as a resource to learn about the features in your Cisco Email Encryption Plug-in. 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 to determine which chapters are relevant to your particular configuration.

This guide is distributed electronically as a PDF. The electronic versions of the guide are available on the Cisco Customer Support Portal. You can also access an HTML online help tool in the appliance GUI:

- In Outlook 2010/2013/2016, click the **Plug-in Options** button on the ribbon or go to **File > Options > Add-in Options > Cisco Email Encryption**.
- In Outlook 2007, click the **Plug-in Options** button on the toolbar or go to **Tools > Options > Cisco Email Encryption > Help**.

Where to Find More Information

Cisco offers the following resources to learn more about the Cisco Email Encryption Plug-in.

**Security Training Services & Certification**

Cisco Security Training Services deliver exceptional education and training for Cisco security products and solutions. Through a targeted curriculum of technical training courses, the program provides up-to-date knowledge and skills transfer to different audiences.

Use one of the following methods to contact Cisco Security Training Services:

**Training.** For question relating to registration, general training, certificates, and certification exams:

- stbu-trg@cisco.com
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 users.

You can access the Cisco Support Community from the following URL:

https://supportforums.cisco.com

Cisco Customer Support

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 page for details about your level of support.

You can request support by phone, email, or online 24 hours a day, 7 days a week. You can contact Cisco Customer Support using one of the following methods:

- Phone support: Contact Cisco Technical Assistance Center (TAC) within U.S. /Canada at 800-553-2447 and at Worldwide Phone Numbers.
- Email: tac@cisco.com

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

Cisco Content Security 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
Cisco Email Encryption Plug-in Overview

When the Cisco Email Encryption Plug-in is installed, (you can access it from the Microsoft Outlook) it enables components on Microsoft Outlook mail client. This single interface allows you to send encrypted email. The encryption plug-in places the Encrypt Message button on the toolbar which enables users to either send encrypted email from their email programs or to flag the email to be encrypted before it leaves their organizations. You can lock or unlock encrypted emails, adding or modifying a lock reason. You can also set an expiration date and time for the encrypted email.

The encryption plug-ins provides a convenient interface that enables you to send encrypted messages by using toolbar buttons and right-click context menus.

The Encryption Plug-in requires the presence and proper configuration of a Cisco Email Security Appliance (ESA) or have a Cisco Registered Envelope Service (CRES) account.
Deploying the Cisco Email Encryption Plug-in

This chapter contains the following sections:

- The Encryption Plug-in, page 2-2
- Installing the Cisco Email Encryption Plug-in, page 2-2
- Configuration Modes, page 2-3
- Deploying the Cisco Email Encryption Plug-in with the Cisco Registered Envelope Service (CRES) Key Server, page 2-4
- Configuring Settings for the Cisco Email Encryption Plug-in, page 2-6
- System Processes Required for the Cisco Email Encryption Plug-in, page 2-6
- TCP Services Required for the Cisco Email Encryption Plug-in, page 2-7
The Encryption Plug-in

The Encryption Plug-in places an Encrypt Message button in the menu bar of an email message to provide an easy way for senders to mark messages to be encrypted and secured before it leaves the organization.

There are two types of encryption available: Flag Encryption and Desktop Encryption. The Flag Encryption option allows you to flag the email for encryption, and the email is encrypted by the Cisco Email Security Appliance (ESA) before the email is sent out of the network. Desktop Encryption allows you to encrypt email from within your email program using the Cisco encryption technology. Then, it sends the encrypted email from your desktop. You may want to use Desktop Encryption if you want to ensure that mail sent within your organization is encrypted.

The Encryption plug-in is designed to work with a functioning and configured Cisco Email Security Appliance (ESA), if one exist in your network. The configuration you use for the Encryption plug-in should be developed in conjunction with the settings on these appliances. If you do not use the same configurations for these appliances, issues may occur when sending encrypted messages.

Note

The Encryption Plug-in requires the presence and proper configuration of a Cisco Email Security Appliance (ESA) or have a Cisco Registered Envelope Service (CRES) account.

Installing the Cisco Email Encryption Plug-in

To install the Cisco Email Encryption Plug-in for groups of users, you will likely want to perform a silent installation. A silent installation allows you to perform an installation without prompting the end user for input. For instructions on performing the silent installation, see Chapter 3, “Performing a Mass Installation.”

Note

Do not install the Cisco Email Security Plug-in 7.x with the Cisco Email Encryption Plug-in 1.2. If you need the reporting functionality, install both the Cisco Email Encryption Plug-in 1.x and the Cisco Email Reporting Plug-in 1.x.
Configuration Modes

The Cisco Email Encryption Plug-in is deployed in three separate configuration modes. The default configuration mode is Decrypt Only.

In order to enable the other configuration modes, the Outlook email account is configured by an updated attachment file received from the administrator. The administrator sends a BCE Config file attachment to the end user’s email account (the default name of the file is BCE_Config_signed.xml). The end user will receive this file as a securedoc.html file. When the end user clicks the securedoc.html attachment, the Outlook application detects the configuration information attached to the message and applies the updated configuration.

Note

The default envelope name is securedoc.html. The attachment name value can be changed by the administrator and the envelope will reflect the newly specified name.

The three 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 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.
- **Decrypt and Encrypt**—Allows encrypting and decrypting of secure email messages.

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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Decrypt Only</th>
<th>Decrypt and Flag</th>
<th>Decrypt and Encrypt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send encrypted message</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Flag message for encryption</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Open encrypted email</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Reply/Reply All/Forward Message</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Email lock and unlock</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Deploying the Cisco Email Encryption Plug-in with the Cisco Registered Envelope Service (CRES) Key Server

Use the following instructions to deploy the Cisco Email Encryption Plug-in so that it is used directly with the Cisco Registered Email Service (CRES) key server.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Decrypt Only</th>
<th>Decrypt and Flag</th>
<th>Decrypt and Encrypt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email expiration</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Email diagnostic</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Read-receipt</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Envelope settings</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Settings</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Step 1  Log into your CRES account: https://res.cisco.com/admin and go to the Accounts tab.

Step 2  Select the account from which you want to enable the Email Encryption Plug-in. 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.

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.

---

**Note**

For localization purposes, do not change or reword the existing Message Security labels Low, Medium, or High.

---

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`, unless it is renamed. Save this file to your local machine.

---

Step 7  To deploy the configuration file to many end users at once, use the **Distribute Signed Configuration to Bulk List** option. To do so:

1. **a.** Browse to the signed BCE Config file created in **Step 6**.
2. **b.** Browse to a comma separated file containing the email addresses of end users.
3. **c.** Change the email subject as needed.
4. **d.** Click **Distribute Config**. To perform a mass installation using the signed BCE Config, see the “**Mass Installation Using the BCE_Config.xml File**” section on page 3-29.

---

**Note**

If you forward the xml configuration file to another end user, versus received from the administrator, the auto configuration will not work and an error appears. You can also send the signed configuration file through email that is encrypted by ESA or CRES to all end users. You should send a message from the email address that is listed as Administrator on the CRES account.

---

**Note**

Do not send the signed BCE Config file to a mailing list. CRES does not support mailing lists.
Configuring Settings for the Cisco Email Encryption Plug-in

After you install the Cisco Email Encryption Plug-in, you can make configuration changes from the Cisco Email Encryption tab in Outlook.

- In Outlook 2010/2013/2016, click the Plug-in Options button on the ribbon or go to File > Options > Add-ins > Add-in Options > Cisco Email Encryption.
- In Outlook 2007, click the Plug-in Options button on the toolbar or go to Tools > Options > Cisco Email Encryption.

You can make changes to the Encryption plug-in installation. Or, you can make changes to general options that affect both plug-in installations. For example, you can enable or disable logging for the Cisco Email Encryption Plug-in or you can modify options for a specific encryption mode.

To change the method for marking email for Encryption, you need to make changes to the BCE_Config.xml file and perform an auto-configuration. Any of the specified settings must be compatible with your Cisco Email Security Appliance (ESA).

To make configuration changes on an Outlook installation, see Chapter 4, “Configuring and Using the Cisco Email Encryption Plug-in for Outlook.”

System Processes Required for the Cisco Email Encryption Plug-in

The Cisco Email Encryption Plug-in requires only essential system processes, such as TCP/IP DNS, DHCP, and etc, which cannot be disabled. However, any nonessential system processes, such as database managers, HTTP servers, and hardware configuration daemons can be disabled without affecting the functionality of the Cisco Email Encryption Plug-in.
TCP Services Required for the Cisco Email Encryption Plug-in

The Cisco Email Encryption Plug-in requires the use of the following TCP/IP services and their associated ports. These ports must be left available for the TCP/IP services to use.

- **DNS (Domain Name System).**
  
  The DNS service translates Internet domain and host names to IP addresses. DNS automatically converts the names we type in our Web browser address bar to the IP addresses of Web servers hosting those sites.
  
  Port number: 53 (TCP/UDP)
  
  For more information, see: [http://en.wikipedia.org/wiki/Domain_Name_System](http://en.wikipedia.org/wiki/Domain_Name_System)
  
  Impact: High
  
  Resolution: This service must be accessible to all end users.

- **SMTP (Simple Mail Transfer Protocol)**
  
  Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.
  
  Port number: 25, 587, 465, 475, 2525 (TCP)
  
  
  Impact: High
  
  Resolution: This service must be accessible to all end users.

- **DHCP (Dynamic Host Configuration Protocol)**
  
  DHCP is a network protocol used to configure devices that are connected to a network (known as hosts) so they can communicate on that network using the Internet Protocol (IP)
  
  Port number: 67, 68 (TCP/UDP)
  
  
  Impact: High
Resolution: This service must be accessible to all end users which obtain IP addresses automatically from DHCP server.

- Net BIOS over TCP/IP
  NetBIOS over TCP/IP (NBT, or sometimes NetBT) is a networking protocol that allows legacy computer applications relying on the NetBIOS API to be used on modern TCP/IP networks.
  Port number: 137(UDP) (name services), 138(UDP) (datagram services), 139(TCP) (session services)
  For more information, see: http://en.wikipedia.org/wiki/NetBIOS_over_TCP/IP
  Impact: High
  Resolution: This service must be accessible to all end users.

- HTTP (Hypertext Transfer Protocol)
  The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems.
  Port number: 80, 8080 (TCP)
  For more information, see: http://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol
  Impact: High
  Resolution: This service must be accessible to all end users.

- HTTPS (Hypertext Transfer Protocol Secure)
  HTTPS is a communications protocol for secure communication over a computer network, with especially wide deployment on the Internet.
  Port number: 443 (TCP)
  For more information, see: http://en.wikipedia.org/wiki/HTTP_Secure
  Impact: High
  Resolution: This service must be accessible to all end users.

- IMAP (Internet message access protocol)
  Internet message access protocol allows an e-mail client to access e-mail on a remote mail server.
Port number: 143, 993 (TCP)
For more information, see:
Impact: High
Resolution: This service must be accessible to all end users.

- POP3 (Post Office Protocol)
Post Office Protocol is used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection.
Port number: 110, 995 (TCP)
For more information, see:
Impact: High
Resolution: This service must be accessible to all end users.
Performing a Mass Installation

This chapter describes how to perform a mass installation on multiple desktops and contains the following sections:

- Installation Prerequisites, page 3-1
- Cisco Email Encryption Plug-in Mass Installation Tool, page 3-2
- Performing the Installation, page 3-12
- Using Custom Configuration Files, page 3-27

Installation Prerequisites

Before you can install the Cisco Email Encryption Plug-in application, ensure that you meet the following requirements:

- Java Runtime Environment 1.8
- Microsoft .NET Framework 4.5.1
- Microsoft Office Primary Interop Assemblies

In case you do not have these items installed, you will be prompted to install all software from prerequisites list by the Plug-in installer.
Cisco Email Encryption Plug-in Mass Installation Tool

The Cisco Email Encryption Plug-in Mass Installation allows creating package for distribution of the Cisco Email Encryption Plug-in for users within your organization.

You can select the server where the distribution package will be stored, local or remote machine on the Server Connectivity step.

Also, you can modify the default configuration by editing common and account options. You might want to use different configuration files to change various aspects of the installation, for example, you can change some of default options by customizing different parameter values. Also, you can predefine configurations only for selected users in a specific domain, localize user interface or even customize the button names.

You can upload the ready customized CommonComponentsConfig.xml and/or config_{n}.xml files.

On the final step, you will get a shared folder path with all files needed to perform the Mass Installation and the ready customized script that you must copy and reuse in the SCCM Administrator Tool.

Options Modified by the Mass Installation

The Cisco Email Encryption Plug-In Mass Installation modifies the following Options used in the process of installation:

- Common Options, such as Language, Logging, Sending usage data to Cisco, Check for updates, and other.
- Account options (configurations predefined for users of the specified domain).

Running the Mass Installation Tool

Run the Cisco Email Encryption Mass Installation from either Start Menu or Program Files folder.
From the Start Menu:

- Click the **Start Menu** button and go to **Cisco Email Encryption Plug-in > Cisco Email Encryption Plug-in Mass Installation**.

OR

From the Program Files:

- Go to the folder where Cisco Email Encryption Plug-in was installed (typically `C:\Program Files (x86)\Cisco\Cisco Email Encryption Plug-in`) and double-click the `Cisco.EmailSecurity.MassInstall.exe` file.

### Preparing the Mass Installation Package and Script

Follow this procedure:

**Step 1** Run the Mass Installation tool.

**Step 2** In the **Welcome** window that appears, click **Next**.
Step 3  In the Server Connectivity window, choose preferable connectivity: use the local machine or use remote machine. If you choose the remote machine, complete the Machine name or IP address, Username, and Password fields, and then click Next.

Step 4  In the Package Options window, specify locations for creating of the installation package, and then click Next.
Step 5  In the **Common Options** window, specify the preferable Plug-in common components configuration for all created accounts, and click **Next**.
Step 6  In the **Account Options** window, you must log in with administrator credentials on key server to receive a valid configuration file and sign it. Then, set up the plug-in options to be applied for the specified domains, and then click **Next**.
Chapter 3      Performing a Mass Installation

Cisco Email Encryption Plug-In Mass Installation

Accounts Options
Set Plug-In options to be applied for the specified domains

Welcome
Server Connectivity
Package Options
Common Options
Accounts Options
Mass Installation
Summary

Key Server address: https://res.cisco.com
Username: Enter username, e.g. user1@domain.com
Passphrase: Enter passphrase

Add Config
Cancel Log In

< Back Next > Cancel

Cisco Email Encryption Plug-In Mass Installation

Accounts Options
Set Plug-In options to be applied for the specified domains

Welcome
Server Connectivity
Package Options
Common Options
Accounts Options
Mass Installation
Summary

domain1.com Encrypt
Key server: res.cisco.com

domain2.com Flag
Key server: res.cisco.com

Domain3.com Decrypt
Key server: res.cisco.com

Add Config

< Back Next > Cancel
Step 7  In the **Accounts Options** window, click the **Edit** icon to set up the plug-in options. Click **Save** and then click **Next**.

Step 8  In the **Mass Installation** window, to start the Mass Installation process, click **Start**.
Step 9  Wait till the processing of Mass Installation is complete and click **Next**.
Step 10 In the **Summary** window, you will receive the package location path and Mass Installation script.

The distribution package with the configuration files to be used during installation is now created in the shared folder. You can copy path to this folder or click 'Open' to view its contents.

Specified command can be used in the command line to install Cisco Email Encryption Plug-In with the predefined settings via SCCM Administration Tool on remote machines within your organization. To work with SCCM Administration Tool, see the *Cisco Email Encryption Plug-in Mass Installation Tool*, page 3-2.

After you copy this script to reuse it in the SCCM tool, click **Finish**.
After the package and the shared folder are created, verify the **Share Permissions** for this folder by checking its properties. The permissions should be set to **Everyone**. If not, please set it manually. The procedure to share folder with other users may vary in different operating systems.
Performing the Installation

To perform the installation, complete the following steps to create a network shared folder, distribution package, New Package Wizard, and New Program Wizard.

To perform the installation:

---

**Step 1** Download the installation package and verify the checksum.

a. Use the Quick Hash GUI and the SHA512 hash algorithm at the following URL to generate the checksum for your installation package:


b. Verify that the generated checksum matches the following:

   E858C451B9E638DD475BE3C79E53B6EA24DEA2827EEE786921BD0643DA2FA963EB72F9A8ECC4DB57DBC4BF9C7B8E7448208E450808E1693E1658C758C8E

---

**Step 2** Create a network shared folder that contains the installation package and give users access to the shared folder.

**Note** You cannot perform an installation from a dropbox, a network drive, or a shared system folder.

---

**Step 3** Open the SCCM administrative tool.
**Step 4**  Create a new software distribution package.
Step 5  Enter a name for the package, and click **Next**.
Step 6  Specify the network source directory that you created in Step 2 by entering the following path to the network shared folder: \sc2007\Shared\MSC.Install\Cisco Email Encryption Plug-in.exe. You can enter the path or browse to the folder. Click Next.

Step 7  Continue to the next step in the New Package Wizard, and click Next.
Step 8  View the confirmation that the New Package Wizard completed successfully, and click Close.
Step 9  Create a new distribution point, and click **Next** on the Welcome page.
**Step 10** Select the new distribution point. Click through the next pages on the New Distribution Points Wizard, and click **Close**.

![New Distribution Points Wizard](image)

Select the new distribution points that you want to copy the package to.

To copy the package to the new distribution points, click Next.
Step 11  Create a new program.
Step 12 In the command line field, enter the following command: “Cisco Email Encryption Plug-in.exe” /exenoui /qn

Note If you want to use customized configuration files, you need to add a special key during this step which enables the installation to use the customized files. You add the special key from the command line (specifying the location of the custom configuration files after the = sign) using the following syntax:

“Cisco Email Encryption Plug-in.exe” /exenoui /qn
UseCustomConfig="\sc2007\Shared\config"

For more information about customizing your configuration files, see Using Custom Configuration Files, page 3-27.

Step 13 In the Run field, enter Hidden, and then click Next.

Step 14 Click through the requirements page, and then click Next.
Step 15  Select the following environment options:

- **Program can run**: Only when the user is logged on. If Run mode is set to administrative rights, then **Program can run** can be set to **Whenever the user is logged on**.

- **Run mode**: Run with user's rights, or run with administrative rights if users don't have sufficient permissions to install new software.

Step 16  Confirm that the New Program Wizard completed successfully, and click **Close**.
Step 17  Create a new advertisement.
Step 18  Enter a name, select the package and program that you created. Select the collection that contains the group of clients where you want to install the plug-in. Click Next.
Step 19   Set the assignment as mandatory. Click Next.

Step 20   Select the switches based on your preferences. At least one Mandatory assignment should be set. Do not select Do Not Run Program, as the program will not start if the connection is slow. Click Next.

Step 21   Click through the New Advertisement Wizard, and click Next.
Step 22 View the confirmation that the New Advertisement Wizard completed successfully, and click Close.
Step 23 View the Advertisement Status in the Advertisement Status window.
Step 24 You can create an advertisement report to view more details by selecting Show Message > All from the Context menu. If an error occurred, you can review the report to see where the error occurred.

Using Custom Configuration Files

The Cisco Email Encryption Plug-in allows you to modify the default configuration by editing a set of XML files included in your installation. You might want to use different configuration files to change aspects of the installation. For example, in the config_1.xml configuration file, you might change some of the encryption options, such as the file flagging method (Only make this change if you are also able to change the method on the Encryption appliance). You may also want to customize the button names, or even localize the text used in the user interface.
Overview

To modify and deploy custom configuration files, complete the following steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Make a copy of the <code>\%allusersprofile%\Cisco\Cisco Email Encryption Plug-In</code> directory. It is required to include the Common folder.</td>
</tr>
<tr>
<td>Note</td>
<td>You must maintain the directory structure of the original files to maintain validity. Make sure that you maintain the structure starting at the Cisco Email Encryption Plug-in directory and include all files with configuration files.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Edit the XML configuration files. Rather than creating new files, Cisco recommends you modify the XML files included in the installation file. For instructions on modifying these files, see Editing the XML Configuration Files, page 3-28.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Run the mass installation as described in Installation Prerequisites, page 3-1, and deploy the customized XML files as described in Deploying the Custom Configuration Files, page 3-31.</td>
</tr>
</tbody>
</table>

Editing the XML Configuration Files

When you install the Cisco Email Encryption Plug-in, configuration data is created and saved in XML files. You can edit the string values to customize the parameter values. However, Cisco does not recommend you remove values or modify the structure of the files.

By default, the plug-in installs configuration files in the `%AllUsersProfile%` directory in the following locations for Outlook:

`%allusersprofile%\Cisco\Cisco Email Encryption Plug In`

The XML files are located in the following default locations:

- `\%allusersprofile%\Cisco\Cisco Email EncryptionPlug-In\Common\config_1.xml, config_{N}.xml`. These numbers are dependent on the count of user accounts. Contains configuration data related to the Desktop Encryption plug-in.
Chapter 3      Performing a Mass Installation

- `\%allusersprofile%\Cisco\Cisco Email EncryptionPlug-In\Common\CommonComponentsConfig.xml`. Contains basic configuration data for the Encryption plug-in, such as the location of the log files and the name of the localization file (`en.xml` is the default localization file). You can use your email program settings to change the log file location, and deploy it with your mass installation program. If you want to create a localization file in a language other than the available localization files, you need to reference the name of the new XML file here.

- `\%allusersprofile%\Cisco\Cisco Email EncryptionPlug-In\Common\Localization\en.xml`. Contains data related to local languages. The default language is English. However, there are several localization files available, including `de.xml`, `es.xml`, `fr.xml`, `it.xml`, `zh.xml`, `pt.xml`, and `ja.xml`. If you want to use a language that is not within the scope of these XML files, you can create a custom XML file and reference it in the CommonConfig.xml file.

⚠️ **Caution**
Do not change any string id settings that are inside the `<` or `>` symbols, as this will prevent your plug-in from functioning properly.

## Mass Installation Using the BCE_Config.xml File

To perform a mass installation using the BCE_Config.xml file:

1. Navigate to the `\%allusersprofile%\Cisco\Cisco Email Encryption Plug-In\Common` directory.
2. Remove the `config_1.xml` file, if any exists.
3. Copy the BCE Config file (named `BCE_Config_signed.xml` by default) to this directory and rename the file back to `config_1.xml`.
4. Navigate to the `\%allusersprofile%\Cisco\Cisco Email Encryption Plug-In\CommonComponentsConfig.xml` file.
5. Verify that the `CommonComponentsConfig.xml` file includes these tags:

```xml
<accountFileNames>
  <accountFileName filePath="config_1.xml" emailAddressAndKeyServer="*" />
</accountFileNames>
```
Tip

Make sure that the accountFileName tag does not include the profileName attribute. If this attribute is present, remove it.

Note

To configure only selected users in a specific domain, you need to modify the CommonComponentsConfig.xml file by specifying the domain as an email address.

For example, to apply the BCE config file to only Cisco users, change the:

```xml
<accountFileName filePath="config_1.xml" emailAddressAndKeyServer="*" />
```

to:

```xml
<accountFileName filePath="config_1.xml" emailAddressAndKeyServer="@cisco.com" />
```

If there is more than one accountFileName tag then the filePath will be config_2.xml, config_3.xml, etc.

For example:

```xml
<accountFileName filePath="config_2.xml" emailAddressAndKeyServer="@cisco.com" />
```

Step 6

Run the mass installation as described in Installation Prerequisites, page 3-1 and deploy the customized XML files as described in Deploying the Custom Configuration Files, page 3-31.

Note

The %allusersprofile%\Cisco\Cisco Email Encryption Plug-In\Common directory content must be copied to \{SHARED_DIR}\{CONFIG_FOLDER}. The Common folder must exist in {CONFIG_FOLDER}. The UseCustomConfig command parameter enables the installation to use the custom configuration file that you modified.
Deploying the Custom Configuration Files

Once you have completed editing the configuration files, you will need to add a special key during deployment to ensure that the installer uses the custom configuration files you modified. The UseCustomConfig command line parameter enables the installation to use custom configuration files and specifies the path to the folder containing configuration files which should be used during the installation.

You add the UseCustomConfig key from the command line during Step 12 of the mass installation (see Installation Prerequisites, page 3-1) using the following syntax:

Cisco Email Encryption Plugin.exe /exenoui /qn
UseCustomConfig="\{SHARED_DIR}\{CONFIG_FOLDER}\"

where the path after the = specifies the path to the customized configuration files.
This chapter introduces the features available in the Cisco Email Encryption Plug-in for Outlook. The Cisco Email Encryption Plug-in includes several types of plug-ins that work with the Outlook email program. This chapter contains the following sections:

- Enabling the Cisco Email Encryption Plug-in, page 4-2
- Configuring the Sending of Usage Data, page 4-2
- Configuring Basic Settings for the Outlook Plug-in, page 4-5
- Configuring the Outlook Plug-in to Check for Updates, page 4-6
- Configuring Common Options Using the BCE_Config File, page 4-8
- Encrypting Email, page 4-9
- Flag and Desktop Encryption Configuration, page 4-11
- Flag Encryption, page 4-13
- Desktop Encryption, page 4-18
- Changing Additional Settings, page 4-40
- Errors and Troubleshooting, page 4-42
- Troubleshooting Using the Diagnostic Tool, page 4-47
- Disabling JavaScript in Envelopes, page 4-50
- Uninstalling the Cisco Email Encryption Plug-in, page 4-50
Enabling the Cisco Email Encryption Plug-in

The first time you start the Cisco Email Encryption Plug-in after installation, it might be disabled by Outlook. If this is the case, you see the following message:

![ADD-IN PROBLEM A problem was detected with an add-in and it has been disabled. View Disabled Add-ins](image)

To enable the Cisco Email Encryption Plug-in, click the View Disabled Add-ins button on the notification bar to display the Disabled Add-ins dialog. To configure Outlook to always allow the add-in to run no matter how much time it requires during startup, click the Always enable this add-in button.

Configuring the Sending of Usage Data

When the Cisco Email Encryption Plug-in is first started, you are asked whether you want to allow anonymous data to be sent to Cisco to help improve the product. When you select the Send anonymous usage data to Cisco check box, the following two types of information will be collected and stored on Cisco servers for analysis:

- General information about the machine the plug-in is running on
- Account-specific information

The details of this information are described below.

You can enable or disable the sending of usage data after the startup by selecting Plug-in Options > Additional Options > Sending usage data tab.

To enable or disable the sending of usage data to Cisco, set the following parameter in the CommonComponentsConfig.xml file:

- callHomeAdminEnabled—Set to true or false to enable or disable the sending of usage data when Outlook starts. The default value is true. If set to false, the user will not receive the notification about usage data collection and will not be able to send anonymous usage data to Cisco.

General Information

The following information is collected:
• Identifier (UUID) - A non-permanent identifier that is generated when the plug-in is first installed. It is used solely to correlate the usage reports so that the usage data can be tracked over time. You can reset the identifier by selecting Plug-in Options > Additional Options > Privacy tab.

• Version of the Operating System

• Version of Microsoft Outlook

• Version of the Cisco Outlook Plug-in

• Version of the Cisco Encryption SDK - This SDK is the library used internally by the plug-in to encrypt and decrypt secure messages.

• Language used for the Operating System

• Names of all of the installed Outlook plug-ins

**Account-Specific Information**

The following information is collected:

• Account Type - The type is either encrypt, decrypt, or flag.

• Server

• Recipients count - The number of recipients added during encryption since installation, which includes recipients that were added during flagging.

• Decrypted count - The number of messages that have been decrypted using the plug-in.

• Encrypted count - The number of messages that have been encrypted on the device since installation, which includes the number of messages that have been flagged.

• Manage messages count - The number of times the Manage Messages screen was accessed.

• Manage messages usage count - The number of messages updated using the Manage Messages screen.
Cisco Email Encryption Plug-in For Outlook

General Settings

General settings for the Cisco Email Encryption Plug-in can be configured from the Options page.

Enable or Disable

By default, the Cisco Email Encryption Plug-in is enabled upon installation. The Cisco Email Encryption Plug-in can be disabled from the following places:

- In Outlook 2010/2013/2016, go to **File > Options** and select **Add-ins** from the left navigation bar. Then, select **COM Add-ins** from the Manage drop-down menu at the bottom of the page, and click **Go**...

- In Outlook 2007, go to **Tools > Trust Center** and select **Add-ins** from the left navigation bar. Then, select **COM Add-ins** from the **Manage** drop-down at the bottom of the page and click **Go**.

![COM Add-Ins Window](image)

From the COM Add-Ins window, clear the Cisco Email Encryption Plug-in check box and click **OK**.
Configuring Basic Settings for the Outlook Plug-in

The end user can configure basic settings from the Cisco Email Encryption tab.

- In Outlook 2010/2013/2016, click the **Plug-in Options** button on the ribbon or go to **File > Options > Add-ins > Add-in Options > Cisco Email Encryption**.
- In Outlook 2007, click the **Plug-in Options** button on the toolbar or go to **Tools > Options > Cisco Email Encryption**.

Cisco Email Encryption tab:

From this tab, the end user can enable encryption options by selecting the **Enable** check box. The end user can also enable additional options by selecting the **Additional Options** button. To further configure the settings, click the **Encryption Options** or **Additional Options** buttons. The end user can also use the Diagnostic tool to run a report on the Cisco Email Encryption Plug-in to send
to Cisco Support when problem-solving. You can also configure the Plug-in to send anonymous usage information (general information about the Plug-in’s usage) to the server when Outlook is started.

### Configuring the Outlook Plug-in to Check for Updates

To configure the plug-in to automatically check for updates, set the following parameters in the checkForUpdates section of the CommonComponentsConfig.xml file:

- **checkAutomatically**—Set to true or false to enable or disable the automatic checking of updates when Outlook starts. The default value is true.
- **serverURL**—Set to the URL that the plug-in will use to check whether a new version is available.
- **ignoredVersion**—Set to the version number that you want the plug-in to ignore when it looks for updates.

### Update Notifications

If the Desktop Encryption plug-in is configured to automatically check for updates and the current version of the Desktop Encryption plug-in is not the latest version, the following dialog box will be displayed when Outlook starts up:

![Update Notification Dialog Box](image)
**Note**

You need to have the appropriate rights to download the Cisco Email Encryption Plug-in application.

To check for updates after Outlook starts up, click the **About** button in the **Plug-in Options** window, and then click the **Check for updates** button in the following dialog box:

![Cisco Email Encryption Plug-In](image_url)
Configuring Common Options Using the BCE_Config File

Options that are common to all Outlook accounts and the entire plug-in are contained in the CommonComponentsConfig.xml file. These options are:

- **diagnosticSupportAddress**—Specifies the email address of the recipient of the message that is sent when the Diagnostic Tool is run. The message contains the output of the Diagnostic Tool.
- **diagnosticReportSubject**—Specifies the subject of the message that is sent when the Diagnostic Tool is run.
- **showPluginOptions**—Set to true or false to enable or disable the Plug-in Options button that opens the Plug-in Options dialog box where you can use the encryption, diagnostic, and additional options. If set to false, the Plug-in Options button will be hidden.
- **showManageMessageButton**—Set to true or false to enable or disable the Manage Messages button that opens the Manage Messages dialog box where you can lock messages or set the expiration date of messages. If set to false, the Manage Messages button will be hidden.
- **checkAutomatically**—Set to true or false to enable or disable the automatic checking of updates when Outlook starts. The default value is true. For more information, see the “Configuring the Outlook Plug-in to Check for Updates” section on page 4-6.
- **serverURL**—Set to the URL that the plug-in will use to check whether a new version is available.
- **callHomeAdminEnabled**—Set to true or false to enable or disable the sending of usage data when Outlook starts. The default value is true. If set to false, the user will not receive the notification about usage data collection and will not be able to send anonymous usage data to Cisco. For more information, see the “Configuring the Sending of Usage Data” section on page 4-2.
- **callHomeEnabled**—Set to true or false to enable or disable the sending of usage data when Outlook starts. The default value is true. If set to false, the user will not be able to send anonymous usage data to Cisco. For more information, see the “Configuring the Sending of Usage Data” section on page 4-2.
If these options are configured in the BCE_Config.xml file, they are copied to the CommonComponentsConfig.xml, when the plug-in applies the BCE_Config.xml. Otherwise, to modify these options in a user environment, you must perform a mass installation with the UseCustomConfig option. For more information, see the “Mass Installation Using the BCE_Config.xml File” section on page 3-29.

In a similar way, you can also configure options in account specific files (config_1.xml, config_2.xml, and so on) by applying the BCE_Config. However, you cannot configure logging settings or plug-in localization using the BCE_Config.xml file.

## Encrypting Email

The encryption plug-in allows end users to encrypt mail from the desktop or flag email to be encrypted before sending email out of their company network. Choose one of the following encryption options:

- **Flag Encryption.** The Flag Encryption option allows the end user to flag email for encryption, and the email is encrypted by the Cisco Email Security Appliance (ESA) before it is sent out of the network. You may want to use Flag Encryption if the end user needs to send encrypted mail outside their organization, but don’t require the email to be encrypted within their organization. For example, their organization works with sensitive medical documents that need to be encrypted before being sent to patients.

- **Desktop Encryption.** Desktop Encryption allows the end user to encrypt email from within Outlook using the Cisco encryption technology. Then, it sends the encrypted email from their desktop. You may want to use Desktop Encryption if the end user wants to ensure that mail sent within their organization is encrypted. For example, their organization requires all sensitive financial data to be encrypted when sent both within and outside of the organization.
Figure 4-1  Workflows for Flag Encryption vs. Desktop Encryption

The encryption method is determined by decrypting the signed BCE Config file attachment from the Outlook email account. Decrypt Only mode is enabled by default. The end user can choose to modify their installation in order to change the encryption method by receiving and decrypting an updated signed BCE Config file from you, the administrator.
Flag and Desktop Encryption Configuration

The default configuration mode for the end user Outlook email account is Decrypt Only. In order to enable the Flag or Encrypt feature, the end user email account is configured by an updated attachment file received from the administrator. Also, the Flag and Encrypt feature can be enabled via Mass Install when a set of configuration files are provided directly to the user's configuration folder. If a decrypted message contains a signed BCE Config file attachment, the Encryption Plug-in for Outlook is automatically configured when the end user launches this configuration file. The Cisco Registered Envelope Service (CRES) is used as a key server. If the end user does not have an account, they are prompted to register.

Three configuration modes are available:

- **Decrypt Only.** Allows decrypting of encrypted emails received.
- **Decrypt and Flag.** 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 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 message.

Launching the Email Encryption Plug-in Configuration File

The end user enables and configures the encryption for their Outlook email account by decrypting the signed BCE Config file attachment from their Outlook email account. If the end user does not see the notification email with the attachment in their inbox, check the spam or junk folder.

When launching the configuration file, the plug-in is configured for the email account that received the notification message with the signed BCE Config file attachment.

**Note**

Normally, the Java Runtime Environment (JRE) is automatically installed during the plug-in installation. However, if this does not happen, please install at least version 1.8 to use with the plug-in.
To enable and configure the Cisco Email Encryption Plug-in for the Outlook email account:

**Step 1**  Open the notification email message with the signed BCE Config file attachment. The end user is asked if they want to apply the settings.

**Step 2**  Click **Yes** to automatically configure the Cisco Email Encryption Plug-In. A message displays after the configuration has been successfully applied.

If you select the **Apply Common Plug-in Setting** check box, common plugin settings will also be applied. For more information about common plugin settings, see the “Configuring Common Options Using the BCE_Config File” section on page 4-8.
Flag Encryption

The Flag Encryption option allows the end user to flag the email for encryption, and the email is encrypted by the Cisco Email Security Appliance (ESA) before the email is sent out of the network. If mail leaving the corporate network needs to be scanned for spam or viruses, the Flag Encryption method should be used.

The Flag Encryption settings are located on the Cisco Email Encryption page. To modify the Flag Encryption settings:

- In Outlook 2010/2013/2016, click the Plug-in Options button on the ribbon or go to File > Options > Add-ins > Add-in Options > Cisco Email Encryption > Encryption Options.
- In Outlook 2007, click the Plug-in Options button on the toolbar or go to Tools > Options > Cisco Email Encryption > Encryption Options.

Enable and disable the Encryption plug-in by selecting or clearing the Enable check box in the Encryption field of the Cisco Email Encryption tab.

Select Enable to enable the email program to send sensitive mail via a secure envelope.
Cisco Email Encryption Add-in Options page:
Flag Encryption Options

When you click **Encryption Options**, the Encryption Accounts page appears. The Encryption Accounts page displays all email user accounts for the Flag Encryption Plug-in. Each row displays an Outlook account email address with the associated key server and the encryption type (Flag or Encrypt). Click **Options** or double-click an Account Address to open the account Encryption Options page.

Encryption Accounts page:

---

**Note**
A new account in Outlook will be automatically added in the Encryption Accounts list. And when an Outlook account is removed, that account is automatically removed from the Encryption Accounts list.
Options for Sending Flag Encrypted Email

When the end user wants to encrypt outgoing email, you will need to mark or “flag” the email for encryption. This allows filters created by you to identify the messages that need to be encrypted.

Note

These methods for flagging email for encryption require changes in email filters to work properly and only an administrator can make these changes.

The Encrypt Message button is available when composing emails. Emails can be marked for encryption using one of the following methods:

General Tab

You can select from the following General options:

<table>
<thead>
<tr>
<th>General Options</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flag Subject Text</td>
<td>Text that can be added to the Subject field of the outgoing email to flag the email for encryption. Enter the text to append to the Subject field to denote that the email should be encrypted (the default value is [SEND SECURE]).</td>
</tr>
<tr>
<td>Flag X-header name/value</td>
<td>An x-header can be added to the outgoing email that will flag the email for encryption. Enter an x-header in the first field (the default value is x-ironport-encrypt). In the second field, enter a value of true or false. If you enter true, then a message with the specified x-header will be encrypted (the default value is true).</td>
</tr>
<tr>
<td>Flag Sensitivity header</td>
<td>Outlook can add a sensitivity header to flag the message for email encryption. Selecting this method allows you to use Outlook's sensitivity header to mark emails for encryption.</td>
</tr>
</tbody>
</table>
Chapter 4  Configuring and Using the Cisco Email Encryption Plug-in for Outlook

Connection Tab

You can select from the following Connection options:

<table>
<thead>
<tr>
<th>Connection Options</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>No proxy</td>
<td>Select if you are not using a proxy.</td>
</tr>
<tr>
<td>Use system proxy settings</td>
<td>Select to use the default system proxy settings.</td>
</tr>
<tr>
<td>Manual proxy configuration</td>
<td>Select to enter settings for a specific proxy.</td>
</tr>
<tr>
<td>Protocol</td>
<td>If you choose not to use default connection settings choose one of the following protocols: HTTP, SOCKS4, SOCKS4a, or SOCKS5.</td>
</tr>
<tr>
<td>Host</td>
<td>Specify a host name or IP address for the system or proxy server.</td>
</tr>
<tr>
<td>Port</td>
<td>Specify a port for the system or proxy server.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter a username if it is required for your server.</td>
</tr>
<tr>
<td>Passphrase</td>
<td>Enter the passphrase associated with the username you entered for your system or proxy server.</td>
</tr>
</tbody>
</table>

Remember Passphrase Tab

Select from the following Remember Passphrase options:

<table>
<thead>
<tr>
<th>Passphrase Options</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Never</td>
<td>When selected, the encryption passphrase is always required when decrypting and encrypting emails.</td>
</tr>
<tr>
<td>Always</td>
<td>When selected, the encryption passphrase is required only for the first time when decrypting an encrypted email. Then the passphrase is cached.</td>
</tr>
<tr>
<td>Minutes</td>
<td>Select this option to ensure that the encryption passphrase is cached. Type the number of minutes to remember the passphrase, or use the arrows to modify the entry. After the specified duration, the end user must re-enter the encryption passphrase to decrypt an encrypted email. The default is 1440 minutes.</td>
</tr>
</tbody>
</table>
Desktop Encryption

The Desktop Encrypt option allows the end user to encrypt email from within Outlook and sends the encrypted email from their desktop.

The Desktop Encryption settings are located on the Cisco Email Encryption page. To modify the Desktop Encryption settings:

- In Outlook 2010/2013/2016, click the **Plug-in Options** button on the ribbon or go to **File > Options > Add-ins > Add-in Options > Cisco Email Encryption > Encryption Options**.

- In Outlook 2007, click the **Plug-in Options** button on the toolbar or go to **Tools > Options > Cisco Email Encryption > Encryption Options**.

The end user can enable and disable the Encryption plug-in by selecting or clearing the **Enable** check box in the Encryption field of the Cisco Email Encryption tab. Select **Enable** to enable the email program to send sensitive mail via a secure envelope.

**Note**

The end user can enable or disable the Encryption plug-in from the Cisco Email Encryption page, although any changes to the encryption mode need to be made by the administrator in the *BCE_config.xml* file.

Desktop Encryption Options

When you click **Encryption Options**, the Encryption Accounts page opens.

The Encryption Accounts page displays all email user accounts for the Flag Encryption Plug-in. Each row displays an Outlook account email address with the associated key server and the encryption type (Flag or Encrypt). Click **Options** or double-click an Account Address to open the account Encryption Options page.
Encryption Accounts page:

![Encryption Accounts](image)

**Note**
A new account in Outlook will be automatically added in the Encryption Accounts list. And when an Outlook account is removed, that account is automatically removed from the Encryption Accounts list.

### General Tab

**Note**
The following table shows all of the possible options in the General tab. Depending on the setting of your *BCE_config.xml* file, some of these options may not be visible or available.

Select from the following General options:

<table>
<thead>
<tr>
<th>General Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use as default encryption account</td>
<td>Select to set the account as the default encryption account.</td>
</tr>
<tr>
<td>Encrypt by default</td>
<td>Select to allow all sent email messages to be encrypted by default.</td>
</tr>
<tr>
<td>Server URL</td>
<td>Enter the URL for your Encryption server.</td>
</tr>
<tr>
<td>General Option</td>
<td>Value</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Always use message body from key server</td>
<td>Enables the plug-in to determine which language to use for the message body, according to the locale set for each recipient. Use this option when you want to send encrypted messages to recipients who have the same locale. If you disable this option, the message body will always use the default language you select for the option below.</td>
</tr>
<tr>
<td>Default language for outgoing messages</td>
<td>Specifies the language that will be used for outgoing messages when you are sending the message for recipients with different locales (the checkbox directly above is checked).</td>
</tr>
<tr>
<td></td>
<td>Specifies the language that will be used for all outgoing messages (the checkbox directly above is unchecked)</td>
</tr>
<tr>
<td>Token File Name</td>
<td>Tokens are customer specific keys used to encrypt data between the email client and the Encryption server. Currently, this information is only used by customer support and should not be modified.</td>
</tr>
<tr>
<td>Default Expiration (days)</td>
<td>Specify, in days, how long the encrypted email remains valid. After the number of expiry days is met, the message expires, and it cannot be opened by the recipient after this period.</td>
</tr>
<tr>
<td>Default read-by (days)</td>
<td>Specify, in days, the time period during which the recipient is expected to read the encrypted message. If the message is not read within the specified time frame, the sender is notified.</td>
</tr>
<tr>
<td>Attachment name</td>
<td>The default envelope name is securedoc.html. The attachment name can be changed and the envelope will reflect the newly specified name.</td>
</tr>
</tbody>
</table>

### Connection Tab

Select from the following Connection options:

<table>
<thead>
<tr>
<th>Connection Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>No proxy</td>
<td>Select if you are not using a proxy.</td>
</tr>
<tr>
<td>Use system proxy settings</td>
<td>Select to use the default system proxy settings.</td>
</tr>
<tr>
<td>Manual proxy configuration</td>
<td>Select to enter settings for a specific proxy.</td>
</tr>
<tr>
<td>Connection Option</td>
<td>Value</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------</td>
</tr>
<tr>
<td>Protocol</td>
<td>If you choose not to use default connection settings choose one of the following protocols: HTTP, SOCKS4, SOCKS4a, or SOCKS5.</td>
</tr>
<tr>
<td>Host</td>
<td>Specify a host name or IP address for the system or proxy server.</td>
</tr>
<tr>
<td>Port</td>
<td>Specify a port for the system or proxy server.</td>
</tr>
<tr>
<td>User Name</td>
<td>Enter a user name if it is required for your server.</td>
</tr>
<tr>
<td>Passphrase</td>
<td>Enter the passphrase associated with the user name you entered for your system or proxy server.</td>
</tr>
</tbody>
</table>

### Remember Passphrase Tab

Select from the following Remember Passphrase options:

<table>
<thead>
<tr>
<th>Passphrase Options</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Never</td>
<td>When selected, the encryption passphrase is always required when decrypting and encrypting emails.</td>
</tr>
<tr>
<td>Always</td>
<td>When selected, the encryption passphrase is required only for the first time when decrypting an encrypted email. Then the passphrase is cached.</td>
</tr>
<tr>
<td>Minutes</td>
<td>Select this option to ensure that the encryption passphrase is cached. From the drop-down, select the cache duration in minutes. After the specified duration, the end user must re-enter the encryption passphrase to decrypt and encrypt emails. The default is 1440 minutes.</td>
</tr>
</tbody>
</table>
Advanced Tab

Note

The following table shows all of the possible options in the General tab. Depending on the setting of your BCE_config.xml file, some of these options may not be visible or available.

Select from the following Advanced options:

<table>
<thead>
<tr>
<th>Advanced Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unsecure server URL</td>
<td>Unsecure base URL to use for message bar help. If omitted, then external secure URL is used. i.e. <a href="http://res.cisco.com">http://res.cisco.com</a>.</td>
</tr>
<tr>
<td>Connection timeout</td>
<td>Length of time to wait for a connection to the key server to be established.</td>
</tr>
<tr>
<td>Socket timeout</td>
<td>Length of time to wait for data from the key server.</td>
</tr>
<tr>
<td>Display &quot;Open offline&quot; check box</td>
<td>When selected, the check box for Open offline is visible on the envelope.</td>
</tr>
<tr>
<td>Display &quot;Remember envelope key&quot;</td>
<td>When selected, the check box for Remember envelope key is visible on the envelope.</td>
</tr>
<tr>
<td>Display &quot;Enable personal security phrase&quot;</td>
<td>When selected, the check box for Enable personal security phrase is visible on the envelope.</td>
</tr>
<tr>
<td>Add message bar</td>
<td>Select to add the message bar to the secure message.</td>
</tr>
<tr>
<td>Show &quot;Reply&quot; button in the message bar</td>
<td>If the message bar is enabled, show Reply in the message bar.</td>
</tr>
<tr>
<td>Show &quot;Forward&quot; button in the message bar</td>
<td>If message bar is enabled, show Forward in the message bar.</td>
</tr>
<tr>
<td>Show &quot;Reply to All&quot; button in the message bar</td>
<td>If the message bar is enabled, show Reply to All in the message bar.</td>
</tr>
<tr>
<td>Suppress applet from opening</td>
<td>Select to suppress opening the envelope with the applet.</td>
</tr>
</tbody>
</table>
Sending Encrypted Email

The default maximum size of an encrypted email is 7 MB before attachments, although this value can be changed by the administrator in the BCE_Config.xml file.

The end user can send secure emails by clicking the Encrypt Message button while composing an email. Before sending a secure message, verify that the Encrypt Message button is selected.

The Encrypt Message button is available when composing emails.
The following shows the **Encrypt Message** button in the **Mail Compose** page and the **Encryption Mail Options** toggle button:

![Image showing encrypt message button and encryption mail options]

To send an encrypted message, choose a key server and enter your passphrase.

To configure the encryption options, click the **Cisco Email Encryption** launcher in the right-bottom corner, and the following **Encryption Mail Options** page appears.

---

**Note**

The following screen shot and table show all options in the Encryption Mail Options, although the options displayed vary dependent on the configuration of the `BCE_config.xml file`.

![Encryption Mail Options dialog box]

---

**Note**

When modifying the Encryption Mail Options, the changes are applied only to the email message being composed.
Select from the following Mail options:

<table>
<thead>
<tr>
<th>Encryption Mail Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Reply</td>
<td>When selected, the recipient is able to reply to the encrypted email and the reply email message is automatically encrypted.</td>
</tr>
<tr>
<td>Allow Reply All</td>
<td>When selected, the recipient is able to reply to all who received the encrypted email and the reply email message is automatically encrypted.</td>
</tr>
<tr>
<td>Allow Forward</td>
<td>When selected, the recipient is able to forward the encrypted email and the forwarded email message is automatically encrypted.</td>
</tr>
<tr>
<td>Message security</td>
<td>From the drop-down list, set the security for the encrypted email. The default value is the value set in the BCE_Config.xml file.</td>
</tr>
</tbody>
</table>

**Note**: Changing the message security here applies only to the message being composed.

- **High**: A high security message requires a passphrase for authentication every time an encrypted message is decrypted.
- **Medium**: If the recipient passphrase is cached, a medium security message does not require a passphrase when the message is decrypted.
- **Low**: A low security message is transmitted securely but does not require a passphrase to decrypt an encrypted message.
Chapter 4  Configuring and Using the Cisco Email Encryption Plug-in for Outlook

When the end user clicks **Send**, the **Secure Envelope Options** page opens, as shown in the “Configuring Secure Envelope Options” section on page 4-28, unless this option is disabled.

Misconfiguration can cause errors. For more information, see Errors and Troubleshooting, page 4-42.

### Propagating Reply Options

When a message is decrypted, all settings for the Reply, Reply All, or Forward options and Message Sensitivity options are inherited from the original message and cannot be changed. For example:

- By default, the message is encrypted when replied to or forwarded.
- If the options Reply, Reply All, or Forwarded are not allowed from the original message, a reply or forwarded message cannot be sent and the end user is notified when they click **Send**.
- Recipients included in the original message cannot be removed when the end user performs the options of Reply, Reply All, or Forwarded.
- Recipients not included in the original message cannot be added when the end user performs the options of Reply, Reply All, or Forwarded.
- Recipients cannot be mixed or moved between the To, Cc, or Bcc fields when the end user performs the options of Reply, Reply All, or Forwarded.
• If the account is configured for Decrypt Only or Flag Encrypt, a reply or forwarded message cannot be sent and the end user is notified when they click **Send**.

• If the account Message Sensitivity is set to High, the Reply, Reply All, or Forwarded message will have High sensitivity.

• If the account Message Sensitivity is set to Medium, the Reply, Reply All, or Forwarded message will have Medium sensitivity.

• If the account Message Sensitivity is set to Low, the Reply, Reply All, or Forwarded message will have Medium sensitivity.

• A Reply, Reply All, or Forwarded message is saved in the Sent Items folder and can be decrypted by the sender.

• If a message contains a signed BCE Config file and is forwarded to another end user, versus received from an administrator, the auto configuration will not work and an error is received.

### Configuring Secure Envelope Options

The end user can configure the Secure Envelope Options that are described in the following table, as shown on the following screen shot:

| Note | Depending on your configuration settings, the language option may not be displayed on this screen and the language of the notification will be chosen according to the preferences of the recipient. |
Read your secure message by opening the attachment, securedoc_20140523125638.html. You will be prompted to open (view) the file or save (download) it to your computer. For best results, save the file first, then open it in a Web browser. For access from a mobile device, forward this message to mobile@res.cisco.com to receive a mobile login URL.

If you have concerns about the validity of this message, contact the sender directly.

First time users - need to register after opening the attachment. For more information, click the following Help link.
About Cisco Registered Envelope Service - https://res.cisco.com/websafe/about
The end user can select from the following Secure Envelope Options:

<table>
<thead>
<tr>
<th>Secure Envelope Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expire on</td>
<td>Select to enable this option. Specify date and time the encrypted email will expire. After date and time is met, the message expires, and it cannot be opened by the recipient after this time. Date and time are displayed in the local time zone of the sender.</td>
</tr>
<tr>
<td>Request a Decryption Notification</td>
<td>Allows the sender to request a decryption notification for the message. When the encrypted message is opened, the sender will receive a notification.</td>
</tr>
<tr>
<td>Language</td>
<td>Select a language to use for the notification text. Once a language is selected from the drop-down list, the recipient notification displays in the selected language.</td>
</tr>
</tbody>
</table>

If the end user’s account is configured for Flag Encryption, the email is flagged to be encrypted before it is sent from their organization. If the end user’s account is configured for Desktop Encryption, the email is encrypted at their desktop before it is sent to the Exchange Server.
Manage Secure Messages

End users can manage secure messages in the following two ways:

- By using the Manage Secure Messages dialog to manage selected messages. Use this dialog to lock, unlock, or update the expiration date of your sent encrypted emails.

- By using the Manage Messages dialog to manage all messages sent from a chosen account. Use this dialog to search for a specific message.

These two methods of managing secure messages are describe in the following sections. Using either method, end users can perform the following on encrypted emails that they sent:

- **Lock email.** The end user can lock encrypted email that were previously sent. They can also set a lock reason or update the lock reason if the message is already locked. A locked email cannot be opened by the recipient.

- **Unlock email.** The end user can unlock encrypted email that they previously sent, allowing the recipient to decrypt the email.

- **Update expiration date.** The end user can set, update, or clear and expiration date on a sent encrypted email. When an encrypted email is expired, the recipient is unable to decrypted the email.

Using the Manage Secure Messages Dialog

**Step 1**
Select the encrypted email that you sent and want to modify, then right-click the email to display the Manage Secure Messages menu option.

**Note**
End users can also access the Manage Secure Messages menu when decrypting an encrypted email. If they are a sender of the current email, they will see the Manage Secure Messages button in the toolbar. When accessing the Manage Secure Messages menu from the toolbar, the expiration settings can be applied for only one message at a time.
Step 2  Choose **Manage Secure Messages**.

If your passphrase is not cached, you will be asked to enter your passphrase.
The Manage Secure Messages page appears:

![Manage Secure Messages](image)

**Step 3**  
To set the lock or expiration option per recipient, select one or more encrypted email messages that you sent, check the **Lock** or **Expire** check boxes, and enter the appropriate information.

**Note**  
When accessing the Manage Secure Messages menu from the toolbar or ribbon, as described in the next section, the expiration settings can be applied for only one message at a time.

---

### Using the Manage Messages Dialog

**Step 1**  
Click the **Manage Messages** button on the ribbon (in Outlook 2010/13) or on the toolbar (in Outlook 2007).

The Manage Messages dialog opens.

**Note**  
This interface enables end users to manage all encrypted messages they have ever sent. If the Internet connection is slow and there are a lot of encrypted messages, the loading process can take a few minutes.

**Step 2**  
To find a specific message, click **Basic Search** or **Advanced Search**.
Step 3 To perform a basic search, enter a keyword that will be searched for in the **To** and **Subject** fields on the following screen.

The maximum string length is 500.

Step 4 To perform an advanced search, set one or more of the following search parameters on the following screen:

- **Keyword 1**—Used to search for messages that contain the keyword in the **To** or **Subject** fields. The maximum string length for the keyword is 500 characters.
- **Keyword 2**—Used in the same way as **Keyword 1**. If both keywords are specified, the search is performed by matching messages that contain both of them.
- **In** (for keyword searches)—Specifies whether the search for keywords is done in the **To**, **Subject**, or **Locked Reason** fields.
• Failed more than—Used to perform a search based on the number of failed attempts. The resulting display shows any messages with a number of mail failed attempts greater than the specified value. The maximum value is 10.

• Status—Used to perform a search based on one of the following status settings: All, Unopened, Opened, Locked, and Expired.

• From/To—Used to perform a search based on a date and time interval. If you set only a **From** date, a search is done for any messages sent after the selected date. If you set only a **To** date, a search is done for any messages sent before the selected date. If you set both dates, a search is done for any messages sent between the selected dates. You can set the date by using either the drop down calendar or by manually entering the date. The default date is the current day and time, but date searched is disabled by default.

• In (for date searches)—Specifies the criteria for date-related searches. The following options are available: Sent, Opened, and Expired.

Step 5  Click **OK**.
Receiving and Replying To Secure Emails

The Desktop Encryption plug-in automatically detects secure emails and attempts to decrypt them in Outlook. When the end user receives an encrypted message, they will usually need to enter their encryption passphrase in order to open the envelope. The secure message can be set with a message security of High, Medium, or Low.

Note

If the end user receives a passphrase-protected security message, they may need to register and set up a user account with Cisco Registered Envelope Service (CRES) to open their encrypted message. After the end user enrolls with the service, they can use their account passphrase to open all Registered Envelopes that they receive. For more information, see Secure Forward, page 4-39.

Message Encryption High page:
Message Encryption Medium page:

You have received a secure message

Read your secure message by opening the attachment, securedoc_20140521T144600.html. You will be prompted to open (view) the file or save (download) it to your computer. For best results, save the file first, then open it in a Web browser. For access from a mobile device, forward this message to mobile@res.cisco.com to receive a mobile login URL.

If you have concerns about the validity of this message, contact the sender directly.

First time users - need to register after opening the attachment. For more information, click the following Help link.
About Cisco Registered Envelope Service - https://res.cisco.com/websafe/about

Email Address: user8203@gmail.com - res.cisco.com
Passphrase: ********

Requested Remember Passphrase

OK Cancel
Message Encryption Low page:

You have received a secure message

Read your secure message by opening the attachment, securedoc_20140521T11444555.html. You will be prompted to open (view) the file or save (download) it to your computer. For best results, save the file first, then open it in a Web browser. For access from a mobile device, forward this message to mobile@res.cisco.com to receive a mobile login URL.

If you have concerns about the validity of this message, contact the sender directly.

First time users - need to register after opening the attachment. For more information, click the following Help link. Help - https://res.cisco.com/websafe/help/topic=ReqEnvelope
About Cisco Registered Envelope Service - https://res.cisco.com/websafe/about

The following describes the Message Security Options:

<table>
<thead>
<tr>
<th>Message Security Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>A high security message requires a passphrase for authentication every time an encrypted message is decrypted.</td>
</tr>
<tr>
<td>Medium</td>
<td>If the recipient passphrase is cached, a medium security message does not require a passphrase when the message is decrypted.</td>
</tr>
<tr>
<td>Low</td>
<td>A low security message is transmitted securely but does not require a passphrase to decrypt an encrypted message.</td>
</tr>
</tbody>
</table>
If the end user receives a secure message that has been locked or expired, they are notified with a message in red text on the Message Security page.

**Secure Reply/Reply All/Forward**

When you reply to or forward an encrypted email, the reply is automatically encrypted by default if you are using Desktop Encryption or Decrypt Only modes. If you are using Flag Encryption, the reply message will be encrypted by the Cisco Email Security Appliance (ESA). The settings of the secure message will determine whether you are allowed to perform any of the following actions:

- Secure Reply
- Secure Reply All
- Secure Forward
Changing Additional Settings

A log file writes and lists all actions that have occurred.

The Additional Options are located on the Cisco Email Encryption page. To modify the Additional Options:

- In Outlook 2010/2013/2016, click the Plug-in Options button on the ribbon or go to File > Options > Add-Ins > Add-in Options > Cisco Email Encryption> Additional Options.

- In Outlook 2007, click the Plug-in Options button on the toolbar or go to Tools > Options > Cisco Email Encryption> Additional Options.

Cisco Email Encryption Add-in Options page:

The Encryption Additional Options page allows you to configure the following types of options, which are described in the sections below:

- Logging
- Sending Usage Data
- Privacy
Logging Tab

The end user can configure the following options from the Logging tab.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Logging</td>
<td>Select to enable logging for the Cisco Email Encryption plug-in.</td>
</tr>
<tr>
<td>Log file name</td>
<td>Specify the name of the log file that will be stored in %ALLUSERSPROFILE%\Cisco\Cisco Email Encryption Plug-in&lt;username&gt;. The log file name should end with a .log extension.</td>
</tr>
<tr>
<td>Log level</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Normal</strong> - By default, this option is enabled. Normal logging includes fatal, recoverable errors, and warnings.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Extended</strong> - Extended logging enables useful information and debugging log messages in addition to the Normal logging messages.</td>
</tr>
</tbody>
</table>

You may want to change logging levels based on the level of troubleshooting you need for a given situation. For example, if you experience issues with the Cisco Email Encryption Plug-in, you might set the logging level to **Extended** to provide developers with the maximum amount of information allowing to reproduce issues and run diagnostics.
Sending Usage Data Tab

The end user can configure the following option from the Sending Usage Data tab.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Send anonymous usage data to Cisco          | Enables the Cisco Email Encryption Plug-in to collect data that will be used to improve the product. The following two types of information will be collected and stored on Cisco servers for analysis:  
  • General information about the machine the plug-in is running on  
  • Account-specific information |

Privacy Tab

The end user can configure the following options from the Privacy tab.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resets Identifier</td>
<td>Resets the identifier used to correlate usage reports.</td>
</tr>
<tr>
<td>Clear All Passphrases</td>
<td>Clears all cached passphrases for all accounts.</td>
</tr>
</tbody>
</table>

Errors and Troubleshooting

This section lists some of the common errors that can occur when using the Cisco Email Encryption Plug-in for Outlook, and it provides troubleshooting tips for fixing these errors.

Note

If the end user receives the same error message several times and the error disrupts the Cisco Email Encryption Plug-in for Outlook functionality, they can try running the repair process. See Repairing Cisco Email Encryption Plug-in for Outlook Files, page 4-46. If the end user encounters the same error after running the repair process, follow the steps to provide Cisco feedback with the Diagnostic tool. See Running the Cisco Email Encryption Diagnostic Tool, page 4-47.
Outlook Startup Errors

Error occurred during configuration file initialization

The following messages may appear while Outlook is starting:

• *An error occurred during* `<file_name>` *configuration file initialization. Some settings have been set to the default values.*

• *Config validation for account* `<account_address>` *has failed. Please set the correct configuration values or contact your administrator.*

These error messages occur if some configuration values are invalid or some configuration files are corrupted in the `%ALLUSERSPROFILE%\Cisco\Cisco Email Encryption Plug-In\<username>` folder.

Solution

The Cisco Email Encryption Plug-in will not restore default values of some encryption options in corrupted configuration files but will turn off some encryption features instead. If the end user receives an error message repeatedly, run the repair process to fix the configuration files. See Repairing Cisco Email Encryption Plug-in for Outlook Files, page 4-46.

Configuration file not found

The following error message may display when Outlook is starting:

• `<file_name>` *configuration file was not found. Settings have been set to the default values.*

Solution

The Cisco Email Encryption Plug-in will not restore default values of some encryption options in corrupted configuration files but will set the decryption mode instead. If the end user receives an error message repeatedly, run the repair process to fix the configuration files. See Repairing Cisco Email Encryption Plug-in for Outlook Files, page 4-46.
Decryption and Encryption Errors

When you click **Send**, the Secure Envelope Options page displays unless you have disabled this option. The email account may receive the following status messages:

**Encryption options are disabled**

If the connectivity issues that you encountered were fixed and the **Encryption Options** are still disabled, try restarting Outlook. If restarting Outlook does not help, contact your administrator for assistance.

**Your account has been locked**

- Your account has been locked. Please contact your account administrator for more information.

**Solution**

Contact the system administrator to unlock the email account.

**Your account has been blocked**

- Your account has been blocked and you must reset your password. Please use the forgot password link to reactivate your account. [Forgot password?](#)

**Solution**

Click the password link and enter the correct answers to the password security challenge questions to reset your password.

**Your account has been suspended**

- You have no attempts remaining. Your account is locked for the next 15 minutes.
Solution

You can attempt to log into https://res.cisco.com/websafe later or contact support at https://res.cisco.com/websafe/help?topic=ContactSupport for assistance.

No recipients

If you do not have a recipient listed in the email that you are sending, you may recieve the following message:

- An error occurred during encryption: no recipients specified.

An error occurred during decryption

An unexpected error occurs during message decryption. For example, the SDK returns an unknown error code or the plug-in reports an exception.

- An error occurred during decryption.

Solution

Run the diagnostic tool and send the diagnostic report to the support team. See Running the Cisco Email Encryption Diagnostic Tool, page 4-47.

An error occurred during encryption

An unexpected error occurs during message encryption. For example, the SDK returns an unknown error code or the plug-in reports an exception.

- An error occurred during encryption.

Solution

Run the diagnostic tool and send the diagnostic report to the support team. See Running the Cisco Email Encryption Diagnostic Tool, page 4-47.
Exceeds allowable limit

The default maximum size of an encrypted email is 7 MB before attachments, although this value can be changed by the administrator in the BCE_Config.xml file. If the encrypted email exceeds the maximum, you may receive one of the following messages:

- This message exceeds the allowable limit and cannot be decrypted.
- This message exceeds the allowable limit and cannot be encrypted.
- An error occurred during encryption: an invalid attachment found.
- Failed to report this message. This message is too large.
- Failed to report {0} messages. {0} messages are too large.

Note

The last two messages for “Failed to report ...” are currently in English only.

Repairing Cisco Email Encryption Plug-in for Outlook Files

To repair Cisco Email Encryption Plug-in:

Step 1 Make sure Outlook is closed.
Step 2 Go to Control Panel > Add or Remove Programs.
Step 3 Find Cisco Email Encryption Plug In in the list of programs and click Uninstall/Change.
Step 4 Click Repair. The installer repair process runs.

Note

You are not able to restore or repair the encryption configuration. The encryption configuration is only sent by the administrator in the BCE_Config.xml file.

Step 5 Perform the action that caused the error. If the same error occurs after running the repair process, follow the steps to provide Cisco feedback with the Diagnostic tool. See Running the Cisco Email Encryption Diagnostic Tool, page 4-47.
Troubleshooting Using the Diagnostic Tool

The Cisco Email Encryption Plug-in includes a diagnostic tool to help Cisco Support in troubleshooting problems. The Diagnostic tool collects important data from the Plug-in tool that can then be sent to Cisco Support to aid them in problem-solving.

The end user may want to use the diagnostic tool if they are receiving errors or if they have issues with the Cisco Email Encryption Plug-in that the repair procedure does not resolve. You can also use the diagnostic tool to share critical information with Cisco engineers when reporting a bug.

See Repairing Cisco Email Encryption Plug-in for Outlook Files, page 4-46 or Running the Cisco Email Encryption Diagnostic Tool, page 4-47.

Note
If you experience errors, review Errors and Troubleshooting, page 4-42 for troubleshooting tips.

Data Collected by the Cisco Email Encryption Diagnostic Tool

The Diagnostic tool collects the following information from your computer:

- Registration information about some COM components
- Environment variables
- Cisco Email Encryption Plug-in output files
- Information about Windows and Outlook
- Your system user name and PC name
- Information about other Outlook plug-ins
- Outlook related Windows Event Log entries

Running the Cisco Email Encryption Diagnostic Tool

The Cisco Email Encryption Diagnostic tool can be run from one of the following places:
• **From the Cisco Email Encryption options tab.** Typically, you run the diagnostic tool from the Cisco Email Encryption options tab.

• **From the “Program Files\Cisco Email Encryption Plug-in” folder** (typically C:\Program Files\Cisco\Cisco Email Encryption Plug-in). This is the folder where your Cisco Email Encryption Plug-in is installed.

• **From the Start Menu> All Programs > Cisco Email Encryption Plug-in > Cisco Email Encryption Plug-in Diagnostic.**

### Running the Diagnostic Tool from the Outlook Options Page

**Step 1** Go to the following to run the Diagnostic tool:

- In Outlook 2010/2013/2016, click the **Plug-in Options** button on the ribbon or go to **File > Options > Add-Ins > Add-in Options > Cisco Email Encryption > Run Diagnostic.**

- In Outlook 2007, click the **Plug-in Options** button on the toolbar or go to **Tools > Options > Cisco Email Encryption> Run Diagnostic.**
Cisco Email Encryption Add-in Options page:

Step 2 Wait a few seconds to allow the Diagnostic tool to collect data. When the Diagnostic tool finishes collecting data, it displays a message indicating that it successfully collected data.

The Diagnostic tool generates the CiscoDiagnosticReport.zip file and saves it to the current user’s My Documents folder. The end user can then send the file to their system administrator or the administrator can send it to their Cisco Support representative. To view the report, double-click the CiscoDiagnosticsReport.zip file.

Running the Diagnostic Tool from the Program Files

There are two ways to run the diagnostic tool from the Program files.

- Run the Diagnostic tool from Start > Programs > Cisco Email Encryption Plug-in > Cisco Email Encryption Plug-in Diagnostic.

-OR-
• Go to the folder where Cisco Email Encryption Plug-in was installed (typically C:\Program Files\Cisco\Cisco Email Encryption Plug-in) and double-click the Cisco.EmailEncryption.Framework.Diagnostic.exe file.

Disabling JavaScript in Envelopes

If incoming emails use JavaScript in the envelope, it can cause errors or may make the envelope impossible to open. To avoid these issues, you can disable JavaScript in generated envelopes, by perform the following procedure:

Step 1 Download the BCE Configuration file template from the key server.
Log in as the administrator on the key server and select Accounts > Manage Accounts > BCE Config > Step2: Download Template.

Step 2 Edit the BCE Configuration file and add <usescript>false<usescript> anywhere under the <encryption> section, or set the value to false if the <usescript> tag already exists.

Step 3 Save the BCE Configuration file and sign it on the key server.

Step 4 Send the signed BCE Configuration file to your users.

Uninstalling the Cisco Email Encryption Plug-in

You can uninstall the Cisco Email Encryption Plug-in via the Control Panel > Add/Remove Program option or by running the setup.exe program.

During the uninstall, the following items are removed:

• All registry entries made by the plug-in.
• Entry for the plug-in from the Add/Remove programs listing.
• Some of the files related to the plug-in. Note that not all of the files are removed.
• The plug-in toolbar (removed from Outlook).
Consulting the plug-in does not affect Outlook performance. Outlook must be closed during the uninstall.

To uninstall the Cisco Email Encryption Plug-in for Outlook:

There are two possible ways to uninstall the Cisco Email Encryption Plug-in for Outlook:

Step 1  Click Start > Control Panel > Add/Remove Programs.

Step 2  Select Cisco Email Encryption Plug-In and click Uninstall/Change > Next > Remove.

The second option to uninstall is

- Double-click the plug-in setup file (the file used to install the plug-in) and select the Remove option to uninstall the Cisco Email Encryption Plug-in.
Cisco End User License Agreement

For information about the Cisco End User License Agreement, see http://www.cisco.com/web/products/software/licensing_center.html.