Cisco Email Security Plug-in 7.6.2
Administrator Guide

Published: December 15, 2017
Revised: September 20, 2019

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
Getting Started with the Cisco Email Security Plug-in 1-1
  Supported Configurations 1-1
  Compliance With Security Configuration Guidelines 1-2
  Related Documents 1-2
  How to Use This Guide 1-3
    Where to Find More Information 1-3
      Security Training Services & Certification 1-3
      Cisco Support Community 1-4
      Cisco Customer Support 1-4
  Cisco Email Security Plug-in Overview 1-5

Deploying the Cisco Email Security Plug-in 2-1
  Components of the Cisco Email Security Plug-in 2-2
    The Reporting Plug-in 2-2
    The Encryption Plug-in 2-3
  Installing the Cisco Email Security Plug-in 2-3
  Configuration Modes 2-4
  Deploying the Cisco Email Security Plug-in with the Cisco Registered Envelope Service (CRES) Key Server 2-5
  Configuring Settings for the Cisco Email Security Plug-in 2-7
  System Processes Required for the Cisco Email Security Plug-in 2-8
  TCP Services Required for the Cisco Email Security Plug-in 2-8
Configuring and Using the Cisco Email Security Plug-in for Outlook  3-1

Enabling the Cisco Email Security Plug-in  3-2
Configuring the Sending of Usage Data  3-2
  General Information  3-3
  Account-Specific Information  3-3
Cisco Email Security Plug-in For Outlook General Settings  3-4
  Enable or Disable  3-4
Configuring Basic Settings for the Outlook Plug-in  3-5
Configuring the Outlook Plug-in to Check for Updates  3-7
  Update Notifications  3-7
Configuring Common Options Using the BCE_Config File  3-9
Reporting Unwanted Emails—Spam, Marketing, Virus, and Phishing Attacks  3-10
  Reporting Options  3-11
  Using the Reporting Plug-in for Outlook  3-13
    Overview  3-13
    Providing Feedback to Cisco  3-14
  Configuring Reporting for Separate Outlook Accounts  3-16
  Configuring the Encryption of Spam Reports  3-16
  Configuring the Tracking of Spam Reports  3-17
Encrypting Email Messages  3-17
  Configuring Easy Open Feature  3-17
  Opening Secure Messages  3-18
  Opening Your First Encrypted Secure Message  3-20
  Encrypting Email  3-21
Flag and Desktop Encryption Configuration  3-23
  Launching the Email Security Plug-in Configuration File  3-23
Flag Encryption  3-25
  Flag Encryption Options  3-27
    Options for Sending Flag Encrypted Email  3-28
Desktop Encryption  3-30
Desktop Encryption Options  3-32
   General Tab  3-32
   Connection Tab  3-35
   Remember Password Tab  3-36
   Advanced Tab  3-36
Sending Encrypted Email  3-38
   Propagating Reply Options  3-41
   Configuring Secure Envelope Options  3-42
Manage Secure Messages  3-44
   Using the Manage Secure Messages Dialog  3-44
   Using the Manage Messages Dialog  3-46
Receiving and Replying To Secure Emails  3-49
   Secure Reply/Reply All/Forward  3-54
Changing Additional Settings  3-55
   Logging Tab  3-57
   Sending Usage Data Tab  3-58
   Privacy Tab  3-58
Errors and Troubleshooting  3-58
   Outlook Startup Errors  3-59
      Error occurred during configuration file initialization  3-59
      Configuration file not found  3-59
   Message Reporting Errors  3-60
      Outlook does not recognize one or more names  3-60
      The connection to the server is unavailable  3-60
      Error occurred during connection to server  3-61
   Decryption and Encryption Errors  3-61
      Your account has been locked  3-61
      Your account has been blocked  3-61
      Your account has been suspended  3-62
No recipients 3-62
An error occurred during decryption 3-62
An error occurred during encryption 3-62
Exceeds allowable limit 3-63
Repairing Cisco Email Security Plug-in for Outlook Files 3-63
Troubleshooting Using the Diagnostic Tool 3-64
Data Collected by the Cisco Email Security Diagnostic Tool 3-64
Running the Cisco Email Security Diagnostic Tool 3-65
Running the Diagnostic Tool from the Outlook Options Page 3-65
Running the Diagnostic Tool from the Program Files 3-67
Disabling JavaScript in Envelopes 3-67
Disabling Java Runtime Environment during Plug-in installation 3-68
Uninstalling the Cisco Email Security Plug-in 3-69

Cisco End User License Agreement A-1
Supported Configurations

For information about operating systems supported for release 7.6, see the Cisco Email Encryption Compatibility Matrix.
Compliance With Security Configuration Guidelines

The Cisco Email Security Plug-in 7.6 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 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, 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

To better understand how Cisco Email Security works, you may want to review some basic information about how email is classified as spam, virus, or as non-spam. For more details on these subjects, you may want to review the following guide:

- *Cisco AsyncOS for Email Security User Guide*. This guide contains information on spam and virus protection. Users can improve the efficacy of the SenderBase network by employing the spam and virus plug-in. When users marks an email as “spam,” “virus,” or “not spam,” they can train the filters to become more effective and improve the performance of all Cisco
Email Security appliances. To find the guide for your release, see: http://www.cisco.com/en/US/products/ps10154/products_user_guide_list.html

How to Use This Guide

Use this guide as a resource to learn about the features in your Cisco Email Security Plug-in. 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 Security.
- In Outlook 2007, click the Plug-in Options button on the toolbar or go to Tools > Options > Cisco Email Security > Help.

Where to Find More Information

Cisco offers the following resources to learn more about the Cisco Email Security 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 Email Security Plug-in Overview

The Cisco Email Security Plug-in adds reporting and encryption menus to the Microsoft Outlook GUI. The reporting plug-in enables users to submit feedback about the type of mail they receive (for example, end users can report spam, phishing, marketing, and virus emails), and the encryption plug-in places an “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.

When the Cisco Email Security Plug-in is installed, it enables components on an Microsoft Outlook mail client. This single interface allows you to seamlessly report emails or send encrypted email. 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. Combining these plug-ins simplifies installation and provides a single interface for end users and Administrators to install and modify.

The reporting and encryption plug-ins provide a convenient interface that enables you to submit feedback and send encrypted messages by using toolbar buttons and right-click context menus. If you are using the reporting plug-in to report a message, a dialog box appears indicating that the message was submitted. The Encryption Plug-in places the *Encrypt Message* button in the menu bar of an email message to provide an easy way for senders to email encrypted messages.

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

---

**Note**

A single-sign-on (SAML) login is not supported for you to use with the Cisco Email Security Plug-in.
Deploying the Cisco Email Security Plug-in

The Cisco Email Security Plug-in framework supports several Cisco Email Security Plug-ins, including the Reporting plug-in and the Encryption plug-in.

This chapter contains the following sections:

- Components of the Cisco Email Security Plug-in, page 2-2
- Installing the Cisco Email Security Plug-in, page 2-3
- Configuration Modes, page 2-4
- Deploying the Cisco Email Security Plug-in with the Cisco Registered Envelope Service (CRES) Key Server, page 2-5
- Configuring Settings for the Cisco Email Security Plug-in, page 2-7
- System Processes Required for the Cisco Email Security Plug-in, page 2-8
- TCP Services Required for the Cisco Email Security Plug-in, page 2-8
Components of the Cisco Email Security Plug-in

The Cisco Email Security Plug-in consists of two commonly used email security plug-ins: the Reporting plug-in and the Encryption plug-in. You may deploy the Cisco Email Security Plug-in on your Outlook email program. When you deploy the Cisco Email Security Plug-in, it installs one or both of the following applications:

- **The Reporting Plug-in.** The Reporting Plug-in enables Outlook users to submit feedback to Cisco Systems about unsolicited and unwanted email messages, such as spam, viruses, phishing, and marketing messages. For details, see The Reporting Plug-in, page 2-2.

- **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 a sender to mark a message to be encrypted. For details, see The Encryption Plug-in, page 2-3.

---

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

---

The Reporting Plug-in

The Reporting Plug-in enables Outlook users to submit feedback to Cisco about unsolicited and unwanted email messages, such as spam, viruses, phishing, and marketing messages. Cisco uses this feedback to update its filters to stop unwanted messages from being delivered to your inbox.

You can also report false positives, which are legitimate email messages that are marked as spam, to Cisco by using the Not Spam button. Legitimate email messages are often referred to as “ham.” Cisco uses reports about false positives to adjust its spam filters to avoid misclassifying legitimate email in the future. Any valid email can be reported as **Not Spam** and it helps to increase filter efficacy.

This plug-in provides a convenient interface that enables you to submit feedback by using toolbar buttons and right-click context menus. When you report a message, a dialog box appears indicating that the message was submitted. The
message data that you submit is used by automated systems to improve the Cisco filters. By submitting message data, you help to reduce the volume of unsolicited email in your inbox.

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, 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.

Installing the Cisco Email Security Plug-in

Follow the given steps to install the Cisco Email Security Plug-in:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Download the Email Security Plug-in installer from the Cisco Software Download Center.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Double-click the <em>Cisco Email Security Plug-in.exe</em> file.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select a language in the <strong>Cisco Email Security Plug-in Setup</strong> window, and click OK.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Next to start the installation program.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Install.</td>
</tr>
</tbody>
</table>
Step 6  
Wait until the Setup Wizard installs the Cisco Email Security Plug-in, and click Finish.

Configuration Modes

The Cisco Email Security 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>X</td>
<td></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>
<tr>
<td>Email expiration</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Email diagnostic (Uses for Reporting and Encryption Plug-ins)</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>

Deploying the Cisco Email Security Plug-in with the Cisco Registered Envelope Service (CRES) Key Server

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

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

**Step 2** Select the account from which you want to enable the Email Security 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.

---

**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 Security Plug-in

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

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

You can make changes to the Reporting plug-in installation or 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 Security 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.

To make configuration changes on an Outlook installation, see Chapter 3, “Configuring and Using the Cisco Email Security Plug-in for Outlook.”

System Processes Required for the Cisco Email Security Plug-in

The Cisco Email Security 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 Security Plug-in.
TCP Services Required for the Cisco Email Security Plug-in

The Cisco Email Security 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

  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)

  For more information, see: http://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

  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)

  For more information, see: http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

  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](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)
  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](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.
This chapter introduces the features available in the Cisco Email Security Plug-in for Outlook. The Cisco Email Security Plug-in includes several types of security plug-ins that work with the Outlook email program. This chapter contains the following sections:

- Enabling the Cisco Email Security Plug-in, page 3-2
- Configuring the Sending of Usage Data, page 3-2
- Configuring Basic Settings for the Outlook Plug-in, page 3-5
- Configuring the Outlook Plug-in to Check for Updates, page 3-7
- Configuring Common Options Using the BCE_Config File, page 3-9
- Reporting Unwanted Emails-Spam, Marketing, Virus, and Phishing Attacks, page 3-10
- Encrypting Email Messages, page 3-17
- Flag and Desktop Encryption Configuration, page 3-23
- Flag Encryption, page 3-25
- Desktop Encryption, page 3-30
- Changing Additional Settings, page 3-55
- Errors and Troubleshooting, page 3-58
- Troubleshooting Using the Diagnostic Tool, page 3-64
- Disabling JavaScript in Envelopes, page 3-67
- Uninstalling the Cisco Email Security Plug-in, page 3-69
Enabling the Cisco Email Security Plug-in

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

To enable the Cisco Email Security 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 Security 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 checkbox, 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:

```plaintext
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.
- Whether non-standard reporting addresses are being used.
Cisco Email Security Plug-in For Outlook General Settings

The Cisco Email Security Plug-in is a platform that supports several Cisco plug-ins, including the Encryption plug-in and the Reporting plug-in. General settings for the Cisco Email Security Plug-in can be configured from the Options page.

Enable or Disable

By default, the Cisco Email Security Plug-in is enabled upon installation. The Cisco Email Security 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.
From the COM Add-Ins window, clear the Cisco Email Security 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 Security 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 Security**.

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

From this tab, the end user can enable encryption and reporting options by selecting the appropriate **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...**, **Reporting Options...**, or **Additional Options...** buttons. The end user can also use the Diagnostic tool to run a report on the Cisco Email Security 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 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:

![Dialog box for update notification](image)

Note

You need to have the appropriate rights to download the Cisco Email Security Plug-in application.
To check for updates after Outlook starts up, click the About button on the Plug-in Options window, and then click the Check for updates button on the following dialog box:
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, reporting, 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 3-7.

- **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 3-2.

- **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 3-2.
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.

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.

### Reporting Unwanted Emails—Spam, Marketing, Virus, and Phishing Attacks

The reporting plug-in allows the end user to report to Cisco that an email received is spam, a marketing email, a phishing attack, or a virus. The end user can also report mail that is misclassified as spam, also sometimes called “ham.”

The end user can enable the Cisco Email Security Reporting Plug-in for Outlook via the Options page in Outlook. To enable Reporting:

- 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 Security**. Select the **Enable** check box in the Reporting field of the Cisco Email Security tab.

- In Outlook 2007, click the **Plug-in Options** button on the toolbar or go to **Tools > Options > Cisco Email Security** tab. Select the **Enable** check box in the Reporting field of the Cisco Email Security tab.
Reporting Options

The Reporting settings are located on the Cisco Email Security page. To modify the Reporting 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 Security** and click the **Reporting Options** button.

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

There are also some reporting options that must be configured in the BCE_Config file. For more information, see the “Configuring the Encryption of Spam Reports” section on page 3-16.

The following Reporting Accounts page displays all accounts configured in Outlook. To configure the reporting options for an account, select the appropriate account and the click Options button. The reporting options for that account will then be displayed.
The following account-specific Reporting Options page displays the reporting options for the selected account, and allows you to enable or disable their functionality. For more information, see the following table.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keep a copy of sent report</td>
<td>By default, when the end user reports an email message to Cisco as spam, virus, misclassified spam, or virus, the reporting email the end user sent is deleted. Selecting this option prevents the email from being deleted.</td>
</tr>
<tr>
<td>Display notification when a single email is successfully reported</td>
<td>When the end user successfully reports an email as spam or virus, they can enable Outlook to display a success message in a dialog box. Clearing this option prevents this dialog box from displaying.</td>
</tr>
<tr>
<td>Display notification when multiple emails are successfully reported</td>
<td>When the end user successfully reports a group of emails as spam or virus, they can enable Outlook to display a success message in a dialog box. Clearing this option prevents this dialog box from displaying.</td>
</tr>
</tbody>
</table>
Using the Reporting Plug-in for Outlook

Overview

The Cisco Email Security Plug-in for Outlook allows the end user to submit feedback to Cisco about spam, virus, phishing, or marketing emails that are received in their inbox. The end user can let Cisco know if an email message is misclassified or if it should be treated as spam, for example. Cisco uses this feedback to update the email filters that prevent unwanted messages from being delivered to their inbox.

The Plug-in provides a convenient interface through Outlook’s menu bar and the right-click message menu to report spam, virus, phishing, marketing, and misclassified emails. After reporting an email, a message appears indicating that
the report has been submitted. The messages the end user reports are used to improve Cisco’s email filters, helping to reduce the overall volume of unsolicited mail to their inbox.

Providing Feedback to Cisco

The Plug-in provides a new toolbar in Outlook containing the following buttons: Spam, Not Spam, Virus, Phish, and Marketing.

These buttons are used to report spam, virus, phishing, and marketing emails (Phishing attacks are emails that link to “spoofed” and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account user names and passwords, social security numbers. For example, the end user might receive an email from infos@paypals.com that fraudulently requests their personal banking information).

The end user can also use right-click context menu to report spam, misclassified mail, virus, phish, and marketing.
And, the end user can use the buttons in the message window to report spam, virus, phish, marketing, and misclassified mail (misclassified mail is mail that was erroneously marked as spam, virus, phish, or marketing).

### Message Rotation for Reported Spam, Virus, Phish, or Marketing Emails

When emails messages are reported as spam, misclassified, virus, phish, or marketing, the messages are processed as follows.

**Inbox messages:**

- Inbox messages reported as spam, virus, phish, or marketing go into the Junk Email folder.
- Inbox messages reported as Not Spam stay in the Inbox folder.

**Junk Messages:**

- Junk messages reported as spam, virus, phish, or marketing stay in the Junk Email folder.
- Junk messages reported as Not Spam go in the Inbox folder.

If an email received is misclassified as spam (i.e. is filtered and sent to the Junk Email folder), the end user can report the email as misclassified by clicking the Not Spam button. This ensures that mail from the sender will not be classified as spam in the future.

The end user can also mark misclassified email from the right-click context menu.
Configuring Reporting for Separate Outlook Accounts

The BCE_Config file now has a reportingComponent section which will be applied for each account separately.

Configuring the Encryption of Spam Reports

To enable or disable the encryption of spam reports, configure the following two options in the “reporting” section of the BCE_Config file:

- **format** - Defines the format of the report. Supported values are:
  - encrypted—Specifies that the report will be encrypted before sending.
  - plain—Specifies that the report will be sent without encryption.
  The default value is encrypted.
- **subject** - Defines the subject of the report. You can include the report type (Spam, Ham, Virus, Phish, Marketing) in the subject by including the string “${reportType}.”
Configuring the Tracking of Spam Reports

To enable tracking the reported messages marked as spam, virus, phish, or marketing, set the following parameter in the BCE_Config file:

`copyAddressInPlainFormat`—Specifies that a copy of the spam report will be sent in plain (.raw) format to custom email address.

Encrypting Email Messages

This section consists of the following sub-sections:

- Configuring Easy Open Feature, page 3-17
- Opening Secure Messages, page 3-18
- Opening Your First Encrypted Secure Message, page 3-20
- Encrypting Email, page 3-21

Configuring Easy Open Feature

The Easy Open feature allows the recipient to open the envelopes from any device without the need to install any client-side application. This can be achieved by storing a copy of the encrypted envelope in Cisco Registered Envelope Service, in addition to sending the envelope as an attachment to the recipient.

When enabled, the Easy Open feature leverages a new template featuring a Read Message button. When the recipient clicks this button, it directs the recipient to authenticate and decrypt the encrypted envelope in Cisco Registered Envelope Service.

To configure the Easy Open feature on your Cisco Email Encryption Plug-in, see the Cisco Registered Envelope Service 5.4.0 Account Administrator Guide.

After you configure the Easy Open feature on your Cisco Email Encryption Plug-in, see Opening Secure Messages, page 3-18.
Opening Secure Messages

Use the following steps to register your user account with Cisco Registered Envelope Service (CRES) to open secure messages:

**Note**
If you have enabled Easy Open for your account, you can view the Read Message button and the securedoc HTML attachment in your notification email message.

**Step 1**
Click the **Read Message** button in the notification email message to read the secure message.
Chapter 3  Configuring and Using the Cisco Email Security Plug-in for Outlook

Step 2  Double-click the secure message in your mailbox. Decryption dialog with the Register button opens.

Step 3  Select your email address from the Email Address drop-down menu and click Register. The New User Registration page opens.

Note  You may need to set up more than one user account if you receive Registered Envelopes at multiple email addresses. You need a separate user account for each address.
Step 4  Complete the form and click **Register**.

Step 5  Check your Inbox folder for an account activation message. Click the activation link in the email.

Step 6  Return to the original email and double-click the secure message.

Step 7  Enter your CRES password in the Password field and click **OK** to read your secure message.

---

**What to do Next**

*Opening Your First Encrypted Secure Message, page 3-20*

---

**Opening Your First Encrypted Secure Message**

If you receive an encrypted secure message, you need to register and set up a user account with Cisco Registered Envelope Service (CRES) to open your encrypted message. After you enroll with the service, you can use your account password to open all encrypted secure messages that you receive.

**New User Registration Options**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Language</td>
<td>Optional. Select a language for your CRES account from the drop-down menu. By default the registration page may appear in English but you can choose from English, French, German, Spanish, Portuguese, or Japanese.</td>
</tr>
<tr>
<td>First Name</td>
<td>Required. Enter the first name of the CRES user account.</td>
</tr>
<tr>
<td>Last Name</td>
<td>Required. Enter the last name of the CRES user account.</td>
</tr>
<tr>
<td>Password</td>
<td>Required. Enter a password for the account. The password should be at least eight characters long and should contain both numbers and letters.</td>
</tr>
</tbody>
</table>
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 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 3-1 Workflows for Flag Encryption vs. Desktop Encryption

Flag Encryption

Email Client with Cisco Email Security Plug-in

Message Flagged for encryption

Exchange Server

Encryption appliance sends key request

Encryption Server

Desktop Encryption

Email Client with Cisco Email Security Plug-in sends key request

Encrypted Message

Exchange Server

Encryption appliance passes encrypted message

Encryption Server

**May not be present.

Note

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. 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 Security 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**

Generally, Java Runtime Environment (JRE) is automatically installed during the plug-in installation. However, if this does not happen, you need to install JRE manually. The supported versions are JRE 1.8 and Open JRE 11.

To enable and configure the security 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 Security Plug-In. A message displays after the configuration has been successfully applied.

If you select the Apply Common Plug-in Setting checkbox, 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 3-9
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 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 Security 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 Security > Encryption Options.
- In Outlook 2007, click the Plug-in Options button on the toolbar or go to Tools > Options > Cisco Email Security > 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 Security tab.

Select Enable to enable the email program to send sensitive mail via a secure envelope.
Cisco Email Security 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 is 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>
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>Password</td>
<td>Enter the password associated with the username you entered for your system or proxy server.</td>
</tr>
</tbody>
</table>

Remember Password Tab

Select from the following Remember Password options:

<table>
<thead>
<tr>
<th>Password Options</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Never</td>
<td>When selected, the encryption password is always required when decrypting and encrypting emails.</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 Security 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 Security > Encryption Options.
- In Outlook 2007, click the Plug-in Options button on the toolbar or go to Tools > Options > Cisco Email Security > 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 Security 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 Security page, although any changes to the encryption mode need to be made by the administrator in the BCE_config.xml file.

<table>
<thead>
<tr>
<th>Password Options</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always</td>
<td>When selected, the encryption password is required only for the first time when decrypting an encrypted email. Then the password is cached.</td>
</tr>
<tr>
<td>Minutes</td>
<td>Select this option to ensure that the encryption password is cached. Type the number of minutes to remember the password, or use the arrows to modify the entry. After the specified duration, the end user must re-enter the encryption password to decrypt an encrypted email. The default is 1440 minutes.</td>
</tr>
</tbody>
</table>
Cisco Email Security Add-in Options page:
Desktop 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:

![Encryption Options window](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>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). 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>General Option</td>
<td>Value</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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 <code>securedoc.html</code>. The attachment name can be changed and the envelope will reflect the newly specified name.</td>
</tr>
<tr>
<td>Message security</td>
<td>Set the security for the encrypted email. The default value is defined in the <code>BCE_Config.xml</code> file.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Changing the message security here applies only to the message being composed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>High</strong>. A high security message requires a password for authentication every time an encrypted message is decrypted.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Medium</strong>. If the recipient password is cached, a medium security message does not require a password when the message is decrypted.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Low</strong>. A low security message is transmitted securely but does not require a password to decrypt an encrypted message.</td>
</tr>
<tr>
<td>Send return receipt</td>
<td>Select to request a return receipt when the sent email is opened by the recipient.</td>
</tr>
<tr>
<td>Show dialog during message encryption</td>
<td>Select to display the encryption options dialog box for each encrypted message.</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>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>Password</td>
<td>Enter the password associated with the user name you entered for your system or proxy server.</td>
</tr>
</tbody>
</table>
Remember Password Tab

Select from the following Remember Password options:

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

Advanced Tab

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>Advanced Option</td>
<td>Value</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</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>Display &quot;Remember me&quot;</td>
<td>When selected, the check box for Remember me is visible on the envelope.</td>
</tr>
<tr>
<td>Display &quot;Auto open&quot;</td>
<td>When selected, the check box for Auto open is visible on the envelope.</td>
</tr>
<tr>
<td>Open in the same window</td>
<td>Select to open the secure message in the same window as the envelope.</td>
</tr>
<tr>
<td>Display “Encryption usage reminder”</td>
<td>When selected, the reminder about using encryption only for business purpose is displayed each time the user performs encryption.</td>
</tr>
</tbody>
</table>
Sending Encrypted Email

Note

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:

![Encrypt Message button](image)

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

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

Note

The following screenshot and table show all of the possible options in the Encryption Mail Options, although the options displayed vary dependent on the configuration of the BCE_config.xml file.
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>
</tbody>
</table>
### Encryption Mail Options

<table>
<thead>
<tr>
<th>Encryption Mail Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td><strong>Note</strong></td>
<td>Changing the message security here applies only to the message being composed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>High.</strong> A high security message requires a password for authentication every time an encrypted message is decrypted.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Medium.</strong> If the recipient password is cached, a medium security message does not require a password when the message is decrypted.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Low.</strong> A low security message is transmitted securely but does not require a password to decrypt an encrypted message.</td>
</tr>
<tr>
<td>Expiration</td>
<td>From the drop-down, specify how long (date and time) the encrypted email remains valid. After the expiry date and time is met, the message expires, and it cannot be opened by the recipient after this time.</td>
</tr>
<tr>
<td>Read By</td>
<td>From the drop-down, specify the date and time by 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>
</tbody>
</table>
When the end user clicks **Send**, the Secure Envelope Options page is displayed, as shown the “Configuing Secure Envelope Options” section on page 3-42, unless this option is disabled.

Misconfiguration can cause errors. For more information, see Errors and Troubleshooting, page 3-58.

**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 Low 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 screenshot:

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.
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 an expiration date on a sent encrypted email. When an encrypted email is expired, the recipient is unable to decrypt 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.
Chapter 3  Configuring and Using the Cisco Email Security Plug-in for Outlook

Manage Secure Messages Menu Option:

Step 2  Choose Manage Secure Messages.

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

![Manage Secure Messages dialog]

**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** checkboxes, 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 are 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 password to open the envelope. The secure message can be set with a message security of High, Medium, or Low.
If the end user receives a password-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 password to open all Registered Envelopes that they receive. For more information, see page 3-55.

Message Security High page:
Message Security Medium page:
Message Security Low page:

This is a secure message
The link to open this message is valid till 09/17/2019 08:35:21 AM UTC.

Read Message

HOW TO OPEN LINK AFTER EXPIRY

☐ To read this message on desktop, open the securedoc_20190917T08518.html attachment in a web browser.

☐ To read this message on a mobile device, forward this message to mobile@res.cisco.com to receive a mobile login URL.

Need Help?
contact the sender directly if you are not sure about the validity of this message.

Email Address* lakshman@ci라도.in - res.cisco.com

The message was transmitted securely but does not require a password.
* - required

Acknowledge Cancel
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 password for authentication every time an encrypted message is decrypted.</td>
</tr>
<tr>
<td>Medium</td>
<td>If the recipient password is cached, a medium security message does not require a password when the message is decrypted.</td>
</tr>
<tr>
<td>Low</td>
<td>A low security message is transmitted securely but does not require a password 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 in 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. 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 Security 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 Security > Additional Options**.

• In Outlook 2007, click the **Plug-in Options** button on the toolbar or go to **Tools > Options > Cisco Email Security > Additional Options**.
Cisco Email Security 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><strong>Option</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Logging</td>
<td>Select to enable logging for the Cisco Email Security 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 Security 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, warnings, and useful information.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Extended</strong> - Extended logging enables debug 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 Security 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 Security 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 Passwords</td>
<td>Clears all cached passwords 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 Security 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 Security Plug-in for Outlook functionality, they can try running the repair process. See Repairing Cisco Email Security Plug-in for Outlook Files, page 3-63. 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 Security Diagnostic Tool, page 3-65.
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 IronPort Email Security Plug-In\<username>` folder.

Solution

The Cisco Email Security 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 Security Plug-in for Outlook Files, page 3-63.

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 Security 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 Security Plug-in for Outlook Files, page 3-63.
Message Reporting Errors

Outlook does not recognize one or more names

The following message may appear when the end user clicks the **Spam**, **Virus**, **Phish**, **Marketing**, or **Not Spam** buttons in Outlook:

*There was error during email reporting. Description: Outlook does not recognize one or more names.*

This error occurs if the end user is using the Reporting plug-in and Outlook cannot recognize the format of the email message they are attempting to report. The end user will need to repair the Reporting plug-in file to ensure that they can report spam and phishing emails (as well as reporting legitimate mail as "Not Spam").

**Solution**

Run the repair process. See Reparing Cisco Email Security Plug-in for Outlook Files, page 3-63.

The connection to the server is unavailable

The following message may appear when the end user clicks **Spam**, **Virus**, **Phish**, **Marketing**, or **Not Spam** buttons plug-in buttons in Outlook and use IMAP protocol or "headers only" Outlook property:

*Error: The connection to the server is unavailable. Outlook must be online or connected to complete this action.*

This error occurs if the end user is trying to report message that downloaded partially (headers only) and the connection to the mail server is off. The Reporting plug-in cannot report a partially downloaded message, and it will attempt to connect to the mail server until it can download a full copy of the message to report.

**Solution**

Ensure that Outlook has a connection with the mail server before reporting emails with headers only.
Error occurred during connection to server

The following error occurs if Outlook is online but your Internet connection has been lost or the server has become temporarily unavailable.

*An HTTP error occurred during connection to server.*

**Solution**

Check your network settings or contact the local administrator.

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:

**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 receive 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 Security Diagnostic Tool, page 3-65.

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 Security Diagnostic Tool, page 3-65.
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 Security Plug-in for Outlook Files

To repair Cisco Email Security Plug-in:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Make sure Outlook is closed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Go to Control Panel &gt; Add or Remove Programs.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Find Cisco Email Security Plug In in the list of programs and click Uninstall/Change.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Repair. The installer repair process runs.</td>
</tr>
</tbody>
</table>

**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 Security Diagnostic Tool, page 3-65. |
Troubleshooting Using the Diagnostic Tool

The Cisco Email Security 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 Security 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 Security Plug-in for Outlook Files, page 3-63 or Running the Cisco Email Security Diagnostic Tool, page 3-65.

*Note*
If you experience errors, review Errors and Troubleshooting, page 3-58 for troubleshooting tips.

Data Collected by the Cisco Email Security Diagnostic Tool

The Diagnostic tool collects the following information from your computer:

- Registration information about some COM components
- Environment variables
- Cisco Email Security 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 Security Diagnostic Tool

The Cisco Email Security Diagnostic tool can be run from one of the following places:

- **From the Cisco Email Security options tab.** Typically, you run the diagnostic tool from the Cisco Email Security options tab.

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

- **From the Start Menu> All Programs > Cisco Email Security Plug-in > Cisco Email Security 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 Security > Run Diagnostic.**

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

![Cisco Email Security Add-in Options window]

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 Security Plug-in > Cisco Email Security Plug-in Diagnostic.**

  -OR-

- Go to the folder where Cisco Email Security Plug-in was installed (typically C:\Program Files\Cisco\Cisco IronPort Email Security Plug-in) and double-click the *Cisco.EmailSecurity.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.
Disabling Java Runtime Environment during Plug-in installation

You can skip to install the Java Runtime Environment during the Cisco Email Security Plug-in setup. In this case, only the reporting functionality will be available. The encryption functionality will not function correctly. If you want to enable the encryption functionality later, you will need to install Java Runtime Environment manually.

To disable Java Runtime Environment:

**Step 1**  Go to Windows Registry Editor and create the following key:

`HKEY_CURRENT_USER\Software\Cisco\Cisco Email Security Plugin`

![Registry Editor screenshot](image)

**Note**  This key can be in Windows Registry Editor already. If the key is not present, then Java Runtime Environment will be installed by default during Plug-in installation.
Step 2 Create the following string value:

ExcludeJavaFromPrerequisiteList

![Registry Editor](image)

Step 3 Run the following command:

CiscoEmailSecurityPlugin.exe /exenoui /qn SkipEncryption="TRUE"

Step 4 Go to Start > Control Panel > Add/Remove Programs and make sure the Cisco Email Security Plug-in application is installed, and Java Runtime Environment is not installed.

Uninstalling the Cisco Email Security Plug-in

You can uninstall the Cisco Email Security 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).
Uninstalling the plug-in does not affect Outlook performance. Outlook must be closed during the uninstall.

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

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

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

**Step 2**
Select **Cisco Email Security 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 Security 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.