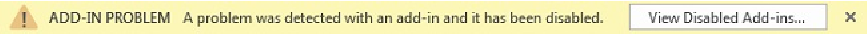
Configuring and Using the Cisco Email Security Plug-in for Outlook

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

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:



ADD-IN PROBLEM A problem was detected with an add-in and it has been disabled.

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:

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:

- Identifer (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.

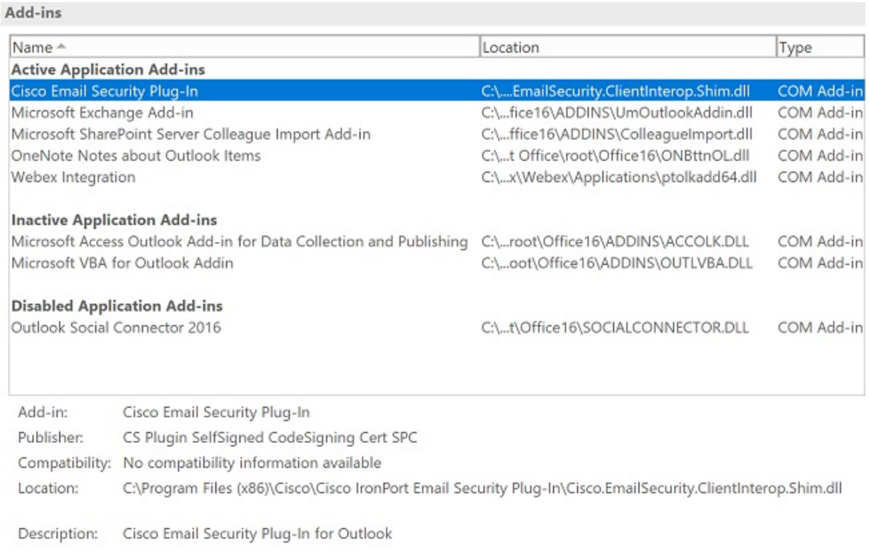
Cisco Email Security Plug-in For Outlook General Settings

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**.



Add-ins

Name	Location	Type
Active Application Add-ins		
Cisco Email Security Plug-In	C:\....EmailSecurity.ClientInterop.Shim.dll	COM Add-in
Microsoft Exchange Add-in	C:\...fice16\ADDINS\UmOutlookAddin.dll	COM Add-in
Microsoft SharePoint Server Colleague Import Add-in	C:\...ffice16\ADDINS\ColleagueImport.dll	COM Add-in
OneNote Notes about Outlook Items	C:\...t Office\root\Office16\ONBttnOL.dll	COM Add-in
Webex Integration	C:\...x\Webex\Applications\ptolkadd64.dll	COM Add-in
Inactive Application Add-ins		
Microsoft Access Outlook Add-in for Data Collection and Publishing	C:\...root\Office16\ADDINS\ACCOLK.DLL	COM Add-in
Microsoft VBA for Outlook Addin	C:\...oot\Office16\ADDINS\OUTLVBA.DLL	COM Add-in
Disabled Application Add-ins		
Outlook Social Connector 2016	C:\...t\Office16\SOCIALCONNECTOR.DLL	COM Add-in

Add-in: Cisco Email Security Plug-In
Publisher: CS Plugin SelfSigned CodeSigning Cert SPC
Compatibility: No compatibility information available
Location: C:\Program Files (x86)\Cisco\Cisco IronPort Email Security Plug-In\Cisco.EmailSecurity.ClientInterop.Shim.dll

Description: Cisco Email Security Plug-In for Outlook

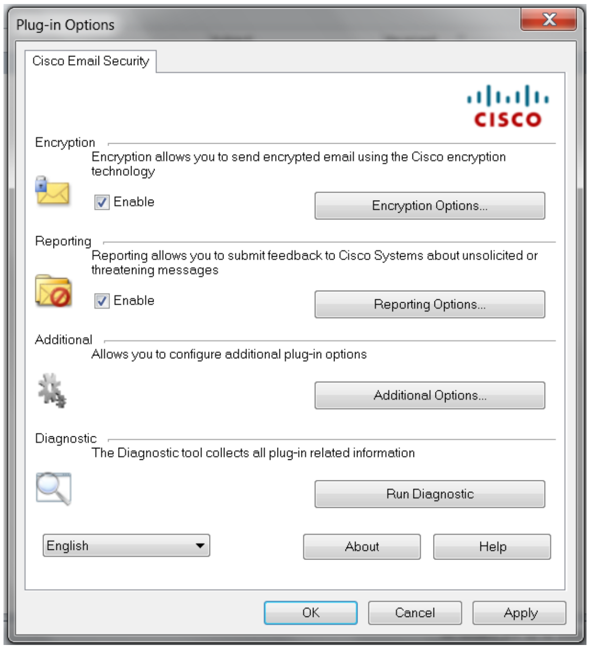
From the COM Add-Ins window, clear the Cisco Email Security Plug-in check box and click **OK**.

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-ins 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:



Encryption
Encryption allows you to send encrypted email using the Cisco encryption technology
☑ Enable

Reporting
Reporting allows you to submit feedback to Cisco Systems about unsolicited or threatening messages
☑ Enable

Additional
Allows you to configure additional plug-in options

Diagnostic
The Diagnostic tool collects all plug-in related information

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.

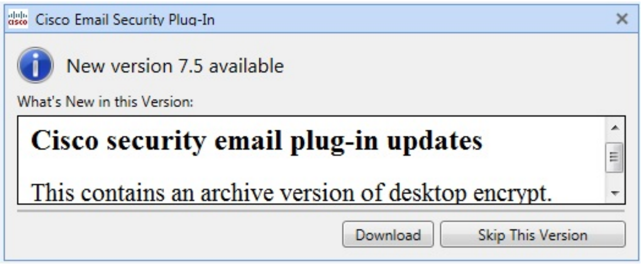
Configuring the Outlook Plug-in to Check for Updates

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:


Cisco Email Security Plug-In

New version 7.5 available

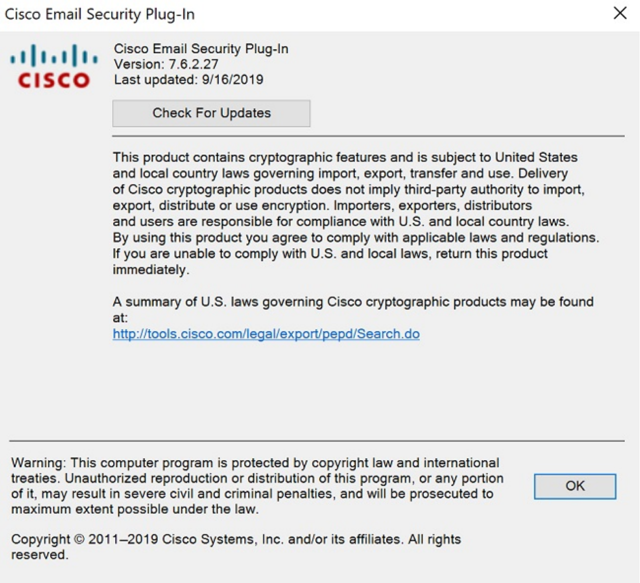
What's New in this Version:

Cisco security email plug-in updates

This contains an archive version of desktop encrypt.

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:


Cisco Email Security Plug-In

Cisco Email Security Plug-In
Version: 7.6.2.27
Last updated: 9/16/2019

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://tools.cisco.com/legal/export/pepd/Search.do

Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

Copyright © 2011–2019 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Configuring Common Options Using the BCE_Config File

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

- diagnosticSupportAddress—Specifies the email address of the recipient of the message that is sent when the Diagnostic Tool is run. The message contains the output of the Diagnostic Tool.

- diagnosticReportSubject—Specifies the subject of the message that is sent when the Diagnostic Tool is run.
- showPluginOptions—Set to true or false to enable or disable the Plug-in Options button that opens the Plug-in Options dialog box where you can use the encryption, 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, on page 4.
- 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, on page 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, on page 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.

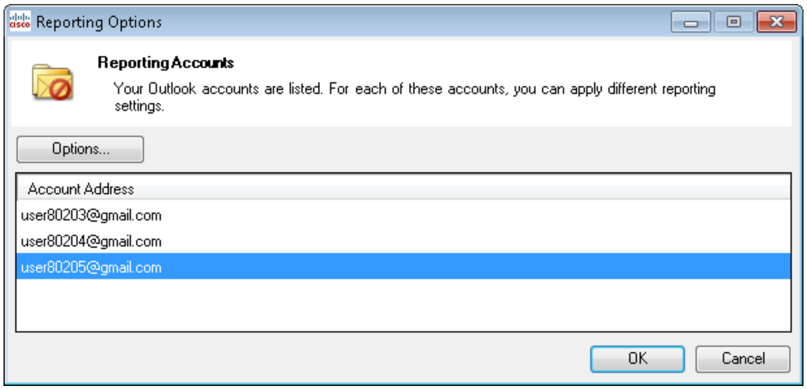
Reporting Options

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_Confg file. For more information, see the Configuring the Encryption of Spam Reports, on page 10.

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.

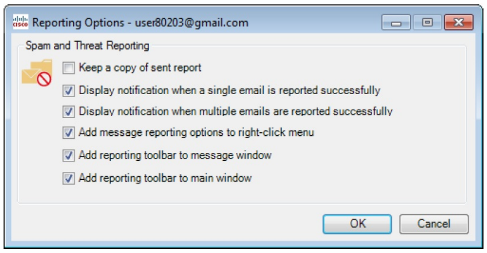


Reporting Accounts

Your Outlook accounts are listed. For each of these accounts, you can apply different reporting settings.

Account Address
user80203@gmail.com
user80204@gmail.com
user80205@gmail.com

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.



Spam and Threat Reporting

- ☐ Keep a copy of sent report
- ☑ Display notification when a single email is reported successfully
- ☑ Display notification when multiple emails are reported successfully
- ☑ Add message reporting options to right-click menu
- ☑ Add reporting toolbar to message window
- ☑ Add reporting toolbar to main window

This table describes the reporting options the end user can configure.

Option	Description
Keep a copy of sent report	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.

Option	Description
Display notification when a single email is successfully reported	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.
Display notification when multiple emails are successfully reported	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.
Add security toolbar to the main window	By default, when the end user installs the Cisco Email Security Plug-in, the plug-in toolbar is added to main Outlook window. Clearing this option prevents this toolbar from being added to main Outlook window.
Add message reporting options to the right-click menu	By default, when the end user installs the Cisco Email Security Plug-in, the Reporting plug-in menu item is added to the Outlook right-click context menu. Clearing this option prevents this menu item from being added to the right-click context menu.
Add security toolbar to the message window	By default, when the end user installs the Cisco Email Security Plug-in, the plug-in toolbar is added to the email message window. Clearing this option prevents this toolbar from being added to the email message window.

Using the Reporting Plug-in for Outlook

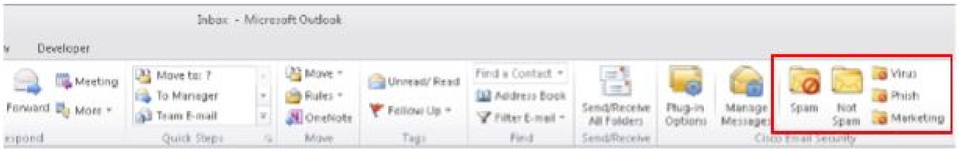
Overview

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.

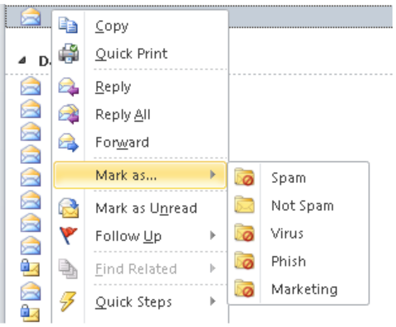
Providing Feedback to Cisco

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

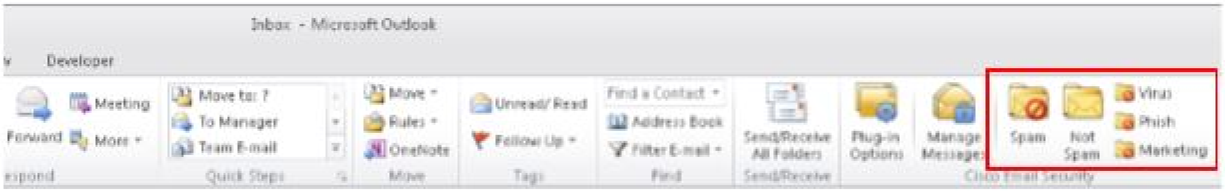


These buttons are used to report spam, virus, phishing, and marketing emails (Phishing attacks are emails that link to "spoofed" and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account user names and passwords, social security numbers. 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.

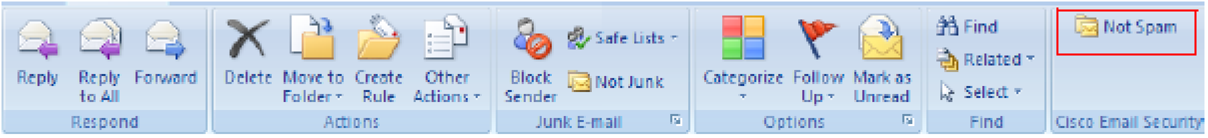
Inbox messages:

- 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.

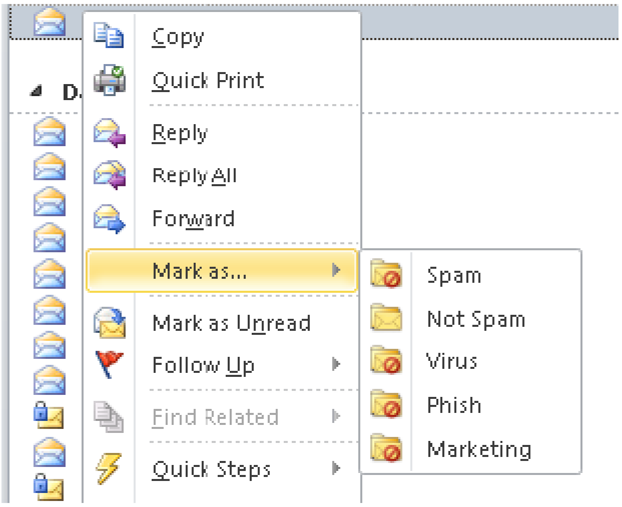
Junk Messages:

- 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, on page 11

Opening Secure Messages, on page 11

Opening Your First Encrypted Secure Message, on page 12

Encrypting Email, on page 13

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, on page 11.

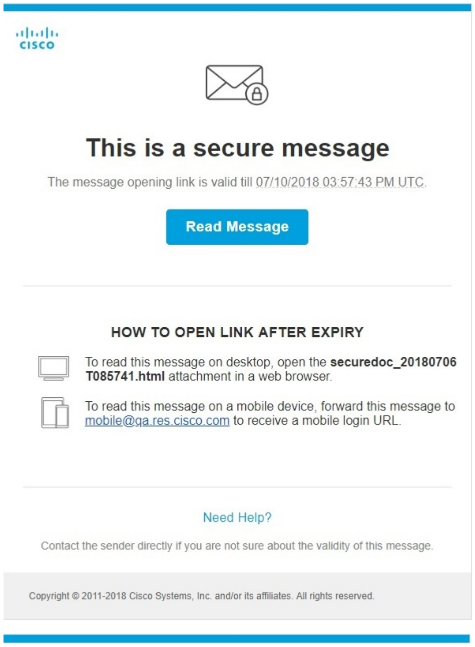
Opening Secure Messages

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.

Procedure

Step 1 Click the **Read Message** button in the notification email message to read the secure message.



This is a secure message

The message opening link is valid till 07/10/2018 03:57:43 PM UTC.

HOW TO OPEN LINK AFTER EXPIRY

To read this message on desktop, open the **securedoc_20180706T085741.html** attachment in a web browser.

To read this message on a mobile device, forward this message to mobile@qa.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.

Copyright © 2011-2018 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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, on page 12

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

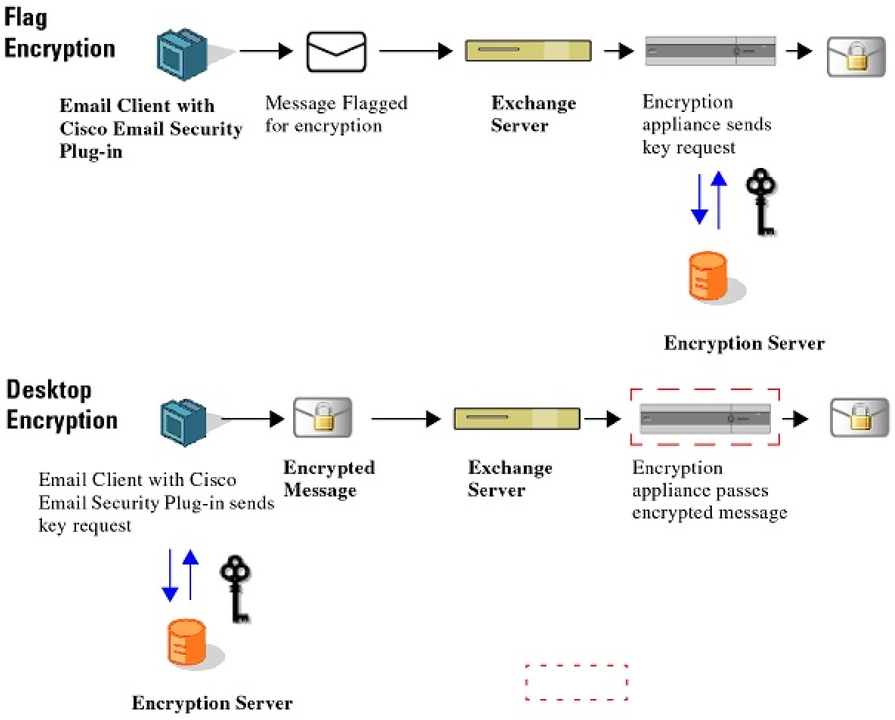
Field	Description
Language	Optional. Select a language for your CRES account from the drop-down menu. By default the registration page may appear in English but you can choose from English, French, German, Spanish, Portuguese, or Japanese.
First Name	Required. Enter the first name of the CRES user account.
Last Name	Required. Enter the last name of the CRES user account.
Password	Required. Enter a password for the account. The password should be at least eight characters long and should contain both numbers and letters.

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 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

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.

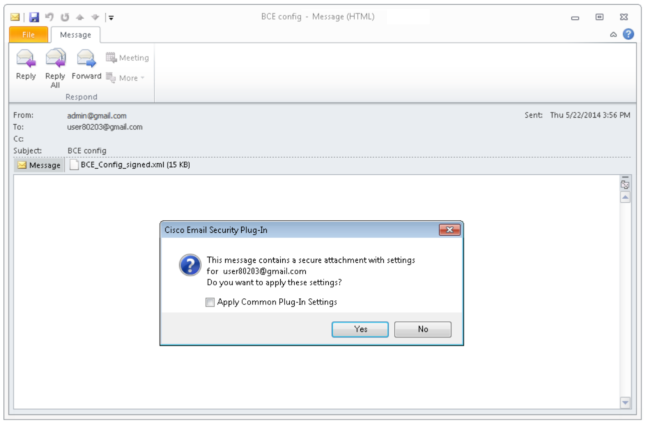
When launching the configuration file, the plug-in is configured for the email account that received the notification message with the signed BCE Config file attachment.

Note Generally, Jave 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:

Procedure

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.



From: admin@gmail.com
To: user80203@gmail.com
Cc:
Subject: BCE config
Sent: Thu 5/22/2014 3:56 PM

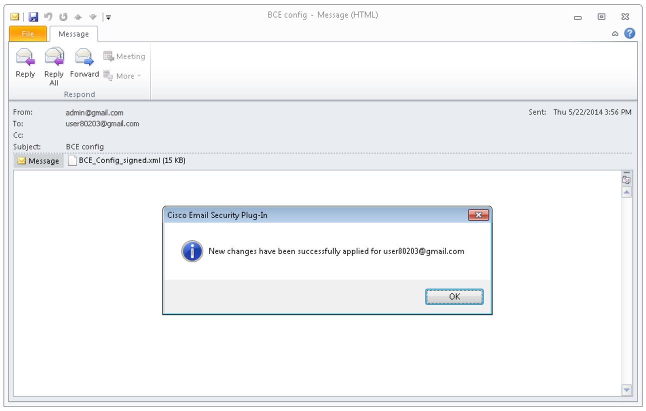
BCE_Config_signed.xml (15 KB)

This message contains a secure attachment with settings for user80203@gmail.com
Do you want to apply these settings?

□ Apply Common Plug-In 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, on page 5.



From: admin@gmail.com
To: user80203@gmail.com
Cc:
Subject: BCE config
Sent: Thu 5/22/2014 3:56 PM

Message | BCE_Config_signed.xml (15 KB)

Cisco Email Security Plug-In

New changes have been successfully applied for user80203@gmail.com

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.

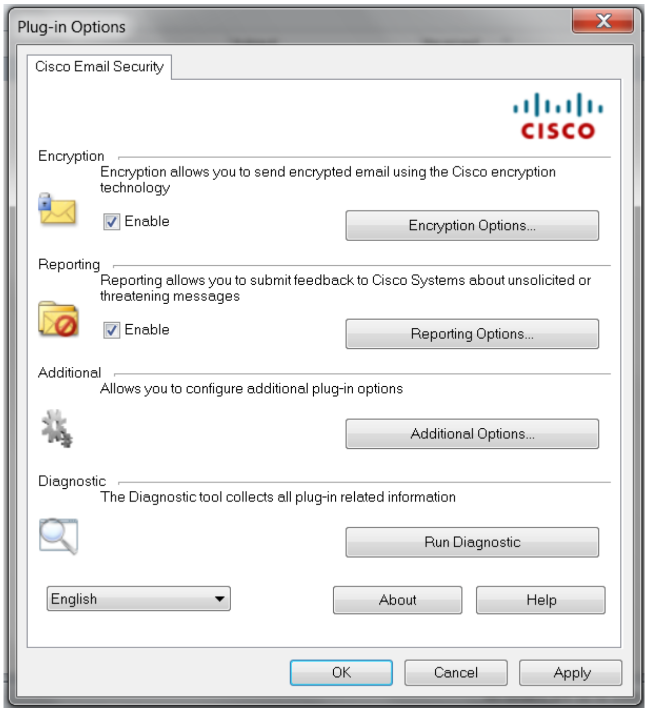
The Flag Encryption settings are located on the Cisco Email Security page. To modify the Flag Encryption settings:

- 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:



Encryption allows you to send encrypted email using the Cisco encryption technology

☑ Enable

Reporting allows you to submit feedback to Cisco Systems about unsolicited or threatening messages

☑ Enable

Allows you to configure additional plug-in options

The Diagnostic tool collects all plug-in related information

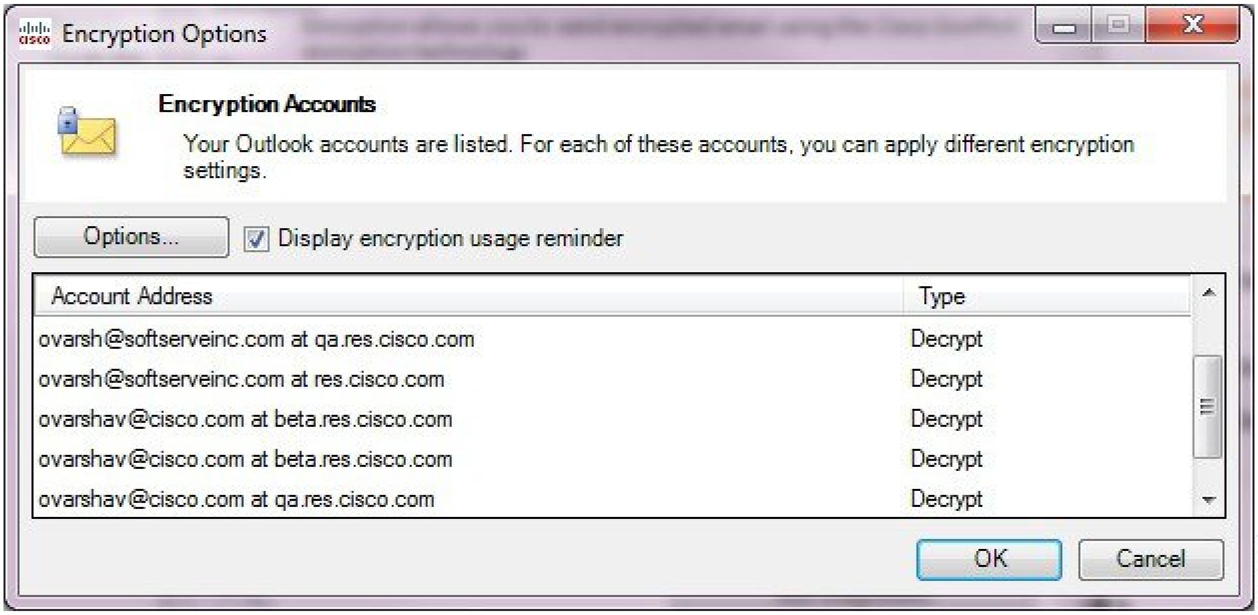
English

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:



Encryption Accounts

Your Outlook accounts are listed. For each of these accounts, you can apply different encryption settings.

☑ Display encryption usage reminder

Account Address	Type
ovarsh@softserveinc.com at qa.res.cisco.com	Decrypt
ovarsh@softserveinc.com at res.cisco.com	Decrypt
ovarshav@cisco.com at beta.res.cisco.com	Decrypt
ovarshav@cisco.com at beta.res.cisco.com	Decrypt
ovarshav@cisco.com at qa.res.cisco.com	Decrypt

371440

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:

General Options	Value
Flag Subject Text	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])*.

General Options	Value
Flag X-header name/value	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).
Flag Sensitivity header	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.

Connection Tab

You can select from the following Connection options:

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

Remember Password Tab

Select from the following Remember Password options:

Password Options	Value
Never	When selected, the encryption password is always required when decrypting and encrypting emails.
Always	When selected, the encryption password is required only for the first time when decrypting an encrypted email. Then the password is cached.

Password Options	Value
Minutes	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 and encrypt emails. The default is 1440 minutes.

Desktop Encryption

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

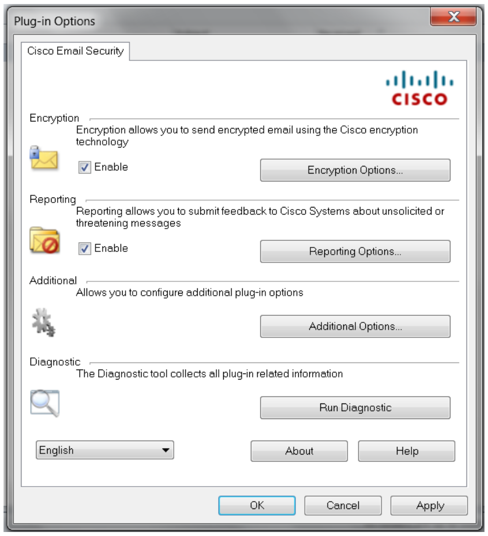
The Desktop Encryption settings are located on the Cisco Email Security page. To modify the Desktop Encryption settings:

- 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.

Cisco Email Security Add-in Options page:



Plug-in Options

Cisco Email Security

Encryption
Encryption allows you to send encrypted email using the Cisco encryption technology
☑ Enable

Reporting
Reporting allows you to submit feedback to Cisco Systems about unsolicited or threatening messages
☑ Enable

Additional
Allows you to configure additional plug-in options

Diagnostic
The Diagnostic tool collects all plug-in related information

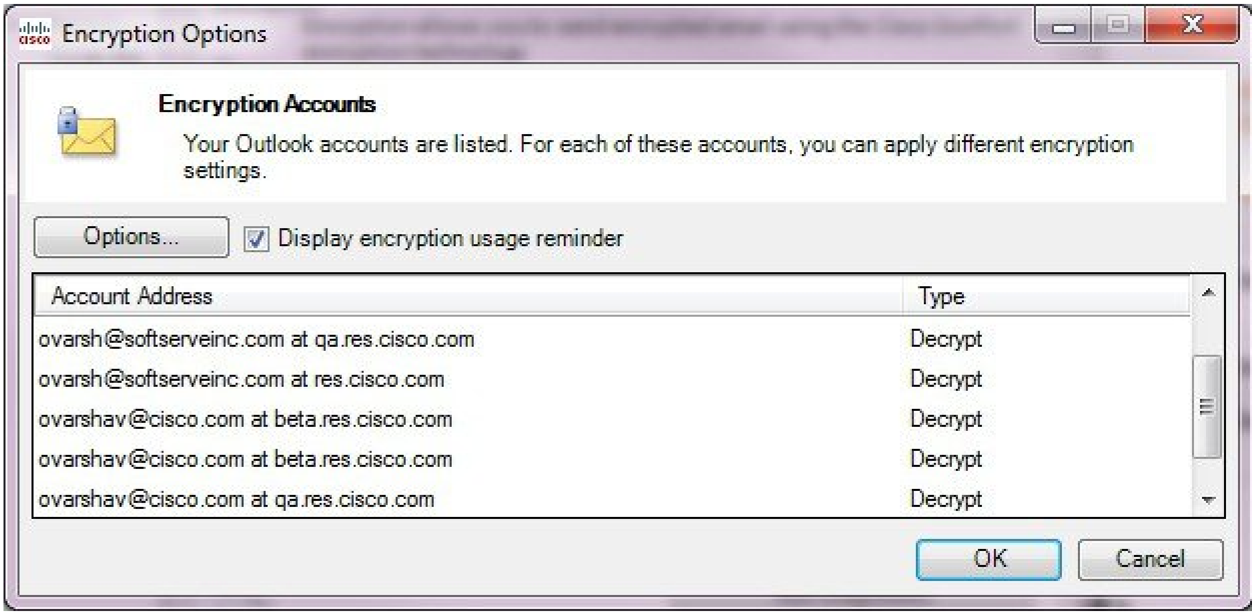
English

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

Encryption Accounts

Your Outlook accounts are listed. For each of these accounts, you can apply different encryption settings.

Options... ☑ Display encryption usage reminder

Account Address	Type
ovarsh@softserveinc.com at qa.res.cisco.com	Decrypt
ovarsh@softserveinc.com at res.cisco.com	Decrypt
ovarshav@cisco.com at beta.res.cisco.com	Decrypt
ovarshav@cisco.com at beta.res.cisco.com	Decrypt
ovarshav@cisco.com at qa.res.cisco.com	Decrypt

OK Cancel

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:

General Option	Value
Use as default encryption account	Select to set the account as the default encryption account.
Encrypt by default	Select to allow all sent email messages to be encrypted by default.

General Option	Value
Server URL	Enter the URL for your Encryption server.
Always use message body from key server	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.
Default language for outgoing messages	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).
Token File Name	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.
Default Expiration (days)	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.
Default read-by (days)	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.
Attachment name	The default envelope name is securedoc.html.The attachment name can be changed and the envelope will reflect the newly specified name.

General Option	Value
Message security	Set the security for the encrypted email. The default value is defined in the BCE_Config.xml file. **Note** Changing the message security here applies only to the message being composed. • **High.** A high security message requires a password for authentication every time an encrypted message is decrypted. • **Medium.** If the recipient password is cached, a medium security message does not require a password when the message is decrypted. • **Low.** A low security message is transmitted securely but does not require a password to decrypt an encrypted message.
Send return receipt	Select to request a return receipt when the sent email is opened by the recipient.
Show dialog during message encryption	Select to display the encryption options dialog box for each encrypted message.

Connection Tab

Select from the following Connection options:

Table 1:

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

Remember Password Tab

Select from the following Remember Password options:

Password Options	Value
Never	When selected, the encryption password is always required when decrypting and encrypting emails.
Always	When selected, the encryption password is required only for the first time when decrypting an encrypted email. Then the password is cached.
Minutes	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.

Advanced Tab

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

Select from the following Advanced options:

Advanced Option	Value
Unsecure server URL	Unsecure base URL to use for message bar help. If omitted, then external secure URL is used. i.e. http://res.cisco.com.
Connection timeout	Length of time to wait for a connection to the key server to be established.
Socket timeout	Length of time to wait for data from the key server.
Display "Open offline" check box	When selected, the check box for Open offline is visible on the envelope.
Display "Remember envelope key"	When selected, the check box for Remember envelope key is visible on the envelope.
Display "Enable personal security phrase"	When selected, the check box for Enable personal security phrase is visible on the envelope.
Add message bar	Select to add the message bar to the secure message.
Show "Reply" button in the message bar	If the message bar is enabled, show Reply in the message bar.

Advanced Option	Value
Show "Forward" button in the message bar	If message bar is enabled, show Forward in the message bar.
Show "Reply to All" button in the message bar	If the message bar is enabled, show Reply to All in the message bar.
Display "Remember me"	When selected, the check box for Remember me is visible on the envelope.
Display "Auto open"	When selected, the check box for Auto open is visible on the envelope.
Open in the same window	Select to open the secure message in the same window as the envelope.
Display "Encryption usage reminder"	When selected, the reminder about using encryption only for business purpose is displayed each time the user performs encryption.

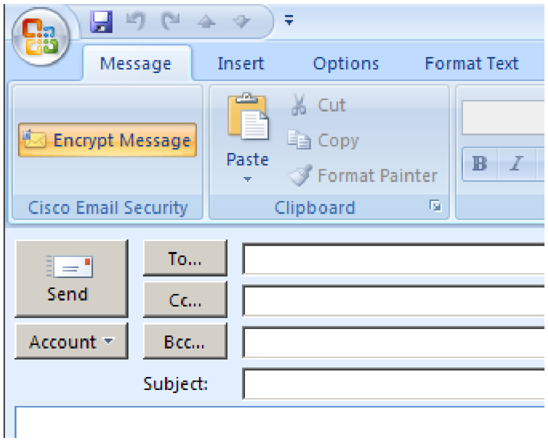
Sending Encrypted Email

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.

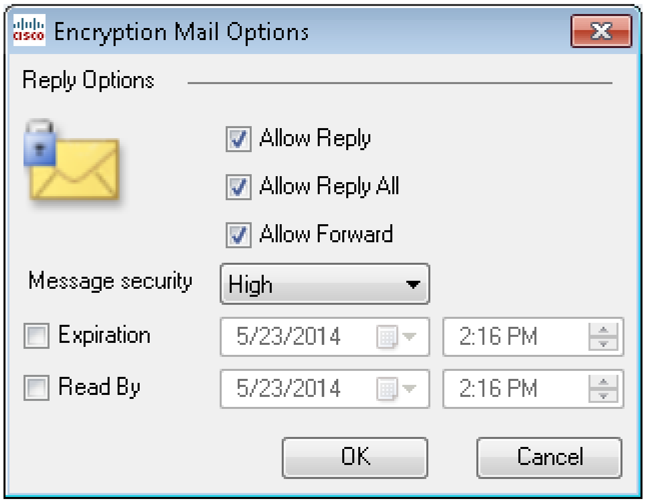
The following shows the Encrypt Message button in the Mail Compose page and the Encryption Mail Options toggle button:



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.



Encryption Mail Options

Reply Options

☑ Allow Reply
☑ Allow Reply All
☑ Allow Forward

Message security: High

☐ Expiration 5/23/2014 2:16 PM
☐ Read By 5/23/2014 2:16 PM

Note When modifying the Encryption Mail Options, the changes are applied only to the email message being composed.

Select from the following Mail options:

Encryption Mail Options	Description
Allow Reply	When selected, the recipient is able to reply to the encrypted email and the reply email message is automatically encrypted.
Allow Reply All	When selected, the recipient is able to reply to all who received the encrypted email and the reply email message is automatically encrypted.
Allow Forward	When selected, the recipient is able to forward the encrypted email and the forwarded email message is automatically encrypted.

Encryption Mail Options	Description
Message security	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. **Note** Changing the message security here applies only to the message being composed. • **High.** A high security message requires a password for authentication every time an encrypted message is decrypted. • **Medium.** If the recipient password is cached, a medium security message does not require a password when the message is decrypted. • **Low.** A low security message is transmitted securely but does not require a password to decrypt an encrypted message.
Expiration	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.
Read By	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.

When the end user clicks **Send**, the Secure Envelope Options page is displayed, as shown the Configuring Secure Envelope Options, on page 28, unless this option is disabled.

Misconfiguration can cause errors. For more information, see Errors and Troubleshooting, on page 38.

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:

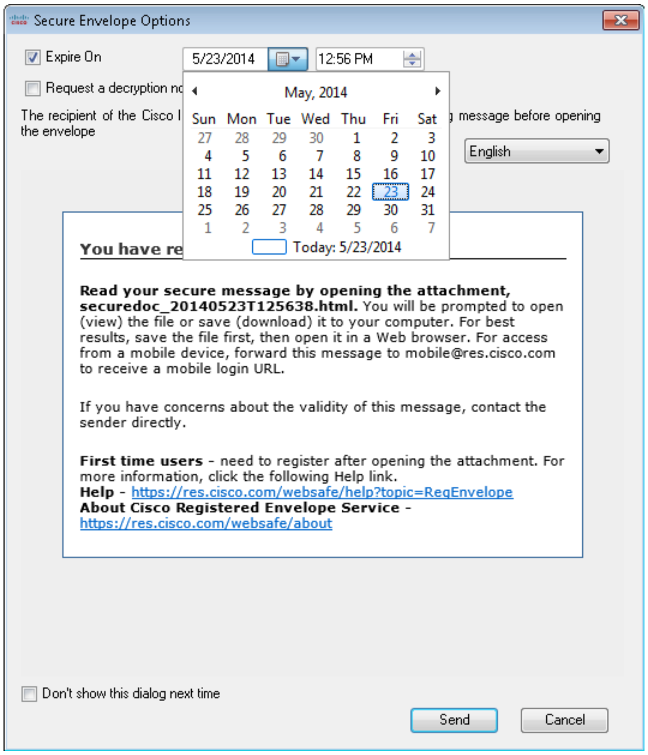
- By default, the message is encrypted when replied to or forwarded.
- If the options Reply, Reply All, or Forwarded are not allowed from the original message, a reply or forwarded message cannot be sent and the end user is notified when they click **Send**.
- Recipients included in the original message 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.



Secure Envelope Options

☑ Expire On 5/23/2014 12:56 PM

☐ Request a decryption nc

The recipient of the Cisco I … message before opening the envelope

English

May, 2014

Sun	Mon	Tue	Wed	Thu	Fri	Sat
27	28	29	30	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

Today: 5/23/2014

You have re

Read your secure message by opening the attachment, securedoc_20140523T125638.html. You will be prompted to open (view) the file or save (download) it to your computer. For best results, save the file first, then open it in a Web browser. For access from a mobile device, forward this message to mobile@res.cisco.com to receive a mobile login URL.

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

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

☐ Don't show this dialog next time

The end user can select from the following Secure Envelope Options:

Secure Envelope Option	Description
Expire on	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.
Request a Decryption Notification	Allows the sender to request a decryption notification for the message. When the encrypted message is opened, the sender will receive a notification.
Language	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.

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

Manage Secure Messages

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

- By using the Manage Secure Messages dialog to manage selected messages. Use this dialog to lock, unlock, or update the expiration date of your sent encrypted emails.
- By using the Manage Messages dialog to manage all messages sent from a chosen account. Use this dialog to search for a specific message.

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

- **Lock email**. The end user can lock encrypted email that were previously sent. They can also set a lock reason or update the lock reason if the message is already locked. A locked email cannot be opened by the recipient.
- **Unlock email**. The end user can unlock encrypted email that they previously sent, allowing the recipient to decrypt the email.
- **Update expiration date**. The end user can set, update, or clear and expiration date on a sent encrypted email. When an encrypted email is expired, the recipient is unable to decrypted the email.

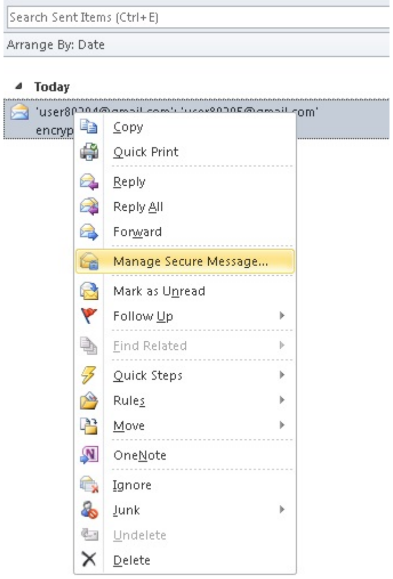
Using the Manage Secure Messages Dialog

Procedure

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.

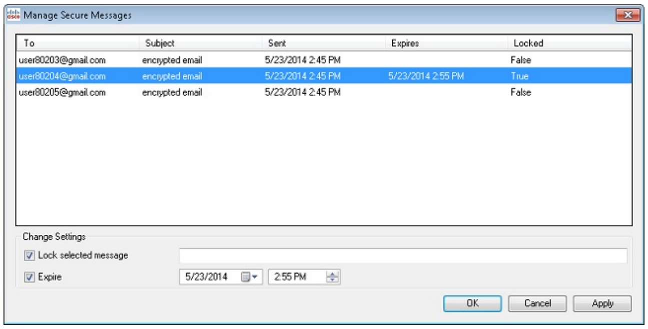
Manage Secure Messages Menu Option:



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

To	Subject	Sent	Expires	Locked
user80203@gmail.com	encrypted email	5/23/2014 2:45 PM		False
user80204@gmail.com	encrypted email	5/23/2014 2:45 PM	5/23/2014 2:55 PM	True
user80205@gmail.com	encrypted email	5/23/2014 2:45 PM		False

Change Settings

☑ Lock selected message

☑ Expire 5/23/2014 2:55 PM

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

Procedure

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

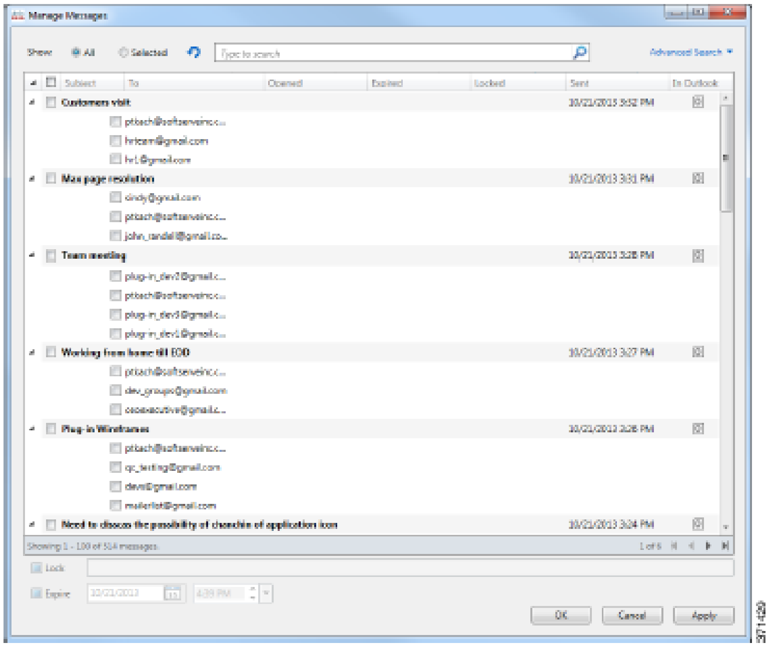
The Manage Messages dialog opens.

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.



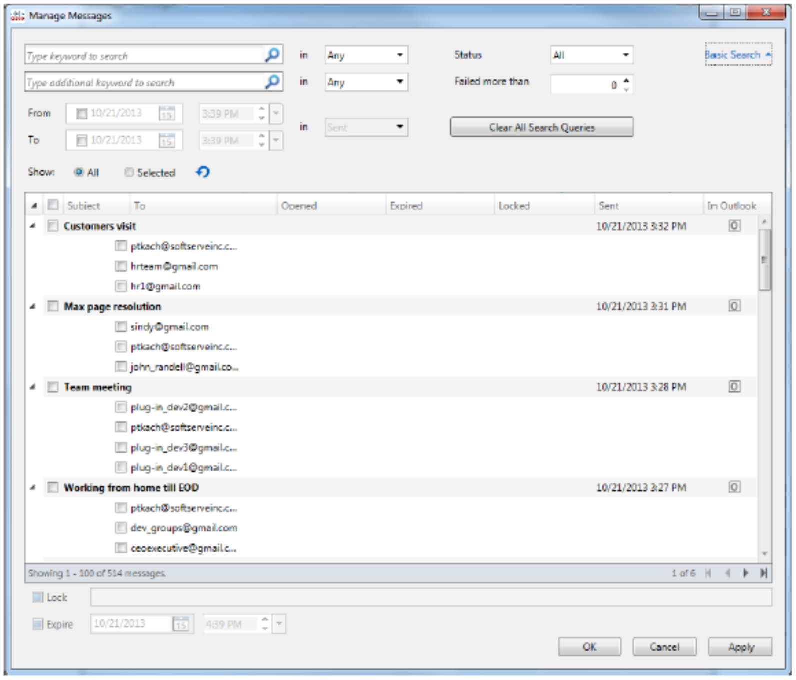
Subject	To	Opened	Expired	Locked	Sent	In Outlook
□ Customers visit					10/21/2013 3:52 PM	
	□ ptkach@softserveinc.c...					
	□ hrteam@gmail.com					
	□ hr1@gmail.com					
□ Max page resolution					10/21/2013 3:31 PM	
	□ cindy@gmail.com					
	□ ptkach@softserveinc.c...					
	□ john_randal@gmail.co...					
□ Team meeting					10/21/2013 3:28 PM	
	□ plug-in_dev2@gmail.c...					
	□ ptkach@softserveinc.c...					
	□ plug-in_dev3@gmail.c...					
	□ plug-in_dev1@gmail.c...					
□ Working from home till EOD					10/21/2013 3:27 PM	
	□ ptkach@softserveinc.c...					
	□ dev_groups@gmail.com					
	□ ciscoexecutive@gmail.c...					
□ Plug-in Wireframes					10/21/2013 3:26 PM	
	□ ptkach@softserveinc.c...					
	□ qc_testing@gmail.com					
	□ dev@gmail.com					
	□ mailerlist@gmail.com					
□ Need to discuss the possibility of chanchin of application icon					10/21/2013 3:24 PM	

Showing 1 - 100 of 514 messages. 1 of 6

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



Type keyword to search in Any
Type additional keyword to search in Any
Status All
Failed more than 0
From □ 10/21/2013 3:39 PM
To □ 10/21/2013 3:39 PM
in Sent
Show: ● All ○ Selected

□ Subject	To	Opened	Expired	Locked	Sent	In Outlook
□ **Customers visit**					10/21/2013 3:32 PM	
	□ ptkach@softserveinc.c...					
	□ hrteam@gmail.com					
	□ hr1@gmail.com					
□ **Max page resolution**					10/21/2013 3:31 PM	
	□ sindy@gmail.com					
	□ ptkach@softserveinc.c...					
	□ john_randell@gmail.co...					
□ **Team meeting**					10/21/2013 3:28 PM	
	□ plug-in_dev2@gmail.c...					
	□ ptkach@softserveinc.c...					
	□ plug-in_dev3@gmail.c...					
	□ plug-in_dev1@gmail.c...					
□ **Working from home till EOD**					10/21/2013 3:27 PM	
	□ ptkach@softserveinc.c...					
	□ dev_groups@gmail.com					
	□ ceoexecutive@gmail.c...					

Showing 1 - 100 of 514 messages. 1 of 6

□ Lock
□ Expire 10/21/2013 4:39 PM

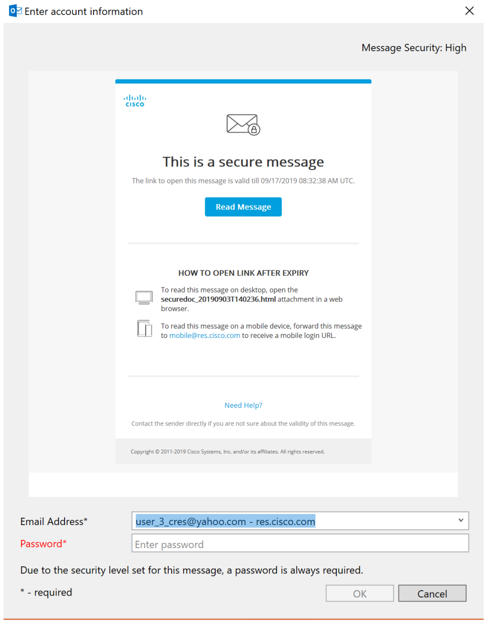
Step 5 Click **OK**.

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.

Note 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 Changing Additional Settings, on page 35.

Message Security High page:



Enter account information ×

Message Security: High

This is a secure message

The link to open this message is valid till 09/17/2019 08:32:38 AM UTC.

Read Message

HOW TO OPEN LINK AFTER EXPIRY

To read this message on desktop, open the **securedoc_20190903T140236.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.

Copyright © 2011-2019 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Email Address* user_3_cres@yahoo.com - res.cisco.com

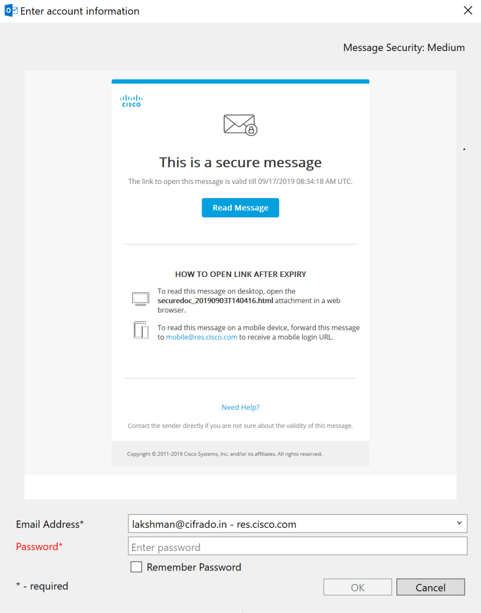
Password* Enter password

Due to the security level set for this message, a password is always required.

* - required

OK Cancel

Message Security Medium page:



Enter account information ×

Message Security: Medium

This is a secure message

The link to open this message is valid till 09/17/2019 08:34:18 AM UTC.

Read Message

HOW TO OPEN LINK AFTER EXPIRY

To read this message on desktop, open the **securedoc_20190903T140416.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.

Copyright © 2011-2019 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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

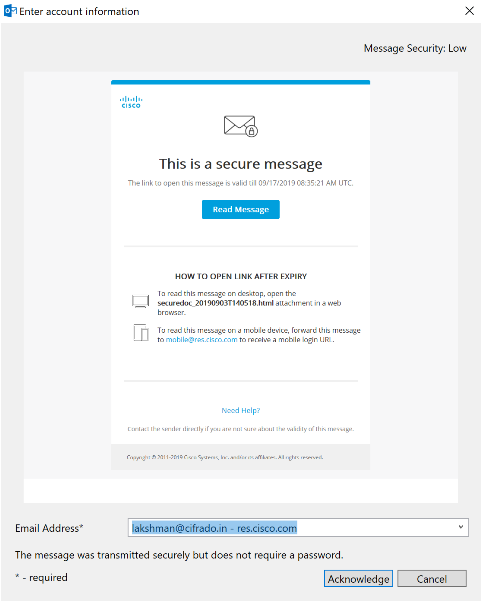
Password* Enter password

□ Remember Password

* - required

OK Cancel

Message Security Low page:



Message Security: Low

This is a secure message

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

HOW TO OPEN LINK AFTER EXPIRY

To read this message on desktop, open the **securedoc_20190903T140518.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.

Copyright © 2011-2019 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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

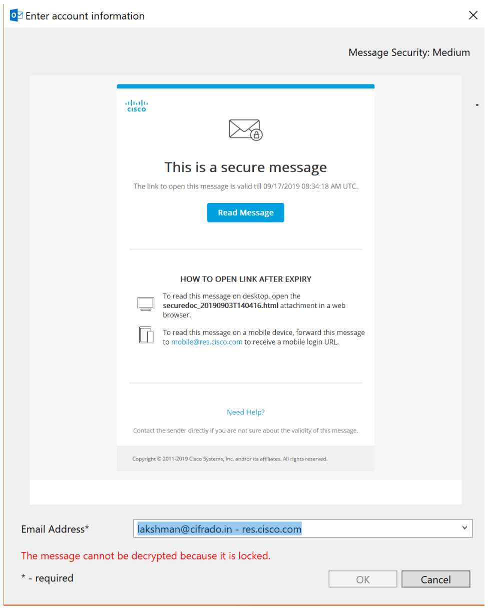
The message was transmitted securely but does not require a password.

* - required

The following describes the Message Security Options:

Message Security Options	Description
High	A high security message requires a password for authentication every time an encrypted message is decrypted.
Medium	If the recipient password is cached, a medium security message does not require a password when the message is decrypted.
Low	A low security message is transmitted securely but does not require a password to decrypt an encrypted message.

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.



Message Security: Medium

This is a secure message

The link to open this message is valid till 09/17/2019 08:34:18 AM UTC.

HOW TO OPEN LINK AFTER EXPIRY

To read this message on desktop, open the **securedoc_20190903T140416.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.

Copyright © 2011-2019 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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

The message cannot be decrypted because it is locked.

* - required

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

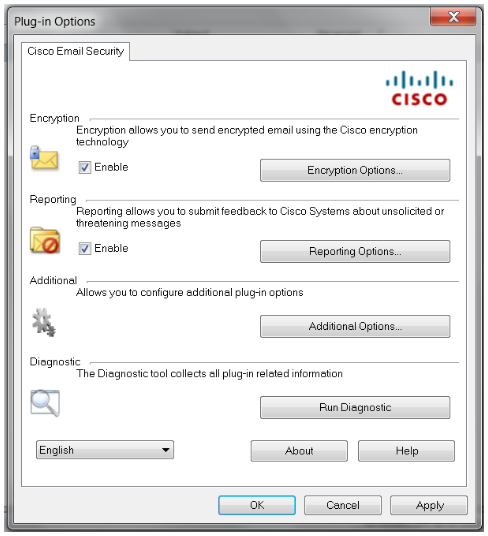
Changing Additional Settings

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:



Encryption
Encryption allows you to send encrypted email using the Cisco encryption technology
☑ Enable

Reporting
Reporting allows you to submit feedback to Cisco Systems about unsolicited or threatening messages
☑ Enable

Additional
Allows you to configure additional plug-in options

Diagnostic
The Diagnostic tool collects all plug-in related information

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.

Option	Description
Enable Logging	Select to enable logging for the Cisco Email Security plug-in.
Log file name	Specify the name of the log file that will be stored in %ALLUSERSPROFILE%\Cisco\Cisco Email Security Plug-in\<username>. The log file name should end with a .log extension.

Option	Description
Log level	Select one of the following: • **Normal** - By default, this option is enabled. Normal logging includes fatal, recoverable errors, warnings, and useful information. • **Extended**- Extended logging enables debug log messages in addition to the Normal logging messages. 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.

Option	Description
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.

Option	Description
Resets Identifier	Resets the identifier used to correlate usage reports.
Clear All Passwords	Clears all cached passwords for all accounts.

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, on page 41. 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 Diagnostic Tool from the Outlook Options Page, on page 42.

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, on page 41.

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, on page 41.

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 Repairing Cisco Email Security Plug-in for Outlook Files, on page 41.

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 later or contact support at 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 recipent listed in the email that you are sending, you may recieve the following message:

- *An error occurred during encryption: no recipients specified.*

An error occurred during decryption

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

An error occurred during decryption.

Solution

Run the diagnostic tool and send the diagnostic report to the support team. See Running the Cisco Email Security Diagnostic Tool, on page 42.

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, on page 42.

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:

Procedure

Step 1 Make sure Outlook is closed.

Step 2 Go to **Control Panel > Add or Remove Programs**.

Step 3 Find Cisco Email Security Plug In in the list of programs and click **Uninstall/Change**.

Step 4 Click **Repair**. The installer repair process runs.

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

Step 5 Perform the action that caused the error. If the same error occurs after running the repair process, follow the steps to provide Cisco feedback with the Diagnostic tool. See Running the Cisco Email Security Diagnostic Tool, on page 42.

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, on page 41 or Running the Cisco Email Security Diagnostic Tool, on page 42

Note If you experience errors, review Errors and Troubleshooting, on page 38 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.**

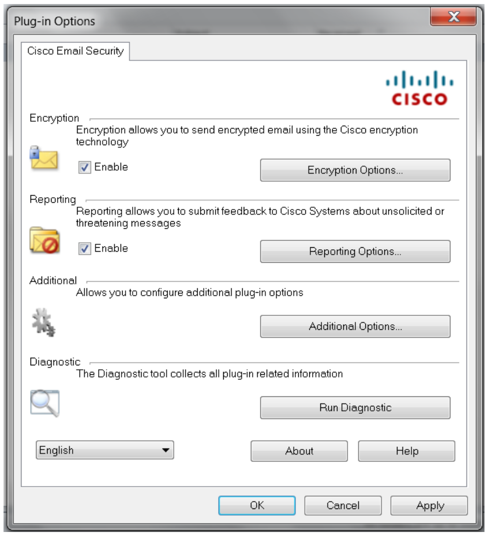
Running the Diagnostic Tool from the Outlook Options Page

Procedure

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:



Plug-in Options

Cisco Email Security

Encryption

Encryption allows you to send encrypted email using the Cisco encryption technology

☑ Enable

Reporting

Reporting allows you to submit feedback to Cisco Systems about unsolicited or threatening messages

☑ Enable

Additional

Allows you to configure additional plug-in options

Diagnostic

The Diagnostic tool collects all plug-in related information

English

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.

Troubleshooting Common Errors in Cisco Diagnostic Tool

All the diagnostic logs need to be in the extended mode for proper debugging

Perform the following steps after the log collection is completed in the running diagnostic tool:

1. Navigate to the following path - *CiscoSecurityDiagnosticReport\Outlook\UsersAppDataFiles\CiscoEmailSecurity.log*

2. Open the log file and check if any of the following issues are present:

    - Issue: Unable to Negotiate TLS Connection, on page 44

Issue: Unable to Negotiate TLS Connection

Problem: The plug-in is unable to connect to the CRES server (res.cisco.com) and negotiate a TLS connection.

Solution: Make sure that you connect the CRES server (res.cisco.com) to the client machine on which the plug-in is installed. If you are running a firewall on your network between the CRES server and the client machine, you need to open the following ports:

- `res.cisco.com` [used for default (decryption), encryption, and flag modes.]
- `verify.res.cisco.com` (used during BCE Config signing)
- `updates.res.cisco.com` (used when you click on the ‘Check for Updates’ option on the 'Plug-in' options in Microsoft Outlook.)

Issue: Unable to Resolve DNS Name

Problem: The plug-in is unable to connect to the CRES server (res.cisco.com) and resolve the DNS name.

Solution: Make sure that the client machine on which the plugin is installed has proper Internet connectivity.

Issue: Unable to Send HTTP Request

Problem: The plug-in is unable to send a HTTP request to the CRES server (res.cisco.com).

Solution: Make sure that you connect the CRES server (res.cisco.com) to the client machine on which the plug-in is installed. If you are running a firewall on your network between the CRES server and the client machine, you need to open the following ports:

- `res.cisco.com` [used for default (decryption), encryption, and flag modes.]
- `verify.res.cisco.com` (used during BCE Config signing.)
- `updates.res.cisco.com` (used when you click on the ‘Check for Updates’ option on the 'Plug-in' options in Microsoft Outlook.)

Issue: Invalid Response from Web Proxy Server - "HTTP/1.0 407 Proxy Authentication Required"

Problem: The plug-in is unable to connect to the CRES application using a proxy server because of any one of the following reasons:

- Proxy server authentication details (username and password) are not provided during installation.
- Invalid proxy server details

Solution: You need to verify the proxy server details provided in the BCE Config file during the plug-in installation.

Issue: Java Runtime Environment Not Found in Client Machine

Problem: The Java Runtime Environment is not insatlled in the client machine that contains the plugin.

Solution: Make sure that Java Runtime Environment is insatlled in the client machine. that contains the plugin.

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:

Procedure

Step 1 Download the BCE Configuration file template from the key server.

Log in as the admininistrator 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

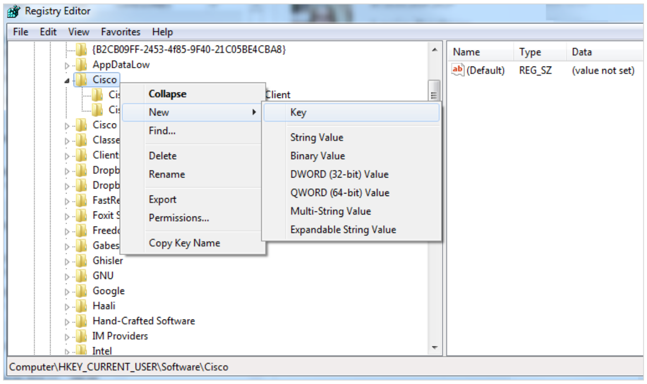
You can skip to install the Java Runtime Environment during the Cisco Email Security Plug-in setup. In this case, only the reporting functionality will be available. The encryption functionality will not function correctly. If you want to enable the encryption functionality later, you will need to install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

To disable Java Runtime Environment:

Procedure

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

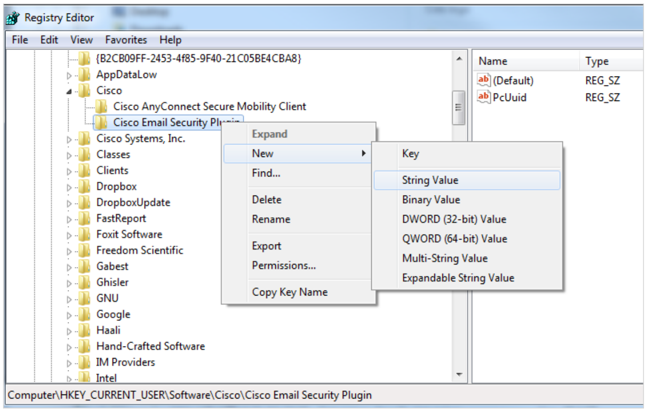
HKEY_CURRENT_USER\Software\Cisco\Cisco Email Security Plugin



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



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).

Note 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:

Procedure

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.