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

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.

- **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.

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:

Procedure

Step 1 Download the Email Security Plug-in installer from the Cisco Software Download Center.

Step 2 Double-click the *Cisco Email Security Plug-in.exe* file.

Step 3 Select a language in the **Cisco Email Security Plug-in Setup** window, and click **OK**.

Step 4 Click **Next** to start the installation program.

Step 5 Click **Install**.

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.

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

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.

Procedure

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

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

Make sure that you open the following TCP services and firewall ports on the network:

Default Port	Protocol	Hostname	Purpose
53	DNS	res.cisco.com	DNS is required to resolve the CRES key server URL. This service must be accessible to all end-users.
443	HTTPS	-	HTTPS is required to access the CRES server for Encryption, Flag & Decrypt (default) modes.
		res.cisco.com	Authentication
		verify.res.cisco.com	BCE Config file signing (for the first time).
		updates.res.cisco.com	For the plug-in updates.