Cisco Email Encryption

This chapter contains the following sections:

Overview of Cisco Email Encryption

AsyncOS supports using encryption to secure inbound and outbound email. To use this feature, you create an encryption profile that specifies characteristics of the encrypted message and connectivity information for the Cisco Registered Envelope Service (managed service) key server.

Next, you create content filters, message filters, and Data Loss Prevention policies to determine which messages to encrypt.

1. An outgoing message that meets the filter condition is placed in a queue on the appliance for encryption processing.
2. Once the message is encrypted, the key used to encrypt it is stored on the key server and the encrypted message is queued for delivery.
3. If a temporary condition exists that prohibits the encryption of emails in the queue (i.e., temporary C-Series busyness or Cisco Registered Envelope Service unavailability), messages are re-queued and retried at a later time.

Note You can also set up the appliance to first attempt to send a message over a TLS connection before encrypting it. For more information, see Using a TLS Connection as an Alternative to Encryption, on page 8.

How to Encrypt Messages with Cisco Registered Envelope Service

Table 1: How to Encrypt Messages with Cisco Registered Envelope Service

Steps	Do This	More Info
Step 1	Set up the Cisco IronPort Encryption appliance on the network.	See Setup and Installation
Step 2	Enable message encryption.	Enabling Message Encryption on the Email Security Appliance , on page 4.
Step 3	Specify the encryption key server and the security settings for the encrypted messages by creating an encryption profile.	Configuring How the Key Service Handles Encrypted Messages, on page 4.
Step 4	Define the conditions that messages must meet in order for the appliance to encrypt them.	Determining Which Messages to Encrypt, on page 8.
Step 5	Determine when to encrypt messages in the email workflow.	• Encrypting and Immediately Delivering Messages using a Content Filter, on page 9. or • Encrypting a Message upon Delivery using a Content Filter, on page 10.
Step 6	(Optional) Flag messages for additional security.	Inserting Encryption Headers into Messages, on page 11.
Step 7	Define groups of users for whom you want to encrypt messages.	Create a mail policy. See Mail Policies
Step 8	Associate the encryption actions that you defined with the user groups you defined.	Associate the content filter with the mail policy. See Mail Policies

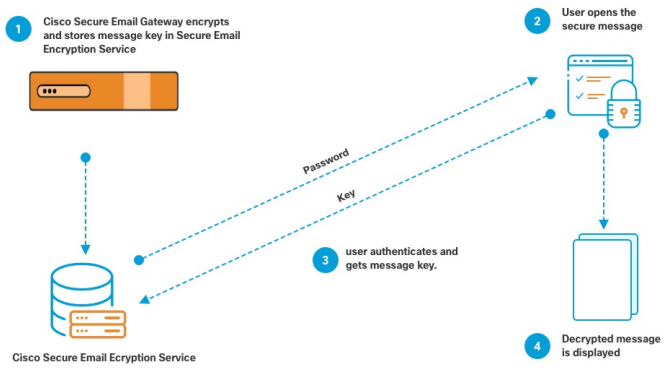
Related Topics

- Encryption Workflow, on page 2

Encryption Workflow

When using email encryption, the appliance encrypts a message and stores the message key on the Cisco Registered Envelope Service (hosted key service). When the recipient opens an encrypted message, the recipient is authenticated by the key service, and the decrypted message is displayed.

Figure 1: Encryption Workflow



The basic workflow for opening encrypted messages is:

1. When you configure an encryption profile, you specify the parameters for message encryption. For an encrypted message, the appliance creates and stores a message key on the hosted key service (Cisco Registered Envelope Service).
2. The recipient opens the secure envelope in a browser.
3. When a recipient opens an encrypted message in a browser, a password may be required to authenticate the recipient's identity. The key server returns the encryption key associated with the message.

Note When opening an encrypted email message for the first time, the recipient is required to register with the key service to open the secure envelope. After registering, the recipient may be able to open encrypted messages without authenticating, depending on settings configured in the encryption profile. The encryption profile may specify that a password isn't required, but certain features will be unavailable.

4. The decrypted message is displayed.

Encrypting Messages using the Email Security Appliance

To use encryption with the appliance , you must configure an encryption profile. You can enable and configure an encryption profile using the encryptionconfig CLI command, or via Security Services > Cisco IronPort Email Encryption in the GUI.

Note If PXE and S/MIME encryption is enabled on the appliance , AsyncOS encrypts messages using S/MIME first, and then using PXE.

Related Topics

- Enabling Message Encryption on the Email Security Appliance , on page 4
- Configuring How the Key Service Handles Encrypted Messages, on page 4
- Configuring the Default Locale of the Envelope, on page 7
- Updating to the Latest Version of the PXE Engine, on page 8

Enabling Message Encryption on the Email Security Appliance

Procedure

Step 1 Click **Security Services > Cisco IronPort Email Encryption**.

Step 2 Click **Enable**.

Step 3 (Optional) Click **Edit Settings** to configure the following options:

- The maximum message size to encrypt. Cisco's recommended message size is 10 MB. The maximum message size the appliance will encrypt is 25 MB.

  Note Encrypting messages larger than the recommended 10 MB limit may slow down the performance of the appliance. If you are using the Cisco Registered Envelope Service, message recipients will be unable to reply to an encrypted message that has attachments larger than 10 MB.

- Email address of the encryption account administrator. When you provision an Encryption Profile, this email address is registered automatically with the encryption server.
- Configure a proxy server.

Note You can configure the preferred storage to store a copy of the encrypted envelope by enabling the **Read from Message** feature in the Secure Emali Encryption Service admin portal. The following storage options are available:

- Cisco Storage
- Microsoft OneDrive Storage

For more details, see the *Cisco Secure Email Encryption Service Account Administrator Guide* on this page.

Configuring How the Key Service Handles Encrypted Messages

You can create one or more encryption profiles if you use a key service. You might want to create different encryption profiles if you want to use different levels of security for different groups of email. For example, you might want messages containing sensitive material to be sent with high security, but other messages to be sent with medium security. In this case, you might create a high security encryption profile to associate with the messages containing certain key words (such as 'confidential'), and create another encryption profile for other outgoing messages.

You can assign an encryption profile to a custom user role to allow delegated administrators assigned to that role to use the encryption profile with their DLP policies and content filters. Only administrators, operators, and delegated users can use encryption profiles when configuring DLP policies and content filters. Encryption profiles that are not assigned to a custom role are available for use by all delegated administrators with mail or DLP policy privileges. See Distributing Administrative Tasks for more information.

Note You can configure multiple encryption profiles for a hosted key service. If your organization has multiple brands, this allows you to reference different logos stored on the key server for the PXE envelopes.

An encryption profile stores the following settings:

- **Key server settings**. Specify a key server and information for connecting to that key server.
- **Envelope settings**. Specify details about the message envelope, such as the level of security, whether to return read receipts, the length of time a message is queued for encryption before it times out, the type of encryption algorithm to use, and whether to enable a decryption applet to run on the browser.
- **Message settings**. Specify details about messages, such as whether to enable secure message forwarding and secure Reply All.
- **Notification settings**. Specify the notification template to use for text and HTML notifications, as well as encryption failure notifications. You create the templates in text resources and select the templates when creating the encryption profile. You can also localize envelopes and specify a message subject for encryption failure notifications. For more information about notifications, see Encryption Notification Templates and Bounce and Encryption Failure Notification Templates.

Procedure

Step 1 In the Email Encryption Profiles section, click **Add Encryption Profile**.

Step 2 Enter a name for the Encryption Profile.

Step 3 Click the **Used By (Roles)** link, select the custom user role you want to have access to the encryption profile, and click **OK**.

Delegated administrators assigned to this custom role can use the encryption profile for any DLP policies and content filters for which they are responsible.

Step 4 In the Key Server Settings section, select Cisco Registered Envelope Service (hosted key service).

Step 5 If you select the Cisco Registered Envelope Service, enter the URL for the hosted key service. The key service URL is https://res.cisco.com .

Step 6 Click **Advanced** under Key Server Settings to specify whether to use HTTP or HTTPS for transferring the envelope's encrypted payload when the recipient opens the envelope. Choose from one of the following:

- **Use the Key Service with HTTP**. Transfers the encrypted payload from the key service using HTTP when the recipient opens the envelope. For Cisco Registered Envelope Service, this is the URL you specified in Step 5.
- Since the payload is already encrypted, transporting it over HTTP is safe and faster than sending over HTTPS. This provides better performance than sending image requests over HTTPS.
- **Use the Key Service with HTTPS**. Transfers the encrypted payload from the key service using HTTPS when the recipient opens the envelope. For Cisco Registered Envelope Service, this is the URL you specified in Step 5.
- **Specify a separate URL for payload transport**. If you don't want to use the key server for your encrypted payload, you can use another URL and specify whether to use HTTP or HTTPS for the payload transfer.

Step 7 In the Envelope Settings section, select the level of message security:

- **High Security**. The recipient must always enter a passphrase to open encrypted messages.
- **Medium Security**. The recipient does not need to enter credentials to open the encrypted message if the recipient credentials are cached.
- **No Passphrase Required**. This is the lowest level of encrypted message security. The recipient does not need to enter a passphrase to open the encrypted message. You can still enable the read receipts, Secure Reply All, and Secure Message Forwarding features for envelopes that are not passphrase-protected.

Step 8 To enable users to open your organization's URL by clicking its logo, you can add a link to the logo. Choose from the following options:

- **No link.** A live link is not added to the message envelope.
- **Custom link URL**. Enter the URL to add a live link to the message envelope.

Step 9 (Optional) Enable read receipts. If you enable this option, the sender receives a receipt when recipients open the secure envelope.

Step 10 (Optional) Click **Advanced** under Envelope Settings to configure the following settings:

- Enter the length of time (in seconds) that a message can be in the encryption queue before timing out. Once a message times out, the appliance bounces the message and sends a notification to the sender.
- Select an encryption algorithm - 'AES 192' or 'AES 256.'

  Note AES provides stronger encryption but also takes longer to decrypt, introducing delays for recipients. AES is typically used in government and banking applications.

- Enable or disable the decryption applet. Enabling this option causes the message attachment to be opened in the browser environment. Disabling this option causes message attachments to be decrypted at the key server. If you disable this option, messages may take longer to open, but are not dependent on the browser environment.

Step 11 In the Message Settings section, do the following:

- To enable secure reply all feature, check the **Enable Secure Reply All** check box.
- To enable secure message forwarding feature, check the **Enable Secure Message Forwarding** check box.

Step 12 (Optional) If you have selected Cisco Registered Envelope Service and this service supports localization of envelopes, enable localization of envelopes. In Notification Settings section, check the **Use Localized Envelope** check box.

Note If you enable localization of envelopes, you cannot select encrypted message HTML or text notification.

If you want to set the default locale of the envelope, see Configuring the Default Locale of the Envelope, on page 7.

Step 13 Select the HTML and text notification templates.

Note The key server uses an HTML or text notification based on the recipient's email application. You must configure notifications for both.

Do the following:

a) Select an HTML notification template. Choose from HTML notifications you configured in text resources. If you did not configure a template, the system uses the default template.
b) Select a text notification template. Choose from text notifications you configured in text resources. If you did not configure a template, the system uses the default template.

Note These options are unavailable if you use localized envelopes.

Step 14 Enter a subject header for encryption failure notifications. The appliance sends a notification if the encryption process times out.

Step 15 Select an encryption failure notification template for the message body. Choose from an encryption failure notification template you configured in text resources. If you did not configure a template, the system uses the default template.

Step 16 Submit and commit your changes.

Step 17 If you use Cisco Registered Envelope Service, you must take the additional step of provisioning your appliance . Provisioning the appliance registers the encryption profile with the hosted key service. To provision the appliance , click the **Provision** button for the encryption profile you want to register.

Configuring the Default Locale of the Envelope

The default locale of the envelope is English. If you have selected Cisco Registered Envelope Service and this service supports localization of envelopes, you can change the locale of the envelope to any one of the following:

- English
- French
- German
- Japanese
- Portuguese
- Spanish
- Italian
- Korean
- Dutch
- Polish
- Russian
- Chinese

Before You Begin

- Create an encryption profile with Cisco Registered Envelope Service as Key Service Type and envelope localization enabled. See Configuring How the Key Service Handles Encrypted Messages, on page 4.
- Make sure that Cisco Registered Envelope Service supports localization of envelopes.

Procedure

Step 1 Click **Security Services** > **Cisco IronPort Email Encryption**.

Step 2 Open an existing encryption profile.

Step 3 In the **Notification Settings** section, choose the locale from the **Localized Envelopes** drop-down list.

Step 4 Click **Submit**.

Step 5 Click **Commit Changes**.

Updating to the Latest Version of the PXE Engine

The Cisco Email Encryption Settings page displays the current versions of the PXE engine and the Domain Mappings file used by your appliance . You can use the **Security Services > Service Updates** page (or the updateconfig command in the CLI) to configure the appliance to automatically update the PXE engine. For more information, see Service Updates.

You can also manually update the engine using the **Update Now** button of the PXE Engine Updates section of IronPort Email Encryption Settings page (or the **`encryptionupdate`** command in the CLI).

Determining Which Messages to Encrypt

After you create an encryption profile, you need to create an outgoing content filter that determines which email messages should be encrypted. The content filter scans outgoing email and determines if the message matches the conditions specified. Once the content filter determines a message matches the condition, the appliance encrypts the message and sends the generated key to the key server. It uses settings specified in the encryption profile to determine the key server to use and other encryption settings.

You can also encrypt messages after they are released after Data Loss Prevention scanning. For more information, see Defining Actions to Take for DLP Violations (Message Actions).

Related Topics

- Using a TLS Connection as an Alternative to Encryption, on page 8
- Encrypting and Immediately Delivering Messages using a Content Filter, on page 9
- Encrypting a Message upon Delivery using a Content Filter, on page 10

Using a TLS Connection as an Alternative to Encryption

Based on the destination controls specified for a domain, your appliance can securely relay a message over a TLS connection instead of encrypting it, if a TLS connection is available. The appliance decides whether to encrypt the message or send it over a TLS connection based on the TLS setting in the destination controls (Required, Preferred, or None) and the action defined in the encryption content filter.

When creating the content filter, you can specify whether to always encrypt a message or to attempt to send it over a TLS connection first, and if a TLS connection is unavailable, to encrypt the message. The following table shows you how an appliance will send a message based on the TLS settings for a domain's destination controls, if the encryption control filter attempts to send the message over a TLS connection first.

Table 2: TLS Support on ESA Appliances

Destination Controls TLS Setting	Action if TLS Connection Available	Action if TLS Connection Unavailable
None	Encrypt envelope and send	Encrypt envelope and send
TLS Preferred	Send over TLS	Encrypt envelope and send
TLS Required	Send over TLS	Retry/bounce message

For more information about enabling TLS on destination controls, see Configuring the Gateway to Receive Email.

Encrypting and Immediately Delivering Messages using a Content Filter

Before You Begin

- To understand the concept of building conditions for content filters, see Overview of Content Filters.
- (Optional) See Inserting Encryption Headers into Messages, on page 11.

Procedure

Step 1 Go to **Mail Policies > Outgoing Content Filters**.

Step 2 In the Filters section, click **Add Filter**.

Step 3 In the Conditions section, click **Add Condition.**

Step 4 Add a condition to filter the messages that you want to encrypt. For example, to encrypt sensitive material, you might add a condition that identifies messages containing particular words or phrases, such as "Confidential," in the subject or body.

Step 5 Click **OK**.

Step 6 Optionally, click **Add Action** and select **Add Header** to insert an encryption header into the messages to specify an additional encryption setting.

Step 7 In the Actions section, click **Add Action**.

Step 8 Select **Encrypt and Deliver Now (Final Action)** from the **Add Action** list.

Step 9 Select whether to always encrypt messages that meet the condition or to only encrypt messages if the attempt to send it over a TLS connection fails.

Step 10 Select the encryption profile to associate with the content filter.

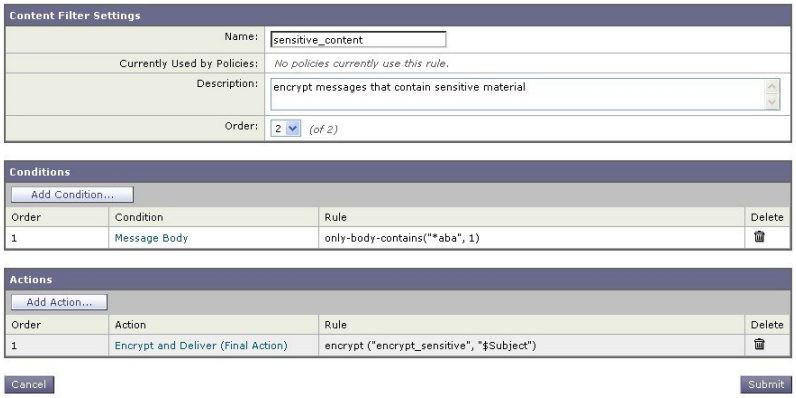
The encryption profile specifies settings about the key server to use, levels of security, formatting of the message envelope, and other message settings. When you associate an encryption profile with the content filter, the content filter uses these stored settings to encrypt messages.

Step 11 Enter a subject for the message.

Step 12 Click **OK**.

The content filter in the following figure shows a content filter that searches for ABA content in the message body. The action defined for the content filter specifies that the email is encrypted and delivered.

Figure 2: Encryption Content Filter



Step 13 After you add the encrypt action, click **Submit**.

Step 14 Commit your changes.

What to do next

After you add the content filter, you need to add the filter to an outgoing mail policy. You may want to enable the content filter on the default policy, or you may choose to apply the filter to a specific mail policy, depending on your organization's needs. For information about working with mail policies, see Overview of Mail Policies.

Encrypting a Message upon Delivery using a Content Filter

Create a content filter to encrypt a message on delivery, which means that the message continues to the next stage of processing, and when all processing is complete, the message is encrypted and delivered.

Before You Begin

- To understand the concept of building conditions for content filters, see Overview of Content Filters.
- (Optional) See Inserting Encryption Headers into Messages, on page 11.

Procedure

Step 1 Go to **Mail Policies > Outgoing Content Filters**.

Step 2 In the Filters section, click **Add Filter**.

Step 3 In the Conditions section, click **Add Condition.**

Step 4 Add a condition to filter the messages that you want to encrypt. For example, to encrypt sensitive material, you might add a condition that identifies messages containing particular words or phrases, such as "Confidential," in the subject or body.

Step 5 Click **OK**.

Step 6 Optionally, click **Add Action** and select **Add Header** to insert an encryption header into the messages to specify an additional encryption setting.

Step 7 In the Actions section, click **Add Action**.

Step 8 Select **Encrypt on Delivery** from the **Add Action** list.

Step 9 Select whether to always encrypt messages that meet the condition or to only encrypt messages if the attempt to send it over a TLS connection fails.

Step 10 Select the encryption profile to associate with the content filter.

The encryption profile specifies settings about the key server to use, levels of security, formatting of the message envelope, and other message settings. When you associate an encryption profile with the content filter, the content filter uses these stored settings to encrypt messages.

Step 11 Enter a subject for the message.

Step 12 Click **OK**.

Step 13 After you add the encrypt action, click **Submit**.

Step 14 Commit your changes.

What to do next

After you add the content filter, you need to add the filter to an outgoing mail policy. You may want to enable the content filter on the default policy, or you may choose to apply the filter to a specific mail policy, depending on your organization's needs. For information about working with mail policies, see Overview of Mail Policies.

Inserting Encryption Headers into Messages

AsyncOS enables you to add encryption settings to a message by inserting an SMTP header into a message using either a content filter or a message filter. The encryption header can override the encryption settings defined in the associated encryption profile, and it can apply specified encryption features to messages.

Note The Cisco Ironport Encryption appliance must be set up to handle flagged messages.

Procedure

Step 1 Go to **Mail Policies > Outgoing Content Filters** or **Incoming Content Filters**.

Step 2 In the Filters section, click **Add Filter**.

Step 3 In the Actions section, click **Add Action** and select **Add/Edit Header** to insert an encryption header into the messages to specify an additional encryption setting.

For example, if you want a Registered Envelope to expire in 24 hours after you send it, type X-PostX-ExpirationDate as the header name and +24:00:00 as the header value.

What to do next

Related Topics

- Encryption Headers, on page 12
- Encryption Headers Examples, on page 13

- For more information about creating an encryption content filter, see Encrypting and Immediately Delivering Messages using a Content Filter, on page 9.
- For information about inserting a header using a message filter, see Using Message Filters to Enforce Email Policies.

Encryption Headers

The following table displays the encryption headers that you can add to messages.

Table 3: Email Encryption Headers

MIME Header	Description	Value
`X-PostX-Reply- Enabled`	Indicates whether to enable secure reply for the message and displays the Reply button in the message bar. This header adds an encryption setting to the message.	A Boolean for whether to display the Reply button. Set to true to display the button. The default value is false .
`X-PostX-Reply-All-Enabled`	Indicates whether to enable secure “reply all” for the message and displays the Reply All button in the message bar. This header overrides the default profile setting.	A Boolean for whether to display Reply All button. Set to true to display the button. The default value is false .
`X-PostX-Forward-Enabled`	Indicates whether to enable secure message forwarding and displays the Forward button in the message bar. This header overrides the default profile setting.	A Boolean for whether to display the Forward button. Set to true to display the button. The default value is false .
`X-PostX-Send-Return-Receipt`	Indicates whether to enable read receipts. The sender receives a receipt when recipients open the Secure Envelope. This header overrides the default profile setting.	A Boolean for whether to send a read receipt. Set to true to display the button. The default value is false .
`X-PostX-Expiration Date`	Defines a Registered Envelope’s expiration date before sending it. The key server restricts access to the Registered Envelope after the expiration date. The Registered Envelope displays a message indicating that the message has expired. This header adds an encryption setting to the message. If you use Cisco Registered Envelope Service, you can log in to the website at http://res.cisco.com and use the message management features to set, adjust, or eliminate the expiration dates of messages after you send them.	A string value containing relative date or time. Use the +HH:MM:SS format for relative hours, minutes, and seconds, and the +D format for relative days. By default, there is no expiration date.
`X-PostX-ReadNotification Date`	Defines the Registered Envelope’s “read by” date before sending it. The local key server generates a notification if the Registered Envelope has not been read by this date. Registered Envelopes with this header do not work with Cisco Registered Envelope Service, only a local key server. This header adds an encryption setting to the message.	A string value containing relative date or time. Use the +HH:MM:SS format for relative hours, minutes, and seconds, and the +D format for relative days. By default, there is no expiration date.

MIME Header	Description	Value
`X-PostX-Suppress-Applet-For-Open`	Indicates whether to disable the decryption applet. The decryption applet causes message attachments to be opened in the browser environment. Disabling the applet causes the message attachment to be decrypted at the key server. If you disable this option, messages may take longer to open, but they are not dependent on the browser environment. This header overrides the default profile setting.	A Boolean for whether to disable the decryption applet. Set to true to disable the applet. The default value is false .
`X-PostX-Use-Script`	Indicates whether to send JavaScript-free envelopes. A JavaScript-free envelope is a Registered Envelope that does not include the JavaScript that is used to open envelopes locally on the recipient's computer. The recipient must use either the Open Online method or the Open by Forwarding method to view the message. Use this header if a recipient domain's gateway strips JavaScript and makes the encrypted message unopenable.This header adds an encryption setting to the message.	A Boolean for whether the JavaScript applet should be included or not. Set to false to send a JavaScript-free envelope. The default value is true .
`X-PostX-Remember-Envelope-Key-Checkbox`	Indicates whether to allow envelope-specific key caching for offline opening of envelopes. With envelope key caching, the decryption key for a particular envelope is cached on the recipient's computer when the recipient enters the correct passphrase and selects the "Remember the password for this envelope" check box. After that, the recipient does not need to enter a passphrase again to reopen the envelope on the computer. This header adds an encryption setting to the message.	A Boolean for whether to enable envelope key caching and display the "Remember the password for this envelope" check box. The default value is false .

Encryption Headers Examples

This section provides examples of encryption headers.

Related Topics

- Enabling JavaScript-Free Envelopes, on page 14
- Enabling Envelope Key Caching for Offline Opening, on page 13
- Enabling Message Expiration, on page 14
- Disabling the Decryption Applet, on page 14

Enabling Envelope Key Caching for Offline Opening

To send a Registered Envelope with envelope key caching enabled, insert the following header into the message:

```
X-PostX-Remember-Envelope-Key-Checkbox: true
```

The “Remember the password for this envelope” check box is displayed on the Registered Envelope.

Enabling JavaScript-Free Envelopes

To send a Registered Envelope that is JavaScript-free, insert the following header into the message:

```
X-PostX-Use-Script: false
```

When the recipient opens the securedoc.html attachment, the Registered Envelope is displayed with an Open Online link, and the Open button is disabled.

Enabling Message Expiration

To configure a message so that it expires 24 hours after you send it, insert the following header into the message:

```
X-PostX-ExpirationDate: +24:00:00
```

The recipient can open and view the content of the encrypted message during the 24-hour period after you send it. After that, the Registered Envelope displays a message indicating that the envelope has expired.

Disabling the Decryption Applet

To disable the decryption applet and have the message attachment decrypted at the key server, insert the following header into the message:

```
X-PostX-Suppress-Applet-For-Open: true
```

Note The message may take longer to open when you disable the decryption applet, but it is not dependent on the browser environment.