Can I preset the expiration time of secure envelopes that are generated from a Cisco Email Security Appliance that uses CRES?

Contents

Introduction

This document describes how to preset the expiration time for secure envelopes that are generated from a Cisco Email Security Appliance (ESA) that implements the Cisco Registered Envelope Service (RES).

Can I preset the expiration time of secure envelopes that are generated from a Cisco Email Security Appliance that uses RES?

Yes, you can add-in SMTP headers to the outgoing messages that will be flagged for encryption. This includes the 'X-PostX-ExpirationDate' header.

The following is an excerpt from the Email Security Appliance User Guide.

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.

Procedure

Step 1 Go toMail Policies > Outgoing Content FiltersorIncoming Content Filters.
Step 2 In the Filters section, clickAdd Filter.
Step 3 In the Actions section, clickAdd Actionand selectAdd/Edit Headerto insert an encryption header int
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-Pos
ExpirationDateas the header name and +24:00:00 as the header value.

What to do next

Related Topics

- For more information about creating an encryption content filter, see Encrypting and Immediately Delivering Messages using a Content Filter.
- 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 a 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 display the Reply butto Set to true to display th button. The default valu 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 display the Reply All bu Set to true to display th button. The default valu 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 display the Forward bu Set to true to display th button. The default valu 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 send a read receipt. Se true to display the butto The default value is fal
`X-PostX-ExpirationDate`	Defines a Registered Envelope’s expiration date before sending it. The key server restricts access to the Registered	A string value containin relative date or time. U the +HH:MM:SS forma

	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.	relative hours, minutes seconds, and the +D fo for relative days. By de there is no expiration d
X-PostX-ReadNotificationDate	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 containin relative date or time. U the +HH:MM:SS forma relative hours, minutes seconds, and the +D fo for relative days. By de there is no expiration d
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 disable the decryption applet. Set to true to di the applet. The default 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 JavaScript applet shou included or not. Set to to send a JavaScript-fr envelope. The default is true.
X-PostX-Remember-Envelope-Key-Checkbox	Indicates whether to allow envelope-specific key caching for the 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" checkbox. After that, the	A Boolean for whether enable envelope key caching and display the "Remember the passw for this envelope" chec The default value is fal

	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.

Encryption Headers Examples

This section provides examples of encryption headers.

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” checkbox 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.