

¿Puedo predefinir el tiempo de vencimiento de los sobres seguros generados a partir de un dispositivo de seguridad Cisco Email Security Appliance que utiliza CRES?

Contenido

[Introducción](#)

[¿Puedo predefinir el tiempo de vencimiento de los sobres seguros que se generan a partir de un dispositivo de seguridad Cisco Email Security Appliance que utiliza RES?](#)

[Inserción de encabezados de cifrado en mensajes](#)

[Procedimiento](#)

[Pasos Siguientes](#)

[Encabezados de cifrado](#)

[Ejemplos de Encabezados de Cifrado](#)

[Habilitación del Almacenamiento en Caché de la Clave del Sobre para la Apertura sin Conexión](#)

[Habilitación de Sobres Libres de Javascript](#)

[Habilitación del vencimiento del mensaje](#)

[Inhabilitación del Applet de Descifrado](#)

Introducción

Este documento describe cómo predefinir el tiempo de caducidad para los sobres seguros generados a partir de un dispositivo de seguridad Cisco Email Security Appliance (ESA) que implementa el servicio Cisco Registered Envelope Service (RES).

¿Puedo predefinir el tiempo de vencimiento de los sobres seguros que se generan a partir de un dispositivo de seguridad Cisco Email Security Appliance que utiliza RES?

Sí, puede agregar encabezados SMTP a los mensajes salientes que se marcarán para el cifrado. Esto incluye el encabezado 'X-PostX-ExpirationDate'.

A continuación se muestra un extracto de la [Guía del Usuario de Email Security Appliance](#).

Inserción de encabezados de cifrado en mensajes

AsyncOS permite agregar parámetros de cifrado a un mensaje insertando un encabezado SMTP en un mensaje utilizando un filtro de contenido o un filtro de mensaje. El encabezado de cifrado puede reemplazar la configuración de cifrado definida en el perfil de cifrado asociado y puede aplicar funciones de cifrado especificadas a los mensajes.

Procedimiento

Paso Vaya a Políticas de correo > Filtros de contenido saliente o filtros de contenido entrante.

1

Paso En la sección Filtros, haga clic en Agregar filtro.

2

Paso En la sección Acciones, haga clic en Agregar acción y seleccione Agregar/editar encabezado para insertar un encabezado de cifrado en los mensajes para especificar una configuración de cifrado adicional.

3 Por ejemplo, si desea que un sobre registrado venza en 24 horas después de enviarlo, escriba X-PostX-ExpirationDateas como el nombre del encabezado y +24:00:00 como el valor del encabezado.

Pasos Siguintes

Temas relacionados

- Para obtener más información sobre cómo crear un filtro de contenido de cifrado, vea [Cifrar y entregar inmediatamente mensajes mediante un filtro de contenido](#).
- Para obtener información sobre cómo insertar un encabezado mediante un filtro de mensajes, vea [Uso de filtros de mensajes para aplicar políticas de correo electrónico](#).

Encabezados de cifrado

En la tabla siguiente se muestran los encabezados de cifrado que se pueden agregar a los mensajes.

Tabla 3. Encabezados de cifrado de correo electrónico

Encabezado MIME	Descripción	Valor
X-PostX-Reply-Enabled	Indica si se debe habilitar una respuesta segura para el mensaje y muestra el botón Responder en la barra de mensajes. Este encabezado agrega una configuración de cifrado al mensaje.	Valor Boolean para mostrar el botón Responder. Establezca el valor en true para mostrar el botón. El valor predeterminado es false.
X-PostX-Reply-All-Enabled	Indica si se debe activar la opción segura "responder a todos" para el mensaje y muestra el botón Responder a todos en la barra de mensajes. Este encabezado anula la configuración predeterminada del perfil.	Valor Boolean para mostrar el botón Responder a todos. Establezca el valor en true para mostrar el botón. El valor predeterminado es false.
X-PostX-Forward-Enabled	Indica si se debe habilitar el reenvío seguro de mensajes y muestra el botón Reenviar en la barra de mensajes. Este encabezado anula la configuración predeterminada del perfil.	Valor Boolean para mostrar el botón Reenviar. Establezca el valor en true para mostrar el botón. El valor predeterminado es false.

X-PostX-Send-Return-Receipt	Indica si se activarán las confirmaciones de lectura. El remitente recibe una confirmación cuando los destinatarios abren el sobre seguro. Este encabezado anula la configuración predeterminada del perfil.	false. Valor booleano para e... una confirmación de lectura. Establezca el en true para mostrar e botón. El valor predeterminado es fa
X-PostX-ExpirationDate	Define la fecha de vencimiento de un sobre registrado antes de enviarlo. El servidor de claves restringe el acceso al sobre registrado después de la fecha de vencimiento. El sobre registrado muestra un mensaje que indica que el mensaje ha caducado. Este encabezado agrega una configuración de cifrado al mensaje. Si utiliza Cisco Registered Envelope Service, puede iniciar sesión en el sitio web en http://res.cisco.com y utilizar las funciones de administración de mensajes para establecer, ajustar o eliminar las fechas de vencimiento de los mensajes después de enviarlos.	Valor de cadena que contiene la fecha o ho relativa. Utilice el form +HH:MM:SS para hor minutos y segundos relativos, y el formato para días relativos. D forma predeterminada hay fecha de vencimi
X-PostX-ReadNotificationDate	Define la fecha de lectura del sobre registrado antes de enviarlo. El servidor de claves local genera una notificación si el sobre registrado no se ha leído antes de esta fecha. Los sobres registrados con este encabezado no funcionan con Cisco Registered Envelope Service, solo un servidor de claves local. Este encabezado agrega una configuración de cifrado al mensaje.	Valor de cadena que contiene la fecha o ho relativa. Utilice el form +HH:MM:SS para hor minutos y segundos relativos, y el formato para días relativos. D forma predeterminada hay fecha de vencimi
X-PostX-Suppress-Applet-For-Open	Indica si se inhabilita el applet de descifrado. El applet de descifrado hace que los archivos adjuntos de mensajes se abran en el entorno del explorador. Si se desactiva el applet, el archivo adjunto del mensaje se descifra en el servidor de claves. Si desactiva esta opción, los mensajes pueden tardar más en abrirse, pero no dependen del entorno del explorador. Este encabezado anula la configuración predeterminada del perfil.	Un valor booleano pa se inhabilita el applet descifrado. Configure true para desactivar e applet. El valor predeterminado es fa
X-PostX-Use-Script	Indica si se enviarán sobres libres de JavaScript. Un sobre libre de JavaScript es un sobre registrado que no incluye el JavaScript que se utiliza para abrir sobres localmente en el equipo del destinatario. El destinatario debe utilizar el método Open Online (Abrir en línea) o el método Open by Forwarding (Abrir mediante reenvío) para ver el mensaje. Utilice este encabezado si la gateway de un dominio de destinatario	Un valor booleano pa saber si se debe inclu no el applet JavaScript. Configure en false pa enviar un sobre libre e JavaScript. El valor predeterminado es tru

elimina JavaScript y hace que el mensaje cifrado no se active. Este encabezado agrega una configuración de cifrado al mensaje.

Indica si se permite el almacenamiento en caché de claves específico del sobre para la apertura sin conexión de sobres. Con el almacenamiento en caché de la clave del sobre, la clave de descifrado de un sobre determinado se almacena en la memoria caché del equipo del destinatario cuando el destinatario introduce la frase de paso correcta y selecciona la casilla de verificación "Recordar la contraseña para este sobre". Después de eso, el destinatario no necesita volver a introducir una frase de paso para volver a abrir el sobre en el equipo. Este encabezado agrega una configuración de cifrado al mensaje.

X-PostX-Remember-Envelope-Key-Checkbox

Un valor booleano que indica si se debe habilitar el almacenamiento en caché de claves de sobre y mostrar la casilla de verificación "Recordar la contraseña de este sobre". El valor predeterminado es false.

Ejemplos de Encabezados de Cifrado

Esta sección proporciona ejemplos de encabezados de cifrado.

Habilitación del Almacenamiento en Caché de la Clave del Sobre para la Apertura sin Conexión

Para enviar un sobre registrado con el almacenamiento en caché de claves de sobre habilitado, inserte el siguiente encabezado en el mensaje:

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

La casilla de verificación "Recordar la contraseña de este sobre" se muestra en el sobre registrado.

Habilitación de Sobres Libres de Javascript

Para enviar un sobre registrado que no tenga JavaScript, introduzca el encabezado siguiente en el mensaje:

```
X-PostX-Use-Script: falso
```

Cuando el destinatario abre el archivo adjunto securedoc.html, se muestra el sobre registrado con un enlace Abrir en línea y el botón Abrir está desactivado.

Habilitación del vencimiento del mensaje

Para configurar un mensaje de modo que venza 24 horas después de enviarlo, inserte el siguiente encabezado en el mensaje:

```
Fecha de vencimiento X-PostX: +24:00:00
```

El destinatario puede abrir y ver el contenido del mensaje cifrado durante el período de 24 horas posterior al envío. Después, el sobre registrado muestra un mensaje que indica que el sobre ha caducado.

Inhabilitación del Applet de Descifrado

Para inhabilitar el applet de descifrado y descifrar el archivo adjunto del mensaje en el servidor de claves, inserte el siguiente encabezado en el mensaje:

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

Nota: El mensaje puede tardar más en abrirse cuando inhabilita el applet de descifrado, pero no depende del entorno del explorador.