

# Posso predefinir o tempo de expiração de envelopes seguros gerados a partir de um Cisco Email Security Appliance que usa CRES?

## Contents

[Introduction](#)

[Posso predefinir o tempo de expiração de envelopes seguros gerados a partir de um Cisco Email Security Appliance que usa RES?](#)

[Inserindo cabeçalhos de criptografia em mensagens](#)

[Procedimento](#)

[O que fazer a seguir](#)

[Cabeçalhos de criptografia](#)

[Exemplos de cabeçalhos de criptografia](#)

[Habilitando cache de chave de envelope para abertura off-line](#)

[Habilitando envelopes sem Javascript](#)

[Habilitando o vencimento da mensagem](#)

[Desativando o miniaplicativo de descriptografia](#)

## Introduction

Este documento descreve como predefinir o tempo de expiração para envelopes seguros gerados a partir de um Cisco Email Security Appliance (ESA) que implementa o Cisco Registered Envelope Service (RES).

## Posso predefinir o tempo de expiração de envelopes seguros gerados a partir de um Cisco Email Security Appliance que usa RES?

Sim, você pode adicionar cabeçalhos SMTP às mensagens de saída que serão sinalizadas para criptografia. Isso inclui o cabeçalho 'X-PostX-ExpirationDate'.

Veja a seguir um trecho do [Guia do usuário do Email Security Appliance](#).

## Inserindo cabeçalhos de criptografia em mensagens

O AsyncOS permite adicionar configurações de criptografia a uma mensagem inserindo um cabeçalho SMTP em uma mensagem usando um filtro de conteúdo ou um filtro de mensagem. O cabeçalho de criptografia pode substituir as configurações de criptografia definidas no perfil de criptografia associado e pode aplicar recursos de criptografia especificados às mensagens.

## Procedimento

**Passo 1** Vá para Políticas de e-mail > Filtros de conteúdo de saída ou Filtros de conteúdo de entrada.

**Passo 2** Na seção Filtros, clique em Adicionar filtro.

**Etapa 3** Na seção Ações, clique em Adicionar Ação e selecione Adicionar/Editar Cabeçalho para inserir um cabeçalho de criptografia nas mensagens para especificar uma configuração de criptografia adicional. Por exemplo, se quiser que um Envelope registrado expire em 24 horas após enviá-lo, digite X-PostX-ExpirationDate como o nome do cabeçalho e +24:00:00 como o valor do cabeçalho.

## O que fazer a seguir

### Tópicos relacionados

- Para obter mais informações sobre como criar um filtro de conteúdo de criptografia, consulte [Criptografia e Entrega imediata de mensagens usando um filtro de conteúdo](#).
- Para obter informações sobre como inserir um cabeçalho usando um filtro de mensagens, consulte [Usando Filtros de Mensagens para Aplicar Políticas de Email](#).

## Cabeçalhos de criptografia

A tabela a seguir exibe os cabeçalhos de criptografia que você pode adicionar às mensagens.

Tabela 3. Cabeçalhos de criptografia de e-mail

Cabeçalho MIME	Descrição	Valor
X-PostX-Reply-Enabled	Indica se uma resposta segura deve ser habilitada para a mensagem e exibe o botão Responder na barra de mensagens. Este cabeçalho adiciona uma configuração de criptografia à mensagem.	Um booleano para se o botão Responder deve ou não o botão Responder. Defina como verdadeiro para exibir o botão. O valor padrão é falso.
X-PostX-Reply-All-Enabled	Indica se a mensagem deve ser habilitada como "responder a todos" e exibe o botão Responder a todos na barra de mensagens. Este cabeçalho substitui a configuração de perfil padrão.	Um booleano para se o botão Responder a todos deve ou não o botão Responder a todos. Defina como verdadeiro para exibir o botão. O valor padrão é falso.
X-PostX-Forward-Enabled	Indica se o encaminhamento de mensagens seguro deve ser ativado e exibe o botão Encaminhar na barra de mensagens. Este cabeçalho substitui a configuração de perfil padrão.	Um booleano para se o botão Forward (Encaminhar) deve ou não o botão Forward (Encaminhar) deve ser exibido. Defina como verdadeiro para exibir o botão. O valor padrão é falso.
X-PostX-Send-Return-Receipt	Indica se os recibos lidos devem ser ativados. O remetente recebe uma	Um booleano para se o botão Return Receipt (Retornar Recibo) deve ou não o botão Return Receipt (Retornar Recibo) deve ser exibido. Defina como verdadeiro para exibir o botão. O valor padrão é falso.

confirmação quando os destinatários abrem o Envelope seguro. Este cabeçalho substitui a configuração de perfil padrão.

enviado um recibo de leitura. Defina como verdadeiro para exibir o botão. O valor padrão é falso.

Define a data de vencimento de um Envelope registrado antes de enviá-lo. O servidor de chaves restringe o acesso ao Envelope registrado após a data de expiração. O Envelope registrado exibe uma mensagem indicando que a mensagem expirou. Este cabeçalho adiciona uma configuração de criptografia à mensagem. Se você usar o Cisco Registered Envelope Service, poderá fazer login no site em <http://res.cisco.com> e usar os recursos de gerenciamento de mensagens para definir, ajustar ou eliminar as datas de expiração das mensagens depois de enviá-las.

Um valor de string contendo data ou hora relativa. Use o formato +HH:MM:SS para horas, minutos e segundos relativos e o formato para dias relativos. Por padrão, não há data de expiração.

Define a data de "leitura por" do Envelope registrado antes de enviá-lo. O servidor de chaves local gera uma notificação se o Envelope registrado não tiver sido lido até essa data. Os Envelopes registrados com esse cabeçalho não funcionam com o Cisco Registered Envelope Service, apenas um servidor de chaves local. Este cabeçalho adiciona uma configuração de criptografia à mensagem.

Um valor de string contendo data ou hora relativa. Use o formato +HH:MM:SS para horas, minutos e segundos relativos e o formato para dias relativos. Por padrão, não há data de expiração.

Indica se o applet de descryptografia deve ser desabilitado. O miniaplicativo de descryptografia faz com que os anexos da mensagem sejam abertos no ambiente do navegador. Desativar o miniaplicativo faz com que o anexo da mensagem seja descryptografado no servidor de chaves. Se você desabilitar essa opção, as mensagens podem demorar mais para serem abertas, mas não dependem do ambiente do navegador. Este cabeçalho substitui a configuração de perfil padrão.

Um booleano para especificar se o applet de descryptografia deve ser desabilitado. Defina como verdadeiro para desabilitar o miniaplicativo. O valor padrão é falso.

Indica se deve ser enviado envelopes sem JavaScript. Um envelope sem JavaScript é um Envelope registrado que não inclui o JavaScript usado para abrir envelopes localmente no computador do destinatário. O destinatário deve usar o método Open Online (Abrir on-line) ou o método Open by Forwarding (Abrir por encaminhamento) para exibir a mensagem. Use esse cabeçalho se o gateway de um domínio do destinatário desmembrar o JavaScript e desabilitar a mensagem criptografada. Este

Um booleano para especificar se o miniaplicativo JavaScript deve ou não ser incluído. Defina como falso para enviar um envelope sem JavaScript. O valor padrão é verdadeiro.

X-PostX-ExpirationDate

X-PostX-ReadNotificationDate

X-PostX-Suppress-Applet-For-Open

X-PostX-Use-Script

cabeçalho adiciona uma configuração de criptografia à mensagem. Indica se deve ser permitido o cache de chaves específicas do envelope para a abertura offline de envelopes. Com o cache da chave de envelope, a chave de descryptografia de um determinado envelope é armazenada em cache no computador do destinatário quando o destinatário digita a senha correta e seleciona a caixa de seleção "Lembrar a senha para este envelope". Depois disso, o destinatário não precisa inserir uma senha novamente para reabrir o envelope no computador. Este cabeçalho adiciona uma configuração de criptografia à mensagem.

X-PostX-Remember-Envelope-Key-Checkbox

Um booleano para se deve ou não ativar o cache da chave de envelope e exibir a caixa de seleção "Lembrar a senha para este envelope". O valor padrão é falso.

## Exemplos de cabeçalhos de criptografia

Esta seção fornece exemplos de cabeçalhos de criptografia.

### Habilitando cache de chave de envelope para abertura off-line

Para enviar um Envelope registrado com cache de chave de envelope habilitado, insira o seguinte cabeçalho na mensagem:

X-PostX-Remember-Envelope-Key-Checkbox: verdadeiro

A caixa de seleção "Lembrar a senha para este envelope" é exibida no Envelope registrado.

### Habilitando envelopes sem Javascript

Para enviar um Envelope registrado sem JavaScript, insira o seguinte cabeçalho na mensagem:

X-PostX-Use-Script: falso

Quando o destinatário abre o anexo securedoc.html, o Envelope registrado é exibido com um link Abrir on-line e o botão Abrir é desativado.

### Habilitando o vencimento da mensagem

Para configurar uma mensagem de modo que ela expire 24 horas depois de ser enviada, insira o cabeçalho a seguir na mensagem:

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

O destinatário pode abrir e exibir o conteúdo da mensagem criptografada durante o período de 24 horas após o envio. Depois disso, o Envelope registrado exibe uma mensagem indicando que o envelope expirou.

## Desativando o miniaplicativo de descriptografia

Para desativar o miniaplicativo de descriptografia e fazer com que o anexo da mensagem seja descriptografado no servidor de chaves, insira o seguinte cabeçalho na mensagem:

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

**Note:** A mensagem pode demorar mais para ser aberta quando você desativa o miniaplicativo de descriptografia, mas não depende do ambiente do navegador.