Est-ce que je peux pré-établir le temps d'expiration des enveloppes sécurisées qui sont générées d'une appliance de sécurité du courrier électronique de Cisco qui utilise CRES ?

Contenu

Introduction

Ce document décrit comment pré-établir le temps d'expiration pour les enveloppes sécurisées qui sont générées d'une appliance de sécurité du courrier électronique de Cisco (ESA) cette des mises en place qu'enveloppe recommandée de Cisco entretiennent (CRES).

Est-ce que je peux pré-établir le temps d'expiration des enveloppes sécurisées qui sont générées d'une appliance de sécurité du courrier électronique de Cisco qui utilise CRES ?

Symptômes

Une option ne peut pas s'avérer à Cisco ESA afin de pré-établir le temps d'expiration des enveloppes sécurisées.

Solution

Ajoutez une en-tête faite sur commande dans la messagerie sortante avant le cryptage.

Afin de configurer un message de sorte qu'il expire pendant 24 heures après que vous l'envoyez, insérez cette en-tête dans le message :

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

Le destinataire peut ouvrir et visualiser le contenu du message crypté au cours de la période de 24 heures après que vous l'envoyiez. Après cela, l'enveloppe recommandée affiche un message qui indique que l'enveloppe a expiré.