

Puis-je prédéfinir la date d'expiration des enveloppes sécurisées générées à partir d'un dispositif de sécurité de la messagerie Cisco qui utilise CRES ?

Contenu

[Introduction](#)

[Puis-je prédéfinir la date d'expiration des enveloppes sécurisées générées à partir d'un dispositif de sécurité de la messagerie Cisco qui utilise RES ?](#)

[Insertion d'en-têtes de chiffrement dans les messages](#)

[Procédure](#)

[Que faire ensuite](#)

[En-têtes de chiffrement](#)

[Exemples d'en-têtes de chiffrement](#)

[Activation de la mise en cache des clés d'enveloppe pour l'ouverture hors ligne](#)

[Activation des enveloppes sans JavaScript](#)

[Activation de l'expiration du message](#)

[Désactivation de l'applet de déchiffrement](#)

Introduction

Ce document décrit comment prédéfinir le délai d'expiration des enveloppes sécurisées générées à partir d'un dispositif de sécurité de la messagerie Cisco (ESA) qui implémente le service de recommandés Cisco (RES).

Puis-je prédéfinir la date d'expiration des enveloppes sécurisées générées à partir d'un dispositif de sécurité de la messagerie Cisco qui utilise RES ?

Oui, vous pouvez ajouter des en-têtes SMTP aux messages sortants qui seront marqués pour chiffrement. Cela inclut l'en-tête 'X-PostX-ExpirationDate'.

Voici un extrait du [Guide d'utilisation](#) de l'[appliance de sécurité de la messagerie](#).

Insertion d'en-têtes de chiffrement dans les messages

AsyncOS vous permet d'ajouter des paramètres de chiffrement à un message en insérant un en-tête SMTP dans un message à l'aide d'un filtre de contenu ou de message. L'en-tête de chiffrement peut remplacer les paramètres de chiffrement définis dans le profil de chiffrement associé et il peut appliquer des fonctions de chiffrement spécifiées aux messages.

Procédure

Étape Accédez à Politiques de messagerie > Filtres de contenu sortant Filtres de contenu entrant.

1

Étape Dans la section Filtres, cliquez sur Ajouter un filtre.

2

Étape Dans la section Actions, cliquez sur Ajouter action et sélectionnez Ajouter/Modifier un en-tête pour insérer un en-tête de chiffrement dans les messages afin de spécifier un paramètre de chiffrement supplémentaire.

3 Par exemple, si vous voulez qu'une enveloppe inscrite expire dans 24 heures après l'avoir envoyé, tapez X-PostX-ExpirationDate comme nom d'en-tête et +24:00:00 comme valeur d'en-tête.

Que faire ensuite

Rubriques connexes

- Pour plus d'informations sur la création d'un filtre de contenu de chiffrement, consultez [Chiffrement et remise immédiate de messages à l'aide d'un filtre de contenu](#).
- Pour plus d'informations sur l'insertion d'un en-tête à l'aide d'un filtre de messages, consultez [Utilisation de filtres de messages pour appliquer les stratégies de messagerie](#).

En-têtes de chiffrement

Le tableau suivant affiche les en-têtes de chiffrement que vous pouvez ajouter aux messages.

En-tête MIME	Description	Valeur
X-PostX-Reply-Enabled	Indique s'il faut activer une réponse sécurisée pour le message et affiche le bouton Réponse dans la barre de messages. Cet en-tête ajoute un paramètre de chiffrement au message.	Valeur booléenne permettant d'afficher ou le bouton Répondre. Affectez la valeur true pour afficher le bouton. La valeur par défaut est false.
X-PostX-Reply-All-Enabled	Indique s'il faut activer la réponse sécurisée " tous les " du message et affiche le bouton Répondre à tous dans la barre de messages. Cet en-tête remplace le paramètre de profil par défaut.	Valeur booléenne permettant d'afficher ou le bouton Répondre à tous. Affectez la valeur true pour afficher le bouton. La valeur par défaut est false.
X-PostX-Forward-Enabled	Indique si le transfert sécurisé des messages doit être activé et affiche le bouton Transfert dans la barre de messages. Cet en-tête remplace le paramètre de profil par défaut.	Valeur booléenne permettant d'afficher ou le bouton Transfert. Affectez la valeur true pour afficher le bouton. La valeur par défaut est false.
	Indique s'il faut activer les accusés de	Valeur booléenne

X-PostX-Send-Return-Receipt	<p>réception en lecture. L'expéditeur reçoit un accusé de réception lorsque les destinataires ouvrent l'enveloppe sécurisée. Cet en-tête remplace le paramètre de profil par défaut.</p>	<p>permettant d'envoyer ou non un accusé de réception en lecture. Affectez la valeur true pour afficher le bouton. La valeur par défaut est false.</p>
X-PostX-ExpirationDate	<p>Définit la date d'expiration d'un recommandé avant de l'envoyer. Le serveur de clés restreint l'accès à l'enveloppe inscrite après la date d'expiration. L'enveloppe inscrite affiche un message indiquant que le message a expiré. Cet en-tête ajoute un paramètre de chiffrement au message. Si vous utilisez Cisco Registered Envelope Service, vous pouvez vous connecter au site Web à l'adresse http://res.cisco.com et utiliser les fonctions de gestion des messages pour définir, ajuster ou éliminer les dates d'expiration des messages après leur envoi.</p>	<p>Valeur de chaîne contenant la date ou l'heure relative. Utilisez le format +HH:MM:SS pour les heures, minutes et secondes relatives, et le format +D pour les jours relatifs. Par défaut, il n'y a pas de date d'expiration.</p>
X-PostX-ReadNotificationDate	<p>Définit le " date avant de l'envoyer. Le serveur de clés local génère une notification si l'enveloppe inscrite n'a pas été lue avant cette date. Les enveloppes inscrites avec cet en-tête ne fonctionnent pas avec le service Cisco Registered Envelope Service, mais uniquement avec un serveur de clés local. Cet en-tête ajoute un paramètre de chiffrement au message.</p>	<p>Valeur de chaîne contenant la date ou l'heure relative. Utilisez le format +HH:MM:SS pour les heures, minutes et secondes relatives, et le format +D pour les jours relatifs. Par défaut, il n'y a pas de date d'expiration.</p>
X-PostX-Suppress-Applet-For-Open	<p>Indique si l'applet de déchiffrement doit être désactivée. L'applet de déchiffrement entraîne l'ouverture des pièces jointes des messages dans l'environnement du navigateur. La désactivation de l'applet provoque le déchiffrement de la pièce jointe du message sur le serveur de clés. Si vous désactivez cette option, l'ouverture des messages peut prendre plus de temps, mais ils ne dépendent pas de l'environnement du navigateur. Cet en-tête remplace le paramètre de profil par défaut.</p>	<p>Valeur booléenne permettant de désactiver ou non l'applet de déchiffrement. Affectez la valeur true pour désactiver l'applet. La valeur par défaut est false.</p>
X-PostX-Use-Script	<p>Indique si les enveloppes JavaScript doivent être envoyées. Une enveloppe sans JavaScript est une enveloppe inscrite qui n'inclut pas le JavaScript utilisé pour ouvrir localement des enveloppes sur l'ordinateur du destinataire. Le destinataire doit utiliser la méthode Open Online ou la méthode Open by Forwarding pour afficher le message. Utilisez cet en-tête si</p>	<p>Valeur booléenne indiquant si l'applet JavaScript doit être incluse ou non. Affectez la valeur false pour envoyer une enveloppe sans JavaScript. La valeur par défaut est true.</p>

la passerelle d'un domaine destinataire supprime JavaScript et rend le message chiffré inutilisable. Cet en-tête ajoute un paramètre de chiffrement au message. Indique s'il faut autoriser la mise en cache des clés spécifiques aux enveloppes pour l'ouverture hors connexion des enveloppes. Avec la mise en cache de la clé d'enveloppe, la clé de déchiffrement d'une enveloppe particulière est mise en cache sur l'ordinateur du destinataire lorsque celui-ci entre la phrase de passe correcte et sélectionne la case " Mémoriser le mot de passe de cette enveloppe ". Après cela, le destinataire n'a plus besoin de saisir une phrase de passe pour rouvrir l'enveloppe sur l'ordinateur. Cet en-tête ajoute un paramètre de chiffrement au message.

Valeur booléenne permettant d'activer ou la mise en cache des clés d'enveloppe et d'afficher la case à cocher " Mémoriser le mot de passe de cette enveloppe ". La valeur par défaut est false.

X-PostX-Remember-Envelope-Key-Checkbox

Exemples d'en-têtes de chiffrement

Cette section fournit des exemples d'en-têtes de chiffrement.

Activation de la mise en cache des clés d'enveloppe pour l'ouverture hors ligne

Pour envoyer une enveloppe inscrite avec la mise en cache des clés d'enveloppe activée, insérez l'en-tête suivant dans le message :

Case à cocher X-PostX-Remember-Envelope-Key : vrai

La case " Mémoriser le mot de passe de cette " d'enveloppe s'affiche sur l'enveloppe inscrite.

Activation des enveloppes sans JavaScript

Pour envoyer un recommandé sans JavaScript, insérez l'en-tête suivant dans le message :

Script d'utilisation X-PostX : faux

Lorsque le destinataire ouvre la pièce jointe securedoc.html, l'enveloppe inscrite s'affiche avec un lien Ouvrir en ligne et le bouton Ouvrir est désactivé.

Activation de l'expiration du message

Pour configurer un message de sorte qu'il expire 24 heures après son envoi, insérez l'en-tête

suivant dans le message :

Date d'expiration X-PostX : +24:00:00

Le destinataire peut ouvrir et afficher le contenu du message chiffré pendant la période de 24 heures qui suit son envoi. Ensuite, l'enveloppe inscrite affiche un message indiquant que l'enveloppe a expiré.

Désactivation de l'applet de déchiffrement

Pour désactiver l'applet de déchiffrement et faire déchiffrer la pièce jointe du message sur le serveur de clés, insérez l'en-tête suivant dans le message :

X-PostX-Suppress-Applet-For-Open : vrai

Note: L'ouverture du message peut prendre plus de temps lorsque vous désactivez l'applet de déchiffrement, mais il ne dépend pas de l'environnement du navigateur.