Configurer les niveaux de sécurité dans le profil de cryptage ESA CRES

Contenu

Introduction

Ce document décrit la configuration des profils CRES (Cisco Registered Envelope Service Encryption) au sein de l'appliance de sécurité de la messagerie (ESA), en fonction des différents niveaux de sécurité autorisés.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration de base ESA
- Chiffrement basé sur la configuration du filtre de contenu
- Service de recommandés Cisco

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

La création du profil CRES est une tâche essentielle pour l'activation et l'utilisation du service de cryptage via l'ESA. Avant de créer plusieurs profils, assurez-vous que vous disposez d'un compte complet provisionné pour un ESA avec la création d'un compte CRES.

Il peut y avoir plusieurs profils et chaque profil peut être configuré avec un niveau de sécurité différent. Cela permet au réseau de maintenir différents niveaux de sécurité par domaine, utilisateur ou groupe.

Configuration

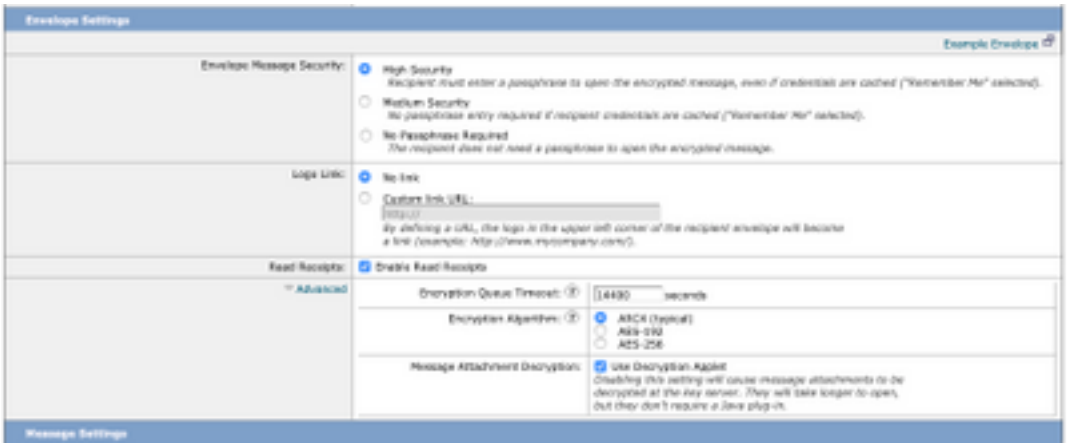
Vous pouvez activer et configurer un profil de chiffrement à l'aide de la commande CLI **encryptionconfig**, ou via **Services de sécurité > Chiffrement de messagerie Cisco IronPort** dans l'interface utilisateur graphique.

Configuration à partir de l'interface utilisateur graphique

Àpartir de ESA, accédez à **Services de sécurité > Chiffrement des e-mails Cisco IronPort > Ajouter un profil de chiffrement**.

Un écran contenant les paramètres du profil de chiffrement s'affiche. Le nom du profil et le reste de la configuration peuvent être personnalisés et dépendent des étiquettes d'identification ou des méthodes de l'organisation.

La configuration qui définit le niveau de sécurité par profil est Envelope Settings, comme l'illustre l'image :



> **Note**: Il est suggéré que le nom du profil contienne : « High », « Low », etc, afin de correspondre au niveau de sécurité configuré ou au nom du groupe auquel le profil est associé pour une identification rapide dans la création de filtres de contenu et de vérification.

Les trois niveaux de sécurité autorisés par l'ESA sont les suivants :

- Haute sécurité : Le destinataire doit toujours saisir une phrase de passe pour ouvrir les messages chiffrés.
- Sécurité moyenne : Le destinataire n'a pas besoin d'entrer des informations d'identification

pour ouvrir le message chiffré si les informations d'identification du destinataire sont mises en cache.
- Aucune phrase de passe requise : Il s'agit du niveau le plus bas de sécurité des messages chiffrés. Le destinataire n'a pas besoin d'entrer une phrase de passe pour ouvrir le message chiffré. Vous pouvez toujours activer les accusés de réception en lecture, la réponse sécurisée tout et les fonctions de transfert sécurisé des messages pour les enveloppes qui ne sont pas protégées par la phrase de passe.

Vous pouvez configurer différents niveaux de sécurité sur ces objets :

Enveloppe la sécurité des messages **:**

- Sécurité élevée ·
- Sécurité moyenne
- Aucune phrase de passe requise

Lien du logo : Afin de permettre aux utilisateurs d'ouvrir l'URL de votre organisation, cliquez sur son logo, vous pouvez ajouter un lien au logo. Choisissez parmi les options suivantes :

- Aucune liaison. Aucun lien en direct n'est ajouté à l'enveloppe du message.
- URL du lien personnalisé. Entrez l'URL pour ajouter un lien en direct à l'enveloppe du message.

Lire les reçus : Si vous activez cette option, l'expéditeur reçoit un accusé de réception lorsque les destinataires ouvrent l'enveloppe sécurisée. Il s'agit d'une sélection facultative.

Avancé :

Délai d'attente de chiffrement : Saisissez la durée (en secondes) pendant laquelle un message peut se trouver dans la file d'attente de chiffrement avant d'expirer. Une fois qu'un message expire, la solution matérielle-logicielle renvoie le message et envoie une notification à l'expéditeur.

Algorithme de chiffrement *:*

- ARC4. ARC4 est le choix le plus courant, il fournit un chiffrement fort avec un délai de déchiffrement minimal pour les destinataires des messages.
- AES. AES fournit un chiffrement plus fort mais prend également plus de temps à déchiffrer, il introduit des délais pour les destinataires. AES est généralement utilisé dans les applications gouvernementales et bancaires.

Décryptage des pièces jointes des messages *:* Activez ou désactivez l'applet de déchiffrement. Après avoir activé cette option, la pièce jointe du message s'ouvre dans l'environnement du navigateur. Une fois cette option désactivée, les pièces jointes des messages sont déchiffrées sur le serveur de clés. Par défaut, l'applet Java est désactivé dans l'enveloppe.

> **Note**: Les navigateurs les plus utilisés ont désactivé Java Applet pour des raisons de sécurité.

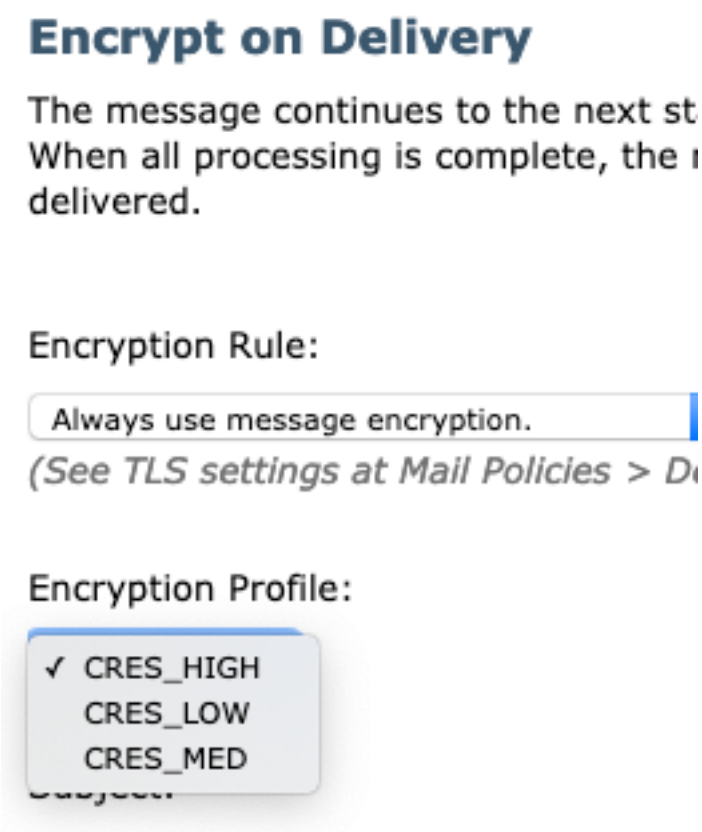
Une fois les profils de chiffrement créés. Assurez-vous qu'il est provisionné, comme l'illustre l'image :

Chacun de ces profils doit être associé via un filtre de contenu pour être appliqué.

> **Attention** : Si le profil n'est pas appelé par un filtre de contenu, les paramètres de chiffrement ne peuvent pas être appliqués.

Àpartir du SEEE, accédez à **Politiques de messagerie > Filtres de contenu sortant > Ajouter un filtre**

Une fois que la condition des utilisateurs, de l'objet, du groupe, de l'expéditeur, etc. a été configurée à l'intérieur du filtre, définissez le niveau de cryptage du filtre sortant, comme illustré dans l'image :



> **Attention** : Tous les filtres de contenu doivent être associés aux stratégies de messagerie sortante pour fonctionner correctement.

> **Note**: Vous pouvez configurer plusieurs profils de chiffrement pour un service de clé hébergé. Si votre entreprise possède plusieurs marques, cela vous permet de référencer différents logos stockés sur le serveur de clés pour les enveloppes PXE.

Configuration à partir de CLI

Àpartir de l'interface de ligne de commande ESA, tapez la commande **encryptionconfig** :

```
ESA.com> encryptionconfig

IronPort Email Encryption: Enabled
```

```
Choose the operation you want to perform:
- SETUP - Enable/Disable IronPort Email Encryption
- PROFILES - Configure email encryption profiles
- PROVISION - Provision with the Cisco Registered Envelope Service

[]> profiles

Proxy: Not Configured

Profile Name         Key Service            Proxied     Provision Status
------------         -----------            -------     ----------------
HIGH-CRES              Hosted Service         No          Not Provisioned
Choose the operation you want to perform:
- NEW - Create a new encryption profile
- EDIT - Edit an existing encryption profile
- DELETE - Delete an encryption profile
- PRINT - Print all configuration profiles
- CLEAR - Clear all configuration profiles
- PROXY - Configure a key server proxy
[]> new

1. Cisco Registered Envelope Service
2. IronPort Encryption Appliance (in network)
Choose a key service:
[1]>

Enter a name for this encryption profile:
[]> HIGH

Current Cisco Registered Key Service URL: https://res.cisco.com
Do you wish to alter the Cisco Registered Envelope Service URL? [N]> N

1. ARC4
2. AES-192
3. AES-256
Please enter the encryption algorithm to use when encrypting envelopes:
[1]>

1. Use envelope service URL with HTTP (Recommended). Improves performance for opening envelopes.
2. Use the envelope service URL with HTTPS.
3. Specify a separate URL for payload transport.
Configure the Payload Transport URL
[1]>

1. High Security (Recipient must enter a passphrase to open the encrypted message, even if
credentials are cached ("Remember Me" selected).)
2. Medium Security (No passphrase entry required if recipient credentials are cached ("Remember
Me" selected).)
3. No Passphrase Required (The recipient does not need a passphrase to open the encrypted
message.)
Please enter the envelope security level:
[1]>

Would you like to enable read receipts? [Y]>

Would you like to enable "Secure Reply All"? [N]> y

Would you like to enable "Secure Forward"? [N]> y

Enter a URL to serve as a link for the envelope logo image (may be blank):
[]>

Would you like envelopes to be displayed in a language other than English ? [N]>
```

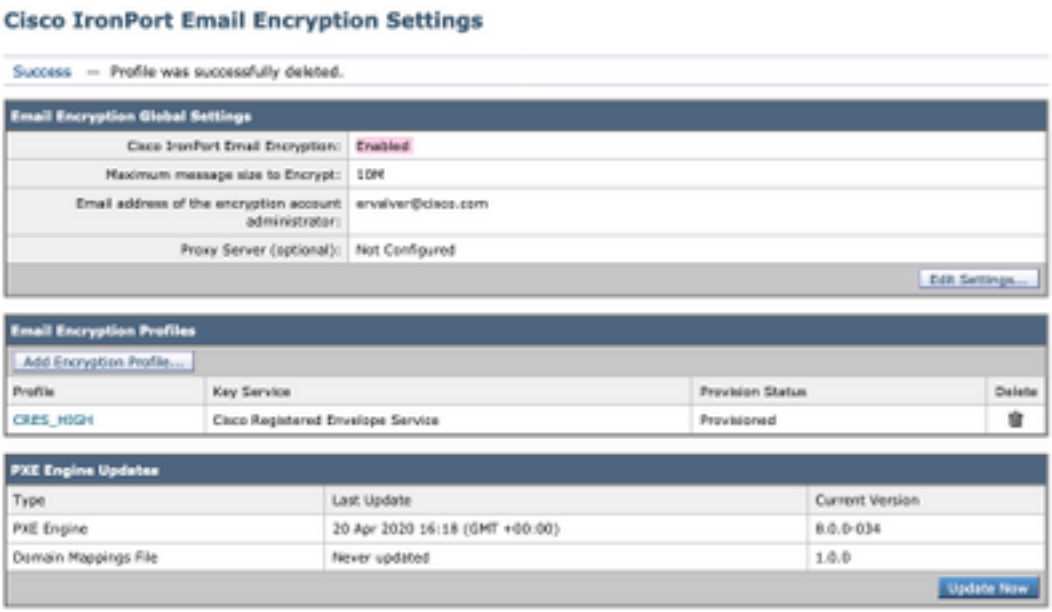
```
Enter the maximum number of seconds for which a message could remain queued waiting to be
encrypted. Delays could be caused by key server outages or resource limitations:
[14400]>

Enter the subject to use for failure notifications:
[[ENCRYPTION FAILURE]]>

Please enter file name of the envelope attached to the encryption notification:
[securedoc_${date}T${time}.html]>


A Cisco Registered Envelope Service profile "HIGH" was added.

   1. Commit this configuration change before continuing.
   2. Return to the encryptionconfig menu and select PROVISION to complete
the configuration.

Proxy: Not Configured

Profile Name         Key Service            Proxied     Provision Status
------------         -----------            -------     ----------------
HIGH-CRES            Hosted Service         No          Not Provisioned
LOW-CRES             Hosted Service         No          Not Provisioned

Choose the operation you want to perform:
- SETUP - Enable/Disable IronPort Email Encryption
- PROFILES - Configure email encryption profiles
- PROVISION - Provision with the Cisco Registered Envelope Service

[]> provision
```

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Vérification à partir de l'interface utilisateur graphique

Àpartir de ESA, accédez à **Services de sécurité > Chiffrement de messagerie Cisco IronPort**, comme indiqué sur l'image :



Note: Assurez-vous que le chiffrement est activé et que le profil configuré est provisionné. Comme le montre l'image.

Vérification à partir de CLI

Àpartir de l'interface de ligne de commande, tapez **encryptconfig** et tapez profile.

```
ESA.com> encryptionconfig

IronPort Email Encryption: Enabled

Choose the operation you want to perform:
- SETUP - Enable/Disable IronPort Email Encryption
- PROFILES - Configure email encryption profiles
- PROVISION - Provision with the Cisco Registered Envelope Service
[]> profiles

Proxy: Not Configured

Profile Name         Key Service            Proxied     Provision Status
------------         -----------            -------     ----------------
CRES_HIGH             Hosted Service         No          Provisioned
```

Note: Assurez-vous que le chiffrement est activé et que le profil configuré est provisionné. Comme le montre l'image.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Àpartir de ESA, accédez à **Administration système > touches de fonction**

Vérifiez que la clé de fonction est appliquée et active. La clé : Le chiffrement des e-mails IronPort doit être actif.

Àpartir de ESA, accédez à **Services de sécurité > Chiffrement des e-mails Cisco IronPort**

Vérifiez que le service de chiffrement est correctement activé.

Vérifiez que le profil de cryptage n'est pas dans un état Non provisionné, comme l'illustre l'image :

Profile	Key Service	Provision Status
HIGH	Cisco Registered Envelope Service	**Not Provisioned**
LOW	Cisco Registered Envelope Service	**Not Provisioned**
MEDIUM	Cisco Registered Envelope Service	**Not Provisioned**

Vérifiez la dernière mise à jour du moteur, comme l'illustre l'image :

PXE Engine Updates		
Type	Last Update	Current Version
PXE Engine	21 Jan 2020 16:01 (GMT +00:00)	7.2.1-015

Àpartir des détails du suivi des messages, vérifiez si une erreur s'affiche.

Erreurs les plus courantes :

`5.x.3 - Temporary PXE Encryption failure`
Solution : Le service est actuellement indisponible ou inaccessible. Vérifiez les problèmes de connectivité et de réseau.

`5.x.3 - PXE Encryption failure. (Message could not be encrypted due to a system configuration issue. Please contact your administrator`
Solution : Cette erreur est associée à :

- Problèmes de licence. Veuillez vérifier les clés de fonction
- Le profil utilisé n'est pas provisionné. Identifier à partir du suivi des messages le profil configuré sur le filtre de contenu et la mise en service
- Aucun profil n'est associé à un filtre de contenu. Parfois, les profils de chiffrement sont supprimés, modifiés avec des noms différents, etc. Le filtre de contenu configuré ne peut pas trouver le profil associé

`5.x.3 - PXE Encryption failure. (Error 30 - The message has an invalid "From" address.)`

`5.x.3 - PXE Encryption failure. (Error 102 - The message has an invalid "To" address.)`
Solution : Régulièrement, ce problème est causé par le remplissage automatique de l'adresse e-mail du client de messagerie de l'expéditeur interne (par exemple Outlook) du destinataire qui contient une “ non valide de l'adresse De ”/« À ».

En règle générale, cela est dû à des guillemets autour de l'adresse e-mail ou à d'autres caractères illégaux dans l'adresse e-mail.

Informations connexes

- Guide d'administration de CRES

- Guide de l'utilisateur final
- Support et documentation techniques - Cisco Systems