Guide des meilleures pratiques pour la prévention de la perte de données et le chiffrement

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Guide des meilleures pratiques pour la prévention de la perte de données et le chiffrement

- 1. Activez le cryptage des e-mails Cisco IronPort sur les ESA
- 2. Enregistrez votre ou vos ESA et votre organisation auprès de RES
- 3. Créer des profils de chiffrement sur les ESA
- 4. Activation de la prévention contre la perte de données (DLP)
- 5. Création d'actions de message Data Loss Prevention
- 6. Création de politiques de prévention des pertes de données
- 7. Application des stratégies DLP à une stratégie de courrier électronique sortant

Conclusion

Informations connexes

Introduction

Ce document décrit les meilleures pratiques de prévention de perte de données (DLP) et de cryptage pour la sécurité de la messagerie Cisco.

Ce document traite de la configuration du cryptage des messages à l'aide de l'appliance de sécurisation de la messagerie Cisco (ESA) et du service de messagerie électronique enregistré Cisco (RES) basé sur le cloud. Les clients peuvent utiliser le cryptage des messages pour envoyer des messages individuels de manière sécurisée sur l'Internet public, à l'aide de différents types de stratégies, notamment le filtrage de contenu et la prévention des pertes de données. La création de ces politiques sera abordée dans d'autres documents de cette série. Ce document vise à préparer l'ESA à envoyer des messages chiffrés afin que les politiques puissent utiliser le chiffrement comme une action.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

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

Ce document traite des étapes suivantes :

1. Activation du chiffrement des e-mails Cisco IronPort
2. Enregistrez vos ESA et votre entreprise auprès de RES
3. Création de profils de chiffrement
4. Activation de DLP
5. Création d'actions de message DLP
6. Création de stratégies DLP
7. Application de stratégies DLP à une stratégie de messagerie sortante

Une fois ces étapes effectuées avec succès, l'administrateur ESA peut créer une stratégie qui utilisera le cryptage comme action.

Le chiffrement des e-mails Cisco IronPort est également appelé chiffrement RES. RES est le nom que nous utilisons pour les « serveurs clés » dans le cloud Cisco. La solution de chiffrement RES utilise le chiffrement à clé symétrique, ce qui signifie que la clé utilisée pour chiffrer le message est la même que celle utilisée pour déchiffrer le message. Chaque message chiffré utilise une clé unique, qui permet à l'expéditeur d'avoir un contrôle granulaire sur un message après son envoi - par exemple, pour le verrouiller ou l'expirer afin que le destinataire ne puisse plus l'ouvrir - sans affecter les autres messages. Lors du chiffrement d'un message, l'ESA stocke la clé de chiffrement et les métadonnées dans CRES relatives à chaque message chiffré.

L'ESA peut décider de chiffrer un message de plusieurs manières : via un « indicateur » (comme le contenu de l'objet), via la mise en correspondance du filtre de contenu ou via la stratégie DLP, par exemple. Une fois que l'ESA décide de chiffrer un message, elle le fait avec un « profil de chiffrement » spécifié créé dans « Services de sécurité > Chiffrement des e-mails Cisco IronPort » — le tableau intitulé « Profils de chiffrement des e-mails ». Par défaut, il n'existe aucun profil de chiffrement. Cette question sera traitée dans la section 3. Création de profils de chiffrement.

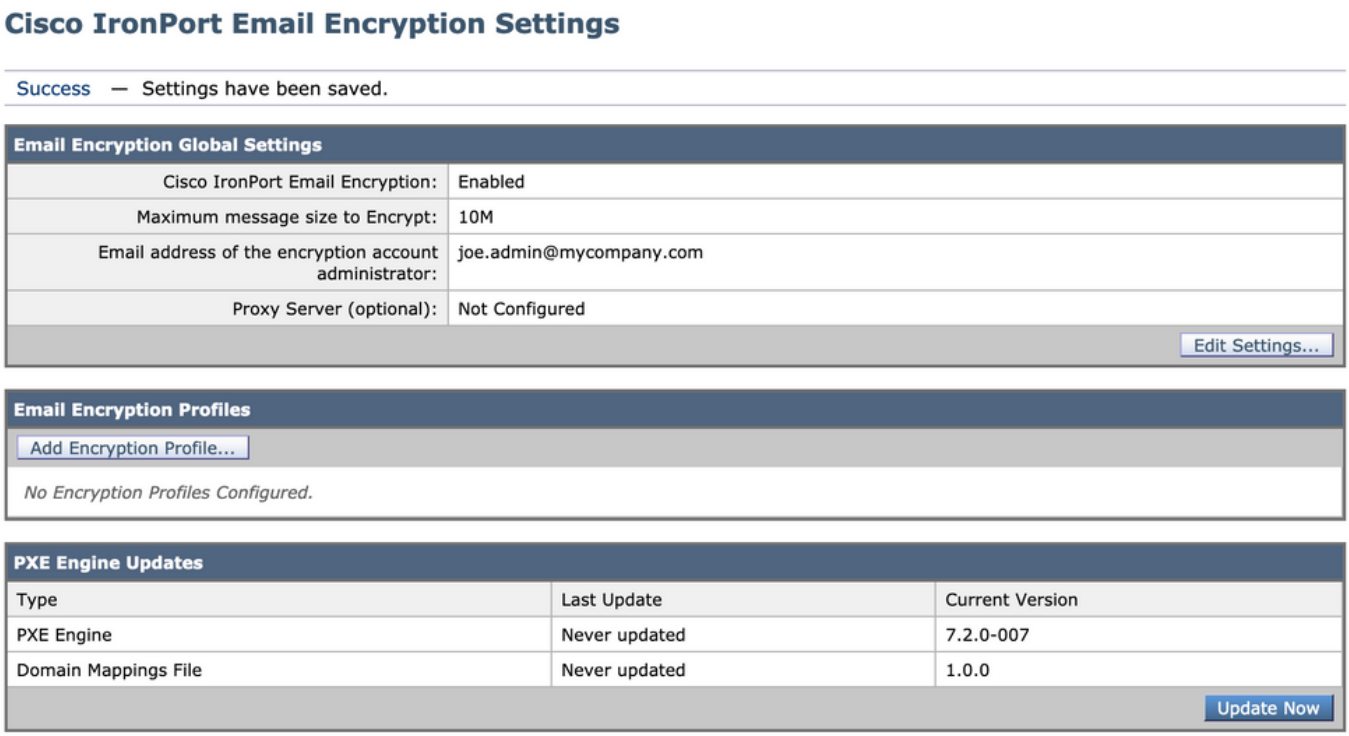
Guide des meilleures pratiques pour la prévention de la perte de données et le chiffrement

1. Activez le cryptage des e-mails Cisco IronPort sur les ESA

Remarque : Si vous avez plusieurs ESA dans un cluster, l'étape #1 ne doit être exécutée qu'une seule fois, car ces paramètres sont généralement gérés au niveau du cluster. Si plusieurs ordinateurs ne sont pas en cluster ou si vous gérez ces paramètres au niveau de l'ordinateur, l'étape #1 doit être exécutée sur chaque ESA.

1. Dans l'interface utilisateur ESA, accédez à Services de sécurité > Chiffrement des e-mails Cisco IronPort.
2. Cochez cette case pour activer le chiffrement des e-mails Cisco IronPort.
3. Acceptez le Contrat de licence de l'utilisateur final (CLUF), le Contrat de licence de cryptage du courrier électronique Cisco IronPort.
4. Dans les paramètres généraux de chiffrement du courrier électronique, cliquez sur Modifier les paramètres...
    - Spécifiez l'adresse e-mail de l'administrateur/de la personne qui est l'administrateur RES principal pour le compte. Ce compte de messagerie sera associé à l'administration de l'environnement RES pour l'entreprise.
    - Facultatif: La taille maximale par défaut des messages à chiffrer est de 10 Mo. Vous pouvez augmenter/diminuer la taille à ce moment-là si vous le souhaitez.
    - Facultatif: Si vous disposez d'un proxy que l'ESA devra passer pour se connecter à RES via HTTPS, ajoutez les paramètres de proxy et d'authentification nécessaires pour lui permettre de passer par le proxy.
5. Envoyez et validez vos modifications de configuration.

À ce stade, vous devriez voir les « Paramètres globaux de chiffrement des e-mails » définis comme suit, mais sans aucun profil répertorié pour le moment :



2. Enregistrez votre ou vos ESA et votre organisation auprès de RES

L'étape #2 s'effectue principalement en dehors de la console d'administration ESA.

Remarque : Les informations d'enregistrement ESA sont également disponibles dans la TechNote suivante : Cisco RES : Exemple de configuration du provisionnement de compte pour les ESA virtuels, hébergés et matériels

---

Veuillez envoyer un e-mail directement à RES : stg-cres-provisioning@cisco.com.

Afin d'approvisionner un compte CRES pour votre profil de cryptage ESA, veuillez nous fournir les informations suivantes :

1. Nom du compte (Veuillez spécifier le nom exact de la société, car vous souhaitez qu'il soit répertorié.)
    1. Pour les comptes clients de sécurité de messagerie électronique cloud (CES)/hébergés, veuillez noter le nom de votre compte pour le terminer par « <Nom du compte> HOSTED »
2. Adresse(s) e-mail à utiliser pour l'administrateur du compte (veuillez spécifier l'adresse e-mail d'administrateur correspondante)
3. Numéro(s) de série complet(s) du matériel
    1. Un numéro de série de l'appliance peut être localisé à partir de l'interface graphique utilisateur ESA (Administration système > Touches de fonction) ou de l'interface de ligne de commande ESA via la commande « version ». Il n'est pas acceptable de fournir une licence de numéro de licence virtuel (VLAN) ou de clé d'activation de produit (PAK), car un numéro de série d'appliance complet est requis pour l'administration du compte CRES.
4. Noms de domaine qui doivent être mappés au compte CRES à des fins d'administration

Remarque : Si vous disposez déjà d'un compte CRES, veuillez indiquer le nom de la société ou le numéro de compte CRES existant. Cela garantit que les nouveaux numéros de série des appliances sont ajoutés au compte approprié et évite la duplication des informations de l'entreprise et le provisionnement.

Soyez assuré que si vous envoyez un e-mail concernant la mise en service d'un compte CRES, nous vous répondrons dans un (1) jour ouvrable. Si vous avez besoin d'une assistance immédiate, envoyez une demande d'assistance au TAC Cisco. Pour ce faire, utilisez le gestionnaire de dossiers d'assistance (https://mycase.cloudapps.cisco.com/case) ou appelez par téléphone (https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html).

Remarque : Après avoir envoyé cette demande par e-mail, la création de votre compte RES de société (s'il n'a pas déjà été créé) et l'ajout des S/N peuvent prendre un jour. La tâche « Provisionner », à l'étape #3, ne fonctionnera pas tant que cette opération n'est pas terminée.

---

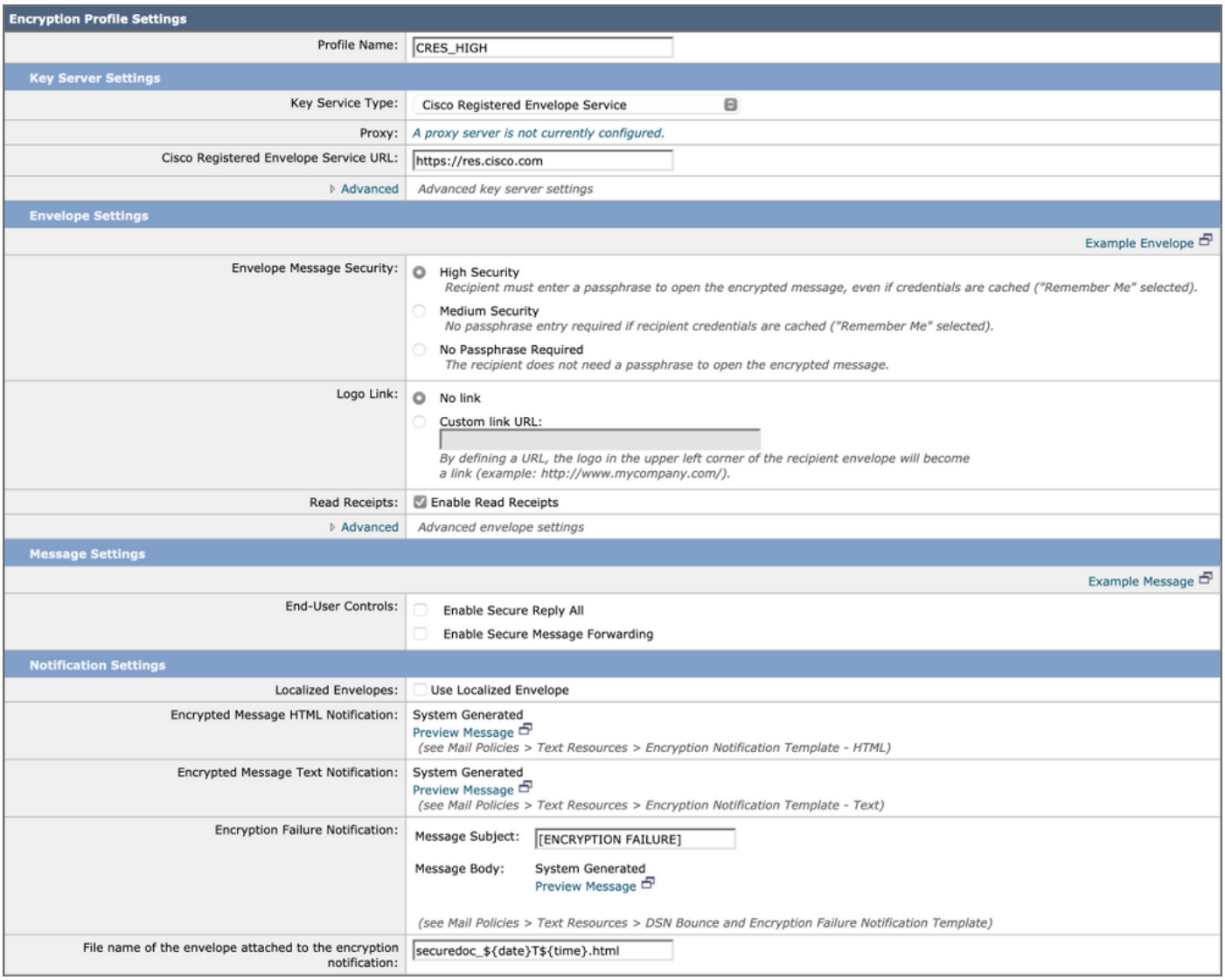
3. Créer des profils de chiffrement sur les ESA

Remarque : Si vous avez plusieurs ESA dans un cluster, l'étape #1 ne doit être exécutée qu'une seule fois, car ces paramètres sont généralement gérés au niveau du cluster. Si plusieurs ordinateurs ne sont pas en cluster ou si vous gérez ces paramètres au niveau de l'ordinateur, l'étape #1 doit être exécutée sur chaque ESA.

Un profil de chiffrement indique comment les messages chiffrés doivent être envoyés. Par exemple, une entreprise peut avoir besoin d'envoyer des enveloppes de haute sécurité pour un segment de ses destinataires, par exemple ceux auxquels elle sait qu'ils enverront fréquemment des données hautement sensibles. La même organisation peut avoir d'autres segments de sa communauté de destinataires qui reçoivent des informations moins sensibles, et qui sont peut-être aussi moins patients avec l'obligation de fournir l'ID utilisateur et le mot de passe pour recevoir le courrier chiffré. Ces destinataires seraient de bons candidats pour une enveloppe de type Faible sécurité. Le fait de disposer de plusieurs profils de chiffrement permet à l'entreprise d'adapter le format de message chiffré au public visé. D'un autre côté, de nombreuses entreprises peuvent se contenter d'un seul profil de chiffrement.

Pour ce document, nous montrerons un exemple de création de trois profils de chiffrement nommés « CRES_HIGH », « CRES_MED » et « CRES_LOW ».

1. Dans l'interface utilisateur ESA, accédez à Services de sécurité > Chiffrement des e-mails Cisco IronPort.
2. Cliquez sur « Ajouter un profil de cryptage...»
3. Le menu Encryption Profile (Profil de cryptage) s'ouvre et vous pouvez nommer votre premier profil de cryptage « CRES_HIGH » (CRES_HIGH).
4. Sélectionnez « Haute sécurité » pour la sécurité des messages de l'enveloppe, si ce n'est déjà fait.
5. Cliquez sur Submit pour enregistrer ce profil.



Répétez ensuite les étapes 2 à 5 pour créer « CRES_MED » et « CRES_LOW » : il vous suffit de modifier la case d'option pour la sécurité des messages d'enveloppe de chaque profil.

- Pour le profil CRES_HIGH, sélectionnez la case d'option « Haute sécurité ».
- Pour le profil CRES_MED, sélectionnez la case d'option « Sécurité moyenne ».
- Pour le profil CRES_LOW, sélectionnez la case d'option Aucun mot de passe requis

Vous remarquerez qu'il existe des options pour Activer les accusés de réception en lecture, Activer la réponse sécurisée à tous et Activer le transfert sécurisé des messages. Dans Envelope Settings, si vous cliquez sur le lien Advanced, vous pouvez sélectionner l'un des trois algorithmes de chiffrement symétrique et spécifier que l'enveloppe est envoyée sans l'applet de chiffrement Java.

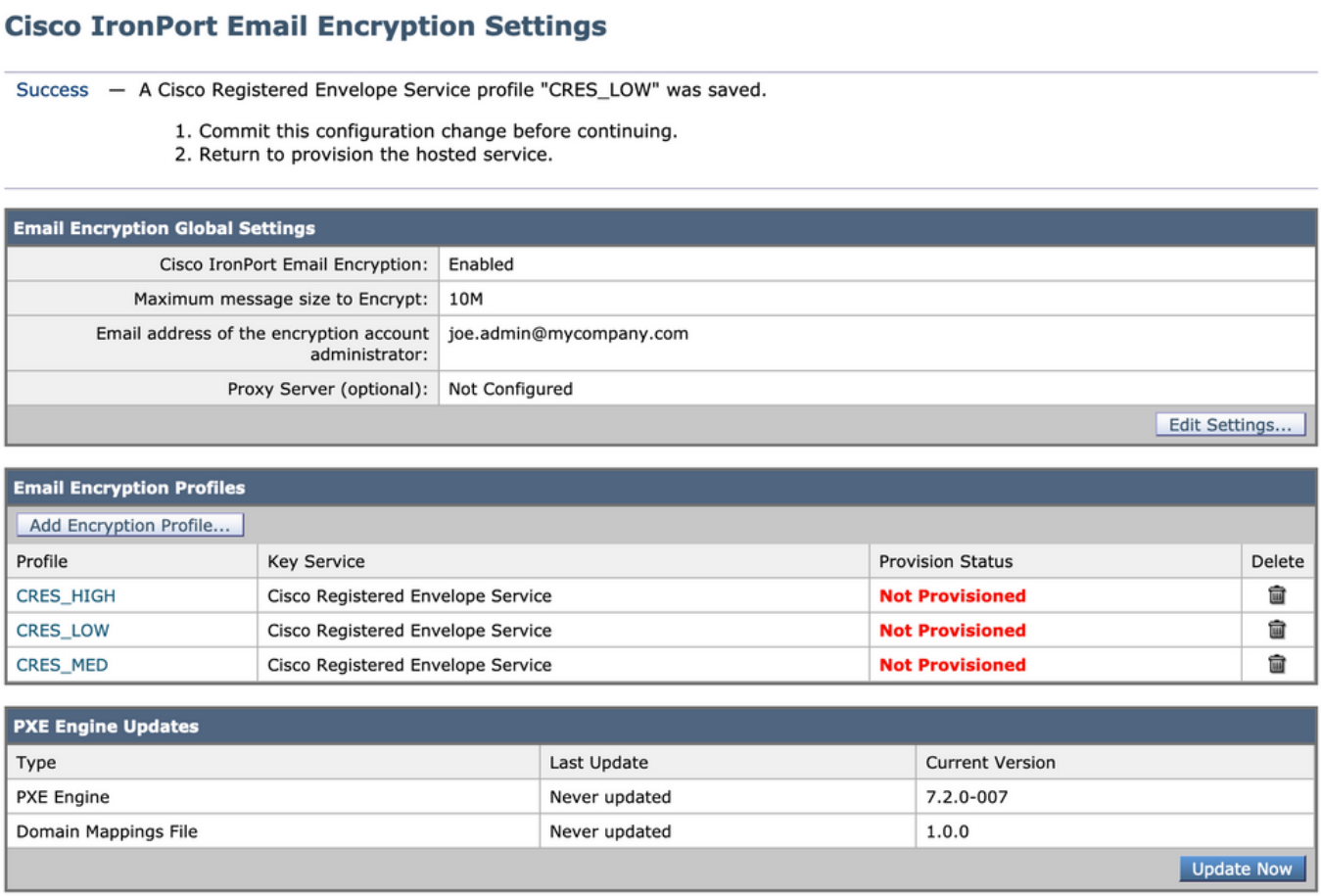
Le lien hypertexte « Exemple de message » s'affiche à droite des paramètres d'enveloppe. Si vous cliquez sur cette option, vous obtiendrez un exemple de l'enveloppe de message sécurisé, que le destinataire verra dans son e-mail après avoir ouvert la pièce jointe HTML.

Lire les accusés de réception signifie que l'expéditeur du message chiffré recevra un e-mail de CRES lorsque le destinataire ouvrira le message sécurisé (ce qui signifie que le destinataire a appuyé sur la clé symétrique et a déchiffré le message).

Le lien hypertexte « Exemple de message » s'affiche à droite des paramètres de message. Si vous cliquez sur cette option, vous verrez à quoi ressemblera le message ouvert, c'est-à-dire ce que le destinataire verra une fois qu'il aura fourni les informations nécessaires dans l'enveloppe et qu'il aura ouvert le message chiffré.

N'oubliez pas de cliquer sur Submit et de valider les modifications.

La ligne du tableau affiche alors un bouton « Provisionner ». Le bouton Provisionner n'apparaît qu'après les modifications de validation.



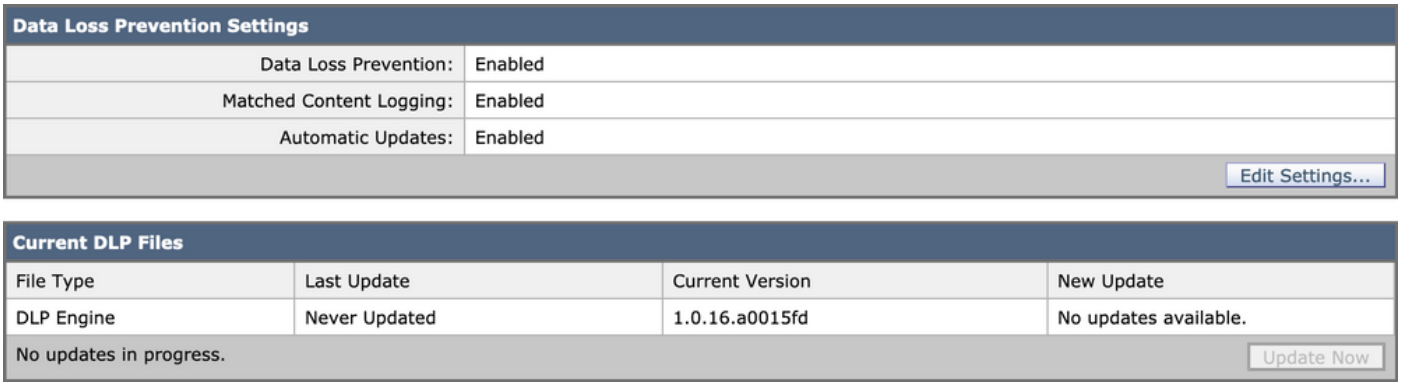
Cliquez à nouveau sur le bouton Provisionner. Cela ne fonctionnera qu'après la création du compte RES de votre entreprise et l'ajout des S/N de l'appliance à votre compte. Si le compte RES est lié au SEC, le processus de provisionnement sera relativement rapide. Si ce n'est pas le cas, ce processus devra d'abord s'achever.

Une fois la mise en service terminée, votre page Cisco IronPort Email Encryption (Cryptage des e-mails Cisco IronPort) affiche le profil comme étant mis en service.

4. Activation de la prévention contre la perte de données (DLP)

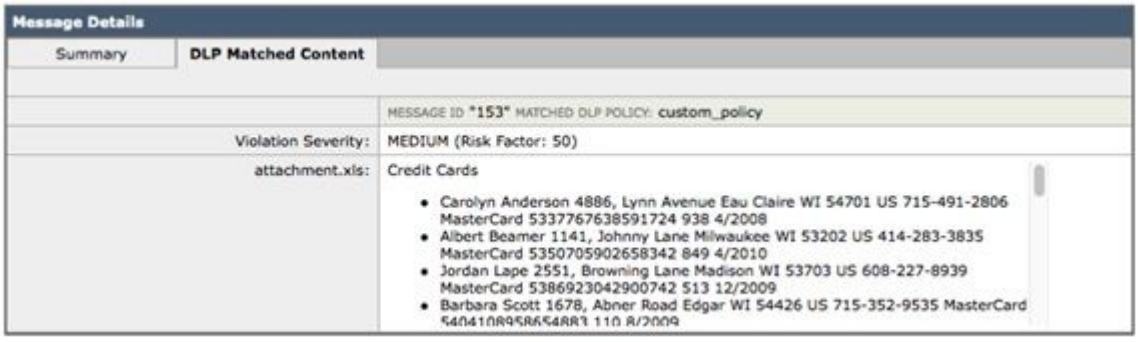
1. Dans l'interface utilisateur ESA, accédez à Services de sécurité > Prévention de perte de données.
2. Cliquez sur Enable... pour activer DLP.

3. Acceptez le CLUF, Contrat de licence de prévention de perte de données.
4. Cochez la case Activer la consignation du contenu correspondant.
5. Cochez la case Activer les mises à jour automatiques.
6. Cliquez sur Submit.



Les mises à jour du moteur DLP et des classificateurs de correspondance de contenu prédéfinis sur votre appliance sont indépendantes des mises à jour des autres services de sécurité. Les mises à jour régulières de 3 à 5 minutes des signatures Talos sont différentes et n'incluent pas la mise à jour des politiques DLP et des dictionnaires. Les mises à jour doivent être activées ici.

Lorsque l'option Journalisation du contenu correspondant est activée, elle permet au suivi des messages d'afficher le contenu de l'e-mail à l'origine de la violation. Voici un exemple de suivi des messages montrant le contenu des e-mails à l'origine de la violation DLP. De cette manière, un administrateur peut savoir exactement quelles données ont déclenché une stratégie DLP spécifique.



Violation de prévention de perte de données

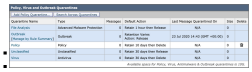
5. Création d'actions de message Data Loss Prevention

Créer des quarantaines DLP

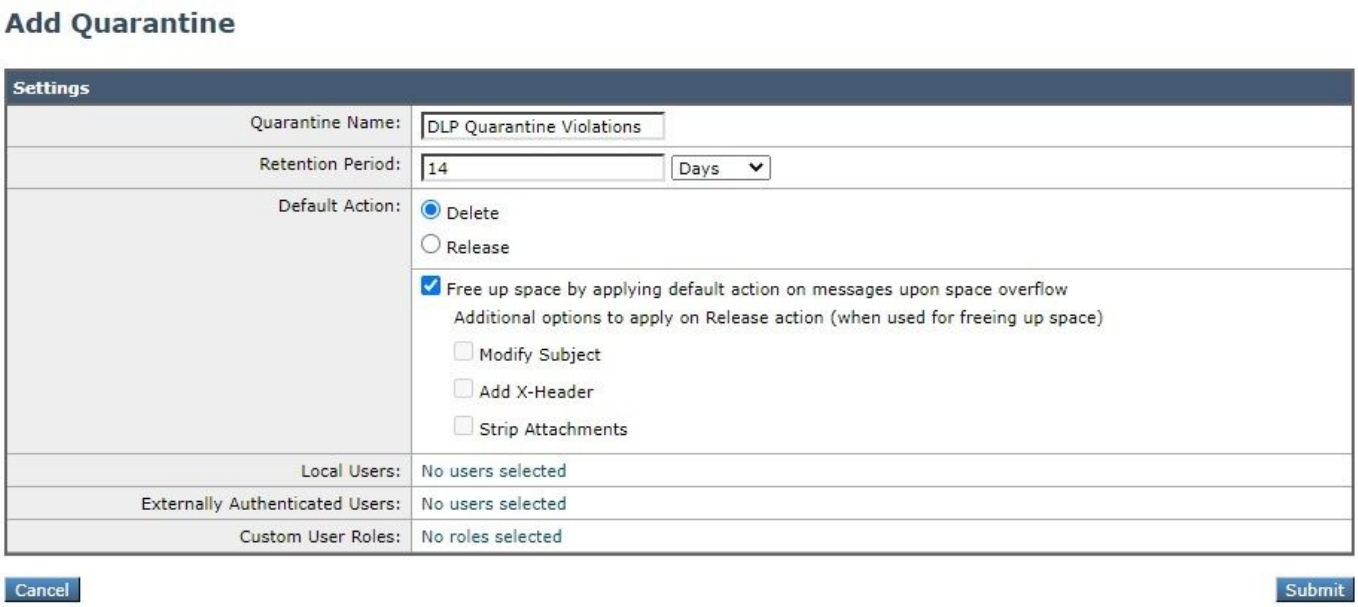
Si vous souhaitez conserver une copie des messages enfreignant les stratégies DLP, vous pouvez créer des quarantaines de stratégie individuelles pour chaque type de violation de stratégie. Ceci est particulièrement utile lors de l'exécution d'un PDV « transparent », où les messages sortants violant les stratégies DLP sont consignés et remis, mais aucune action n'est entreprise sur les messages.

1. Sur le SMA, accédez à Email > Message Quarantine > Policy, Virus, and Outbreak

Quarantines

2. Voici à quoi devrait ressembler la table Quarantaines avant de commencer : 
Stratégie Quarantaine des virus et des attaques
3. Cliquez sur le bouton « Ajouter une quarantaine de stratégie » et créez une quarantaine à utiliser par les stratégies DLP.

Vous trouverez ci-dessous un exemple de mise en quarantaine effectuée pour une violation DLP moyenne. La segmentation des quarantaines est possible et peut être souhaitée pour plusieurs règles DLP :



Exemple de quarantaine DLP

À propos des actions de message DLP

Les actions de message DLP décrivent les actions que l'ESA entreprendra lorsqu'il détectera une violation DLP dans un e-mail sortant. Vous pouvez spécifier des actions DLP principales et secondaires et différentes actions peuvent être affectées à différents types et niveaux de gravité de violation.

Les principales actions sont les suivantes :

- Livrer
- Goutte
- Quarantaine

Dans le cas d'un état en lecture seule où les violations DLP sont consignées et signalées mais où les messages ne sont pas arrêtés, mis en quarantaine ou chiffrés, l'action Remettre est la plus souvent utilisée.

Les actions secondaires incluent :

- Envoi d'une copie à une quarantaine personnalisée ou à la quarantaine « Stratégie ».
- Chiffrez le message. L'appliance chiffre uniquement le corps du message. Il ne chiffre pas

les en-têtes de message.
- Modification de l'en-tête Subject.
- Ajout de texte/HTML d'avertissement au message.
- Envoi du message à un autre hôte de messagerie de destination.
- Envoi de copies en copie cachée du message.
- Envoi d'une notification de violation DLP à l'expéditeur et/ou aux autres contacts.

Ces actions ne s'excluent pas mutuellement : vous pouvez combiner certaines d'entre elles au sein de différentes stratégies DLP pour divers besoins de traitement pour différents groupes d'utilisateurs.

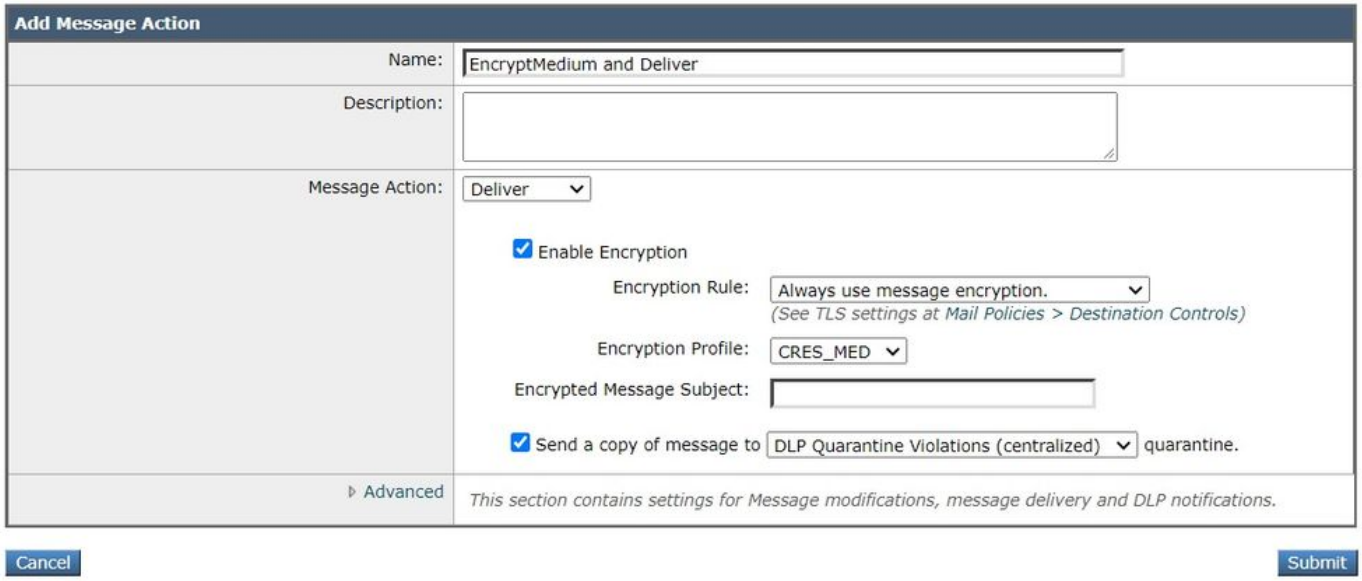
Nous allons mettre en oeuvre les actions DLP suivantes : Encrypt

Ces actions supposent que le chiffrement est sous licence et configuré sur l'ESA et que trois profils ont été créés pour une sécurité élevée, moyenne et faible, comme cela a été fait dans les sections précédentes :

- CRES_HAUT
- CRES_MED
- CRES_FAIBLE

Création des actions de message DLP

1. Accédez à Politiques de messagerie > Personnalisations des messages DLP.
2. Cliquez sur le bouton « Ajouter une action de message » et ajoutez les actions DLP suivantes. Assurez-vous de valider la modification après avoir envoyé votre action de message



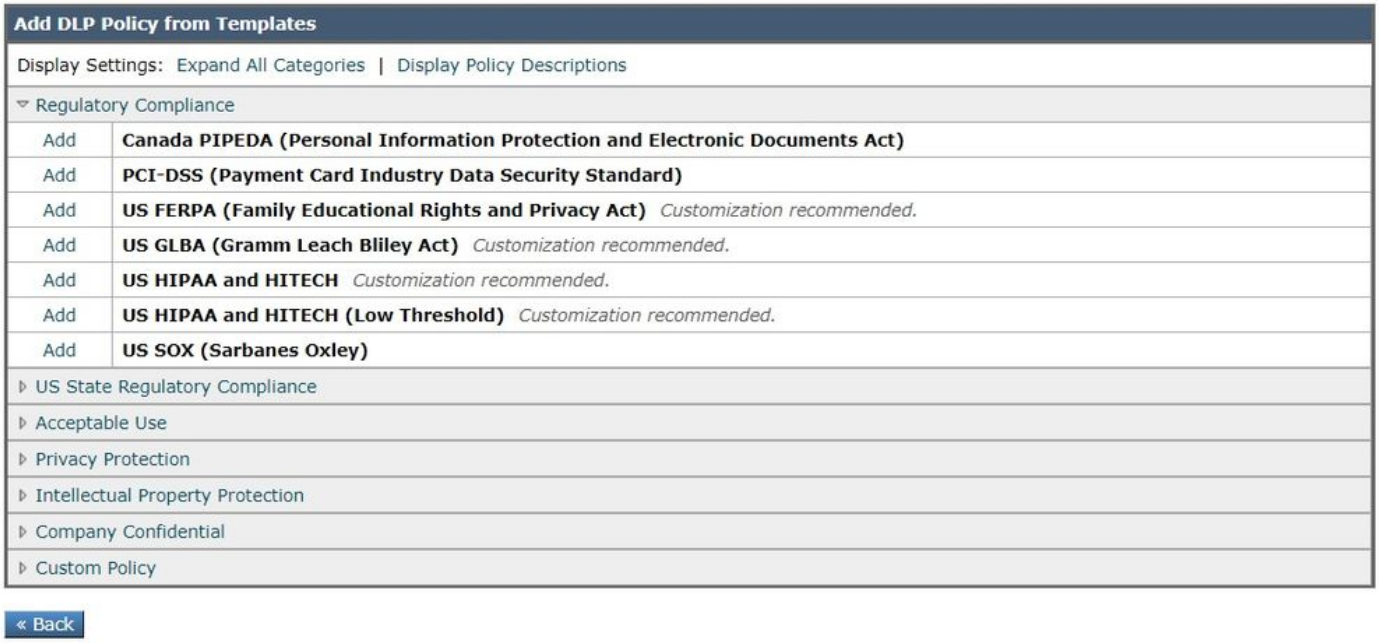
Action du message

6. Création de politiques de prévention des pertes de données

Une stratégie DLP inclut :

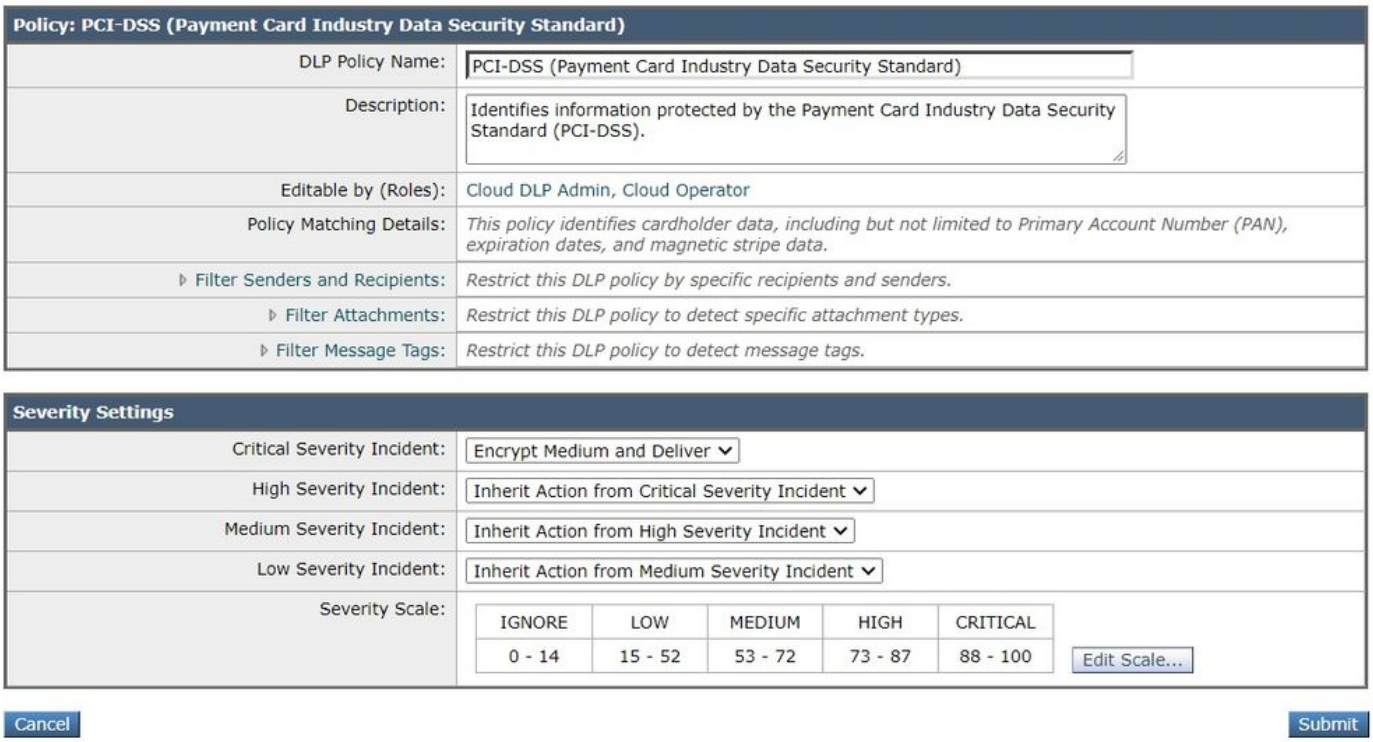
- Ensemble de conditions déterminant si un message sortant contient des données sensibles
- Actions à entreprendre lorsqu'un message contient de telles données.

1. Accédez à : Politiques de messagerie > Gestionnaire de stratégies DLP
2. Cliquez sur Ajouter une stratégie DLP.
3. Ouvrez le triangle de divulgation « Conformité aux réglementations ».



Modèle de stratégie DLP

4. Pour la politique PCI, cliquez sur le bouton « Ajouter » à gauche de PCI-DSS.



Exemple de règle DLP PCI-DSS

5. Pour l'incident de gravité critique, sélectionnez l'action « Chiffrer le support et remettre » que

nous avons précédemment configurée. Nous pourrions modifier les incidents de gravité inférieure, mais pour l'instant, laissons-les hériter de notre incident de gravité critique. Soumettez, puis validez la modification.

7. Application des stratégies DLP à une stratégie de courrier électronique sortant

1. Naviguez jusqu'à l'adresse : Politiques de messagerie > Politiques de messagerie sortante
2. Cliquez sur la cellule de contrôle DLP pour la stratégie par défaut. Si vous ne l'avez pas encore activé, le message « Disabled » s'affiche.
3. Modifiez le bouton déroulant de Désactiver DLP à Activer DLP et vous verrez immédiatement la stratégie DLP que vous venez de créer.
4. Cochez la case « Activer tout ». Soumettez, puis validez les modifications.

Conclusion

En résumé, nous avons montré les étapes nécessaires pour préparer un dispositif de sécurité de la messagerie électronique Cisco pour l'envoi d'un e-mail chiffré :

1. Activation du chiffrement des e-mails Cisco IronPort
2. Enregistrez vos ESA et votre entreprise auprès de RES
3. Création de profils de chiffrement
4. Activation de DLP
5. Création d'actions de message DLP
6. Création de stratégies DLP
7. Application de stratégies DLP à une stratégie de messagerie sortante

Des détails supplémentaires sont disponibles dans le Guide de l'utilisateur ESA correspondant à votre version du logiciel ESA. Les guides de l'utilisateur sont disponibles à l'adresse suivante :

http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-user-guide-list.html

Informations connexes

- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.