データ損失防止および暗号化のベストプラクティスガイド

内容

概要

このドキュメントでは、Cisco Eメールセキュリティのデータ損失防止(DLP)および暗号化のベストプラクティスについて説明します。

このドキュメントでは、Cisco Eメールセキュリティアプライアンス(ESA)およびクラウドベースのCisco Registered Envelope Service(RES)を使用したメッセージ暗号化の設定について説明します。 メッセージ暗号化を使用すると、コンテンツフィルタリングやDLPなどのさまざまなタイプのポリシーを使用して、個々のメッセージをパブリックインターネット経由で安全に送信できます。 これらのポリシーの作成については、このシリーズの他のドキュメントで説明します。 このドキュメントでは、ポリシーが暗号化をアクションとして使用できるように、ESAが暗号化メールを送信する準備を整えることを中心に説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

このドキュメントでは、次の手順について説明します。

1. Cisco IronPort Email Encryptionの有効化
2. ESAおよび組織をRESに登録します
3. 暗号化プロファイルの作成
4. DLPの有効化
5. DLPメッセージアクションの作成
6. DLPポリシーの作成
7. DLPポリシーの発信電子メールポリシーへの適用

これらの手順が正常に完了すると、ESA管理者は、暗号化をアクションとして使用するポリシーを正常に作成できます。

Cisco IronPort Email Encryptionは、RES Encryptionとも呼ばれます。 RESは、シスコクラウドの「キーサーバ」に使用する名前です。 RES暗号化ソリューションでは、対称キー暗号化が使用されます。つまり、メッセージの暗号化に使用されるキーは、メッセージの復号化に使用されるキーと同じです。 暗号化されたメッセージはすべて一意のキーを使用します。これにより、送信者はメッセージの送信後に詳細な制御を行うことができます。たとえば、ロックしたり期限切れにしたりすることで、受信者は他のメッセージに影響を与えることなくメッセージを開けなくなります。 メッセージを暗号化すると、ESAは暗号化されたメッセージごとに暗号化キーとメタデータをCRESに保存します。

ESAは、「フラグ」（件名コンテンツなど）、コンテンツフィルタ照合、DLPポリシーなど、さまざまな方法でメッセージを暗号化できます。 ESAがメッセージの暗号化を決定すると、[Security Services] > [Cisco IronPort Email Encryption]で作成された指定の[Encryption Profile]（「Email Encryption Profiles」という名前のテーブル）を使用してメッセージが暗号化されます。デフォルトでは、暗号化プロファイルはありません。 これについては、「*3.*暗号化プロファイルの作成」で説明します。

データ損失防止および暗号化のベストプラクティスに関するベストプラクティスガイド

1. ESAでCisco IronPort Email Encryptionを有効にする

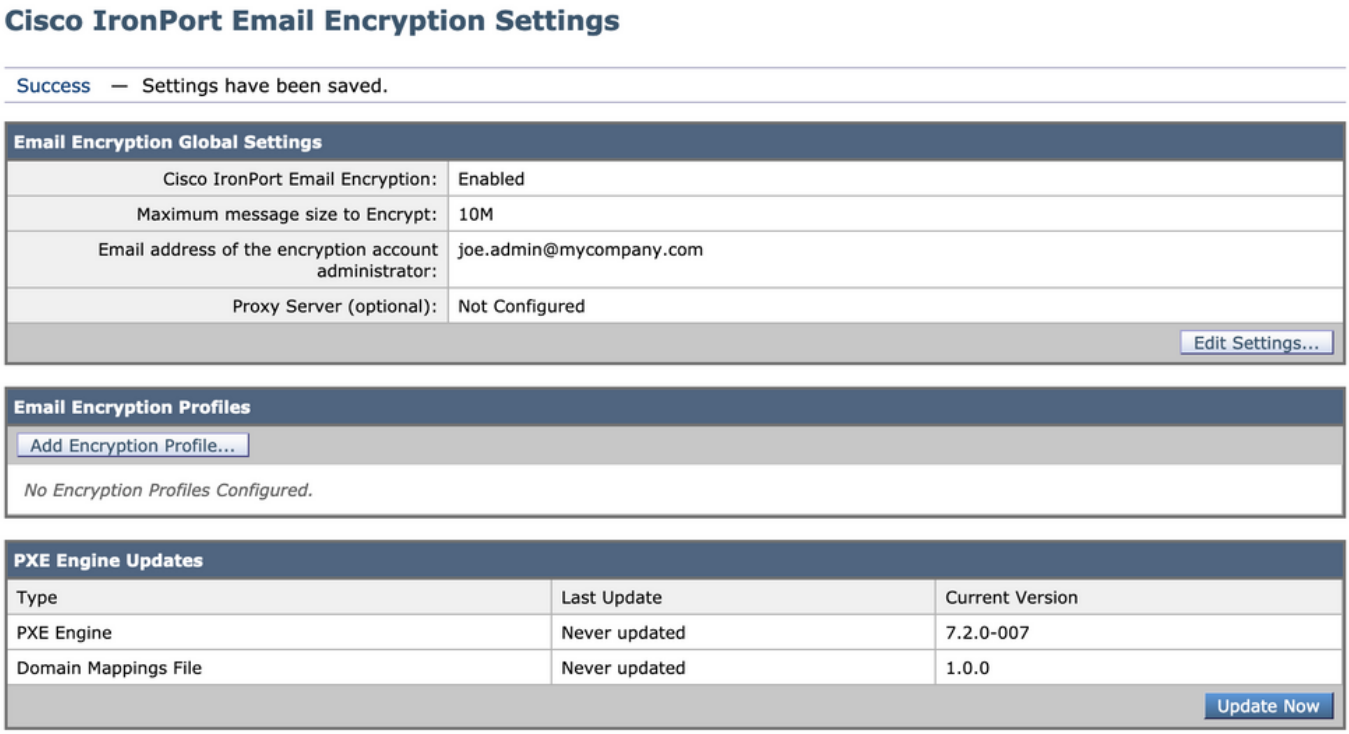
> **注：**クラスタに複数のESAがある場合は、ステップ#1の手順を1回だけ実行する必要があります。これは、これらの設定が通常はクラスタレベルで管理されるためです。 クラスタ化されていない複数のマシンがある場合、またはマシンレベルでこれらの設定を管理している場合は、各ESAでステップ#1を実行する必要があります。

1. ESA UIから、[**Security Services**] > [**Cisco IronPort Email Encryption**]に移動します。
2. Cisco IronPort Email Encryptionを有効にするには、このチェックボックスをオンにします。
3. エンドユーザライセンス契約書(EULA)、Cisco IronPort Email Encryptionライセンス契約書

に同意します。

4. [電子メール暗号化の*グローバル設定*]で[設定の編**集]をクリックします。** アカウントのプライマリRES管理者である管理者/個人の電子メールアドレスを指定します。 この電子メールアカウントは、会社のRES環境の管理に関連付けられます。オプション：暗号化するデフォルトの最大メッセージサイズは10Mです。 必要に応じて、この時点でサイズを増減できます。オプション：ESAがHTTPS経由でRESに接続するために経由する必要があるプロキシがある場合は、プロキシの通過を許可するために必要なプロキシと認証設定を追加します。
5. 設定変更を送信して確定します。

この時点で、[Email Encryption Global Settings]が次のように設定されているはずです。ただし、プロファイルはまだリストされていません。



2. ESAおよび組織をRESに登録する

ステップ#2は、主にESA管理コンソールの外部に参加します。

> **注：**ESA登録情報は、次のテクニカルノートにも記載されています。Cisco RES:仮想、ホスト、およびハードウェア ESA のアカウント プロビジョニングの設定例

電子メールをRES(stg-cres-provisioning@cisco.com)宛てに送信してください。

ESAの暗号化プロファイルのCRESアカウントをプロビジョニングするには、次の情報を提供してください。

1. アカウントの名前（**正確な会社名を指定してください。記載が必要です。**）Cloud Email Security(CES)/Hostedカスタマーアカウントの場合は、アカウント名を「<アカウント名> HOSTED」で終了するように設定してください
2. アカウント管理者に使用する電子メールアドレス（**対応する管理者電子メールアドレスを指定してください**）

3. 完全なアプライアンスのシリアル番号 アプライアンスのシリアル番号は、ESA GUI([System Administration] > [Feature Keys])またはESA CLIから「version」コマンドを使用して確認できます。 CRESアカウント管理には完全なアプライアンスシリアル番号が必要なため、仮想ライセンス番号(VLN)または製品アクティベーションキー(PAK)ライセンスの提供は許可されません。
4. 管理目的でCRESアカウントにマッピングする必要があるドメイン名

注：すでにCRESアカウントをお持ちの場合は、会社名または既存のCRESアカウント番号を入力してください。これにより、新しいアプライアンスのシリアル番号が正しいアカウントに追加され、会社情報の重複やプロビジョニングが回避されます。

CRESアカウントのプロビジョニングに関してメールを送信する場合は、1営業日以内に対応します。すぐにサポートとサポートが必要な場合は、Cisco TACでサポートリクエストをオープンしてください。これは、Support Case Manager(https://mycase.cloudapps.cisco.com/case)または電話(https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html)で行うことができます。

> **注**：このリクエストを電子メールで送信した後、会社のRESアカウントが作成され（まだ作成されていない場合）、S/Nsが追加されるまで1日かかることがあります。 ステップ#3の「プロビジョニング」タスクは、この作業が完了するまで機能しません。

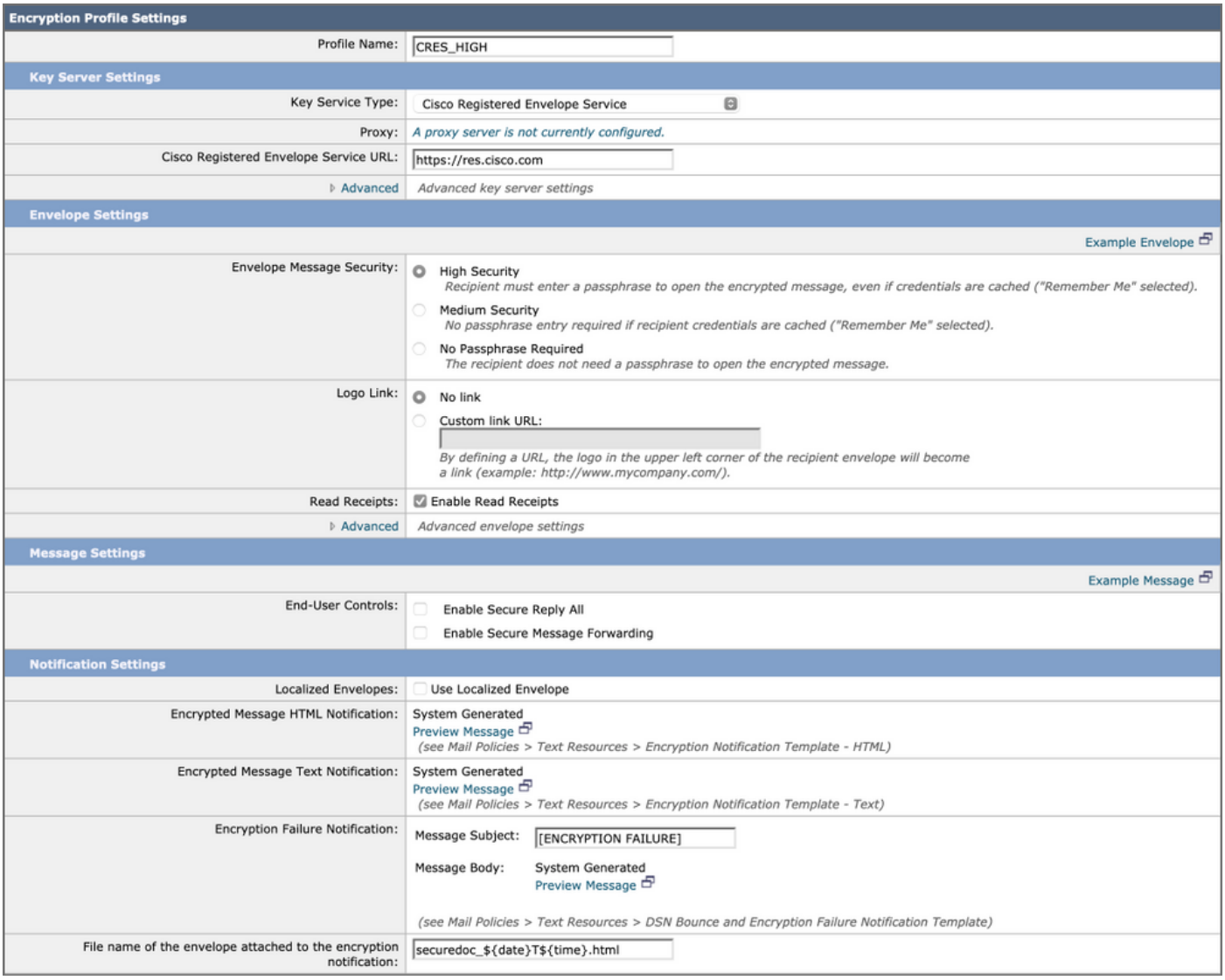
3. ESAでの暗号化プロファイルの作成

> **注**：クラスタに複数のESAがある場合は、ステップ#1の手順を1回だけ実行する必要があります。これは、これらの設定が通常はクラスタレベルで管理されるためです。 クラスタ化されていない複数のマシンがある場合、またはマシンレベルでこれらの設定を管理している場合は、各ESAでステップ#1を実行する必要があります。

暗号化プロファイルは、暗号化されたメッセージの送信方法を指定します。 たとえば、組織は、機密性の高いデータを頻繁に送信することを知っている受信者など、受信者の1セグメントに対してセキュリティの高いエンベロープを送信する必要があります。 同じ組織に、受信者コミュニティの他のセグメントが機密情報を受け取らず、ユーザIDとパスワードを提供して暗号化されたメールを受け取る必要がある患者も少ない可能性があります。 これらの受信者は、セキュリティの低いタイプのエンベロープの候補になります。 複数の暗号化プロファイルを使用すると、暗号化されたメッセージ形式を対象者に合わせてカスタマイズできます。 一方、多くの組織は、1つの暗号化プロファイルだけで問題なく動作します。

このドキュメントでは、「CRES_HIGH」、「CRES_MED」、「CRES_LOW」という3つの暗号化プロファイルの作成例を示します。

1. ESA UIから、[Security Services] > [Cisco IronPort Email Encryption]に移動します。
2. [Add Encryption Profile...]をクリックします。"
3. [Encryption Profile]メニューが開き、最初の暗号化プロファイルに「CRES_HIGH」という名前を付けることができます。
4. [エンベロープメッセージのセキュリティ(Envelope Message Security)]が選択されていない場合は、[高セキュリティ(High Security)]を選択します。
5. [送信]をクリックして、このプロファイルを保存します。



次に、手順2 ~ 5を繰り返して「CRES_MED」と「CRES_LOW」を作成します。各プロファイルのエンベロープメッセージセキュリティのオプションボタンを変更するだけです。

- CRES_HIGHプロファイルで、[High Security]オプションボタンを選択します。
- CRES_MEDプロファイルで、[Medium Security]オプションボタンを選択します。
- CRES_LOWプロファイルで、[No Password Required]オプションボタンを選択します

[開封確認を有効にする(Enable Read Receipts)]、[全員に安全に返信する(Enable Secure Reply All)]、および[メッセージ転送を有効にする(Enable Secure Message Forwarding)]にはオプションがあります。 [エンベロープ設定]で[詳細設定]リンクをクリックすると、3つの対称暗号化アルゴリズムのいずれかを選択できます。また、エンベロープがJava暗号化アプレットなしで送信されるように指定することもできます。

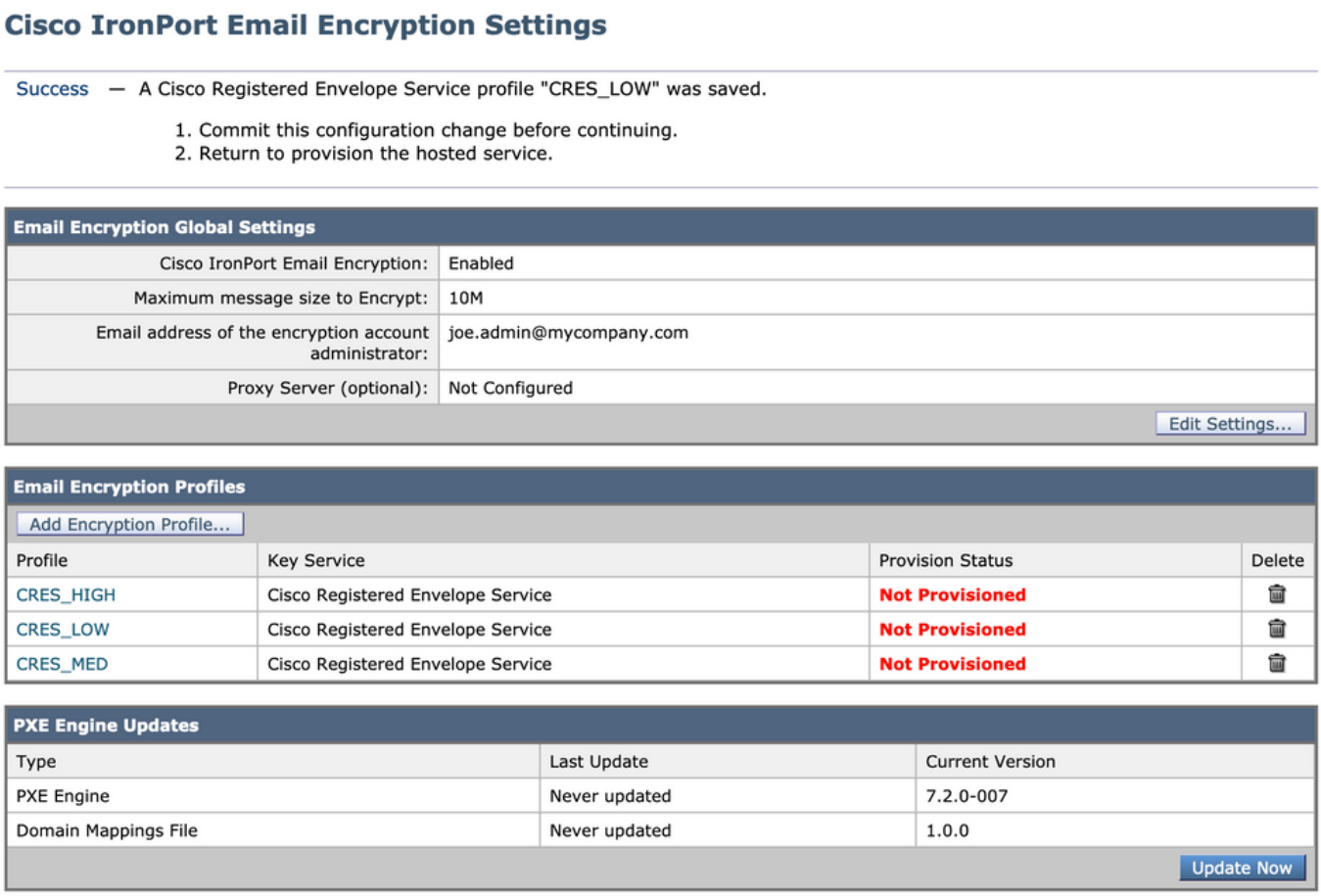
エンベロープ設定の右側に、「メッセージ例」のハイパーテキストリンクが表示されます。 クリックすると、受信者がHTMLの添付ファイルを開いた後に電子メールに表示されるメッセージの保護エンベロープの例が表示されます。

[Read Receipts]は、受信者がセキュアメッセージ（受信者が対称キーをプルダウンしてメッセージを復号化したことを意味する）を開くと、暗号化されたメッセージの送信者がCRESから電子メールを受信することを意味します。

[Message Settings]の右側に、「Example Message」ハイパーテキストリンクが表示されます。クリックすると、開封したメッセージの内容が表示されます。エンベロープに必要な情報を入力し、暗号化されたメッセージを開封すると、受信者に表示されます。

必ず[送信]をクリックして変更を**確定する**ようにしてください。

テーブル内の行に「プロビジョニング」ボタンが表示されます。 [Provision]ボタンは、[Commit changes]を実行するまで表示されません。

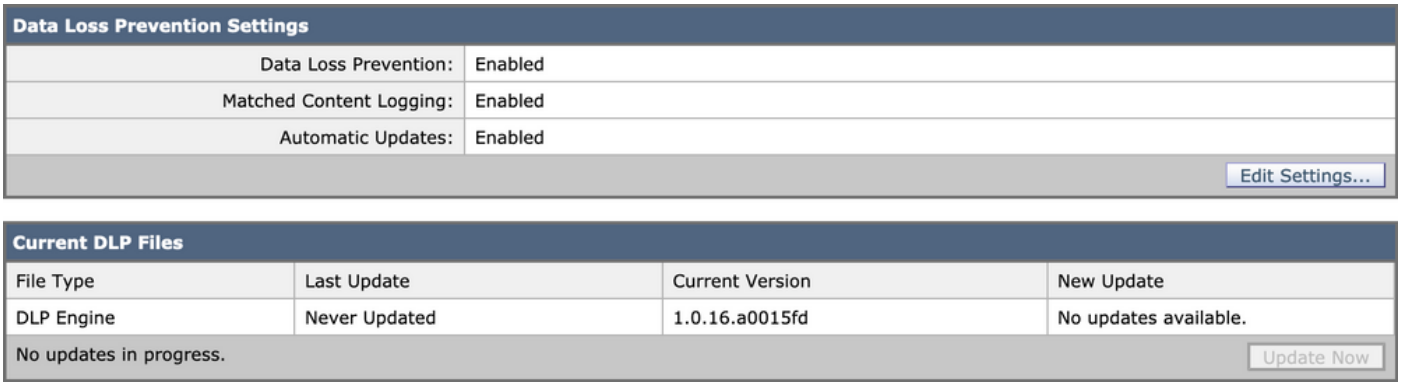


[プロビジョニング(Provision)]ボタンを再度クリックします。これは、会社のRESアカウントが作成され、アプライアンスのS/Nがアカウントに追加された後にのみ機能します。 RESアカウントがESAにリンクされている場合、プロビジョニングプロセスは比較的迅速に実行されます。 そうでない場合は、そのプロセスを最初に完了する必要があります。

プロビジョニングが完了すると、[Cisco IronPort Email Encryption]ページにプロビジョニング済みのプロファイルが表示されます。

4.データ損失防止(DLP)の有効化

1. ESA UIから、[**Security Services**] > [**Data Loss Prevention**]**に移動します。**
2. DLPを有効**にするには、[有効**..]をクリックします。
3. EULA、Data Loss Prevention License Agreementに同意します。
4. [Enable matched content logging]チェックボックスをオンにします。
5. [自動更新を有効にする]チェックボックスをオンにします。
6. [Submit] をクリックします。



Data Loss Prevention Settings

Data Loss Prevention:	Enabled
Matched Content Logging:	Enabled
Automatic Updates:	Enabled

Edit Settings...

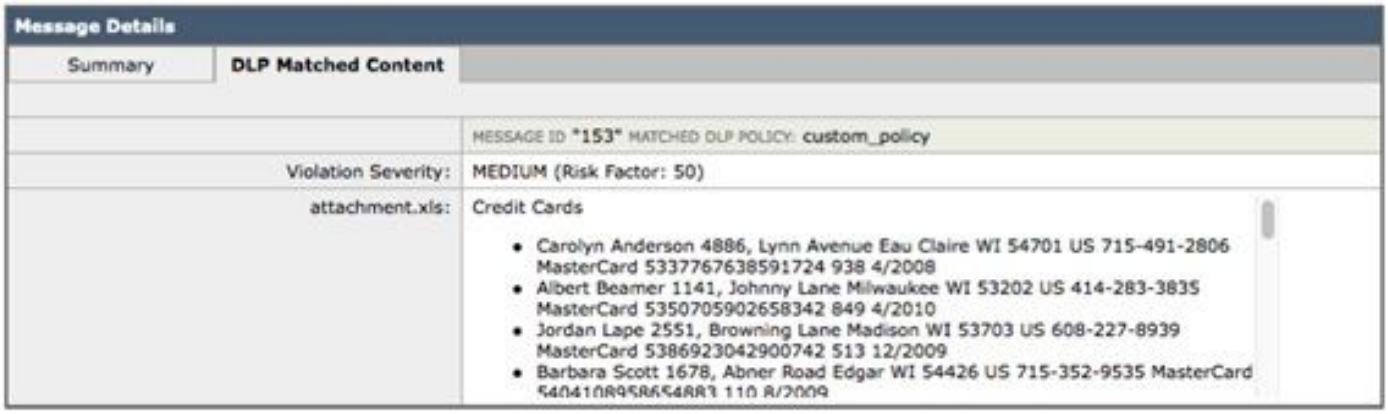
Current DLP Files

File Type	Last Update	Current Version	New Update
DLP Engine	Never Updated	1.0.16.a0015fd	No updates available.

No updates in progress. Update Now

DLPエンジンおよびアプライアンス上の事前定義されたコンテンツ照合分類子の更新は、他のセキュリティサービスの更新とは独立しています。3 ~ 5分間の定期的なTalosシグニチャの更新は異なり、DLPポリシーと辞書の更新は含まれません。アップデートは、ここで有効にする必要があります。

[Matched Content Logging]が有効になっている場合、メッセージ追跡は違反の原因となった電子メールの内容を表示できます。DLP違反の原因となった電子メールコンテンツを示すメッセージトラッキングの例を次に示します。 これにより、管理者は、特定のDLPポリシーをトリガーしたデータを正確に把握できます。



Message Details

Summary | **DLP Matched Content**

MESSAGE ID "153" MATCHED DLP POLICY: custom_policy

Violation Severity: MEDIUM (Risk Factor: 50)

attachment.xls: Credit Cards

- Carolyn Anderson 4886, Lynn Avenue Eau Claire WI 54701 US 715-491-2806 MasterCard 5337767638591724 938 4/2008
- Albert Beamer 1141, Johnny Lane Milwaukee WI 53202 US 414-283-3835 MasterCard 5350705902658342 849 4/2010
- Jordan Lape 2551, Browning Lane Madison WI 53703 US 608-227-8939 MasterCard 5386923042900742 513 12/2009
- Barbara Scott 1678, Abner Road Edgar WI 54426 US 715-352-9535 MasterCard

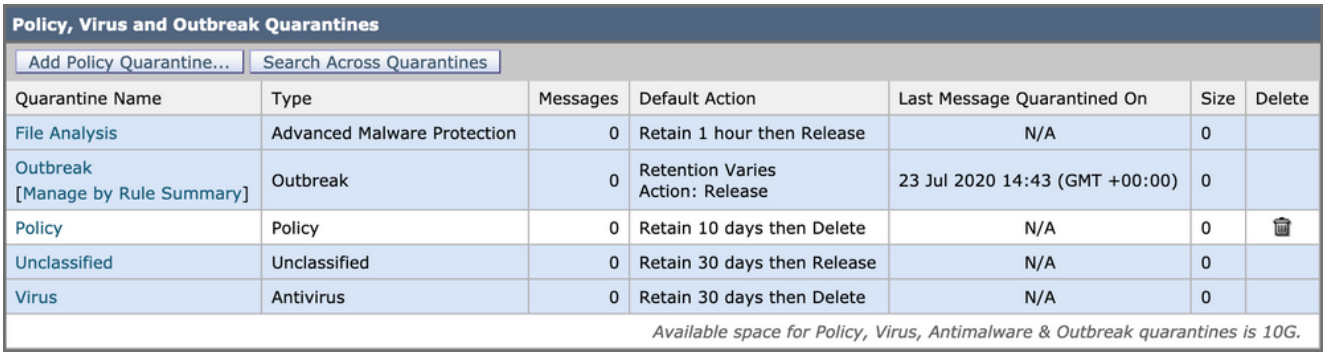
データ損失防止違反

5.データ損失防止メッセージアクションの作成

DLP隔離の作成

DLPポリシーに違反するメッセージのコピーを保持したい場合は、ポリシー違反のタイプごとに個別のポリシー隔離を作成できます。これは、DLPポリシーに違反するアウトバウンドメッセージが口グに記録されて配信されるが、メッセージに対してアクションが実行されない「透過的」POVを実行する場合に特に便利です。

1. SMAで、[Email] > **[Message Quarantine] > [Policy, Virus, and Outbreak Quarantines]に移動します**
2. 開始する前に、Quarantinesテーブルは次のようになります。



Policy, Virus and Outbreak Quarantines

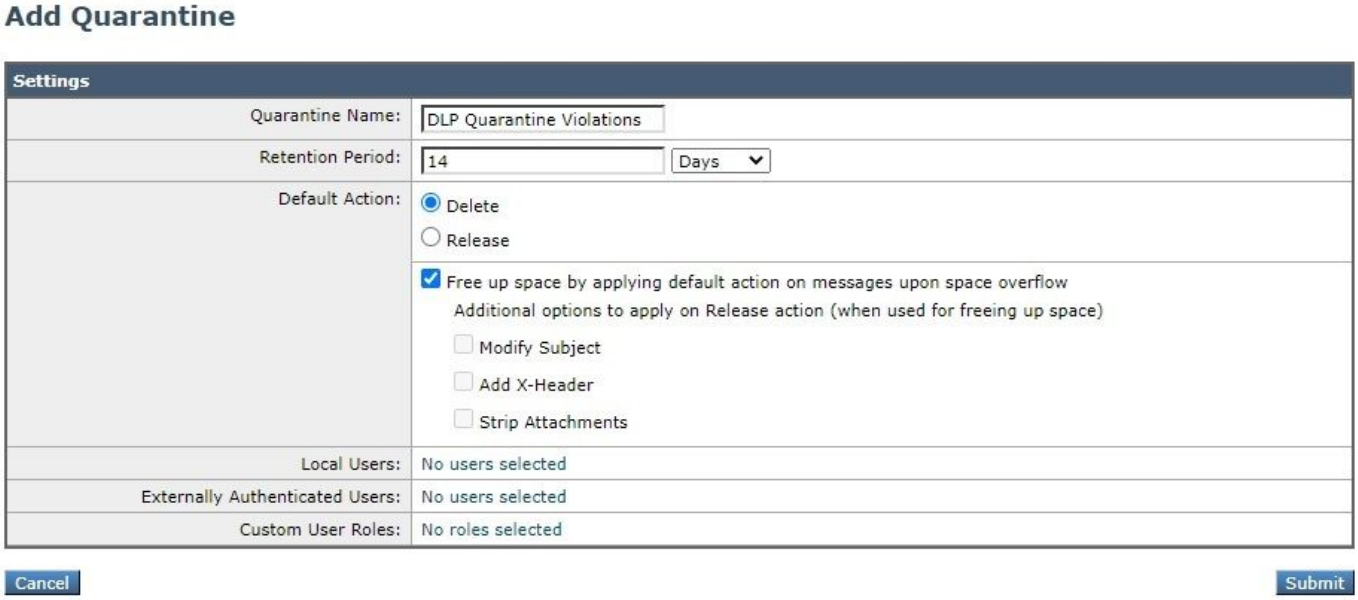
Add Policy Quarantine... | Search Across Quarantines

Quarantine Name	Type	Messages	Default Action	Last Message Quarantined On	Size	Delete
File Analysis	Advanced Malware Protection	0	Retain 1 hour then Release	N/A	0	
Outbreak [Manage by Rule Summary]	Outbreak	0	Retention Varies Action: Release	23 Jul 2020 14:43 (GMT +00:00)	0	
Policy	Policy	0	Retain 10 days then Delete	N/A	0	
Unclassified	Unclassified	0	Retain 30 days then Release	N/A	0	
Virus	Antivirus	0	Retain 30 days then Delete	N/A	0	

Available space for Policy, Virus, Antimalware & Outbreak quarantines is 10G.

ポリシーウイルスおよびアウトブレイク隔離

3. [Add Policy Quarantine]ボタンをクリックし、DLPポリシーで使用する検疫を作成します。次に、中程度のDLP違反に対する検疫の例を示します。隔離のセグメント化が可能で、複数のDLPルールに対して必要な場合があります。



Add Quarantine

Settings

Quarantine Name:	DLP Quarantine Violations
Retention Period:	14 Days
Default Action:	◉ Delete ○ Release
	☑ Free up space by applying default action on messages upon space overflow Additional options to apply on Release action (when used for freeing up space) ☐ Modify Subject ☐ Add X-Header ☐ Strip Attachments
Local Users:	No users selected
Externally Authenticated Users:	No users selected
Custom User Roles:	No roles selected

Cancel | Submit

DLP検疫の例

DLPメッセージアクションについて

DLPメッセージアクションは、発信電子メールでDLP違反を検出したときにESAが実行するアクションを説明します。プライマリDLPアクションとセカンダリDLPアクションを指定できます。違反タイプや重大度ごとに異なるアクションを割り当てることができます。

主なアクション：

- 提供
- [Drop]
- Quarantine

DLP違反が記録されて報告されるが、メッセージが停止/隔離または暗号化されていない読み取り専用状態では、Deliverアクションが最も頻繁に使用されます。

2番目のアクションは次のとおりです。

- 任意のカスタム検疫または「ポリシー」検疫にコピーを送信しています。
- **メッセージを暗号化します。**アプライアンスはメッセージ本文のみを暗号化します。メッセージヘッダーは暗号化されません。

- 件名ヘッダーを変更しています。
- 免責事項テキスト/HTMLをメッセージに追加します。
- メッセージを代替宛先メールホストに送信する。
- メッセージのBCCコピーを送信しています。
- 送信者またはその他の連絡先にDLP違反通知を送信しています。

これらのアクションは相互に排他的ではありません。ユーザグループごとに異なる処理ニーズに応じて、いくつかのアクションを異なるDLPポリシー内で組み合わせることができます。

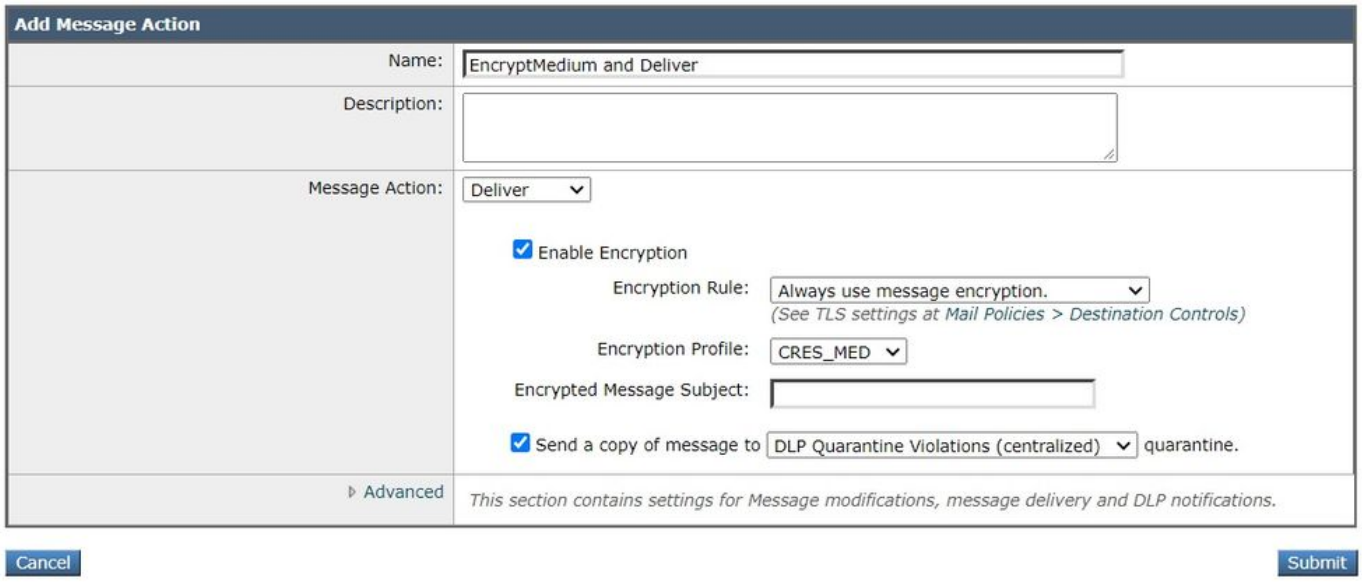
次のDLPアクションを実装します

次のアクションは、暗号化がESAでライセンスおよび設定され、前のセクションで行ったように、高、中、低のセキュリティ用に3つのプロファイルが作成されていることを前提としています。

- CRES_HIGH
- CRES_MED
- CRES_LOW

DLPメッセージアクションの作成

1. [*Mail Policies*] > [*DLP Message Customizations*]に移動します。
2. [Add Message Action]ボタンをクリックし、次のDLPアクションを追加します。 メッセージアクションの送信後に必ず変更をコミットしてください



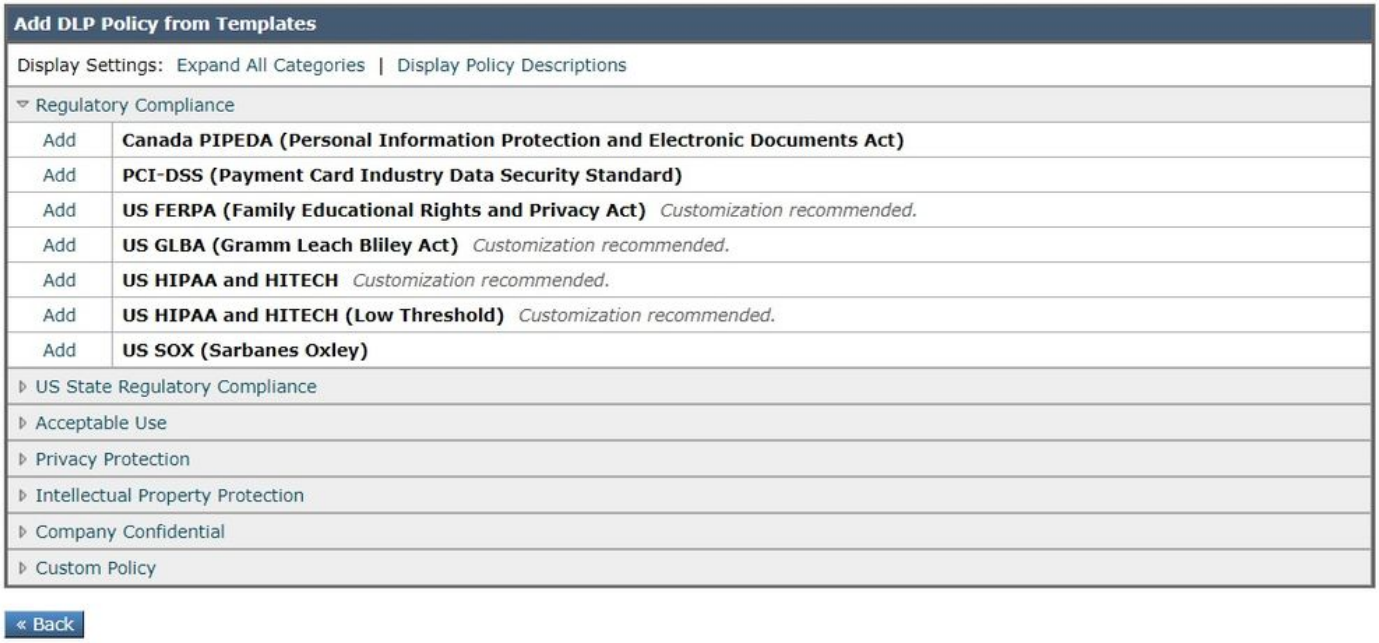
メッセージアクション

6.データ損失防止ポリシーの作成

DLPポリシーには次のものが含まれます。

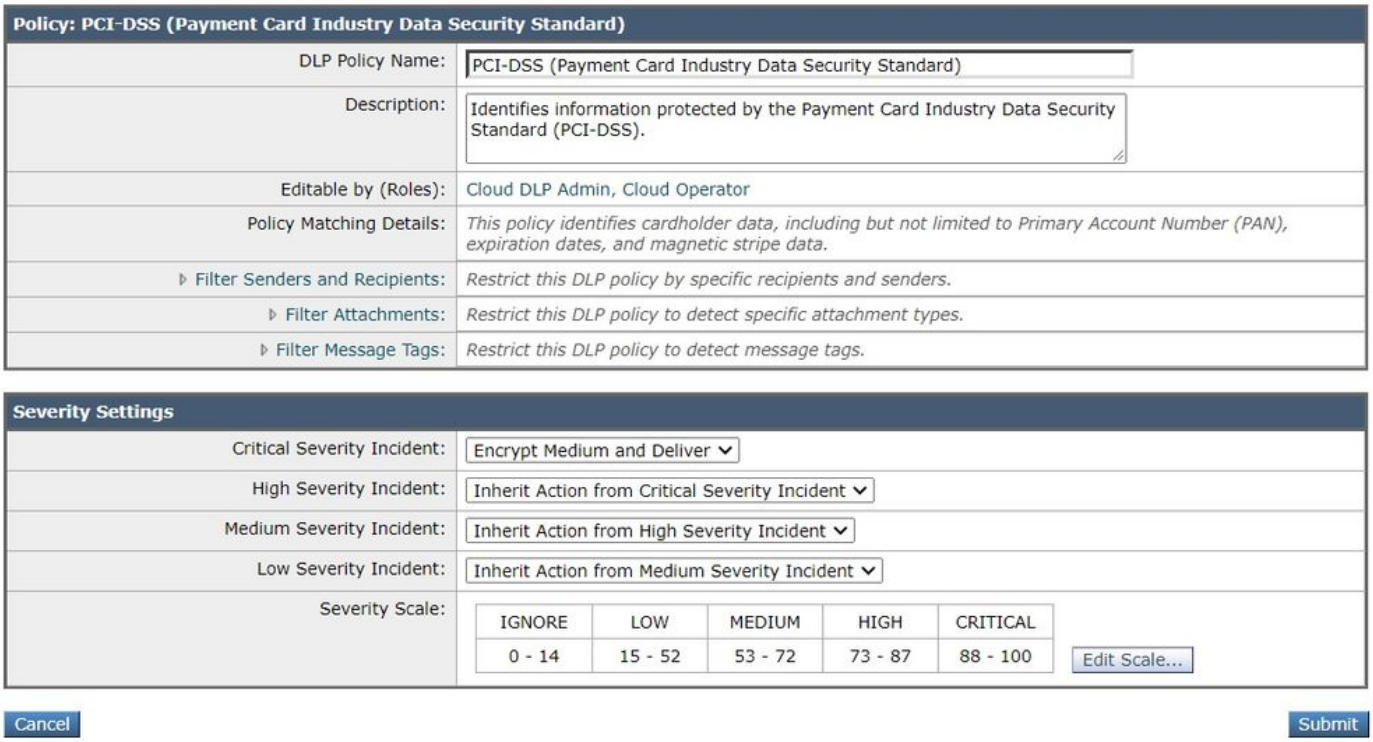
- 発信メッセージに機密データが含まれているかどうかを決定する一連の条件
- メッセージにそのようなデータが含まれている場合に実行されるアクション。

1. [メールポリシー] > [*DLPポリシーマネージャ*]に移動します。
2. [*Add DLP Policy*]をクリックします
3. 「コンプライアンス」の公開トライアングルを開きます。



DLPポリシーテンプレート

4. PCIポリシーの場合は、PCI-DSSの左側にある[Add]ボタンをクリックします。



PCI-DSSのDLPルールの例

5. [Critical Severity Incident]で、以前に設定した[Encrypt Medium and Deliver]アクションを選択します。重大度の低いインシデントは変更できますが、ここでは重大度の低いインシデントを継承させてください。変更を送信し、確定します。

7. DLPポリシーの発信電子メールポリシーへの適用

1. 次のとおりに移動します。[Mail Policies] > [Outgoing Mail Policies]
2. デフォルトポリシーのDLPのコントロールセルをクリックします。まだ有効になっていない場合は、「Disabled」と表示されます。
3. プルダウンボタンを[Disable DLP]から[Enable DLP]に変更すると、作成したDLPポリシーが

すぐに表示されます。
4. [Enable All]チェックボックスをクリックします。[Submit]をクリックし、変更を[Commit]します。

結論

要約すると、暗号化された電子メールを送信するためにCisco Eメールセキュリティアプライアンス(ESA)を準備するために必要な手順を示しています。

1. Cisco IronPort Email Encryptionの有効化
2. ESAおよび組織をRESに登録します
3. 暗号化プロファイルの作成
4. DLPの有効化
5. DLPメッセージアクションの作成
6. DLPポリシーの作成
7. DLPポリシーの発信電子メールポリシーへの適用

詳細については、ご使用のESAソフトウェアリリースに対応する『ESA User Guide』を参照してください。 ユーザガイドは、次のリンクから入手できます。

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

関連情報

- テクニカル サポートとドキュメント – Cisco Systems