ESA CRES暗号化プロファイルのセキュリティレベルの設定

内容

概要

このドキュメントでは、Eメールセキュリティアプライアンス(ESA)内のCisco Registered Envelope Service Encryption(CRES)プロファイルの設定について、許可されるさまざまなセキュリティレベルに重点を置いて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ESAの基本設定
- コンテンツフィルタ設定に基づく暗号化
- Cisco Registered Envelope Service

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

CRESプロファイルの作成は、ESAを介して暗号化サービスをアクティブ化および使用するためのコアタスクです。複数のプロファイルを作成する前に、CRESアカウントを作成してESAに対して完全なアカウントがプロビジョニングされていることを確認します。

複数のプロファイルを設定でき、各プロファイルに異なるセキュリティレベルを設定できます。これにより、ネットワークはドメイン、ユーザ、またはグループごとに異なるセキュリティレベルを維持できます。

設定

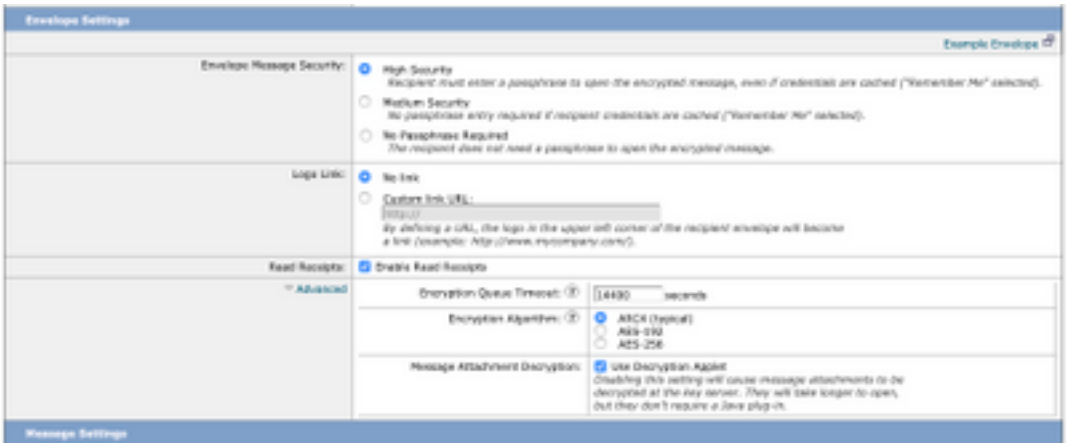
暗号化プロファイルを有効および設定するには、**encryptionconfig CLIコマンドを使用**するか、GUIで**[Security Services] > [Cisco IronPort Email Encryption]を選択**します。

GUI からの設定

ESAから**[Security Services] > [Cisco IronPort Email Encryption] > [Add Encryption Profile]に移動します。**

[Encryption Profile Settings]が表示されます。プロファイル名とその他の設定はカスタマイズ可能で、組織の識別タグまたは方法によって異なります。

プロファイルごとにセキュリティレベルを定義する設定は、図に示すように[Envelope Settings]です。



> **注**：プロファイル名には次のものが含まれることが推奨されます。コンテンツフィルタの作成と検証を迅速に識別するために、設定されたセキュリティレベルまたはプロファイルが関連付けられているグループの名前と一致させるため、「高」、「低」など。

ESAで許可されるセキュリティの3つのレベルは次のとおりです。

- 高セキュリティ：暗号化されたメッセージを開くには、受信者は常にパスフレーズを入力する必要があります。
- 中セキュリティ：受信者の資格情報がキャッシュされている場合、受信者は資格情報を入力して暗号化されたメッセージを開く必要はありません。
- パスフレーズは不要：これは、暗号化されたメッセージセキュリティの最低レベルです。受

信者は、暗号化されたメッセージを開くためにパスフレーズを入力する必要はありません。パスフレーズで保護されていないエンベロープに対しては、開封確認、全員への返信、およびメッセージ転送機能を有効にできます。

次のオブジェクトに対して、さまざまなレベルのセキュリティを設定できます。

エンベロープメッセージセキュリティ:

- ・ 高セキュリティ
- 中程度のセキュリティ
- パスフレーズは不要

ロゴリンク：ユーザが組織のURLを開けるようにするには、ロゴをクリックし、ロゴへのリンクを追加します。次のオプションから選択します。

- リンクなし.ライブリンクはメッセージエンベロープに追加されません。
- カスタムリンクURL。URLを入力して、メッセージエンベロープにライブリンクを追加します。

開封確認：このオプションを有効にすると、受信者がセキュリティで保護されたエンベロープを開封したときに、送信者は受信確認を受け取ります。これはオプションの選択です。

[Advanced]：

暗号化キューのタイムアウト：メッセージがタイムアウトになるまでの時間（秒）を入力します。メッセージがタイムアウトすると、アプライアンスはメッセージをバウンスし、送信者に通知を送信します。

Encryption Algorithm（暗号化アルゴリズム）：

- ARC4. ARC4は最も一般的な選択肢で、メッセージ受信者の復号遅延を最小限に抑えて強力な暗号化を提供します。
- AES.AESは、より強力な暗号化を提供しますが、復号化に時間がかかり、受信者に遅延が生じます。AESは通常、政府および銀行のアプリケーションで使用されます。

メッセージ添付の復号化:復号化アプレットを有効または無効にします。このオプションを有効にすると、メッセージの添付ファイルがブラウザ環境で開かれます。このオプションを無効にすると、メッセージの添付ファイルがキーサーバで復号化されます。デフォルトでは、エンベロープではJavaアプレットは無効になっています。

> **注**：セキュリティ上の理由により、最も使用されているブラウザではJavaアプレットが無効になっています。

暗号化プロファイルが作成されたら、 イメージに示すように、プロビジョニングされていることを確認します。

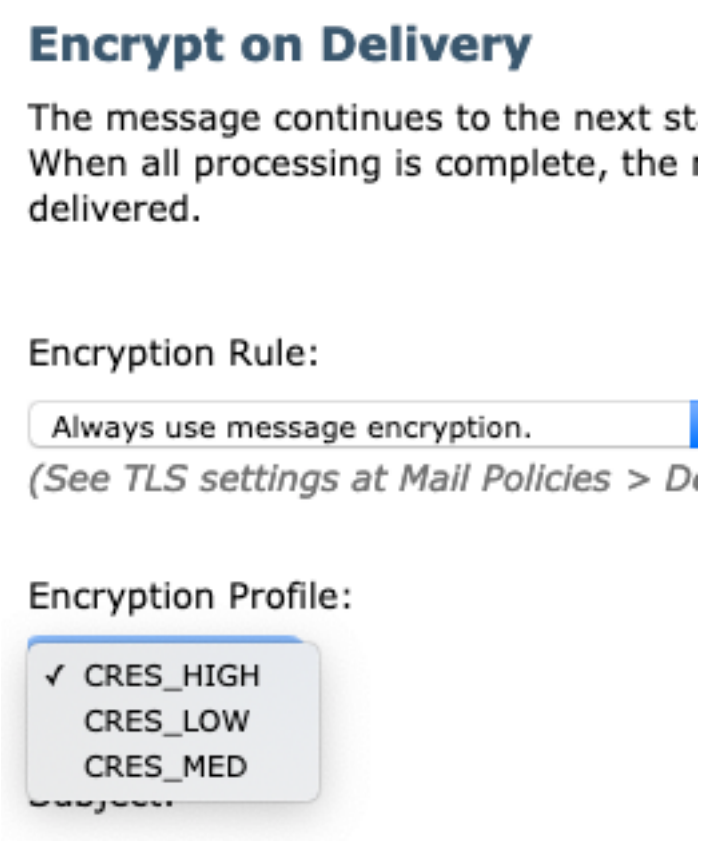
これらのプロファイルを適用するには、コンテンツフィルタを介して関連付ける必要があります。

> **注意**：コンテンツフィルタによってプロファイルが呼び出されない場合、暗号化設定は適用

できません。

ESAから、[Mail Policies] > [**Outgoing Content Filters] > [Add a filter]に移動します**

ユーザ、件名、グループ、送信者などの条件がフィルタ内で設定されたら、次の図に示すように、発信フィルタの暗号化レベルを定義します。



注意：正常に機能するには、すべてのコンテンツフィルタを発信メールポリシーに関連付ける必要があります。

注：ホステッドキーサービスに複数の暗号化プロファイルを設定できます。組織に複数のブランドがある場合は、PXEエンベロープのキーサーバに保存されている別の口ゴを参照できます。

CLI からの設定

ESA CLIで**encryptionconfig**コマンドを入力します。

```
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]]>
```

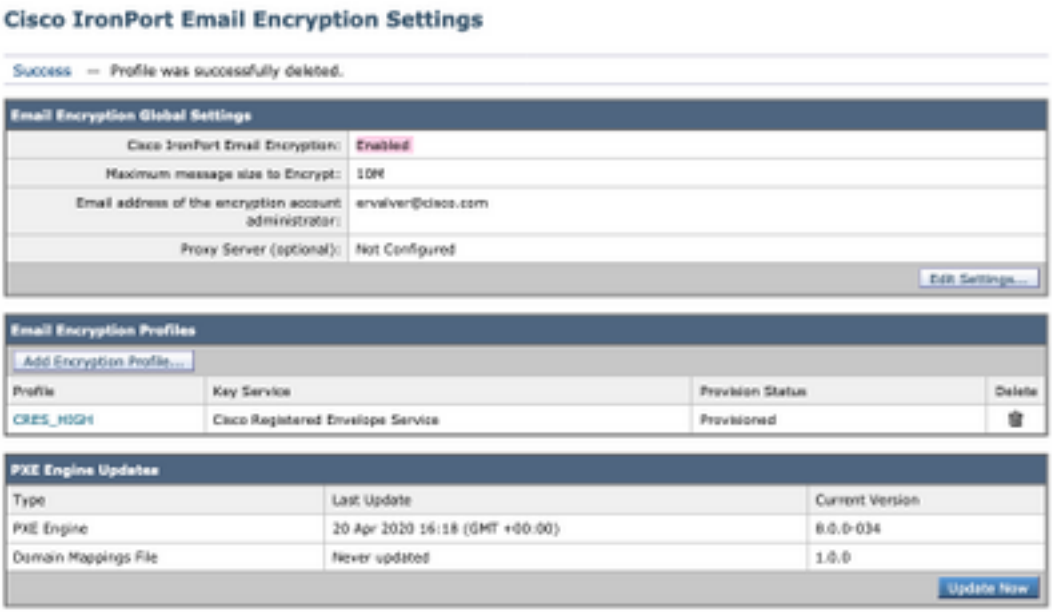
```
Please enter file name of the envelope attached to the encryption notification:
[securedoc_${date}T${time}.html]>


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
```

確認

ここでは、設定が正常に機能しているかどうかを確認します。

GUIからの検証

図に示すように、ESAから[Security Services] > [Cisco IronPort Email Encryption]に移動します。



注：暗号化が有効になっており、設定されているプロファイルがプロビジョニングされていることを確認します。図に示すように。

CLIからの検証

CLIから**encryptconfig**とtype profilesコマンドを入力します。

```
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
```

> **注**：暗号化が有効になっており、設定されているプロファイルがプロビジョニングされていることを確認します。図に示すように。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

ESAから、**[System Administration] > [feature keys]に移動します**

機能キーが適用され、アクティブであることを確認します。キー：IronPort Email Encryptionがアクティブになっている必要があります。

ESAから**[Security Services] > [Cisco IronPort Email Encryption]に移動します**

暗号化サービスが正しく有効になっていることを確認します。

次の図に示すように、暗号化プロファイルが[Not Provisioned]ステータスになっていないことを確認します。

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**

図に示すように、エンジンの最後のアップデートを確認します。

PXE Engine Updates

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

[Message Tracking details]で、エラーが表示されているかどうかを確認します。

最も一般的なエラー：

`5.x.3 - Temporary PXE Encryption failure`
ソリューション：サービスは現在利用できないか、到達不能です。接続とネットワークの問題を確認します。

`5.x.3 - PXE Encryption failure. (Message could not be encrypted due to a system configuration issue. Please contact your administrator`
ソリューション：このエラーは次のエラーに関連しています。

- ライセンスの問題機能キーを確認してください
- 使用されたプロファイルはプロビジョニングされません。コンテンツフィルタおよびプロビジョニングで設定されたプロファイルをメッセージトラッキングから特定する
- コンテンツフィルタに関連付けられたプロファイルはありません。暗号化プロファイルが削除されたり、異なる名前で変更されたりすることがあります。設定されたコンテンツフィルタで、関連付けられたプロファイルが見つかりません

`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.)`
ソリューション：定期的に、この問題は、内部送信者の電子メールクライアント（Outlookなど）が、無効な「From」/「To」アドレスを含む受信者の電子メールアドレスを自動的に入力することによって発生します。

これは通常、電子メールアドレスの引用符や、電子メールアドレスの他の不正な文字が原因で発生します。

関連情報

- CRES管理ガイド
- エンドユーザガイド
- テクニカル サポートとドキュメント – Cisco Systems