在ESA CRES加密配置檔案中配置安全級別

目錄

簡介

本檔案介紹在郵件安全裝置(ESA)內針對所允許的不同安全級別來設定思科註冊信封服務加密(CRES)設定檔。

必要條件

需求

思科建議您瞭解以下主題：

- ESA基本配置
- 基於內容過濾器配置的加密
- 思科註冊信封服務

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

建立CRES配置檔案是通過ESA啟用和使用加密服務的核心任務。建立多個配置檔案之前，請確保通過建立CRES帳戶為ESA調配了完整的帳戶。

可以有多個配置檔案，每個配置檔案都可以配置不同的安全級別。這允許網路按域、使用者或組維護不同級別的安全性。

設定

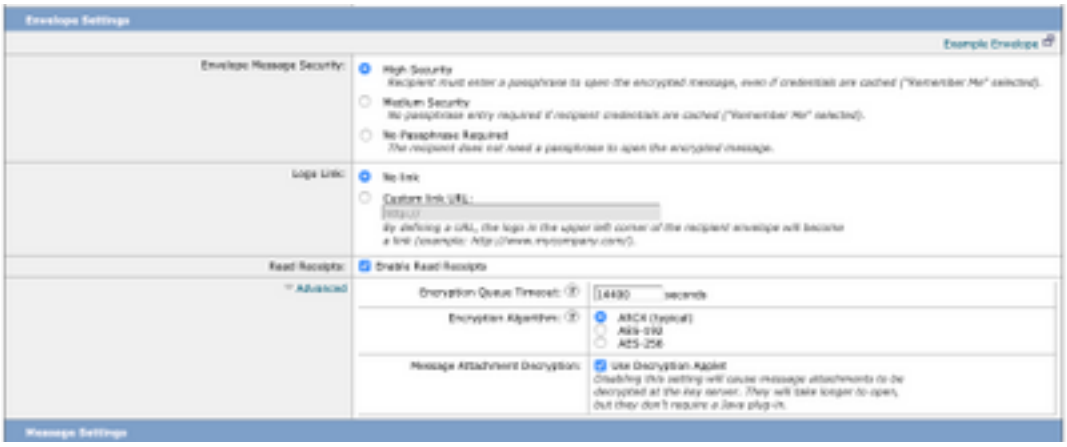
您可以使用**encryptionconfig** CLI命令，或通過GUI中的**安全服務> Cisco IronPort電子郵件加密**來啟用和配置加密配置檔案。

在GUI上配置

從ESA導航到**安全服務> Cisco IronPort郵件加密>**新增加密配置檔案。

將顯示一個包含加密配置檔案設定的螢幕。配置檔名稱和其餘配置可以自定義，具體取決於組織的標識標籤或方法。

定義每個配置檔案安全級別的配置是「Envelope Settings」，如下圖所示：



> **附註**：建議配置檔名稱包含：「高」、「低」等，以便與配置的安全級別或配置式與之關聯的組的名稱相匹配，從而在內容過濾器的建立和驗證過程中快速識別該組。

ESA允許的三個安全級別是：

- 高安全性：收件人必須始終輸入密碼才能開啟加密郵件。
- 中等安全性：如果收件人憑據已快取，則收件人無需輸入憑據即可開啟加密郵件。
- 無需密碼短語：這是加密郵件安全的最低級別。收件人無需輸入密碼即可開啟加密郵件。您仍然可以為沒有密碼保護的信封啟用讀回執、安全回覆所有和安全郵件轉發功能。

您可以在以下對象上配置不同級別的安全性：

信封郵件安全:

- ·高安全性
- 中等安全性
- 無需密碼短語

徽標連結：若要使使用者能夠開啟您組織的URL，請按一下其徽標，您可以向該徽標新增連結。從以下選項中選擇：

- 無連結。即時連結不會新增到郵件信封中。

- 自定義連結URL。輸入URL以將即時連結新增到郵件信封。

已讀回執：如果啟用此選項，則當收件人開啟安全信封時，發件人將收到回執。這是一個可選選擇。

高級：

加密隊列超時：輸入消息在超時之前可以在加密隊列中的時間長度（秒）。郵件超時後，裝置將退回郵件並向發件人傳送通知。

加密演算法:

- ARC4。ARC4是最常見的選擇，它提供強大的加密功能，使消息接收者的解密延遲最小。
- AES。AES提供更強的加密，但解密所需的時間也更長，這會導致收件人延遲。AES通常用於政府和銀行應用中。

郵件附件解密:啟用或禁用解密小程式。啟用此選項後，它會在瀏覽器環境中開啟郵件附件。禁用此選項後，將導致郵件附件在金鑰伺服器上解密。預設情況下，在信封中禁用Java Applet。

附註：由於安全原因，最常用的瀏覽器已禁用Java Applet。

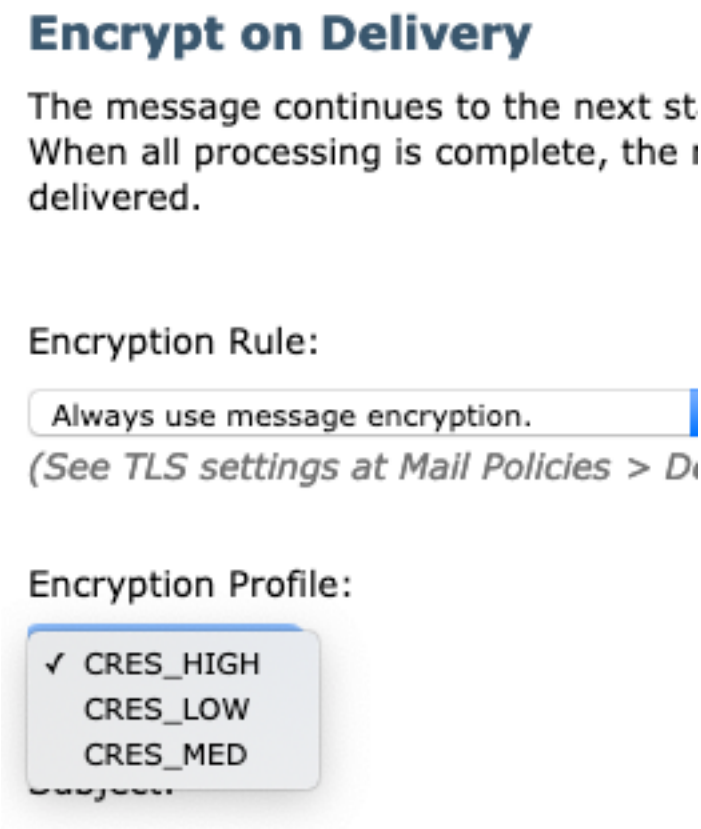
建立加密配置檔案後。 確保已布建，如下圖所示：

要應用這些配置檔案，必須通過內容過濾器將其中的每個配置檔案相關聯。

注意：如果配置檔案不是由內容過濾器呼叫的，則無法應用加密設定。

從ESA導航到**郵件策略> 傳出內容過濾器> 新增過濾器**

一旦在篩選器中配置了使用者、主題、組、發件人等的條件，請定義傳出篩選器的加密級別，如下圖所示：



注意：所有內容過濾器都必須與傳出郵件策略相關聯，才能正常工作。

附註：您可以為託管金鑰服務配置多個加密配置檔案。如果您的組織有多個品牌，這允許您引用PXE信封金鑰伺服器上儲存的不同徽標。

從CLI進行配置

從ESA CLI鍵入encryptionconfig**命**令：

```
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.
```

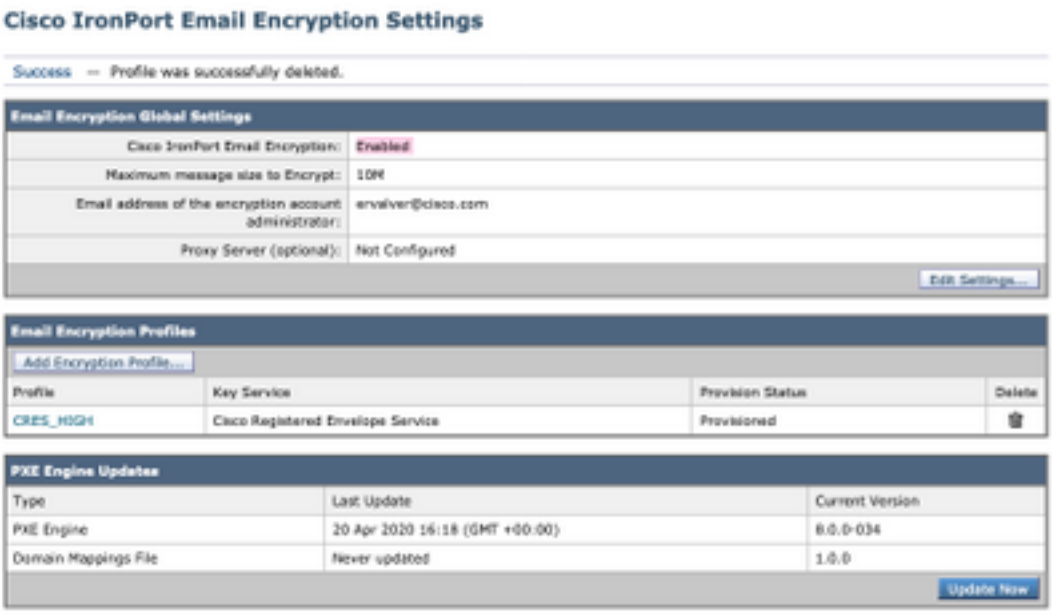
```
Proxy: Not Configured

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
```

驗證

使用本節內容，確認您的組態是否正常運作。

從GUI驗證

從ESA導航到**安全服務>** Cisco IronPort電子郵件加密，如下圖所示：



附註：請確保已啟用加密，且已設定配置的配置檔案。如下圖所示。

從CLI驗證

在CLI中鍵入**encryptconfig**和type profiles命令。

```
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
```

附註：請確保已啟用加密，且已設定配置的配置檔案。如下圖所示。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

從ESA導航到**系統管理>**功能鍵

驗證功能金鑰已應用且處於活動狀態。關鍵：IronPort郵件加密必須處於活動狀態。

從ESA導航到**安全服務> Cisco IronPort郵件加密**

驗證是否正確啟用了加密服務。

驗證加密設定檔是否未處於「Not Provisioned」狀態，如下圖所示：

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**

驗證引擎上次更新，如下圖所示：

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

從郵件跟蹤詳細資訊中，驗證是否顯示錯誤。

最常見的錯誤：

```
5.x.3 - Temporary PXE Encryption failure
```

解決方案：服務當前不可用或無法訪問。檢驗連通性和網路問題。

```
5.x.3 - PXE Encryption failure. (Message could not be encrypted due to a system configuration
issue. Please contact your administrator
```

解決方案：此錯誤與：

- 許可證問題。請驗證功能金鑰
- 未設定使用的配置檔案。從郵件中識別在內容過濾和調配上配置的配置檔案
- 沒有與內容過濾器關聯的配置檔案。有時會刪除加密配置檔案，使用不同的名稱修改加密配置

檔案等。並且配置的內容篩選器找不到關聯的配置檔案

```
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.)
```

解決方案：通常，此問題是由內部發件人的電子郵件客戶端（如Outlook）自動填充收件人電子郵件地址造成的，該電子郵件地址包含無效的「發件人」/「收件人」地址。

這通常是由電子郵件地址的引號或電子郵件地址中的其他非法字元造成的。

相關資訊

- CRES管理指南
- 最終使用手冊
- 技術支援與文件 - Cisco Systems