資料丟失預防和加密的最佳實踐指南

目錄

簡介

本檔案介紹思科電子郵件安全的資料丟失防護(DLP)和加密的最佳實踐。

本文討論使用思科郵件安全裝置(ESA)和基於雲的思科註冊信封服務(RES)設定郵件加密。 客戶可以使用各種型別的策略（包括內容過濾和DLP），通過公共Internet安全地傳送單個郵件。 建立這些策略將在本系列的其他文檔中討論。 本文檔重點介紹ESA準備傳送加密郵件，以便策略可以將加密用作操作。

必要條件

需求

本文件沒有特定需求。

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

本檔案將討論以下步驟：

1. 啟用Cisco IronPort電子郵件加密
2. 向RES註冊您的ESA和組織
3. 建立加密配置檔案
4. 啟用DLP
5. 建立DLP消息操作
6. 建立DLP策略
7. 將DLP策略應用於傳出電子郵件策略

成功完成這些步驟後，ESA管理員可以成功建立將加密用作操作的策略。

Cisco IronPort電子郵件加密也稱為RES加密。 RES是我們用於思科雲中「關鍵伺服器」的名稱。 RES加密解決方案使用對稱金鑰加密 — 這意味著用於加密消息的金鑰與用於解密消息的金鑰相同。 每封加密郵件都使用唯一的金鑰，這樣傳送者就可以對郵件傳送後進行精細控制，例如鎖定郵件或使其過期，以便接收者不再能開啟郵件，而不會影響任何其他郵件。 在對郵件加密時，ESA將加密金鑰和後設資料儲存在CRES中，以供每個加密郵件使用。

ESA可以決定以多種方式加密郵件 — 例如，通過「標籤」（如主題內容）、內容過濾器匹配或DLP策略。 ESA決定加密郵件後，會使用在「安全服務」>「Cisco IronPort郵件加密」（名為「郵件加密配置檔案」）中建立的指定「加密配置檔案」進行加密。 預設情況下，沒有加密配置檔案。 *3.*建立加密配置檔案*中將對此進行討論*。

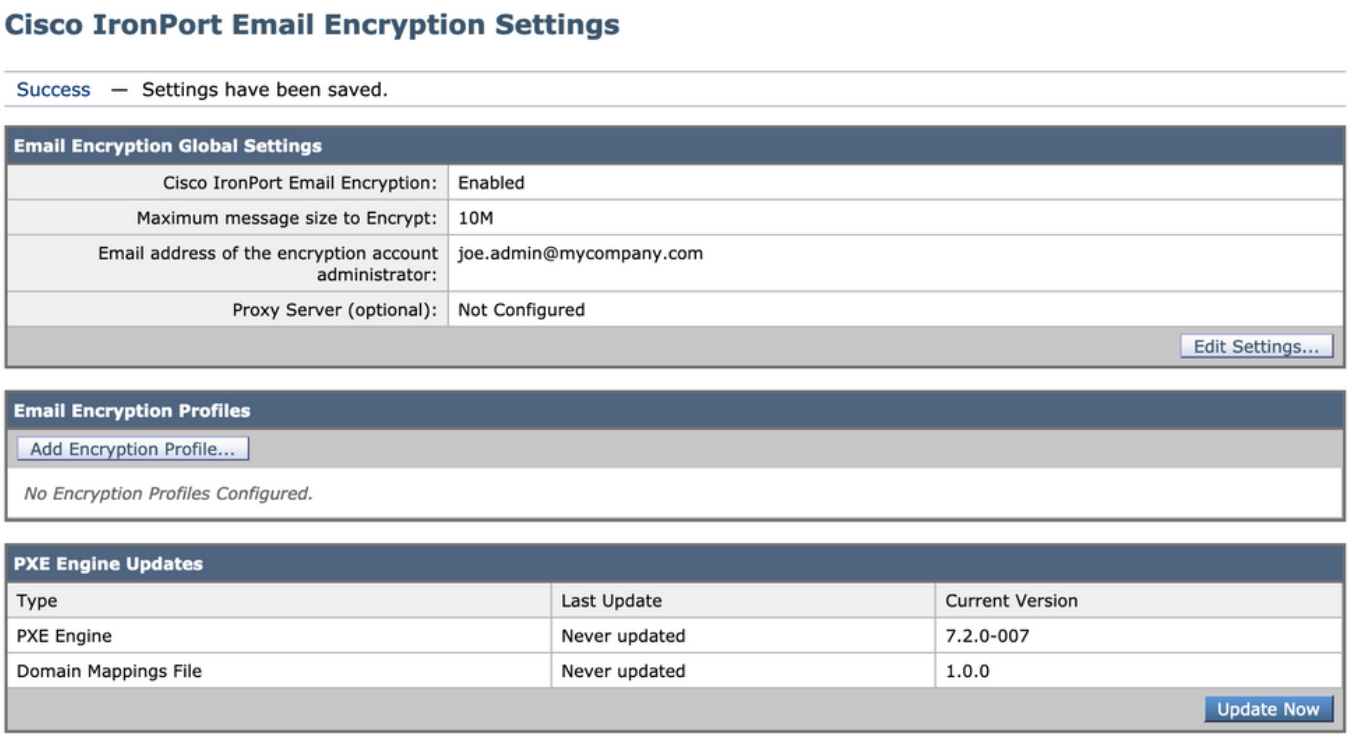
資料丟失防護和加密最佳做法指南

1.在ESA上啟用Cisco IronPort電子郵件加密

> **附註**：如果群集中有多個ESA，則只需執行一次步驟#1，因為這些設定通常在群集級別進行管理。 如果有多台電腦沒有群集化，或者您正在電腦級別管理這些設定，則應在每個ESA上執行步驟#1。

1. 從ESA UI導航至**安全服務> Cisco IronPort郵件加密**。
2. 選中此框以啟用Cisco IronPort電子郵件加密。
3. 接受終端使用者許可協定(EULA)和Cisco IronPort郵件加密許可協定。
4. 在*Email Encryption Global Settings*中，按一下**Edit Settings...** 指定作為帳戶主要RES管理員的管理員/人員的電子郵件地址。 此電子郵件帳戶將與公司的RES環境管理相關聯。可選：要加密的預設最大郵件大小為10M。 如果需要，可以此時增加/減少大小。可選：如果您有ESA需要通過HTTPS連線到RES的代理，請新增必要的代理和身份驗證設定以允許其通過Proxy。
5. 提交並提交您的配置更改。

此時，您應該看到「電子郵件加密全域性設定」設定為類似設定，但是尚未列出配置檔案：



2.向RES註冊您的ESA和組織

第#2步主要參與ESA管理控制檯之外。

> **附註**：ESA註冊資訊也可在以下TechNote中找到：Cisco RES:虛擬、託管和硬體ESA的帳戶調配配置示例

請傳送電子郵件至RES:stg-cres-provisioning@cisco.com。

為了為您的ESA加密配置檔案設定CRES帳戶，請向我們提供以下資訊：

1. 帳戶名**稱（請指定確切的公司名稱，因為您需要列出此名稱。）**對於Cloud Email Security(CES)/託管客戶帳戶，請將您的帳戶名稱以「<Account Name> HOSTED」結尾
2. 要用於帳戶管理員的電子郵件地址(**請指定相應的管理員電子郵件地址)**
3. 完整的裝置序列號 通過「version」命令，可以從ESA GUI（系統管理>功能金鑰）或ESA CLI找到裝置序列號。 提供虛擬許可證編號(VLN)或產品啟用金鑰(PAK)許可證是不可接受的，因為CRES帳戶管理需要完整的裝置序列號。
4. 出於管理目的，應對映到CRES帳戶的域名

附註：如果您已經擁有CRES帳戶，請提供公司名稱或現有的CRES帳號。這將確保將任何新的裝置序列號新增到正確的帳戶中，並避免公司資訊和調配的重複。

請放心，如果您通過郵件傳入有關調配CRES帳戶的資訊，我們將在一個(1)工作日內回覆。如果您需要即時支援和協助，請向Cisco TAC提交支援請求。這可以通過支援案例管理器(https://mycase.cloudapps.cisco.com/case)或通過電話(https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html)來完成。

> **附註**：通過電子郵件傳送此請求後，可能需要一天時間建立您的公司RES帳戶（如果尚未建立

）並新增S/N。 完成此步驟之前，第#3步中的「調配」任務無法工作。

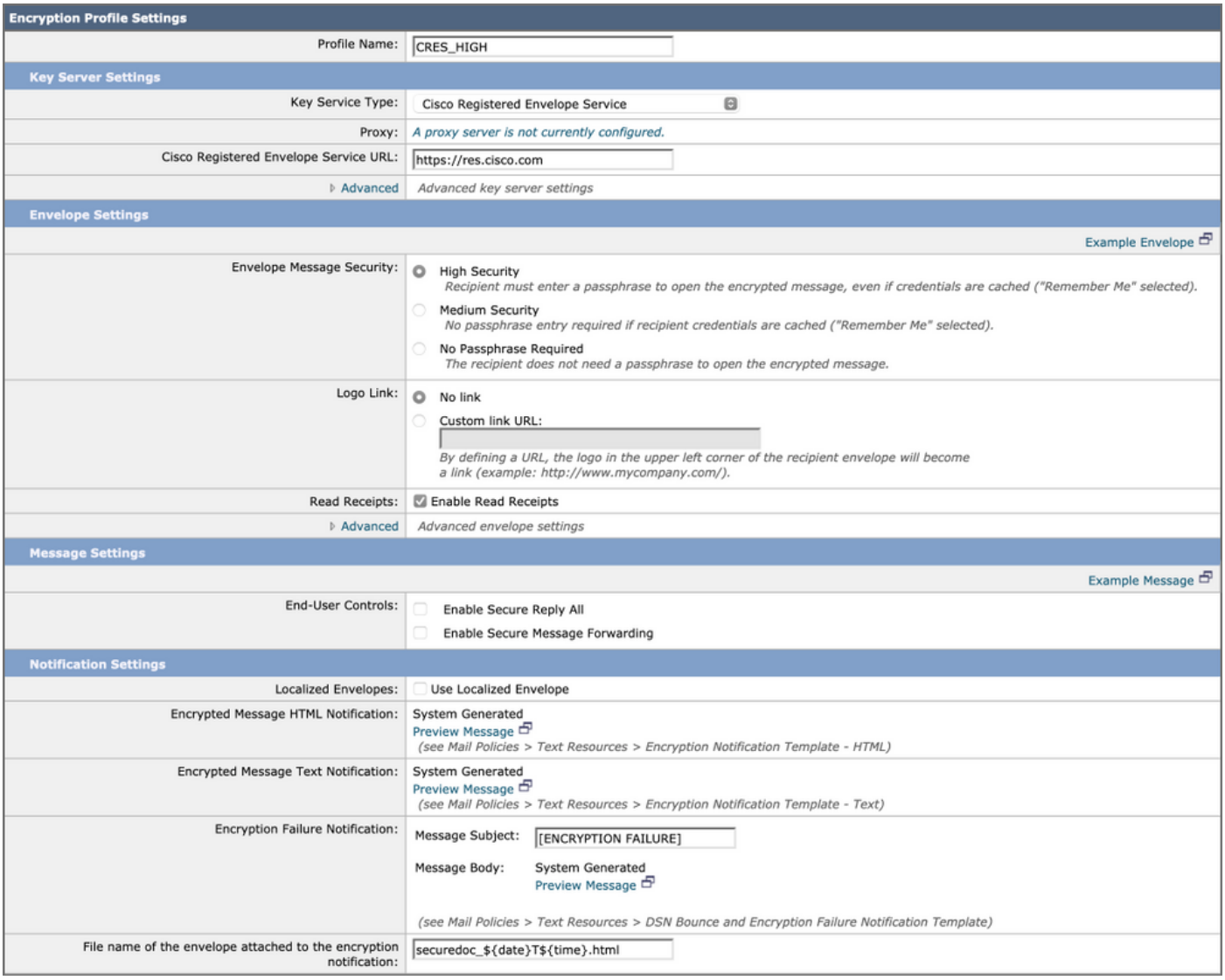
3.在ESA上建立加密配置檔案

> **附註**：如果群集中有多個ESA，則只需執行一次步驟#1，因為這些設定通常在群集級別進行管理。 如果有多台電腦沒有群集化，或者您正在電腦級別管理這些設定，則應在每個ESA上執行步驟#1。

加密配置檔案指定應如何傳送加密消息。 例如，組織可能需要為其收件人的某一部分傳送高安全性信封，例如知道將經常向其傳送高度敏感資料的收件人。 同一組織的收件人社群的其他部分可能收到不太敏感的資訊，也可能對必須提供使用者ID和密碼才能接收加密郵件不太耐心。 這些收件人將是低安全型別信封的良好候選。 擁有多個加密配置檔案使組織可以針對受眾定製加密消息格式。另一方面，許多組織可能只使用一個加密配置檔案就沒問題。

在本文檔中，我們將顯示一個建立三個加密配置檔案的示例，分別名為"CRES_HIGH"、"CRES_MED"和"CRES_LOW"。

1. 從ESA UI導航至**安全服務> Cisco IronPort郵件加密**。
2. 按一下「新增加密配置檔案……」"
3. 將會開啟「加密配置檔案」選單，您可以將第一個加密配置檔案命名為「CRES_HIGH」。
4. 如果尚未選擇「信封郵件安全」，請選擇「高安全性」。
5. 按一下**Submit**儲存此配置檔案。



接下來，重複步驟2-5以建立"CRES_MED"和"CRES_LOW" — 只需更改每個配置檔案的「信封郵件安全性」單選按鈕。

- 對於CRES_HIGH配置檔案，選擇「高安全性」單選按鈕。
- 對於CRES_MED配置檔案，選擇「Medium Security」單選按鈕。
- 對於CRES_LOW配置檔案，選擇「無需密碼」單選按鈕

您會注意到有「啟用已讀回執」、「啟用安全全部回覆」和「啟用安全郵件轉發」的選項。 在「信封設定」中，如果按一下「高級」連結，則可以選擇三種對稱加密演算法之一，並指定傳送信封時不使用Java加密applet。

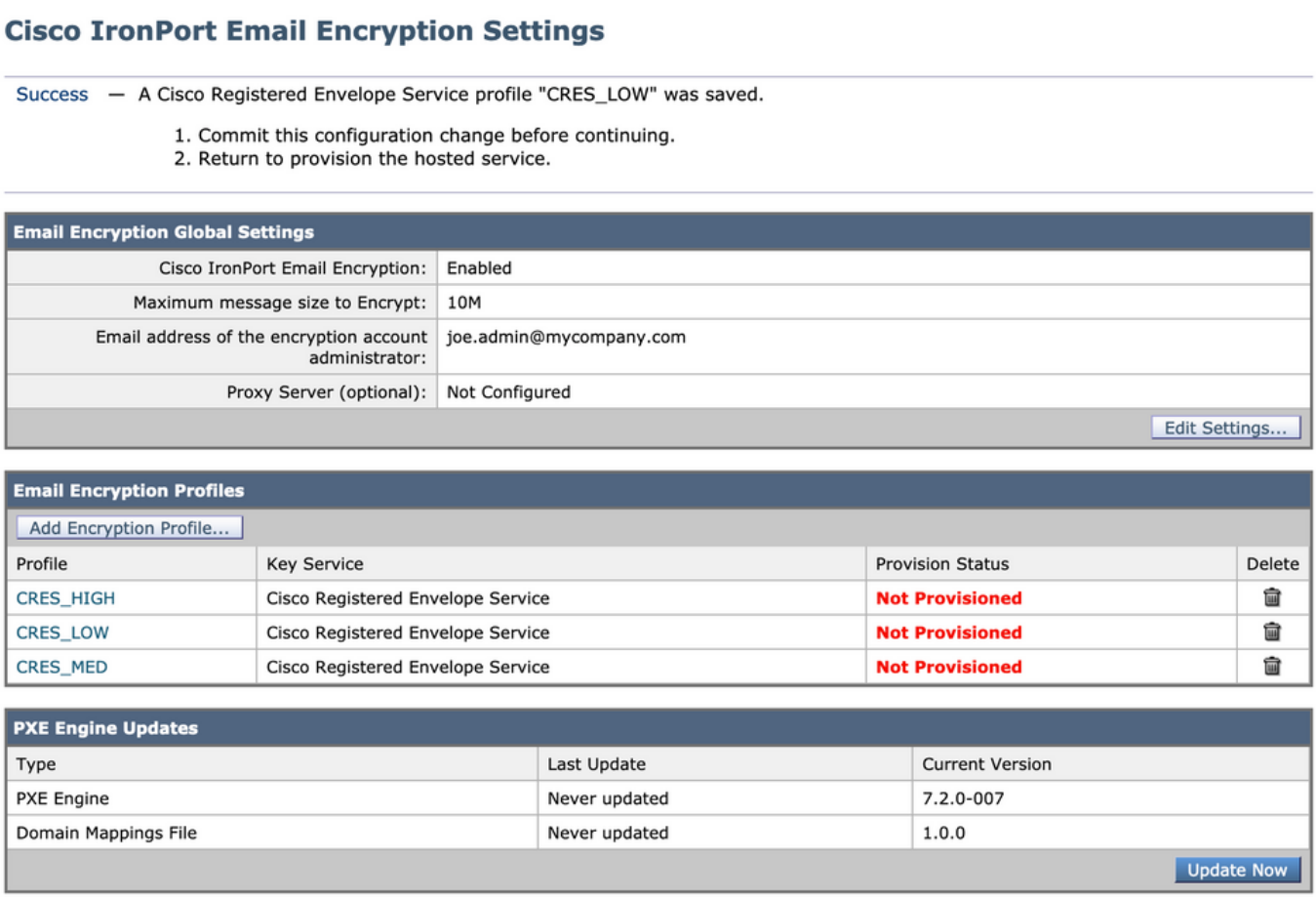
在「信封設定」的右側，您將看到「示例消息」超文本連結。 如果按一下此按鈕，將會向您顯示一個安全郵件信封的示例 — 收件人開啟HTML附件後在電子郵件中看到的內容。

「讀取回執」表示當收件人開啟安全郵件（表示收件人提取對稱金鑰並解密郵件）時，加密郵件的發件人將從CRES接收電子郵件。

在「消息設定」的右側，您將看到「示例消息」超文本連結。 如果按一下此按鈕，將會顯示開啟的郵件將顯示的內容 — 收件人已在信封中提供必要資訊並開啟加密郵件後會看到的內容。

請始終記得按一下**Submit**並提交更改。

然後，表中的行將顯示「調配」按鈕。 提交更改後，才會顯示「預配」按鈕。

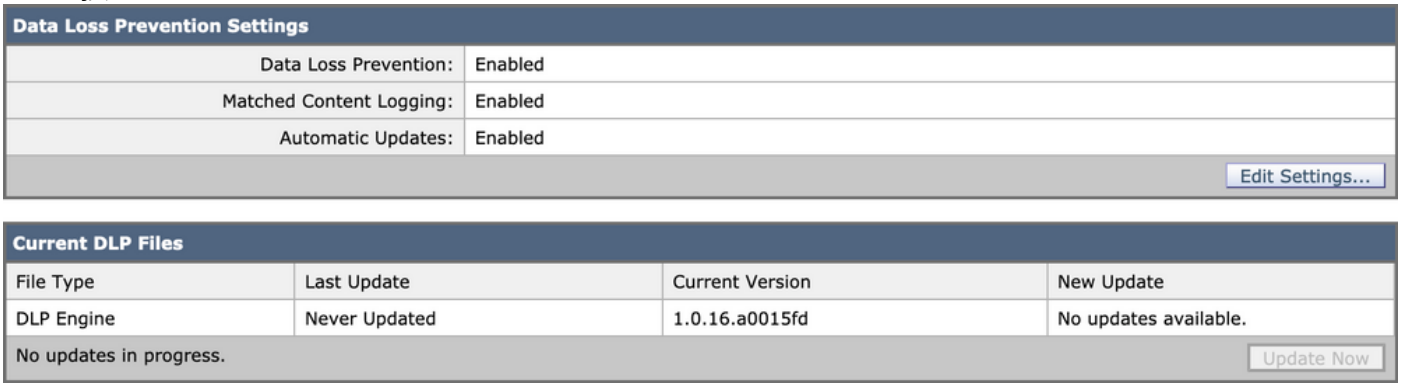


再次按一下Provision按鈕，僅在建立公司RES帳戶並將裝置S/N新增到您的帳戶後才能使用此功能。 如果RES帳戶連結到ESA，調配過程將相對較快地進行。 如果沒有，那麼這個過程必須首先完成。

調配完成後，您的Cisco IronPort郵件加密頁面會將配置檔案顯示為已調配。

4.啟用資料丟失防護(DLP)

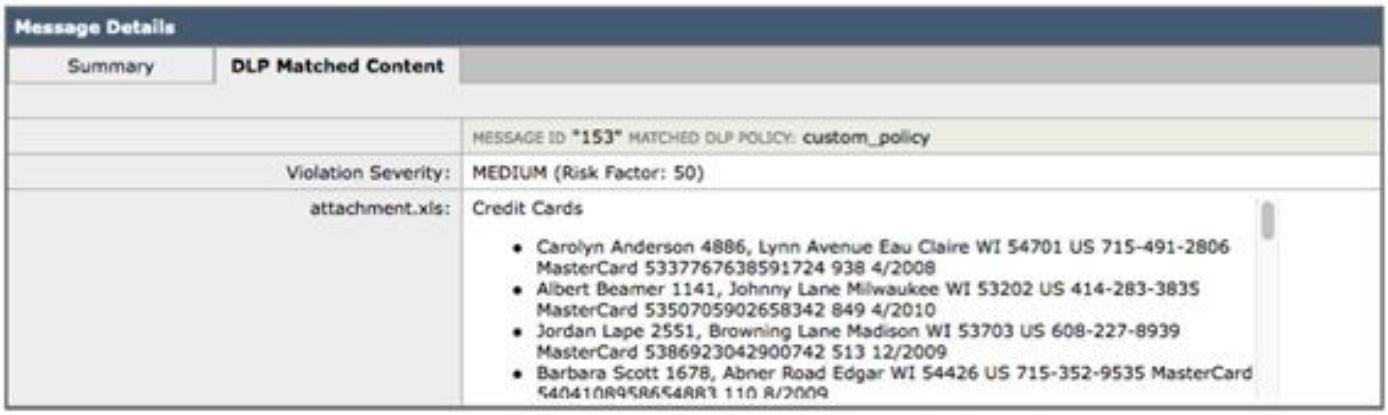
1. 從ESA UI導航到**Security Services > Data Loss Prevention**。
2. 按一下**Enable...**以啟用DLP。
3. 接受EULA、資料丟失保護許可協定。
4. 按一下「啟用匹配的內容日誌記錄」覈取方塊。
5. 按一下啟用自動更新覈取方塊。
6. 按一下「**Submit**」。



裝置上的DLP引擎和預定義內容匹配分類器的更新與其他安全服務的更新無關。3-5分鐘的常規

Talos簽名更新不同，不包括更新DLP策略和字典。必須在此處啟用更新。

啟用「匹配的內容記錄」後，允許郵件跟蹤顯示導致違規的電子郵件的內容。以下是顯示導致DLP違規的電子郵件內容的郵件跟蹤示例。 這樣，管理員可以準確瞭解觸發特定DLP策略的資料。



防資料丟失違規

5.建立防資料丟失消息操作

建立DLP隔離區

如果要保留違反DLP策略的郵件副本，可以為每種型別的策略違規建立單獨的策略隔離區。在運行「透明」POV時，這尤其有用，因為會記錄並傳送違反DLP策略的出站消息，但對消息不執行任何操作。

1. 在SMA上，導航到**電子郵件>郵件隔離>策略、病毒和爆發隔離**
2. 開始之前，隔離區表應如下所示
   ：

Policy, Virus and Outbreak Quarantines

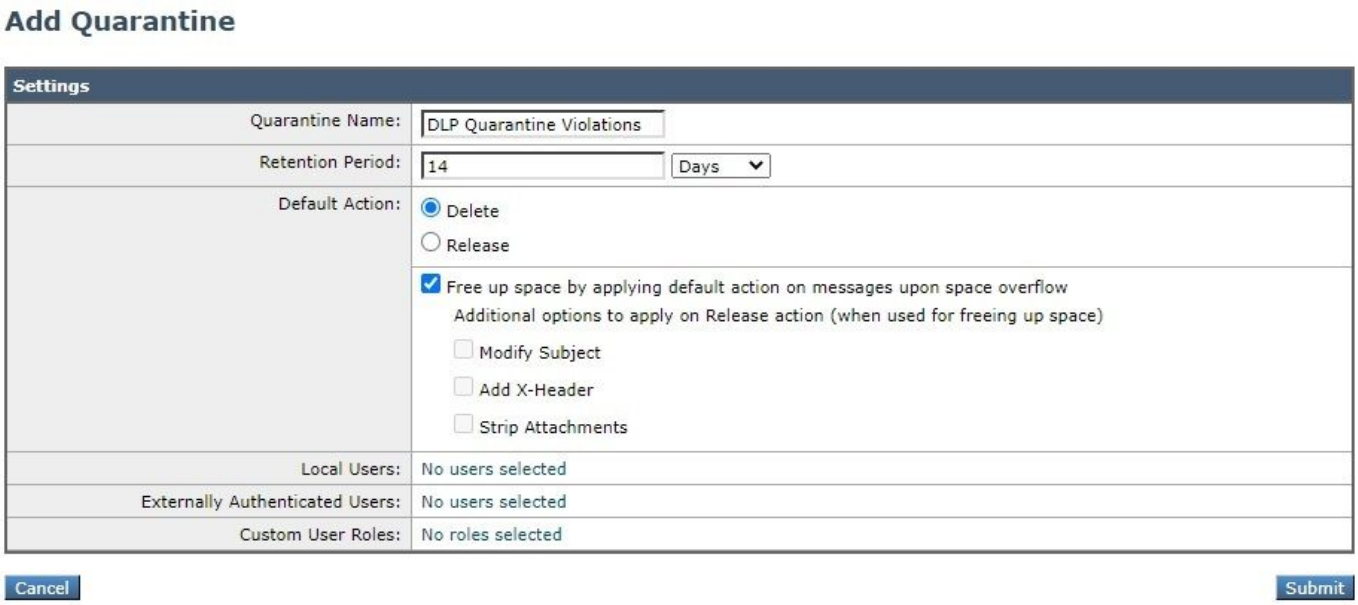
Add Policy Quarantine... | Search Across Quarantines

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.

   策略病毒和爆發隔離
3. 按一下「新增策略隔離」按鈕，並建立要由DLP策略使用的隔離。

以下是針對中型DLP違規進行的隔離示例。隔離區分段是可能的，並且可能適用於多個DLP規則：



DLP隔離示例

關於DLP消息操作

DLP消息操作描述了ESA在檢測到傳出電子郵件中的DLP違規時將採取的操作。您可以指定主要和輔助DLP操作，並且可以為不同的違規型別和嚴重性分配不同的操作。

主要操作包括：

- 交付
- drop
- 隔離

對於只讀狀態，即會記錄和報告DLP違規，但郵件不會被停止/隔離或加密，則通常使用「傳送」操作。

輔助操作包括：

- 將副本傳送到任何自定義隔離區或「策略」隔離區。
- **加密訊息。**裝置僅加密郵件正文。不會加密郵件標頭。
- 變更主題標題。
- 向郵件新增免責宣告文本/HTML。
- 將郵件傳送到備用目標郵件主機。
- 正在傳送郵件的密件抄送副本。
- 向發件人和/或其他聯絡人傳送DLP違規通知。

這些操作不是相互排斥的 — 您可以將其中一些操作組合到不同的DLP策略中，以滿足不同使用者組的各種處理需求。

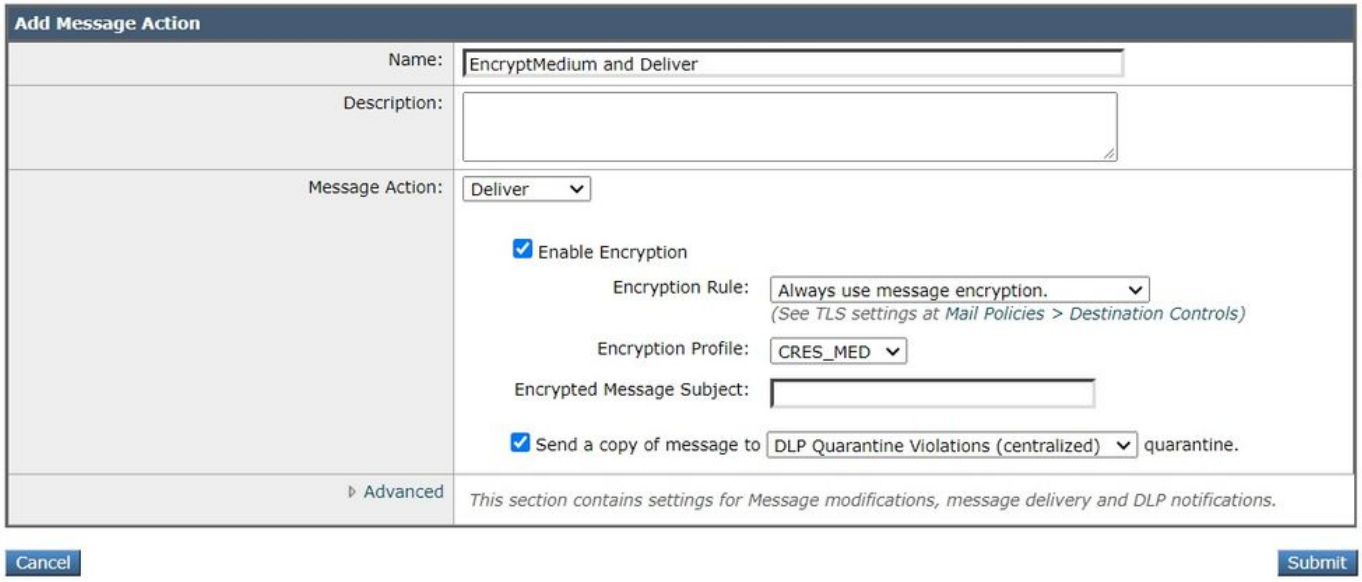
我們將實施以下DLP操作：**Encrypt**

這些操作假定加密已在ESA上許可和配置，並且已按照前面幾節中的步驟為高、中和低安全性建立了三個配置檔案：

- CRES_HIGH
- CRES_MED
- cres_LOW

建立DLP消息操作

1. 轉到*郵件策略> DLP郵件自定義。*
2. 按一下「新增消息操作」按鈕並新增以下DLP操作。 確保在提交郵件操作後提交更改



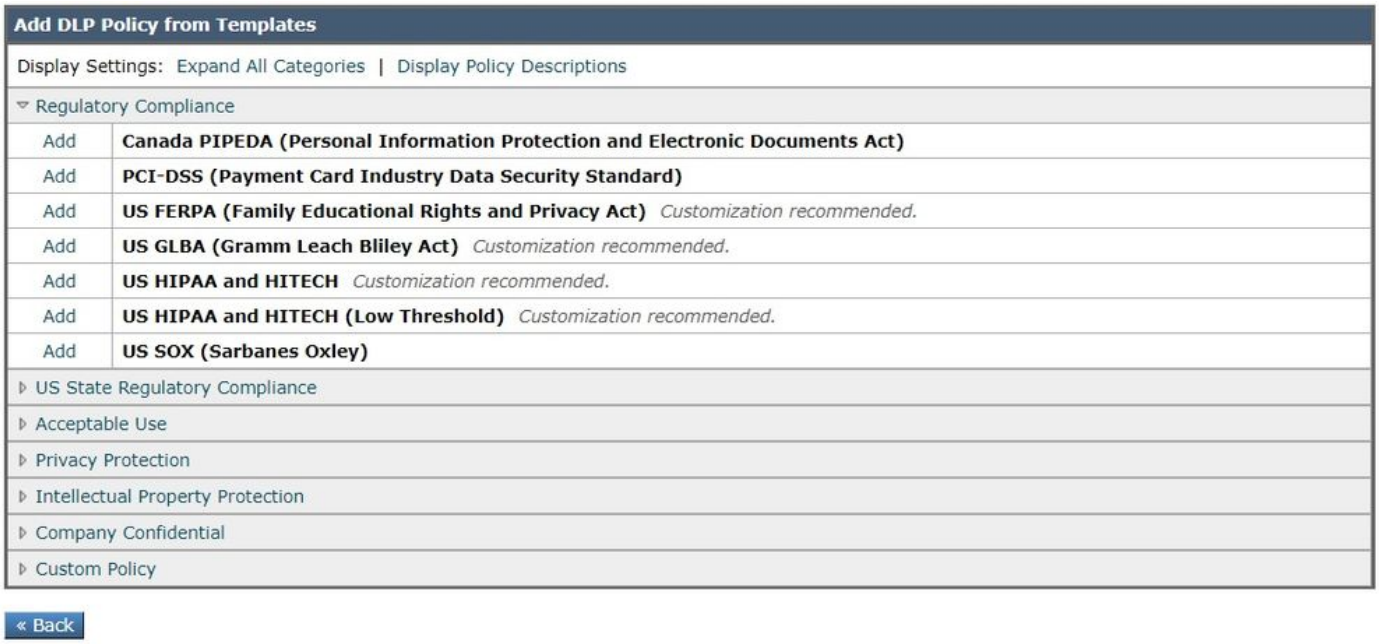
郵件操作

6.制定資料丟失防護策略

DLP策略包括：

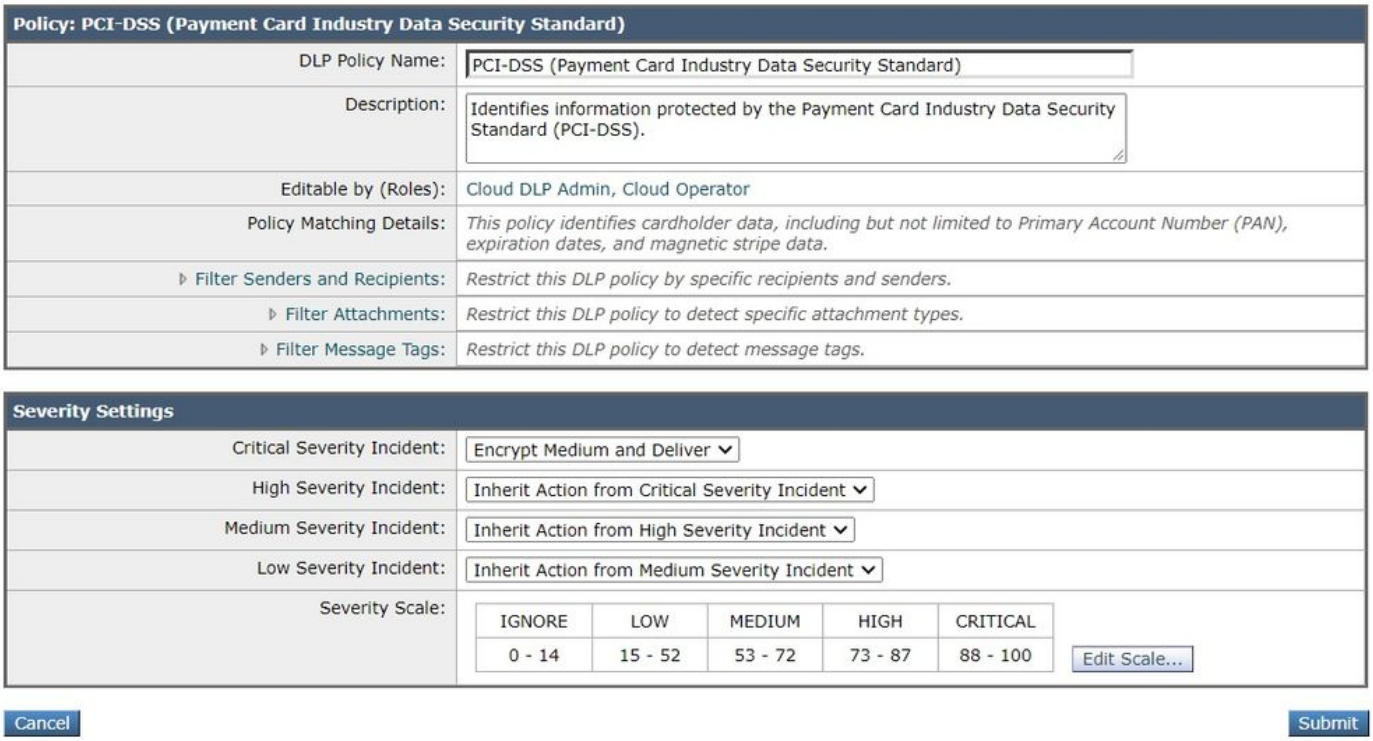
- 確定傳出郵件是否包含敏感資料的一組條件
- 消息包含此類資料時要執行的操作。

1. 導航到：*Mail Policies > DLP Policy Manager*
2. 單擊*「新增DLP策略」*
3. 開啟「合規性」披露三角形。



DLP策略模板

4.對於PCI策略，按一下PCI-DSS左側的「新增」按鈕。



PCI-DSS示例DLP規則

5.對於嚴重性嚴重性事件，選擇我們之前配置的「加密介質並傳送」操作。我們可以更改嚴重性較低的突發事件，但就目前而言，讓我們讓它們繼承我們的嚴重性突發事件。提交，然後提交更改。

7.將DLP策略應用於傳出電子郵件策略

1. 導覽至：郵件策略>傳出郵件策略
2. 點選預設策略的DLP的控制單元格。如果尚未啟用，則會顯示為「已禁用」。
3. 將「禁用DLP」下拉按鈕更改為「啟用DLP」，您將立即看到剛剛建立的DLP策略。
4. 按一下「啟用全部」覈取方塊。提交，然後提交更改。

結論

總而言之，我們展示了準備思科電子郵件安全裝置以傳送加密電子郵件的必要步驟：

1. 啟用Cisco IronPort電子郵件加密
2. 向RES註冊您的ESA和組織
3. 建立加密配置檔案
4. 啟用DLP
5. 建立DLP消息操作
6. 建立DLP策略
7. 將DLP策略應用於傳出電子郵件策略

與您的ESA軟體版本對應的《ESA使用手冊》提供了更多詳細資訊。 使用手冊位於以下連結：

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

相關資訊

- 技術支援與文件 - Cisco Systems