將思科電子郵件威脅防禦(ETD)與思科安全訪問整合的步驟：

目錄

簡介

本文檔說明了在ETD SMTP內聯模式下將Cisco Email Threat Defense(ETD)與Cisco Secure Access(SA)整合到Email DLP的步驟。這可確保所有通過ETD的出站電子郵件在思科安全訪問(SA)的幫助下被掃描以獲取DLP。

概觀

在當今的分散式工作環境中，電子郵件仍是企業的主要通訊工具，因此也是網路攻擊和資料洩露的最常見目標。為了應對這些不斷演變的挑戰，思科通過郵件威脅防禦(ETD)和安全訪問郵件資料丟失防護(DLP)提供全面的郵件安全方法。

通過將思科電子郵件威脅防禦的威脅檢測功能與安全訪問電子郵件DLP的強大資料保護功能相結合，組織可以制定多層防禦策略。這種方法不僅能保護來自外部參與者的收件箱，還能確保敏感的企業資料受到嚴格控制，而不管使用者位於何處，也不管使用者以何種方式訪問其電子郵件。

必要條件

訪問下面的控制檯。

1. 內嵌模式下的思科電子郵件威脅防禦主控台(ETD)。

   ETD控制檯用作您的郵件安全狀態的集中管理平面。訪問此控制檯是配置您的環境以防禦高級威脅的第一步。

   - 為什麼「內嵌模式」很重要：在內嵌模式中設定ETD時，它充當郵件傳輸代理(MTA)或位於郵件流路徑中的直接整合。這樣，系統便可以在郵件傳送到接收人的收件箱之前檢查、阻止或修改郵件。
2. 思科安全存取主控台(SA)

思科安全訪問是統一雲交付的安全平台，可將包括資料丟失防護(DLP)在內的各種安全服務整合到單個聚合架構中。

- 為什麼需要SA控制檯：安全訪問控制檯是組織安全策略的協調中心。當ETD處理威脅特定的電子郵件流時，您可在安全訪問控制檯中定義更廣泛DLP策略，以控制如何在整個企業中識別和處理敏感資料。
- 控制檯角色：此控制檯允許管理員建立和應用資料分類規則（例如，識別PII、信用卡號或內部專案代碼）。 通過訪問SA控制檯，您可以確保電子郵件DLP策略與您的整體安全策略同步，從而在兩個電子郵件流量之間實現一致的實施。

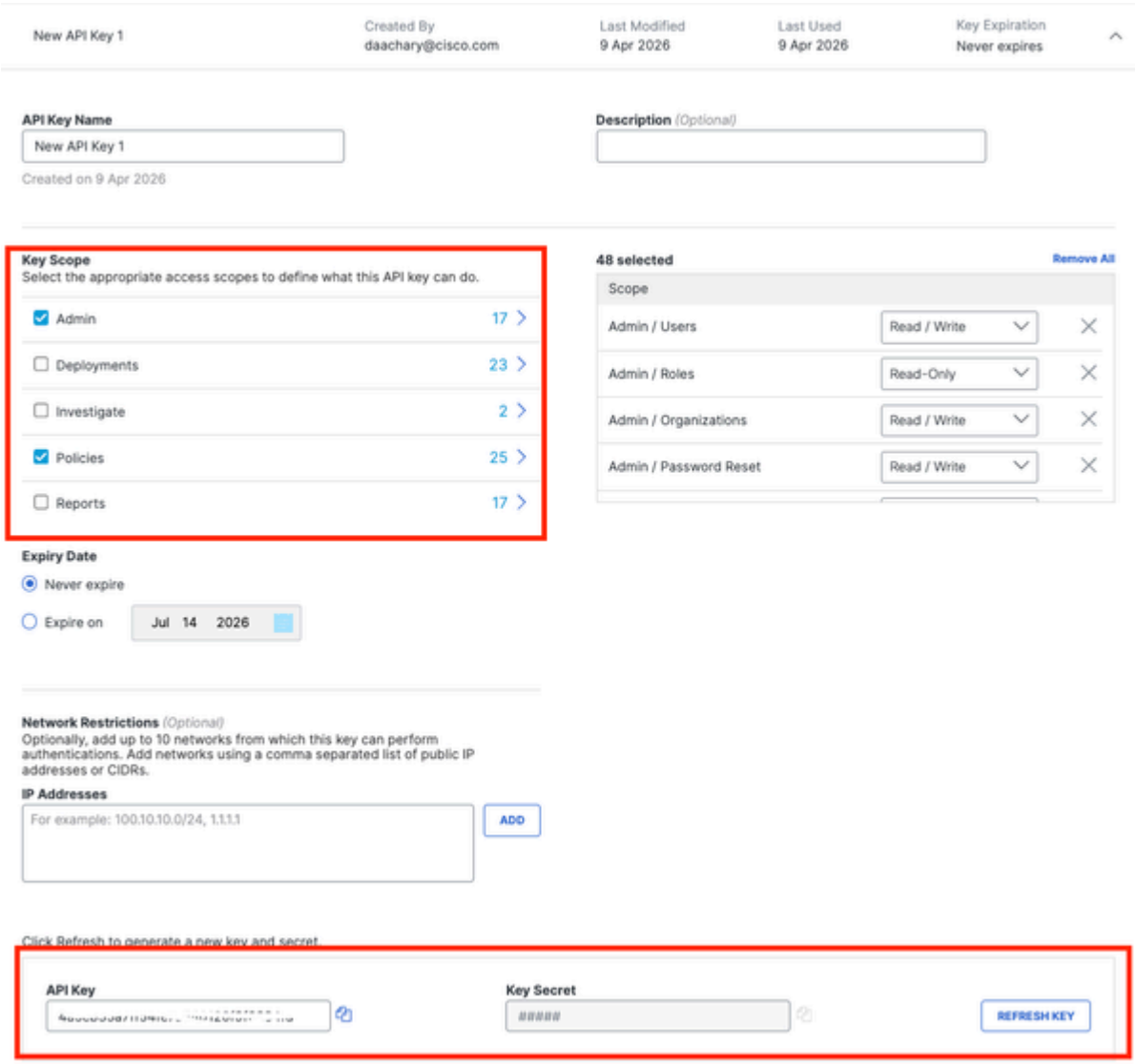
設定

整合步驟

步驟 1:在Cisco Secure Access中生成API憑證

要開始，您必須在安全訪問控制檯內生成必要的API憑據以授權連線。

1. 登入到Cisco Secure Access控制板。
2. 導覽至Admin>API Keys。
3. 選擇該選項以建立新的API金鑰。
4. 將以下範圍分配給金鑰:AdminandPolicy。
   - [螢幕截圖:安全訪問API金鑰配置]



步驟 2:配置金鑰過期

根據組織的安全策略定義API金鑰的生命週期。

- 選項 1:永不過期 — 提供不間斷服務，無需手動輪換。
- 選項 2:特定日期 — 設定已定義的到期時間表。
  - 重要說明：如果選擇設定到期日，請確保計畫輪換流程。必須在到期日期之前重新配置ETD控制檯中的API金鑰，以防止DLP服務中斷。

步驟 3:保護您的憑據

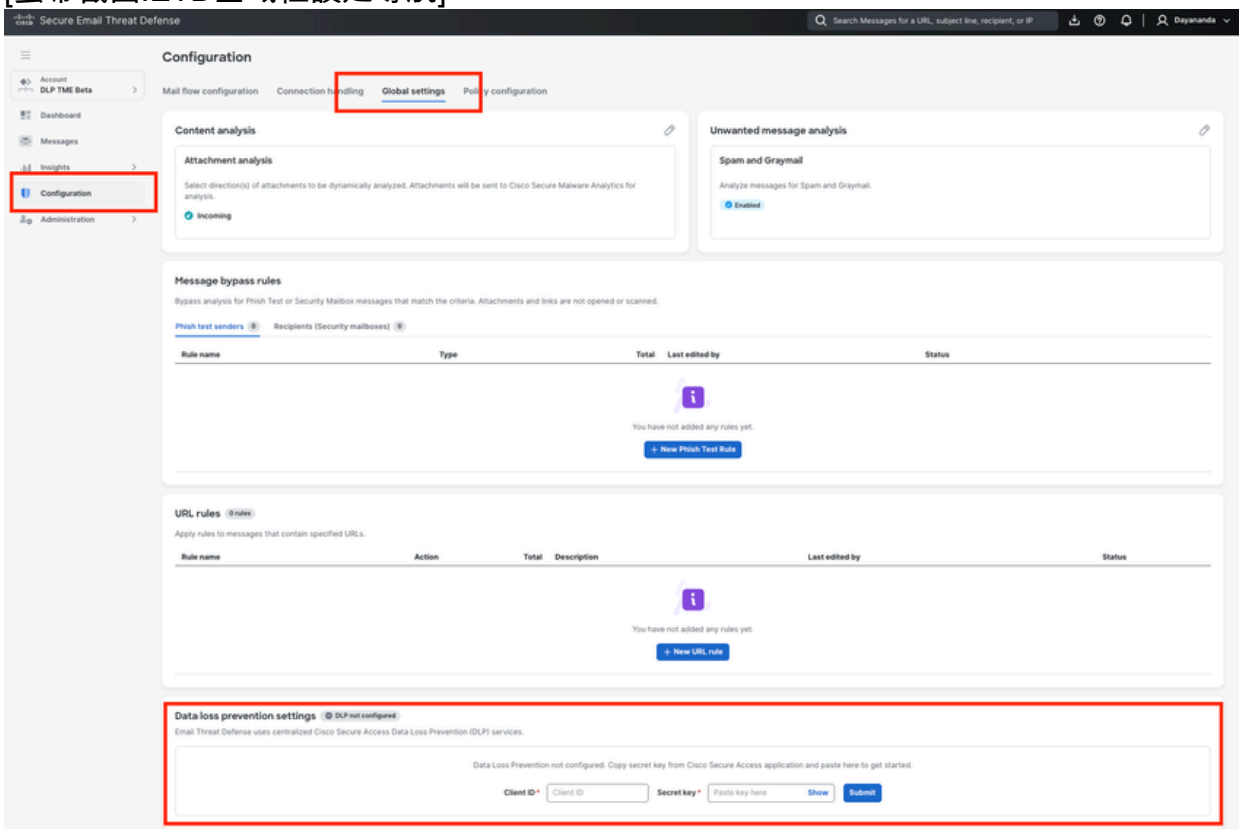
生成金鑰後，系統將顯示API Key和Key Secret。

- 操作：將這些憑證複製並儲存到一個安全位置（例如，密碼管理器）。
- 警告：導出此螢幕後，Key Secretate將不可見。如果丟失，您將需要生成新的金鑰對。

步驟 4:訪問ETD配置

如果您的憑證受到保護，請前往ETD控制檯完成連結。

1. 登入到Cisco ETDconsole。
2. 導覽至Configuration>Global Settings。
    - [螢幕截圖:ETD全域性設定導航]
    -



步驟 5:最終確定整合

通過輸入從Secure Access獲得的憑據完成握手。

1. 在Global Settings選單中，找到Data Loss Prevention(DLP)部分。
2. 輸入您在第3步中儲存的Client ID(API Key)和Secret Key(Key Secret)。
3. 儲存更改。

成功驗證後，思科ETD和思科安全訪問之間的整合已完成，您的DLP策略將準備就緒，可在您的電子郵件流量中實施。

現在，ETD和安全接入的整合已經完成。
附註：請參閱如何在思科安全訪問(SA)和思科郵件威脅防禦(ETD)中配置郵件DLP策略」，以在思科安全訪問中為郵件DLP建立DLP策略。

疑難排解說明

如果在整合過程中或整合之後遇到問題，請檢視以下常見方案和補救步驟：

1. ETD中未接受API憑證

- 症狀：在ETD中輸入客戶端ID和金鑰時，系統返回身份驗證錯誤。
- 解析度：
  - 驗證API金鑰是否使用完全所需的作用域：「Admin」和「Policy」建立。如果選擇了其他作用域或這些作用域丟失，連線將失敗。
  - 將客戶端ID或金鑰貼上到ETD控制檯時，請確保不會意外複製前導或尾部空格。

2.丟失或遺忘的金鑰金鑰

- 症狀：您已導航離開Secure Access API建立螢幕，並且無法再檢視金鑰金鑰。
- 解決方案：出於安全原因，金鑰金鑰僅在建立時顯示一次。如果您沒有安全地儲存它，則必須刪除Secure Access中未完成的API金鑰並生成一個新金鑰。

3. DLP策略未對電子郵件流量強制實施

- 症狀：整合顯示成功，但配置的DLP策略無法捕獲或阻止敏感電子郵件。
- 解析度：
  - 檢查API過期：如果您為API金鑰過期選擇了「選擇特定日期」（步驟2），請驗證金鑰是否未過期。如果存在，則必須生成並應用新的金鑰對。
  - 驗證ETD部署模式：確保以內聯模式部署Cisco ETD。ETD必須位於直接郵件流路徑中，才能根據安全訪問DLP裁決主動阻止或修改郵件。
  - 同步時間：初次整合後，請允許後端系統在測試DLP規則之前同步策略。

4.穩定時期後的服務中斷

- 症狀：DLP實施在正常運行幾個月後突然停止工作。
- 解析度：這通常是由過期的API金鑰導致的。導航至Admin -> API Keyin Cisco Secure Access以檢查用於ETD的金鑰的狀態。實施金鑰輪替流程，以在到達到期日期之前更新

ETD中的憑據。

摘要

將思科電子郵件威脅防禦(ETD)與思科安全訪問(SA)整合是建立統一資料丟失防護(DLP)策略的關鍵步驟。通過在安全訪問控制檯中生成具有「管理」和「策略」範圍的安全API金鑰，並在ETD的全域性設定中配置這些憑據，管理員可在兩個平台之間建立無縫的通訊網橋。

此握手完成後，ETD可以主動將電子郵件後設資料傳遞給安全訪問DLP引擎。這使您的組織能夠從單個集中控制面板（安全訪問）管理所有資料保護策略，同時保持對您的電子郵件流量(ETD)的深入可視性和強制性。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。