如何在思科安全訪問(SA)和思科電子郵件威脅防禦(ETD)中配置電子郵件DLP策略

目錄

簡介

電子郵件仍然是非故意或未經授權的資料暴露的最常見管道之一。為幫助組織保護通過電子郵件共

用的敏感資訊，思科通過整合思科安全訪問(SA)和思科郵件威脅防御(ETD)，提供電子郵件資料丟失防范(DLP)功能。

在此架構中，所有電子郵件DLP策略建立、配置和實施操作均在Cisco Secure Access中執行。思科郵件威脅防禦提供郵件可視性和郵件跟蹤，而思科安全訪問則充當定義DLP規則和實施行為的策略引擎。

本文說明如何使用預定義的DLP模板或自定義DLP模板，在Cisco安全訪問中建立電郵DLP策略。

必要條件

開始配置過程之前，請確保滿足以下要求：

- 管理訪問：您必須對思科郵件威脅防禦內聯控制檯和思科安全訪問控制檯具有「完全管理員」許可權。
- 活動訂閱：確保您的電子郵件威脅防禦和安全訪問租戶均處於活動狀態且已調配。
- 連線：必須成功建立郵件威脅防禦和安全訪問之間的API整合。
- 郵件流配置：必須在內聯模式中正確部署電子郵件威脅防禦，以確保它正在主動檢查電子郵件流量。

重要：雖然此解決方案同時使用思科安全訪問和思科郵件威脅防禦，但本文中介紹的所有郵件DLP規則配置步驟都僅在思科安全訪問中執行。

要求和採用元件

要成功實施電子郵件DLP策略，需要使用以下元件：

- 思科電子郵件威脅防禦(ETD):充當電子郵件檢查點。它捕獲出站電子郵件流量，並促進DLP引擎執行分析所需的通訊流。
- 思科安全訪問(SA)- DLP引擎：這是所有DLP配置駐留的主要元件。您將使用Secure Access控制檯定義：
    - 資料標識符：系統應監控的特定模式或敏感資料型別（例如PII、信用卡號或內部專案代碼）。
    - DLP策略：規定系統在檢測到敏感資料（如阻止、加密或通知）時如何反應的規則。
    - 策略操作：由DLP引擎觸發的自動響應，例如阻止傳送電子郵件或應用強制加密。
- 整合框架：允許ETD將電子郵件後設資料傳遞給安全訪問DLP引擎以進行策略評估和後續實施的後端連線。

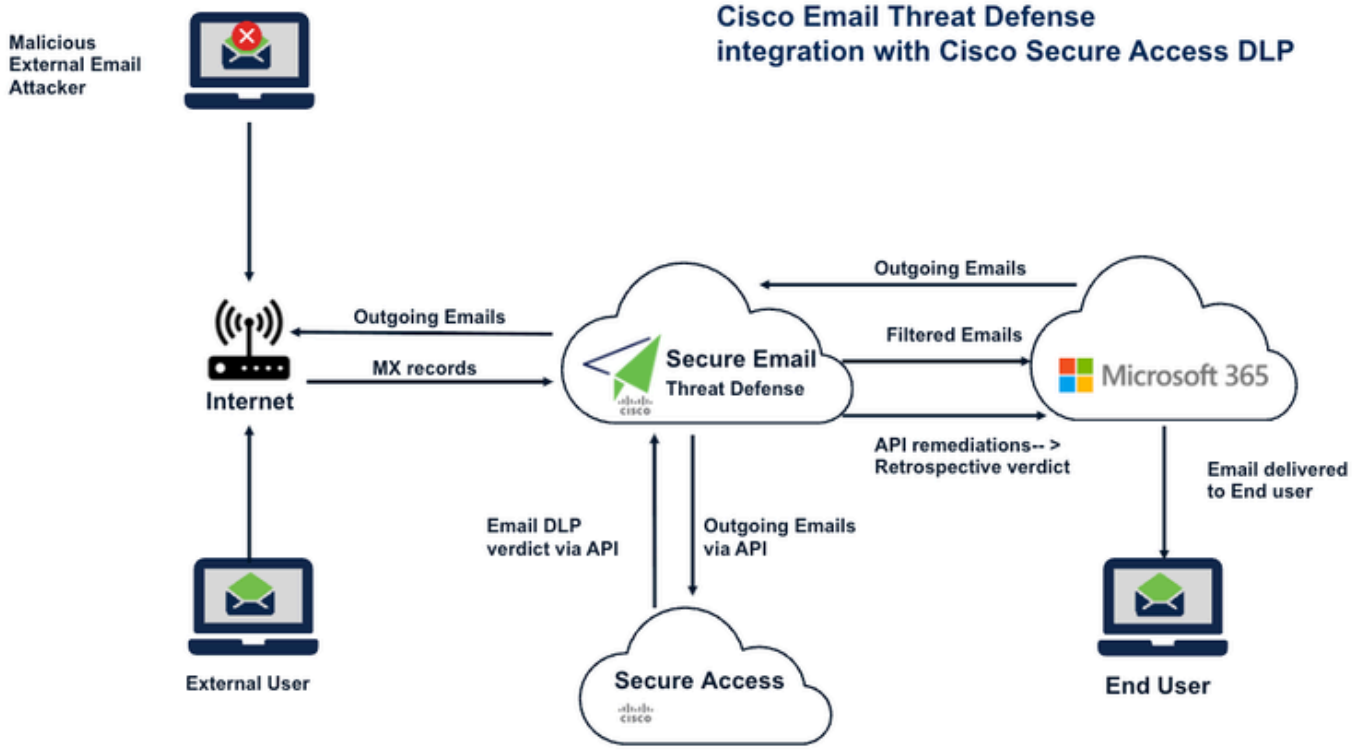
電子郵件DLP策略功能

在Cisco Secure Access中建立電子郵件DLP策略時，可以配置：

- 規則名稱和說明
- 嚴重性級別
- 資料分類
- 檢查範圍，包括：
  - 電子郵件主題
  - 郵件正文
  - 附件名稱
  - 附件內容
- 檔案控制元件，包括：
  - MIP標籤
  - 提圖斯標籤
- 發件人條件
- 收件人條件
- 策略操作：
  - 監視
  - 封鎖
- 可選的使用者通知

網路圖表

找到說明思科安全郵件威脅防禦與思科安全訪問整合的網路圖以及流量流程圖。



附註：在上圖中，Exchange伺服器是O365，但此DLP配置可以在支援SMTP的任何Exchange伺服器上完成。

附註：請參閱「將思科電子郵件威脅防禦(ETD)與思科安全訪問整合的步驟：」文章，以通過API整合思科電子郵件威脅防禦和思科安全訪問。

設定

在思科安全訪問中配置電子郵件DLP策略

步驟 1:登入到Cisco Secure Access

使用具有所需許可權的管理員帳戶登入到Cisco Secure Access(SA)控制檯。

步驟 2:導航到Email DLP Rule Creation

從Secure Access控制面板導航至：

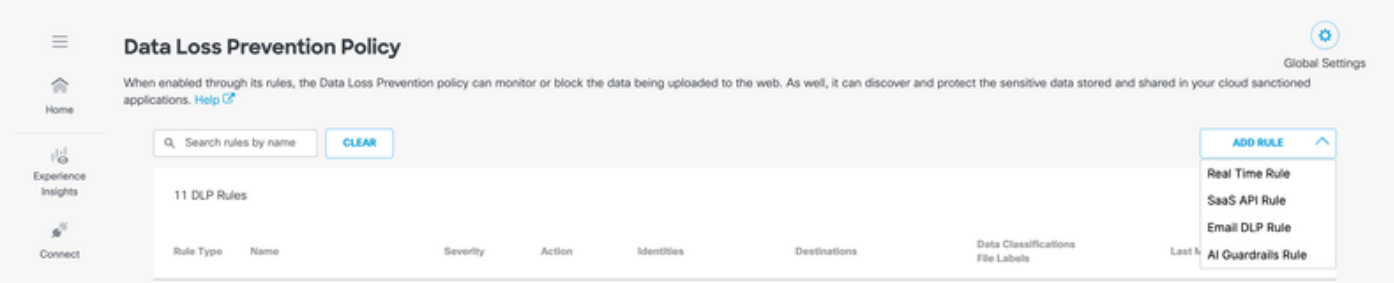
Secure > Policy > Data Loss Prevention Policy > Add Rule > Email DLP Rule

這將開啟Add New Email Rule頁。

Cisco Secure Access提供了兩種建立電子郵件DLP規則的方法：

- 使用預定義的DLP模板建立電子郵件DLP規則
- 使用自定義DLP模板建立電子郵件DLP規則

圖1.導航至電子郵件DLP規則建立



選項 1:使用預定義的DLP模板建立電子郵件DLP規則

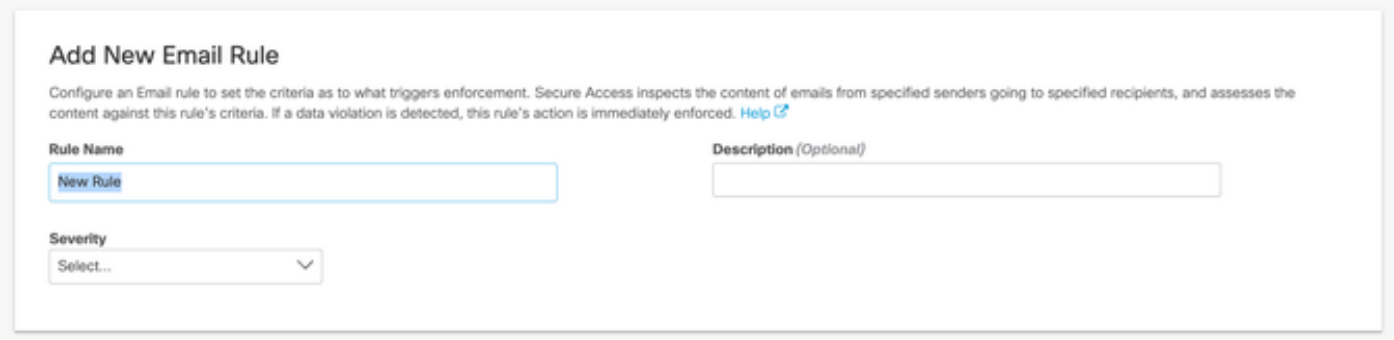
步驟 3:配置基本規則資訊

導航到ADD RULE > Email DLP Rule視窗，

在Add New Email Rule視窗中，輸入以下詳細資訊：

- 規則名稱
  輸入電子郵件DLP規則的描述性名稱。
- 說明
  提供規則的用途的簡短摘要。
- 嚴重性
  為策略選擇相應的嚴重性級別：
    - 低
    - 中
    - 高
    - 嚴重

這些欄位有助於對規則進行分類，以實現管理、報告和操作可視性。



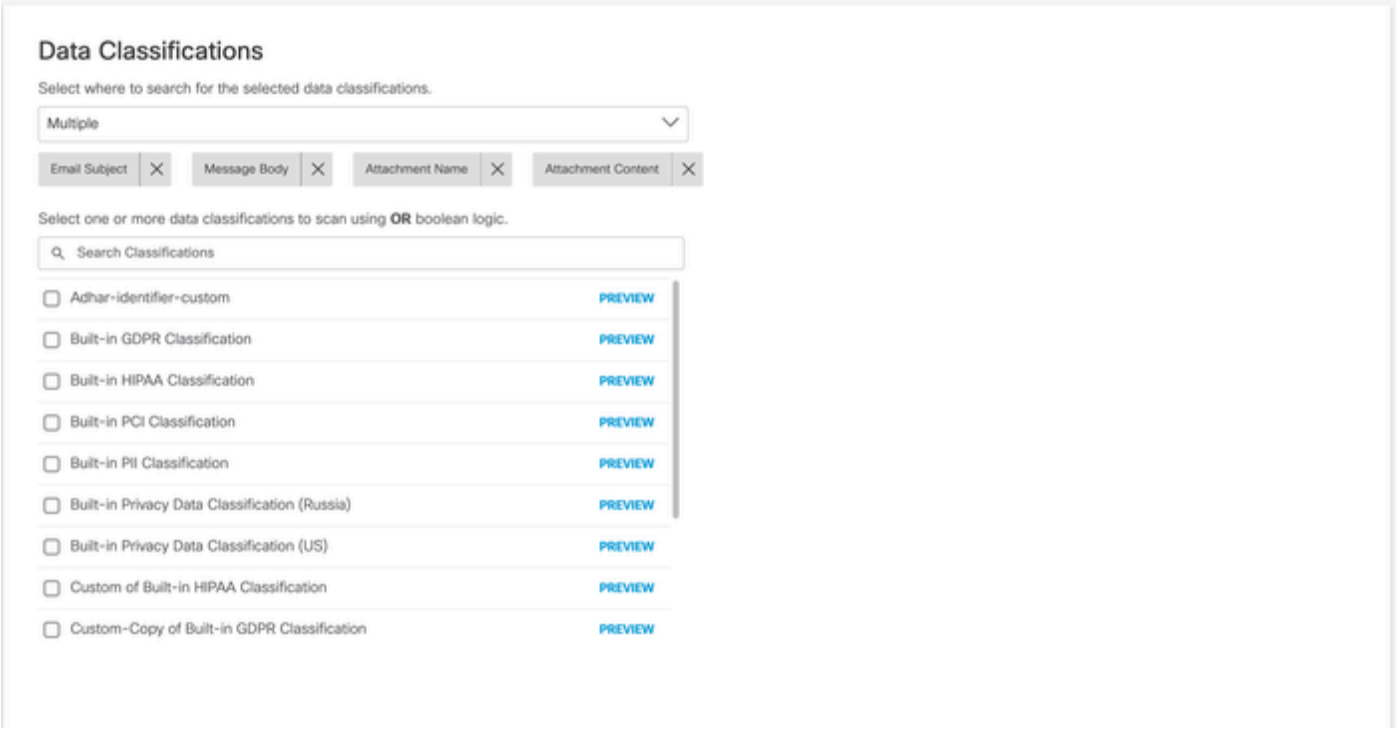
步驟 4:選擇資料分類

在Data Classifications下，選擇用於檢查電子郵件內容是否存在潛在DLP違規的預定義DLP模板。

接下來，選擇應匹配所選分類的位置。支援的檢查位置包括：

- 電子郵件主題
- 郵件正文
- 附件名稱
- 附件內容

這允許策略檢查郵件內容和附件中的敏感資訊。



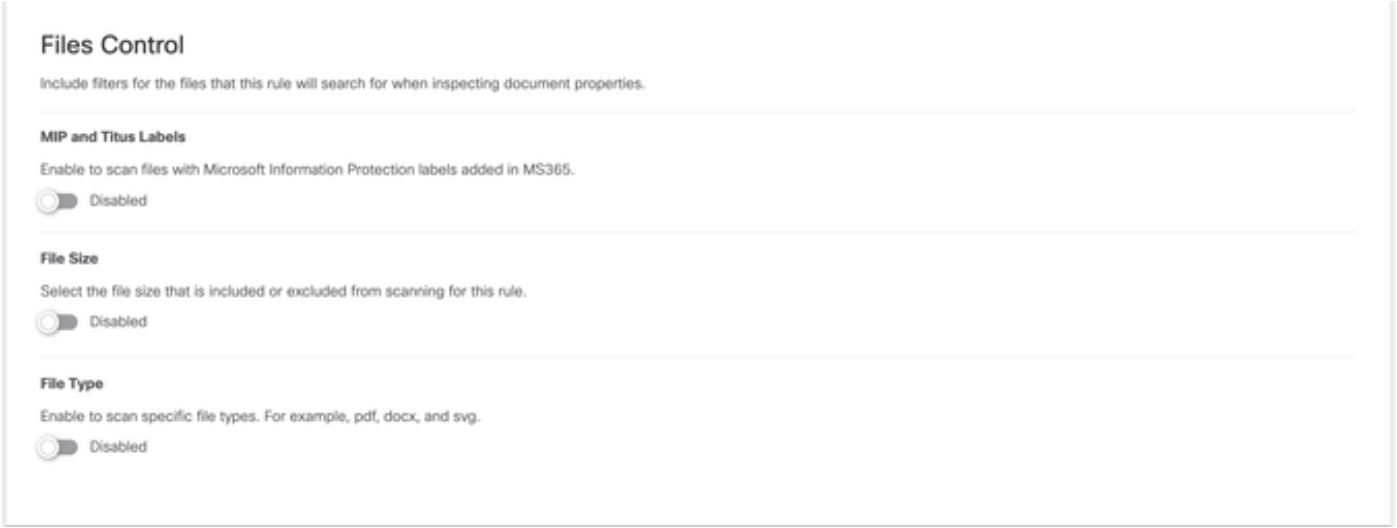
步驟 5:配置檔案控制元件

在Files Control下，為規則配置基於檔案的檢查標準。

其中包括以下支援：

- MIP標籤
- 提圖斯標籤

當DLP實施必須考慮與附加檔案關聯的敏感度標籤或後設資料時，這些設定非常有用。



步驟 6:定義發件人範圍

在發件人部分中，指定策略應用於哪些發件人。

可用選項包括：

- 所有發件人
- 特定發件人
- 排除特定發件人

這樣，您就可以將規則廣泛應用或限製為選定的使用者或組。

步驟 7:定義收件人範圍

在Recipients部分，選擇應包括在策略評估中或從策略評估中排除的使用者或組。

可用選項包括：

- 包括所有使用者
- 包括特定使用者
- 排除特定使用者

這有助於根據目標收件人定製策略實施。

步驟 8:選擇策略操作

在Action部分，選擇思科安全訪問應如何處理被明確標識為違反DLP規則的電子郵件。

可用操作包括：

- 監視
  允許使用電子郵件，並記錄事件以進行可視性和報告。
- 封鎖
  郵件被丟棄，以防止傳輸敏感資料。

附註：目前，可以允許通過Monitor操作或通過Block操作刪除已正確識別的電郵。

重要：電子郵件DLP操作僅在Cisco Secure Access中配置。如果安全訪問阻止了電子郵件，則此事件也顯示在Cisco ETD郵件跟蹤中。

步驟 9:配置使用者通知

通知選項僅對參與者可用。

在User Notifications下，配置當電子郵件與DLP策略匹配時是否應通知使用者。
可以選擇通知「參與者經理」或「自定義收件人」。「自定義收件人」可以是任何人。

根據需要將電子郵件模板從「預設」配置為「自定義」通知。

如果啟用，通知可以幫助提高使用者感知並減少重複違反策略的情況。根據您組織的操作和合規性要求配置此設定。

步驟 9:配置使用者通知

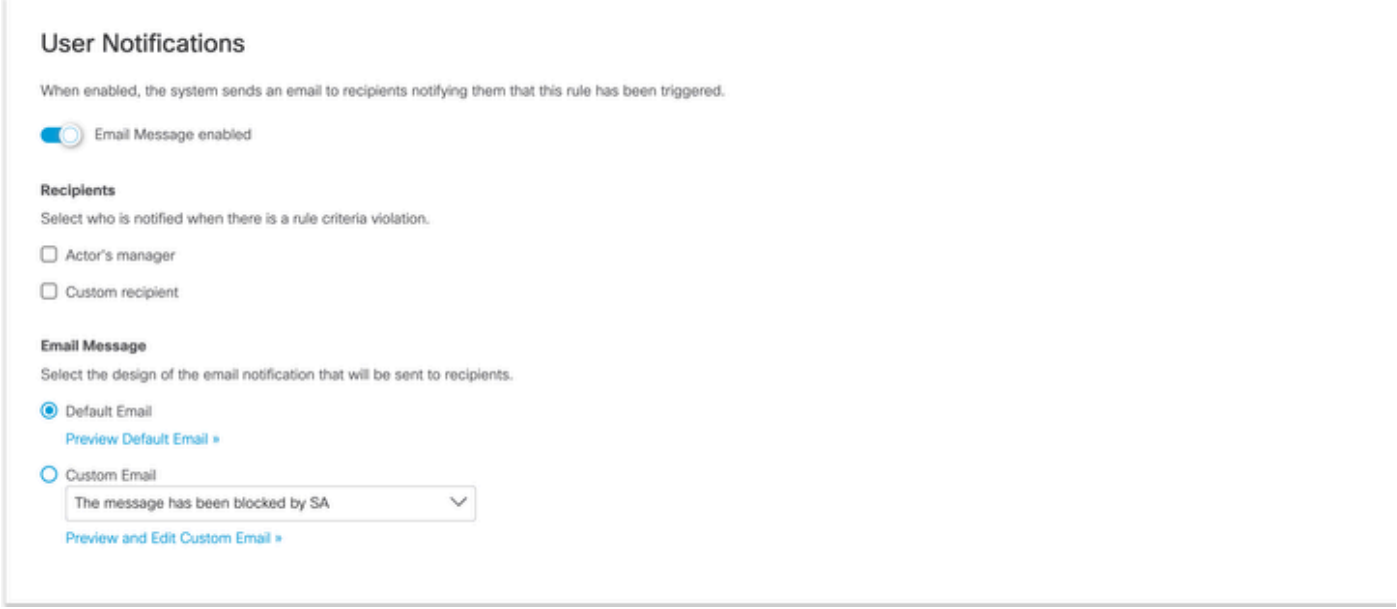
使用者通知是提高安全意識和確保合規性的強大工具。通過在電子郵件觸發DLP策略時提醒使用者或管理員，您可以立即提供有關違規的反饋和情景。

附註：通知設定主要針對電子郵件收件人和指定的利益相關者。

要配置通知，請執行以下操作：

1. 定義通知接收人:在User Notifications部分下，指定接收警報的人員。有兩個主要選項：
    - 演員經理:將通知直接傳送給觸發策略違規的使用者的經理。
    - 自定義收件人：允許您指定任何電子郵件地址（例如，安全運營中心或特定部門主管）。
2. 選擇消息模板:您可以在Defaultnotification模板或Customnotification之間進行選擇。
    - 建議：如果您的組織具有特定合規性消息或內部品牌要求，請使用Customoption定製電子郵件正文，為收件人提供清晰、可操作的說明。
3. 審閱並儲存:配置後，請確保設定與組織的操作和合規性策略一致。

最佳實踐:啟用這些通知是一種有效的減少重複策略違規的方法，它可以即時培訓使用者有關敏感資料處理過程的資訊。



附註：通知選項可能因租戶配置和策略設定而異。

步驟 10:檢視並儲存規則

完成規則配置後：

1. 檢視所有配置的設定。
2. 驗證所選的資料分類、檢查範圍、發件人和收件人條件以及操作是否與您的預期策略行為匹配。
3. 按一下Saveto建立電子郵件DLP規則。

郵件DLP策略現在在Cisco Secure Access中處於活動狀態。

選項 2:使用自定義DLP模板建立電子郵件DLP規則

建立自定義DLP模板涉及兩個主要階段：定義自定義標識符和配置資料分類。

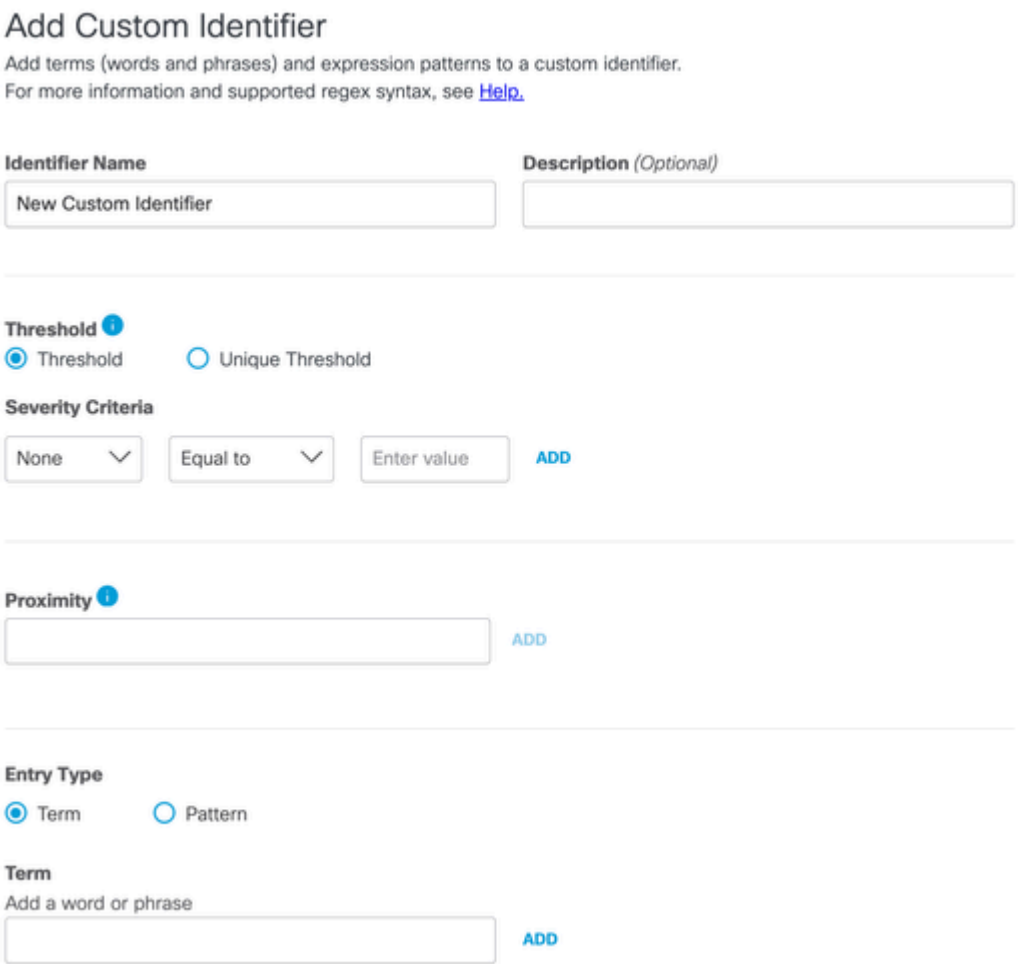
附註：資料分類引擎非常靈活，允許您使用單個自定義識別符號或由AND/OR布林運算子連結的自定義識別符號和預定義識別符號的組合來構建策略。

步驟 11:建立自定義識別符號

要定義用於檢測的新資料模式，請執行以下步驟：

1. 登入到Secure AccessDashboard。
2. 導覽至安全>資料分類。
3. 按一下新增自定義標識符。
4. 在「新增自定義識別符號」(Add Custom Identifier)視窗中配置以下引數：

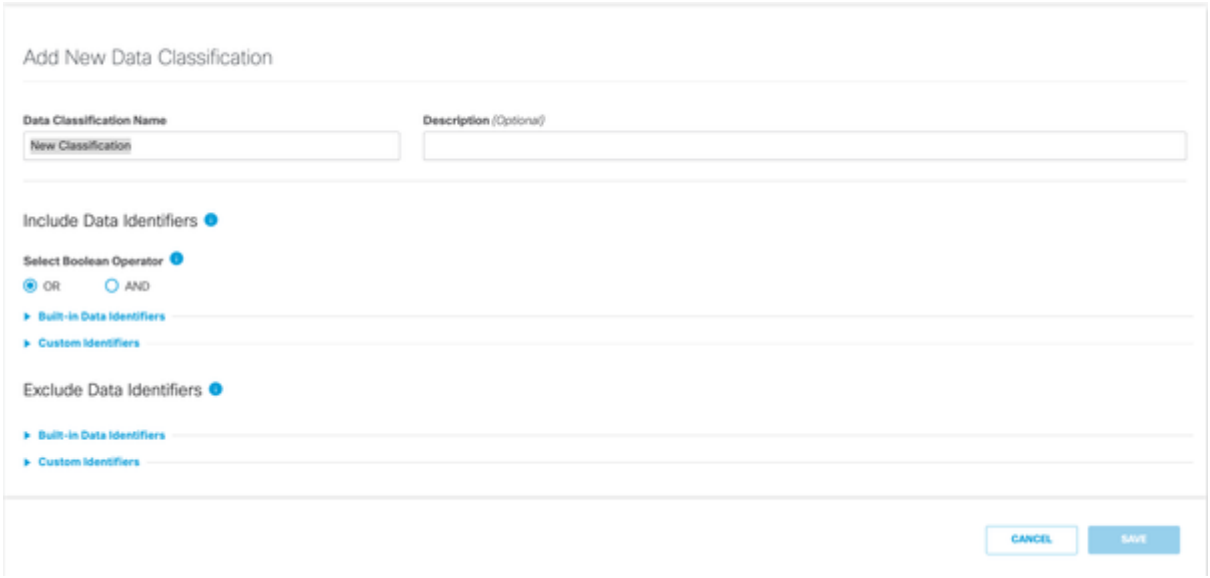
- 名稱和說明:提供要檢測的資料型別的唯一名稱和簡短說明。
- 閾值:
  - 閾值:監視檢測資料的總頻率。
  - 唯一閾值:僅監視資料的重複出現次數，忽略重複項。
- 嚴重性標準：根據檢測頻率分配嚴重性級別(Very Low、Low、Medium、High)。可以使用比較運算子(如等於、大於、小於或範圍)。
- 鄰近度:設定接近閾值。這適用於在此識別符號內集體定義的所有術語和模式，而不是單個術語。
- 條目型別:定義系統識別資料的方式：
  - 字詞:一個特定的詞或短語。
  - 模式:正規表示式(regex)用於檢測特定資料格式（例如，信用卡號或內部專案代碼）。



步驟 12:配置資料分類

儲存自定義識別符號後，您可以將其整合到資料分類對象中：

1. 導覽至Secure > Data Classification > Add（使用右上角的按鈕）
2. 從可用清單中選擇新建立的Custom Identifier。
3. （可選）使用AND/OR邏輯將自定義識別符號與預定義識別符號組合以縮小檢測範圍。
4. 儲存配置，使其可用於您的電子郵件DLP策略。
5. 有關詳細資訊，請參閱下面的螢幕截圖。
6. 現在，請按照步驟4到步驟10中的相同步驟使用自定義資料分類建立策略。



此配置可確保您的組織能夠檢測專門針對您的內部資料結構和法規遵從性要求而定製的敏感資訊。

疑難排解

如果電子郵件DLP規則未按預期運行，請檢視以下內容：

規則與電子郵件不匹配

- 確認已選擇correctdata classification模板。
- 驗證相關檢查位置是否已啟用：
  - 電子郵件主題
  - 郵件正文
  - 附件名稱
  - 附件內容
- 確保發件人和收件人過濾器不會無意中排除測試電子郵件。

電子郵件未被阻止

- 驗證規則操作是否設定為Blockand notMonitor。
- 確認已儲存並啟用規則。
- 確保電子郵件內容與配置的DLP條件完全匹配。

DLP事件在ETD中不可見

- 確認思科ETD和思科安全訪問已正確整合。
- 確認ETD正在積極處理相關電子郵件流量。
- 檢查策略事件是否首先出現在思科安全訪問中。

未檢測到基於附件的匹配

- 確認在檢查範圍內選擇了Attachment Name和/或Attachment Contents。
- 如果諸如MIPorTitusare等標籤是規則邏輯的一部分，請驗證檔案控制設定。

最佳實踐

部署電子郵件DLP策略時，請考慮以下最佳做法：

- 從Monitormode開始，在實施Block之前驗證策略行為。
- 使用清晰和描述性的規則名稱來簡化管理。
- 仔細觀察發件人和收件人條件，以減少意外匹配。
- 在廣泛部署之前使用代表性資料進行測試。
- 定期檢查ETD郵件跟蹤，以驗證受阻止或監控的電子郵件活動。
- 在需要特定於業務的資料識別符號時，請使用自定義模板。

摘要

Cisco Secure Access是在整合的Cisco Secure Access和Cisco Email Threat Defense部署中配置電子郵件DLP策略的中央平台。雖然ETD提供可視性和郵件跟蹤，但所有DLP規則建立、分類選擇、實施操作和通知均在Secure Access中配置。

通過使用預定義或自定義DLP模板，管理員可以檢查電子郵件內容和附件、定義發件人和收件人範圍，並應用Monitor或Block操作以幫助防止通過電子郵件丟失敏感資料。

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）。