通過協調整合ISE和SecureX OnPremises

目錄

簡介

本文檔介紹通過協調將身份服務引擎和SecureX與來自Cisco Secure GitHub的工作流整合的步驟。

必要條件

思科建議您瞭解以下主題：

- 思科ISE配置體驗
- ISE API知識
- SecureX協調知識

需求

您必須在網路中部署思科ISE並具有活動的SecureX帳戶。協調工作流程通過SecureX瀏覽器擴展觸發。

在我們的示例中，要使用的工作流是從Cisco Secure GitHub頁面匯入的，此過程也適用於自定義工作流。

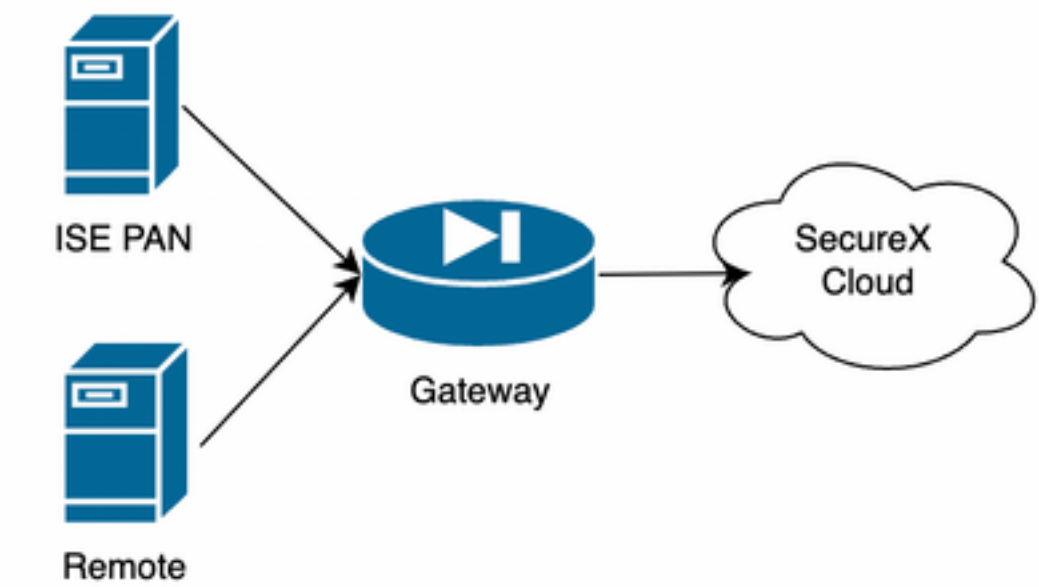
採用元件

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。

- 身分識別服務引擎ISE版本3.1
- SecureX帳戶
- SXO遠端裝置版本1.7

設定

網路圖表



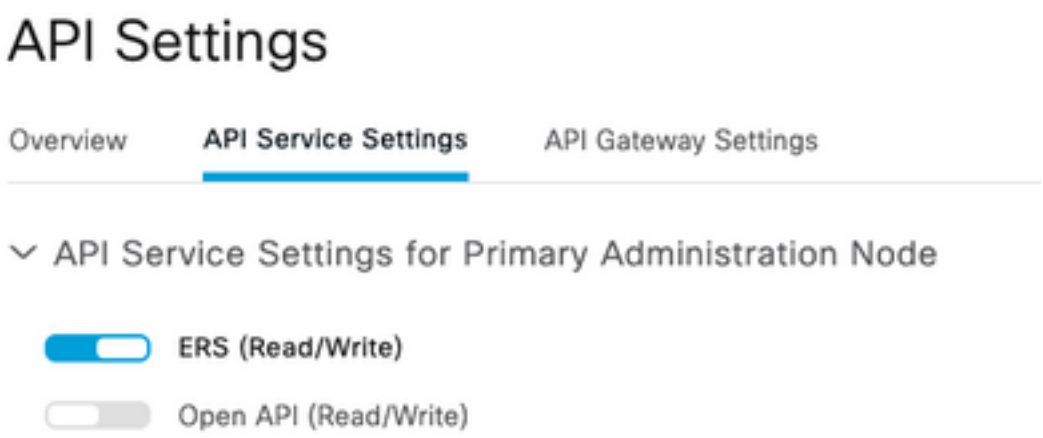
在我們的示例中，ISE PAN和遠端伺服器位於同一子網中，以便直接連線。

由於ISE是本地裝置，遠端伺服器與Secure-X雲聯絡並將資訊轉發到ISE PAN

組態

ISE PAN配置

1.導航到**管理>系統>設定> API設定>API服務設定**並啟用**ERS（讀/寫）**

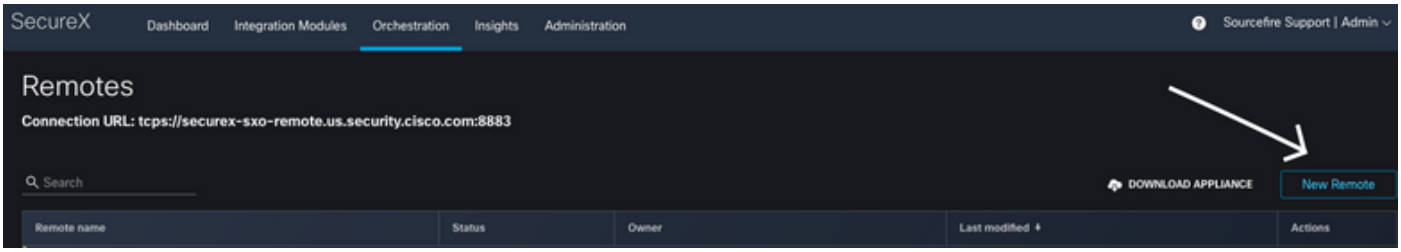


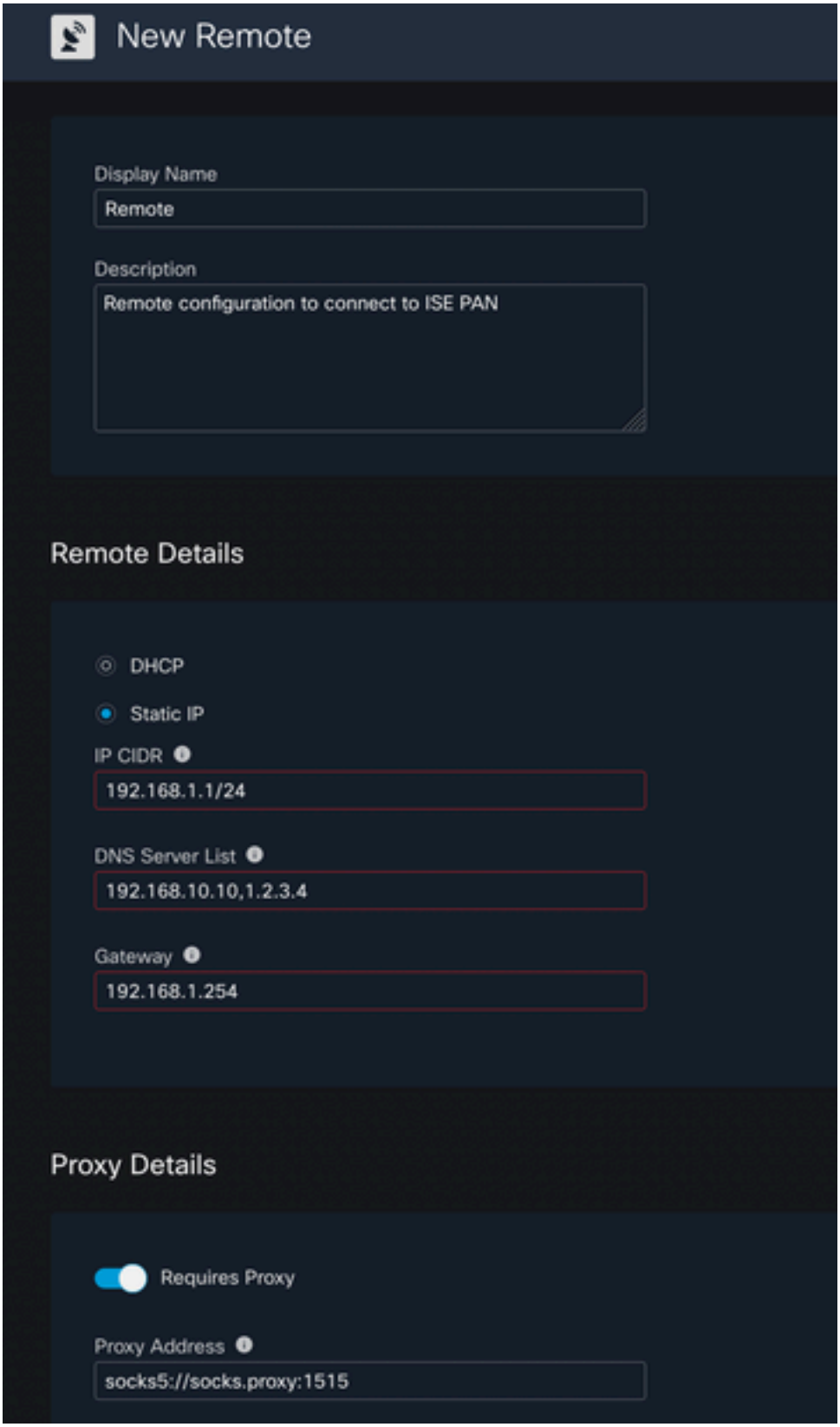
2.（可選）為Secure-X連線建立新使用者，導航到**Administration > System > Admin Access > Administrator > Admin Users**，然後建立新使用者，該新使用者必須具有「ERS Admin」許可權，或者該使用者可以是超級管理員使用者。

配置和部署遠端伺服器

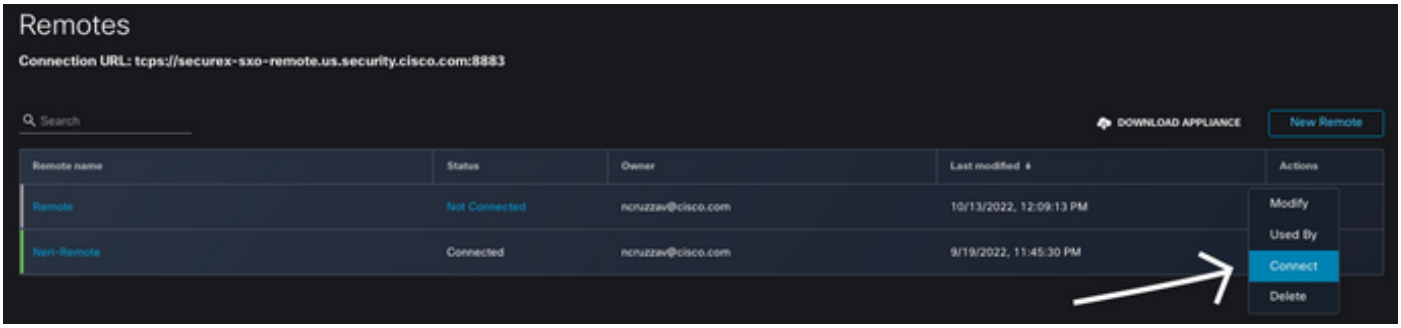
1.配置遠端伺服器，在Secure-X控制檯上，導航到**Orchestration > Admin > Remote Configuration**並選擇選項**New Remote**,IP地址資訊是建立VM時要使用的資訊，並且它必須位於部署ISE PAN的同一子網中。

附註：如果通過代理連線到雲，則目前僅支援SOCKS5代理用於此目的。

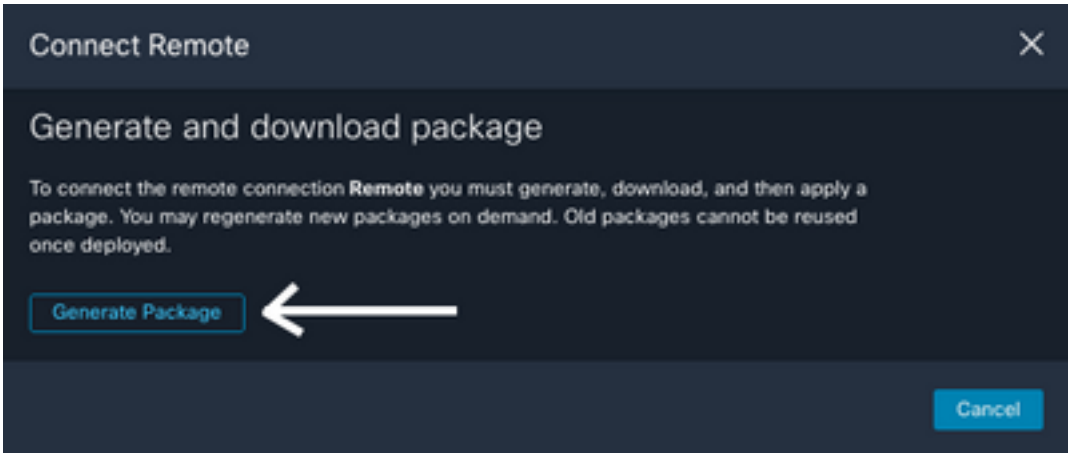




2.下載要用於VM部署的已配置設定，儲存資訊後，遠端電腦將顯示為「Not Connected」(未連接)，在操作下導航，然後選擇Connect



選擇**Generate Package**，此操作將下載一個.zip檔案，其中包含部署虛擬機器時剛剛配置使用的資訊。



3.下載並安裝VM，在**New Remote** 選擇**DOWNLOAD APPLIANCE** 旁，此操作將下載用於部署遠端伺服器的OVA映像。

有關遠端VM規格，請參閱SecureX Remote Setup指南

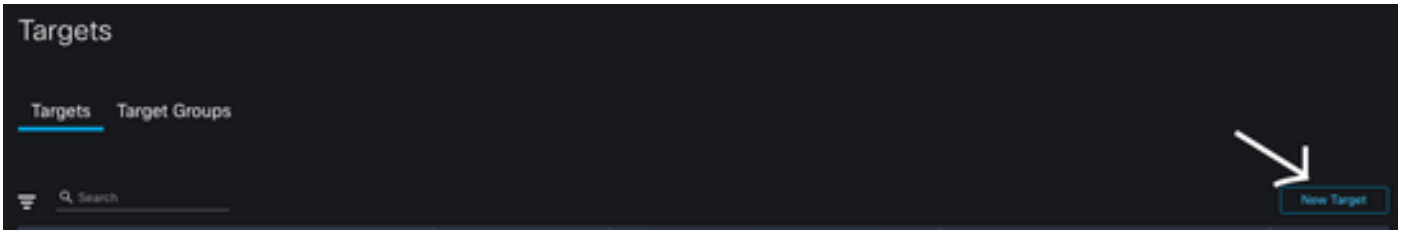
建立VM時，必須在**編碼使用者資料**上使用ZIP檔案內下載的資訊，這樣在啟動後將配置的遠端資訊填充到伺服器中。

4.一旦虛擬機器啟動，它將自動連線到SecureX帳戶，以驗證連線是否已啟動，在遠端配置下，您必須看到狀態更改為「已連線」。

在SecureX上配置目標

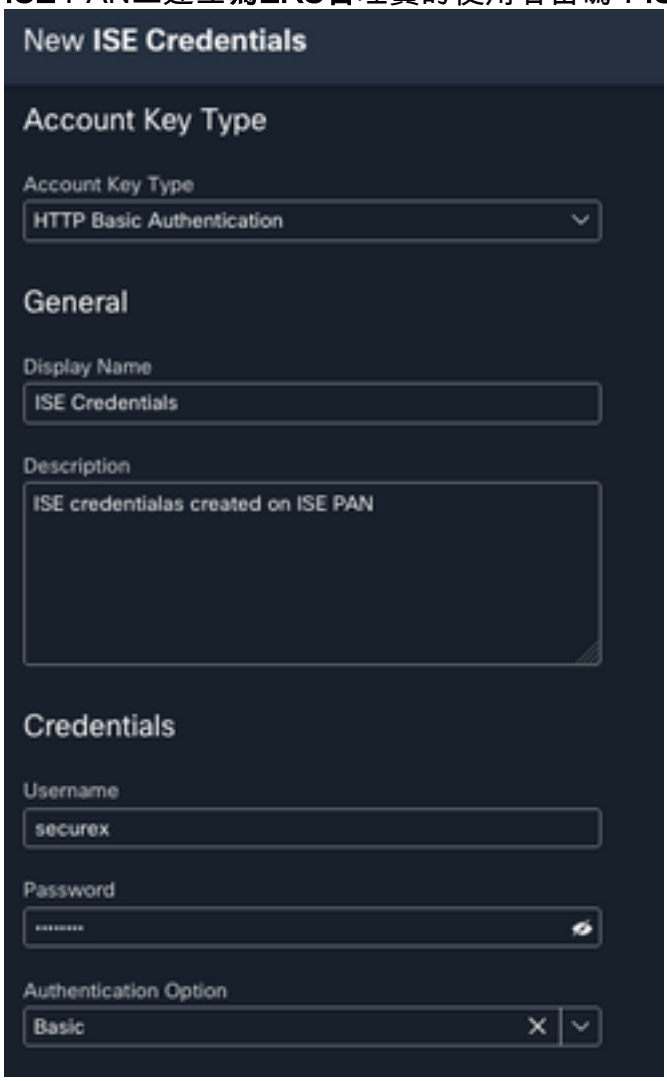
為了使協調與裝置配合使用對於配置**Target非常重要**，Secure X使用此目標傳送API呼叫並通過協調與裝置互動

1.定位至**協調>目標>新目標**

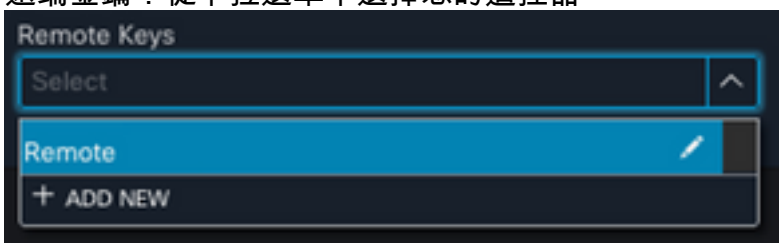


2.使用下一條准則填寫目標資訊

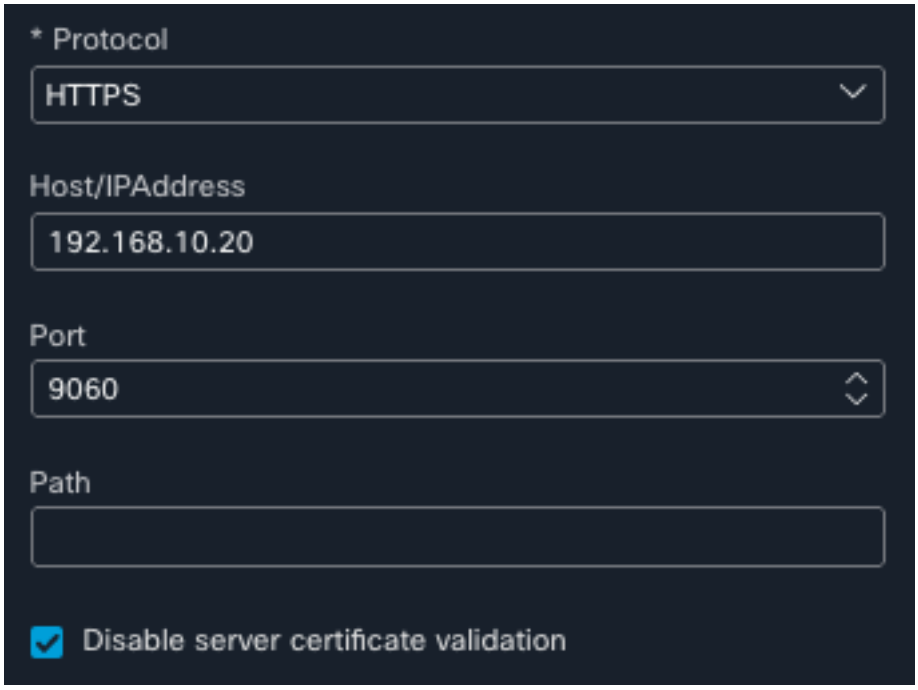
- 顯示名稱：目標識別符號
- 說明:識別目標用途的小描述
- 帳戶金鑰：在此您需要配置使用者/密碼以通過API訪問ISE 無帳戶金鑰：**假**預設帳戶金鑰：選擇**Add New** 帳戶金鑰型別：**HTTP基本身份驗證**顯示名稱：帳戶金鑰識別符號使用者名稱:在ISE PAN上建立**為ERS管**理員的使用者密碼：ISE PAN上建立的使用者**的密碼**驗證選項：**基本**



- 遠端：在這裡，您需要選擇先前配置的遠端連線
  遠端金鑰：從下拉選單中選擇您的遙控器



- HTTP:在此您需要配置ISE PAN的API**資訊** 通訊協定:**HTTPS**主機/IP地址：**ISE PAN專用IP**連接埠:**9060**路徑：留空禁用伺服器證書驗證：**選中此框**



- 代理：由於代理配置已包括在遠端配置中，因此您可以將此部分留空
- 選擇**提交**

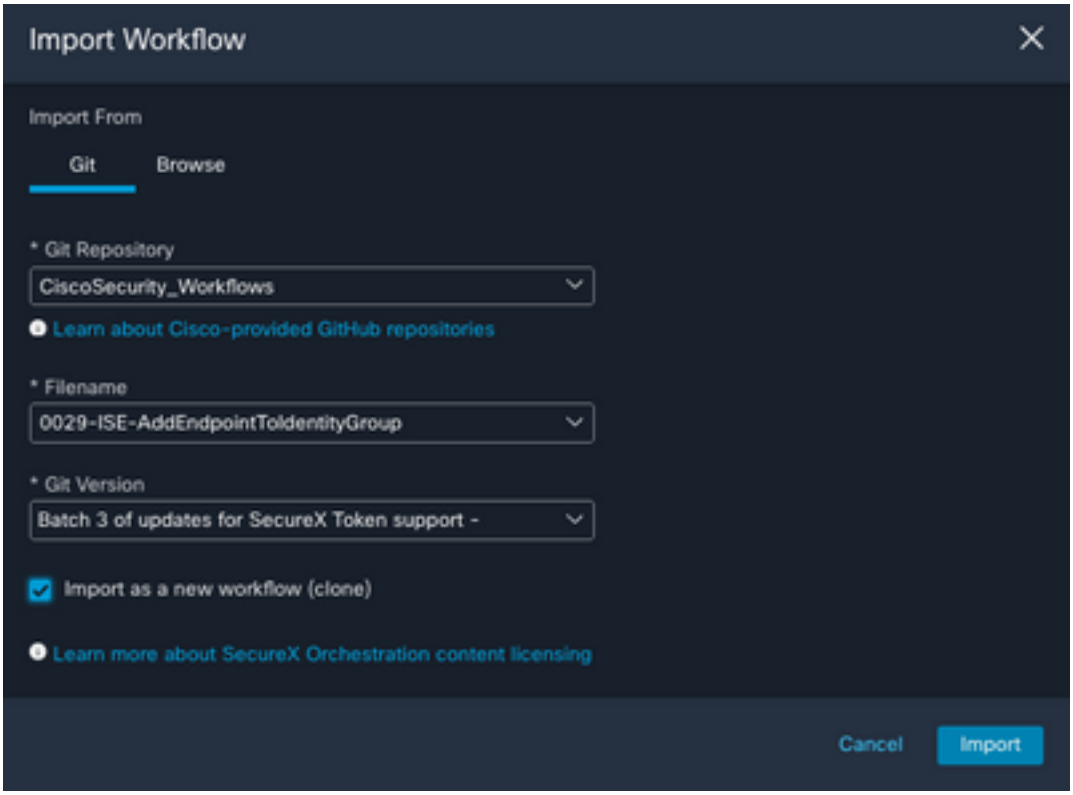
從Cisco Secure GitHub匯入工作流

在本示例中，要使用的工作流是「向身份組新增終端」，您可以使用Cisco Secure GitHub頁面上列出的任何工作流，或者您可以建立自定義工作流。

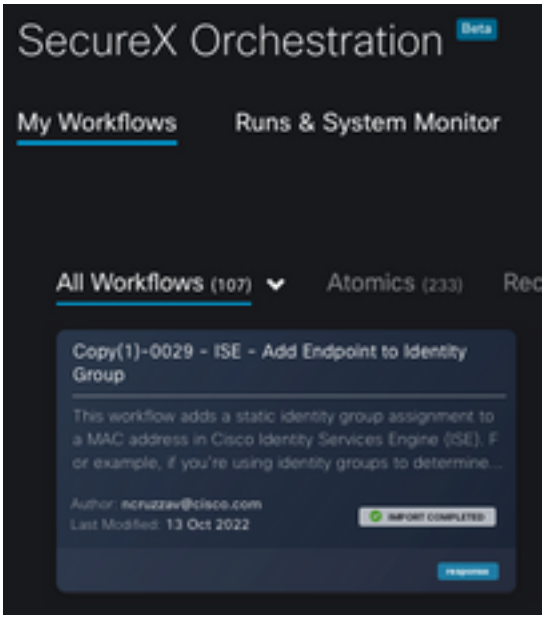
1.定位至**協調>我的工作流>匯入工作流**

2.要匯入工作流，請填寫以下資訊並選擇「**導入**」；要標識要匯入的工作流，可以按名稱或按工作流編號進行搜尋

- Git儲存庫：**CiscoSecurity_Workflows**（工作流所在的位置）
- 檔名：**0029-ISE-AddEndpointToIdentityGroup**（選擇要使用的工作流數）
- Git版本：**SecureX令牌支援的第3批更新**（最新版本）
- 作為新工作流匯入（克隆）：**選中**（此操作將匯入工作流並建立其克隆）

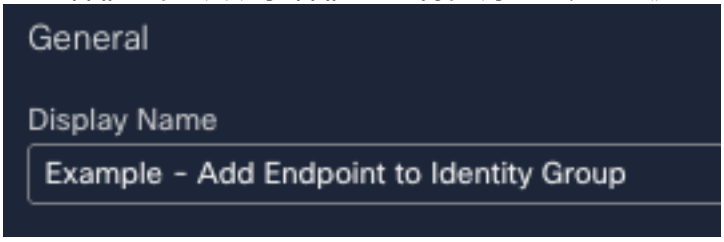


3.匯入後，新模板將顯示在**My Workflows**下，選擇新建立的工作流以編輯引數，使其與ISE配**合**

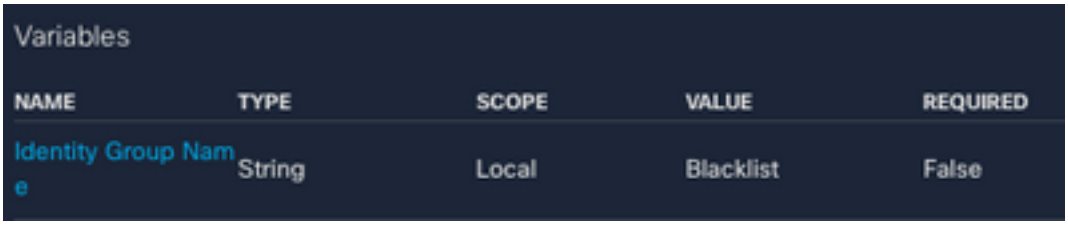


4.由於這是一個預生成工作流，因此您只需修改工作流的3個部分：

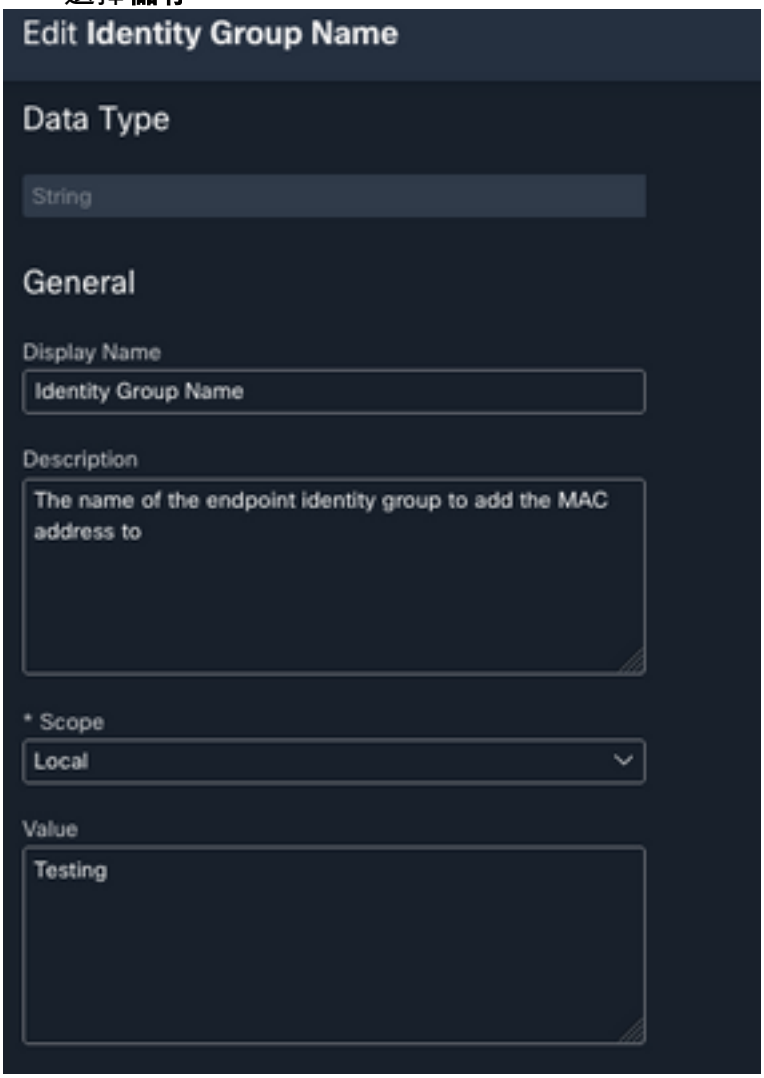
- 名稱：更改顯示名稱以獲得更好的識別符號



- 身份組變數 在變數下，編輯**身份組變數**(預設情況下為**Balcklist**)，選擇變數並配置要通過業務流程修改的身份組名稱



- 選擇**儲存**



- 目標：配置以前配置的**目標** 目標型別：**HTTP終結點**目標：**已配置目標的名稱**

驗證

配置完所有內容後，就到了測試工作流程的時候了

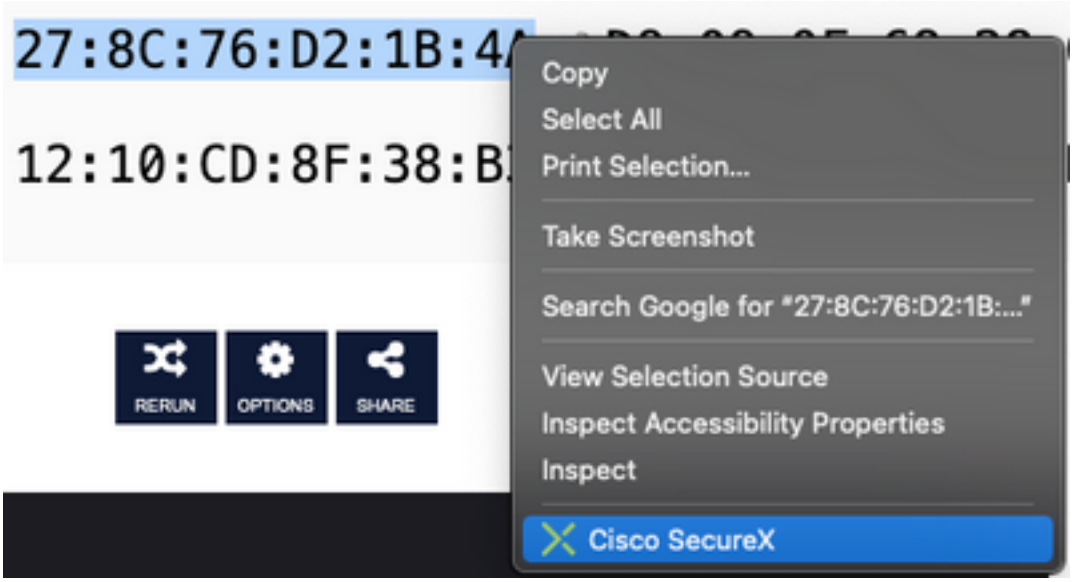
測試的工作流程將執行以下操作：如果您在網頁中找到MAC地址，它可能位於ISE本身或其他網頁（如威脅響應）；通過SecureX瀏覽器擴展，工作流通過API在ISE資料庫內查詢該MAC地址，如果MAC不存在，則可觀察項將新增到終端身份組中，而無需複製值並訪問ISE。

要演示這一點，請看下一個示例：

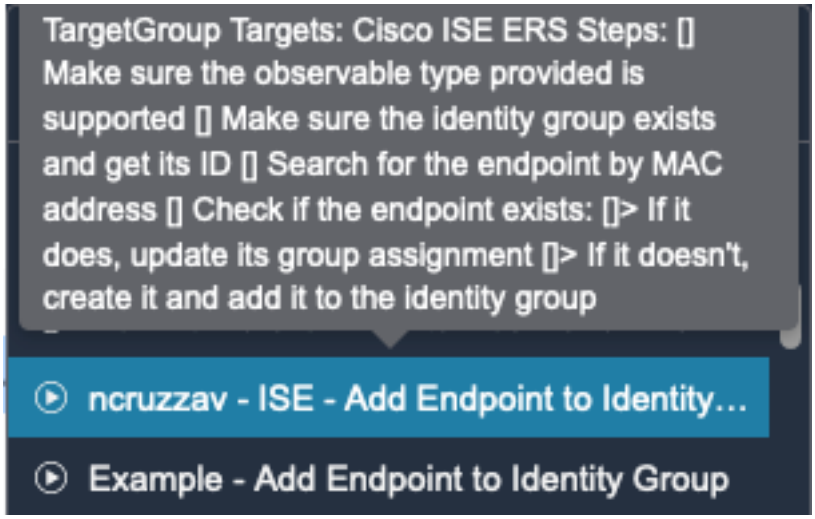
1.所選工作流程使用可觀察型別**「MAC地址」**

2.在網頁上查詢MAC地址並執行按一下右鍵。

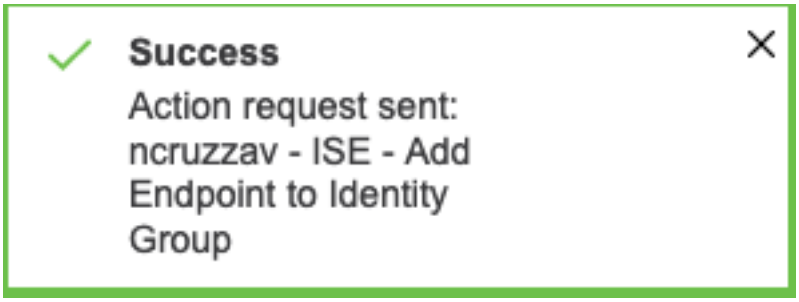
3.選擇**SecureX**選項



4.選擇之前建立的**工作**流

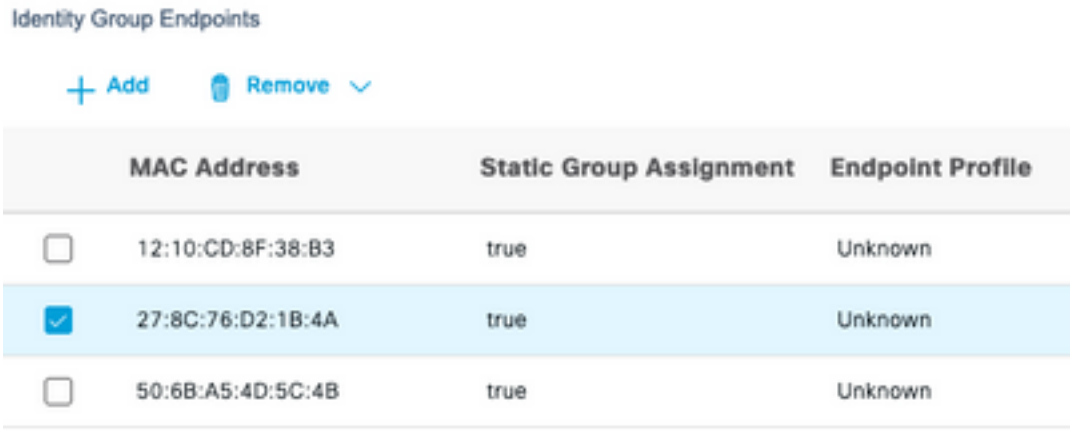


5.確認任務已成功執行



6.在**ISE PAN** 上，導航到**管理>身份管理>組>終端身份組>（在工作流上配置的組）**

7.開啟工作流中配置的**終端身份組**，並確認所選的MAC地址已新增到該MAC地址清單中



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）。