

通過協調整合ISE和SecureX OnPremises

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[組態](#)

[ISE PAN配置](#)

[配置和部署遠端伺服器](#)

[在SecureX上配置目標](#)

[從Cisco Secure GitHub匯入 workflow](#)

[驗證](#)

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。

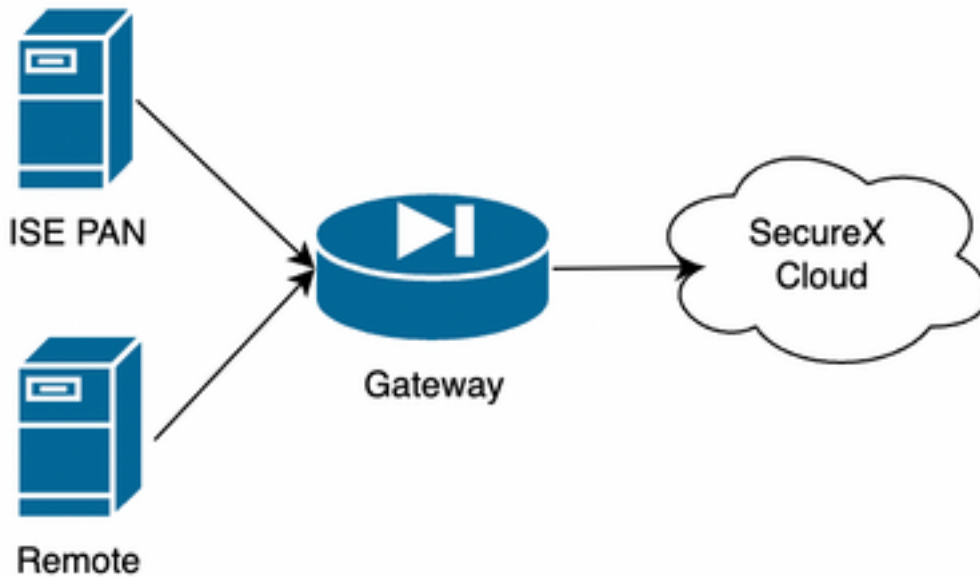
採用元件

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)

API Settings

Overview **API Service Settings** API Gateway Settings

▼ API Service Settings for Primary Administration Node

ERS (Read/Write)

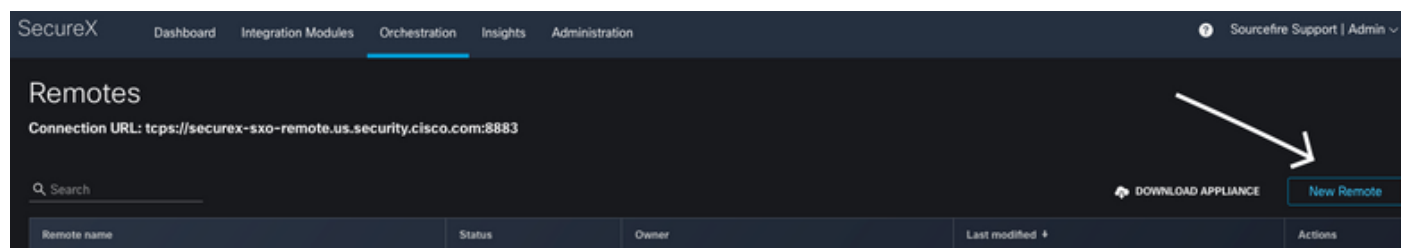
Open API (Read/Write)

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。



New Remote

Display Name
Remote

Description
Remote configuration to connect to ISE PAN

Remote Details

DHCP
 Static IP

IP CIDR ⓘ
192.168.1.1/24

DNS Server List ⓘ
192.168.10.10,1.2.3.4

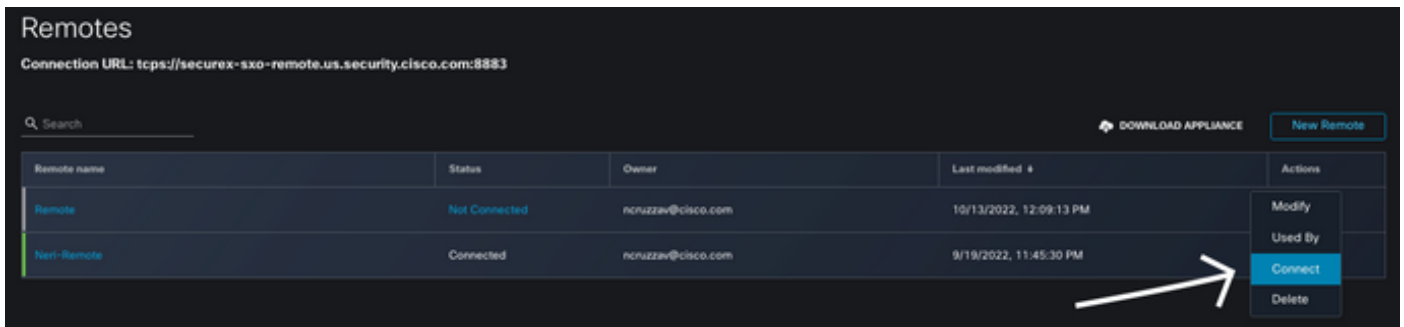
Gateway ⓘ
192.168.1.254

Proxy Details

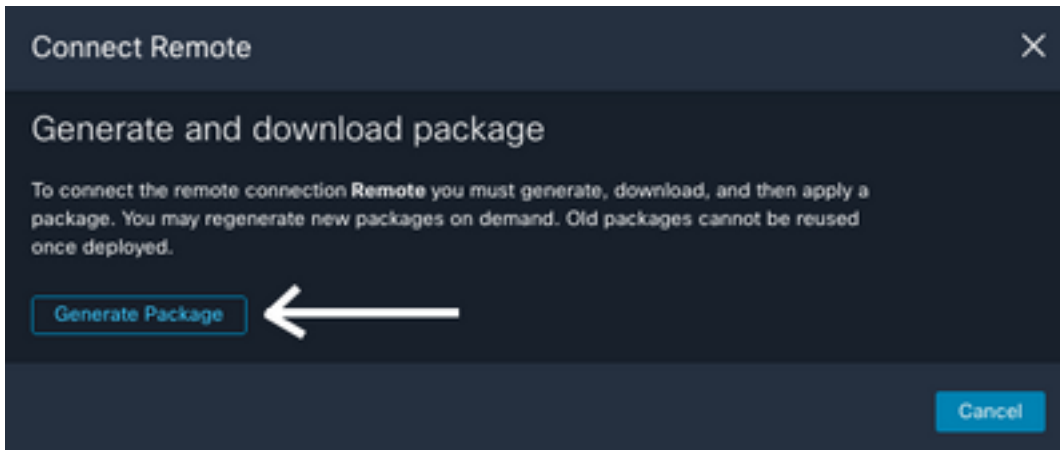
Requires Proxy

Proxy Address ⓘ
socks5://socks.proxy:1515

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」。

Remote name	Status	Owner	Last modified
Remote	Connected	ncruzzav@cisco.com	10/13/2022, 12:09:13 PM

在SecureX上配置目標

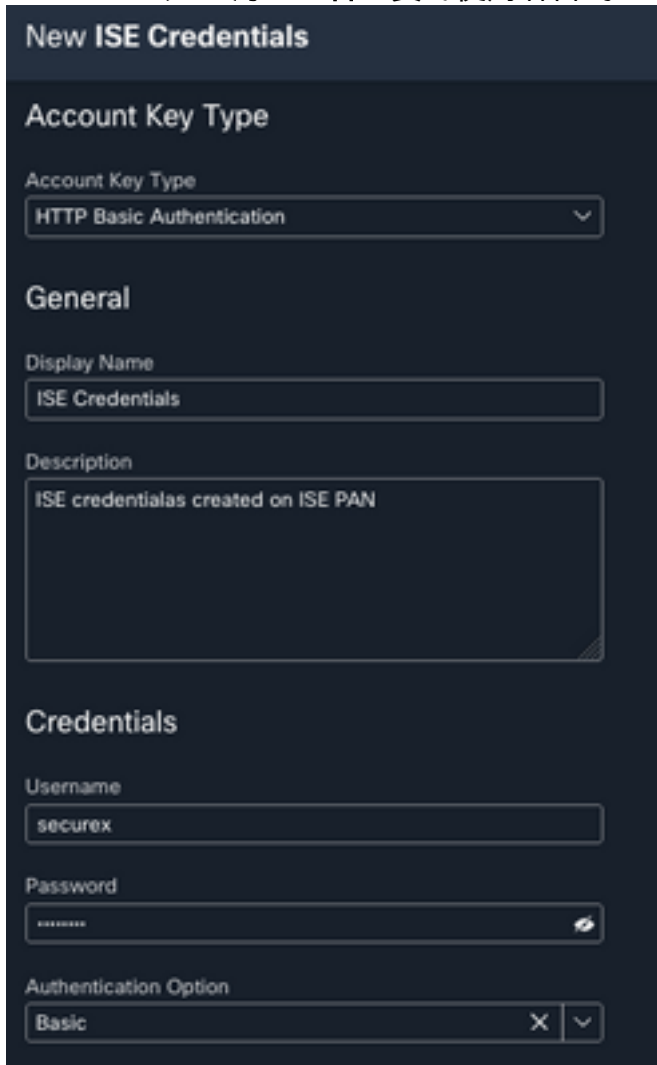
為了使協調與裝置配合使用對於配置**Target**非常重要，Secure X使用此目標傳送API呼叫並通過協調與裝置互動

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



New ISE Credentials

Account Key Type

Account Key Type
HTTP Basic Authentication

General

Display Name
ISE Credentials

Description
ISE credentials created on ISE PAN

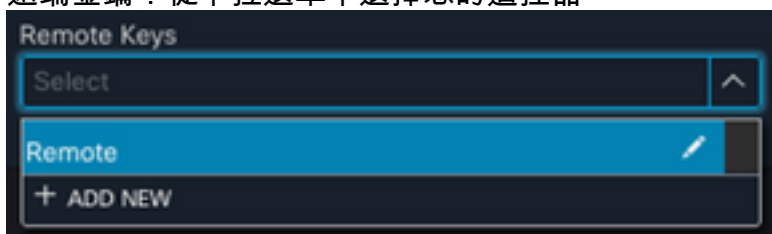
Credentials

Username
securex

Password

Authentication Option
Basic

- 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



Remote Keys

Select

Remote

+ ADD NEW

- 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

* Protocol
HTTPS

Host/IPAddress
192.168.10.20

Port
9060

Path

Disable server certificate validation

- 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 workflow

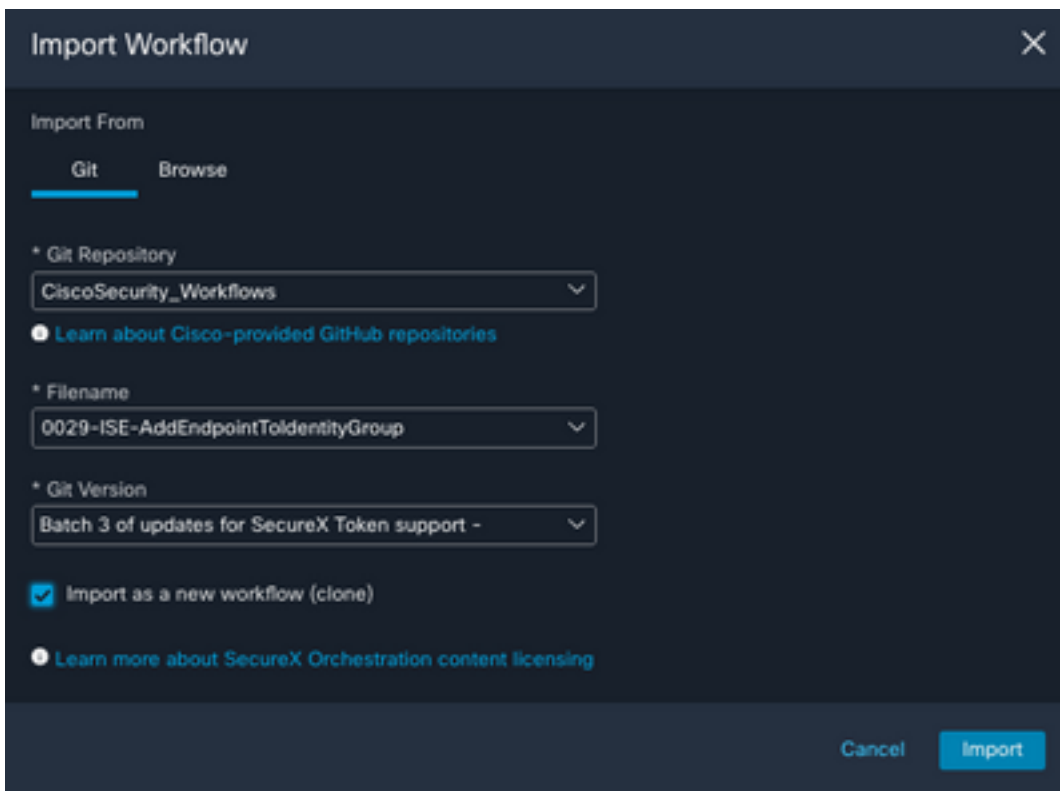
在本示例中，要使用的工作流是「向身份組新增終端」，您可以使用[Cisco Secure GitHub頁面](#)上列出的任何工作流，或者您可以建立自定義工作流。

1. 定位至協調>我的工作流>匯入工作流

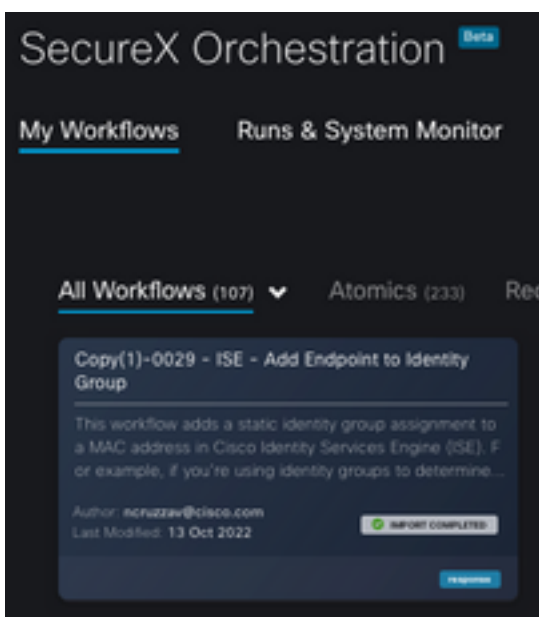


2. 要匯入工作流，請填寫以下資訊並選擇「導入」；要標識要匯入的工作流，可以按名稱或按工作流編號進行搜尋

- 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）

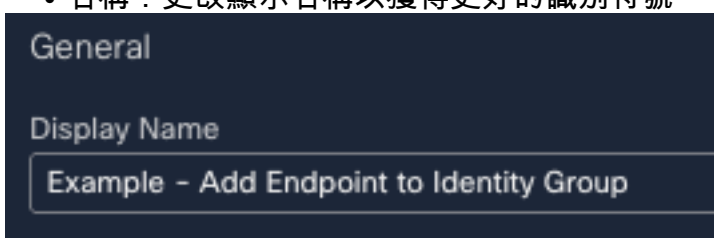


3. 匯入後，新模板將顯示在 **My Workflows** 下，選擇新建立的工作流以編輯引數，使其與 ISE 配合



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

Variables				
NAME	TYPE	SCOPE	VALUE	REQUIRED
Identity Group Name	String	Local	Blacklist	False

- 選擇儲存

Edit Identity Group Name

Data Type

String

General

Display Name
Identity Group Name

Description
The name of the endpoint identity group to add the MAC address to

* Scope
Local

Value
Testing

- 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

Target

* Target Type ●
HTTP Endpoint

No target

Execute on this target

* Target
remote

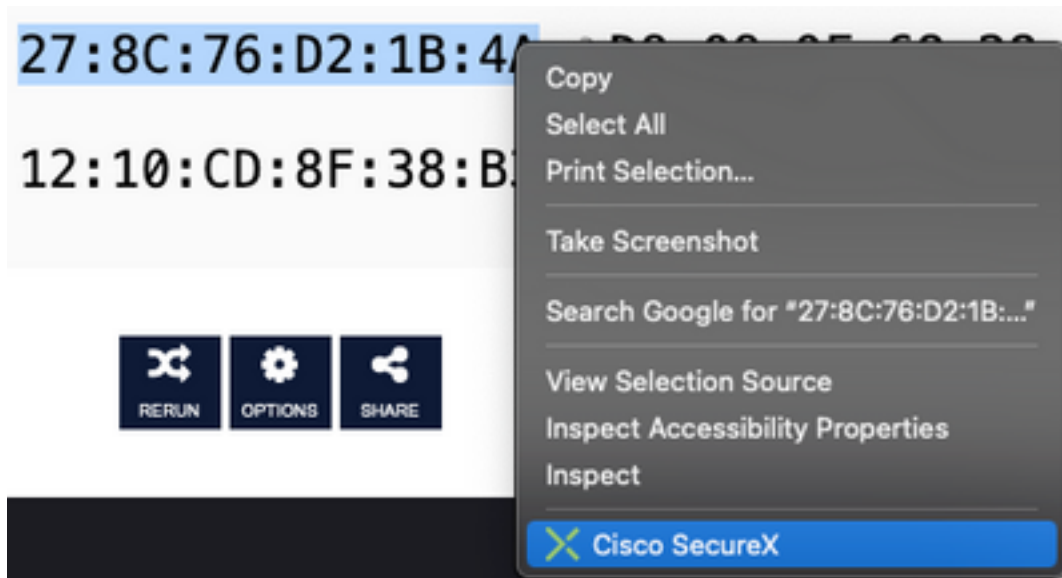
驗證

配置完所有內容後，就到了測試工作流程的時候了

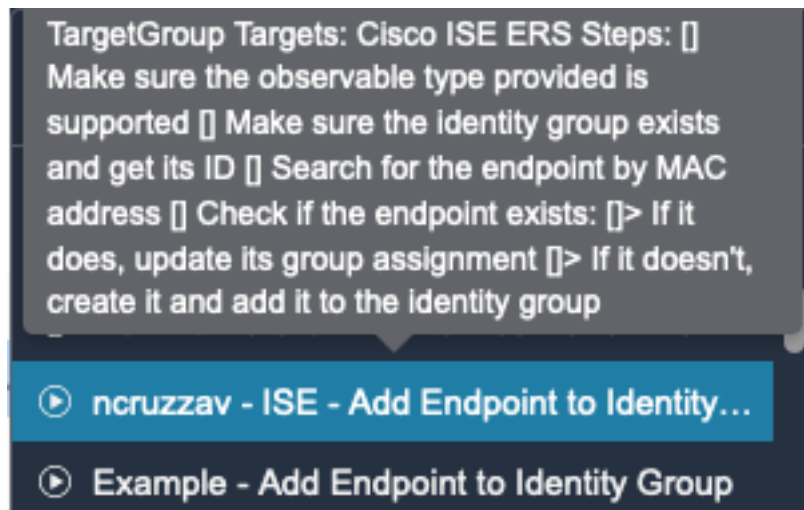
測試的工作流程將執行以下操作：如果您在網頁中找到MAC地址，它可能位於ISE本身或其他網頁（如威脅響應）；通過SecureX瀏覽器擴展，工作流通過API在ISE資料庫內查詢該MAC地址，如果MAC不存在，則可觀察項將新增到終端身份組中，而無需複製值並訪問ISE。

要演示這一點，請看下一個示例：

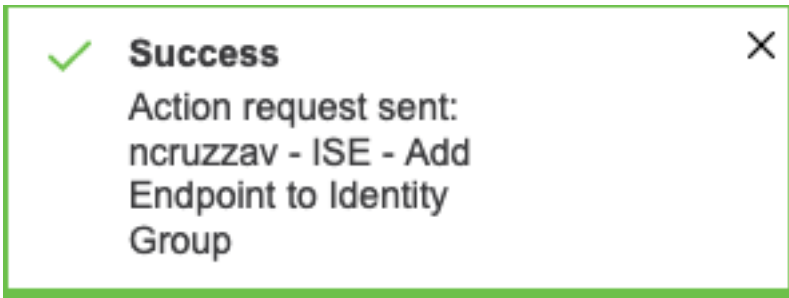
1. 所選工作流程使用可觀察型別「MAC地址」
2. 在網頁上查詢MAC地址並執行按一下右鍵。
3. 選擇SecureX選項



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

Identity Group Endpoints

+ Add Remove ▾

	MAC Address	Static Group Assignment	Endpoint Profile
<input type="checkbox"/>	12:10:CD:8F:38:B3	true	Unknown
<input checked="" type="checkbox"/>	27:8C:76:D2:1B:4A	true	Unknown
<input type="checkbox"/>	50:6B:A5:4D:5C:4B	true	Unknown

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）。