面向終端的AMP與Splunk整合

目錄

簡介

本檔案介紹進階惡意軟體防護(AMP)和Splunk之間的整合程式。

作者：Uriel Islas和Juventino Macias，編輯者：Jorge Navarrete，思科TAC工程師。

必要條件

需求

思科建議您瞭解：

- AMP端點版
- 應用程式開發介面(API)
- 斯普倫克
- Splunk上的管理員使用者

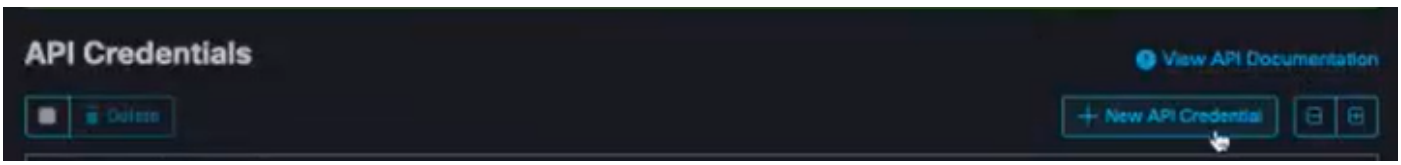
採用元件

- AMP公共雲
- Splunk例項

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

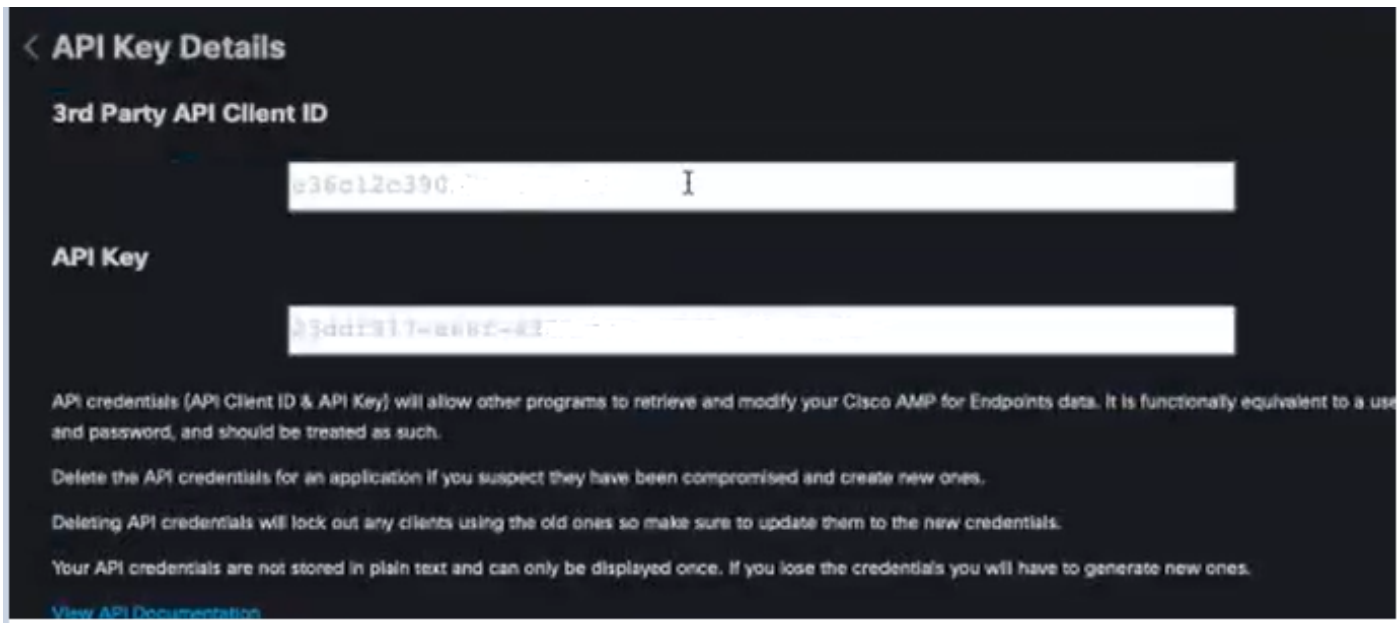
步驟1.導航到AMP控制檯(https://console.amp.cisco.com)，然後導航到**Accounts>API Credentials**，您可以在其中建立事件流。



步驟2。若要執行此整合，請勾選**讀取/寫入**覈取方塊，如下所示：

附註：如果您想收集有關事件的詳細資訊，請選中**Enable Command Line**框，以獲得從檔案儲存庫生成的稽核日誌，請選中**Allow API access to File Repository**框。

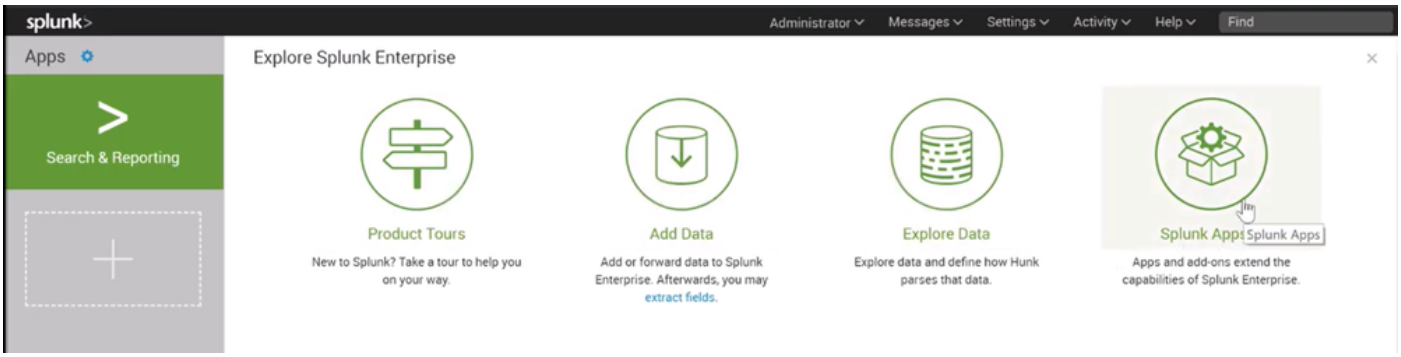
步驟3.建立事件流後，它將顯示API客戶端ID和API金鑰，這是Splunk所必需的。



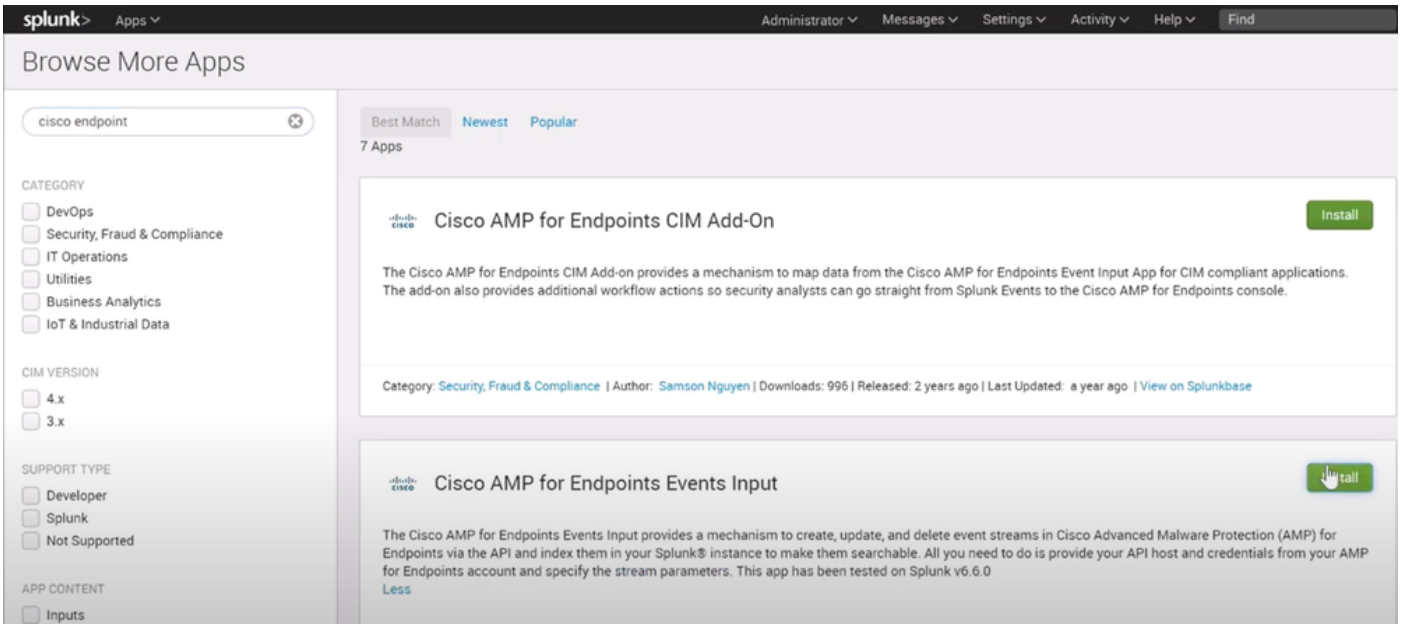
注意：此資訊無法以任何方式恢復，如果丟失，必須建立一個新的API金鑰。

步驟4.為了將Splunk與面向終端的AMP整合，請確保Splunk上存在帳戶**Admin**。

步驟5.登入Splunk後，繼續從Splunk應用下載AMP。

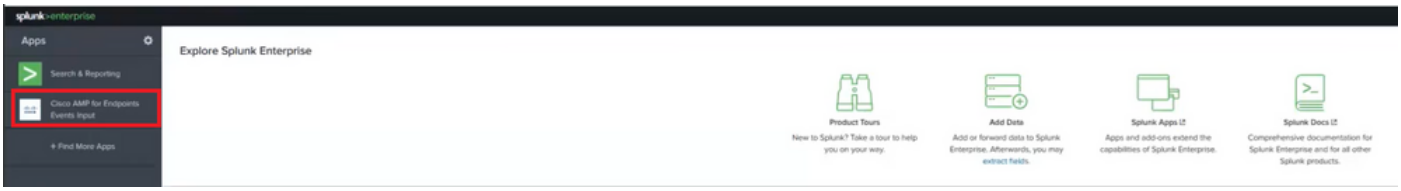


步驟6.在應用瀏覽器上搜尋思科端點並進行安裝（面向端點的思科AMP事件輸入）。

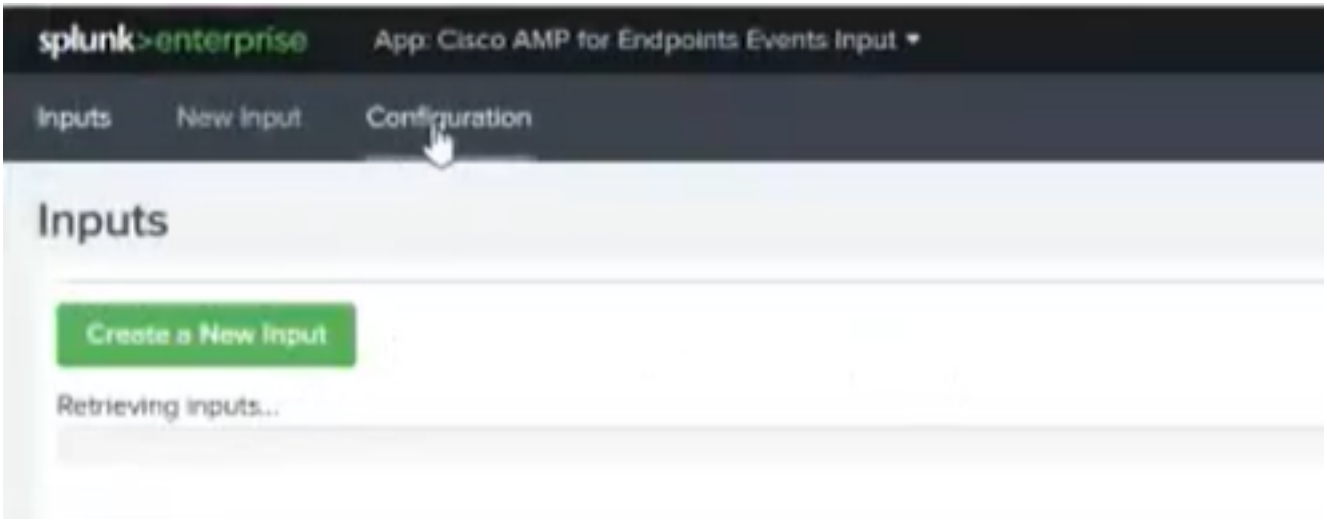


步驟7.需要重新啟動會話才能完成Splunk上的安裝。

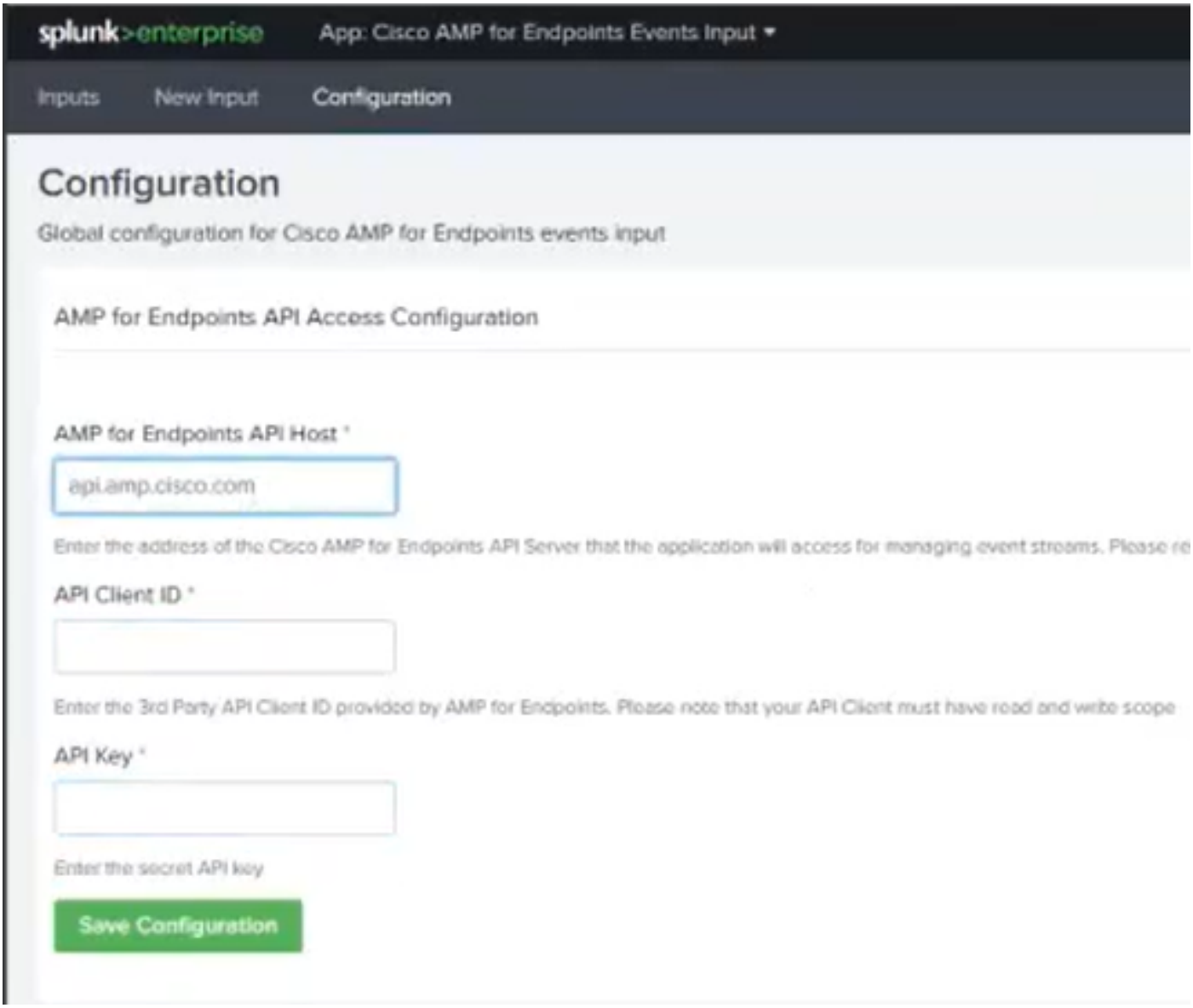
步驟8.在Splunk下登入後，按一下螢幕左側的**Cisco AMP For Endpoints**。



步驟9.按一下螢幕頂部的**Configuration**標籤。

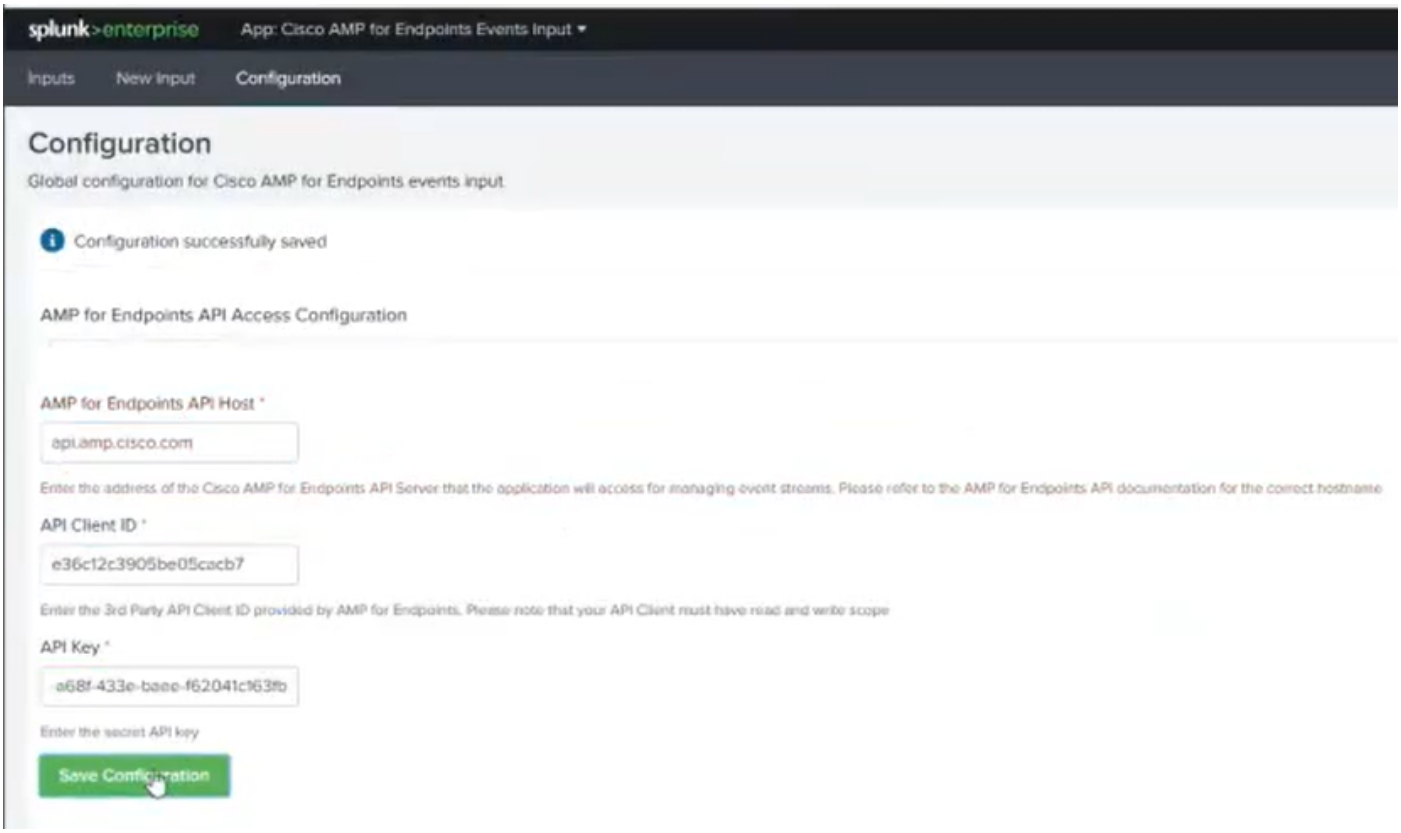


步驟10.鍵入以前從AMP控制檯生成的API憑據。

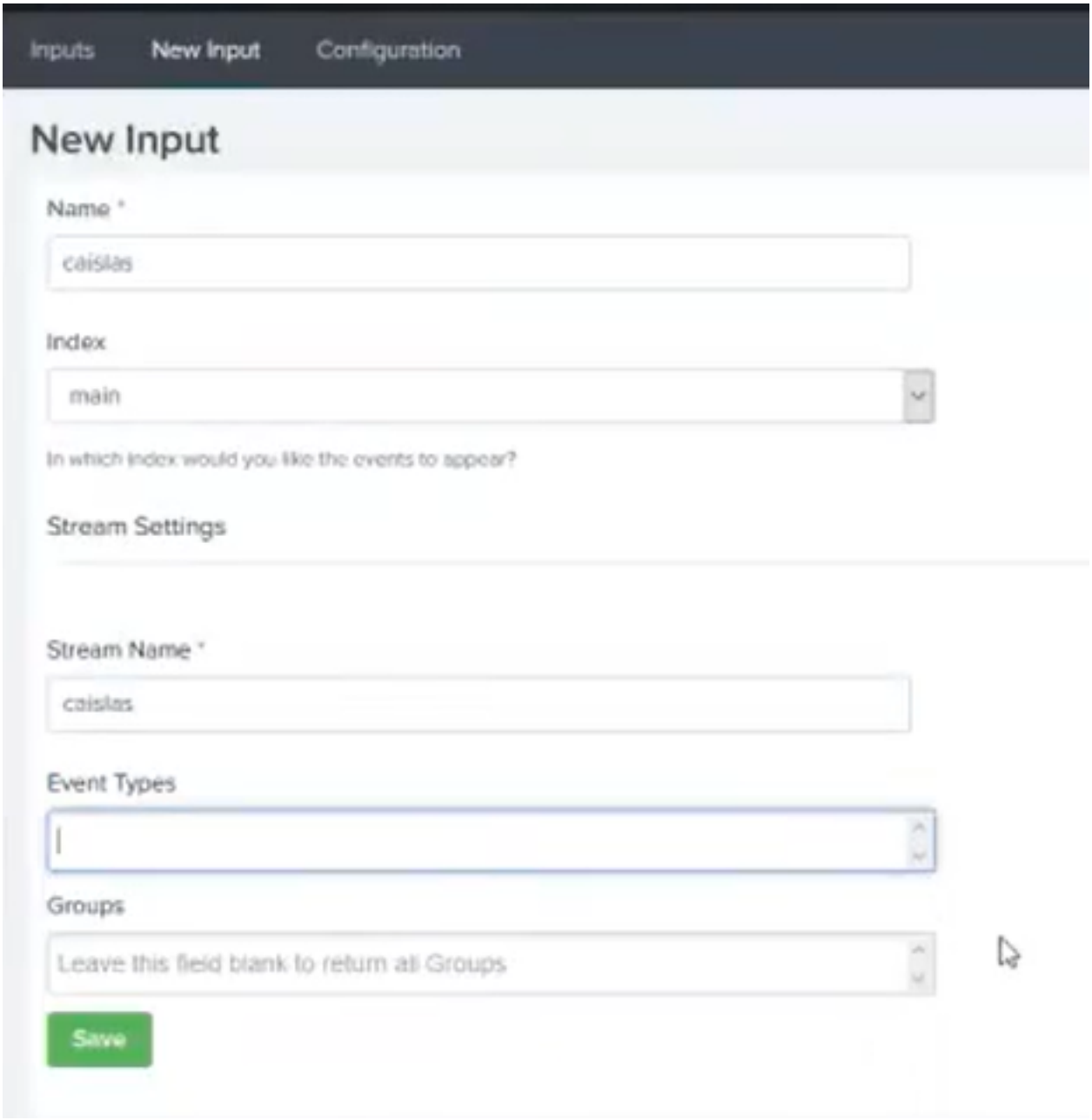


附註：API主機點可能因組織指向的雲資料中心而異：
北美洲:api.amp.cisco.com
歐洲:api.eu.amp.cisco.com
亞太地區、日本及中國：api.apjc.amp.cisco.com

步驟11.在Splunk控制檯上包含並儲存API憑證，以將其與AMP連結。

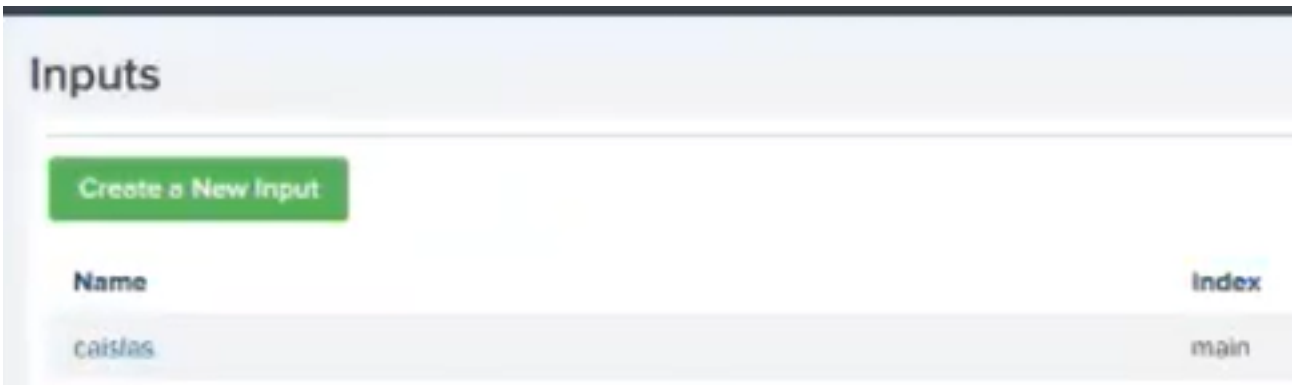


步驟12.返回**Input**以建立您的事件流。



附註：如果要從AMP獲取所有組的所有事件，請將**Event Types**和**Groups**欄位留空。

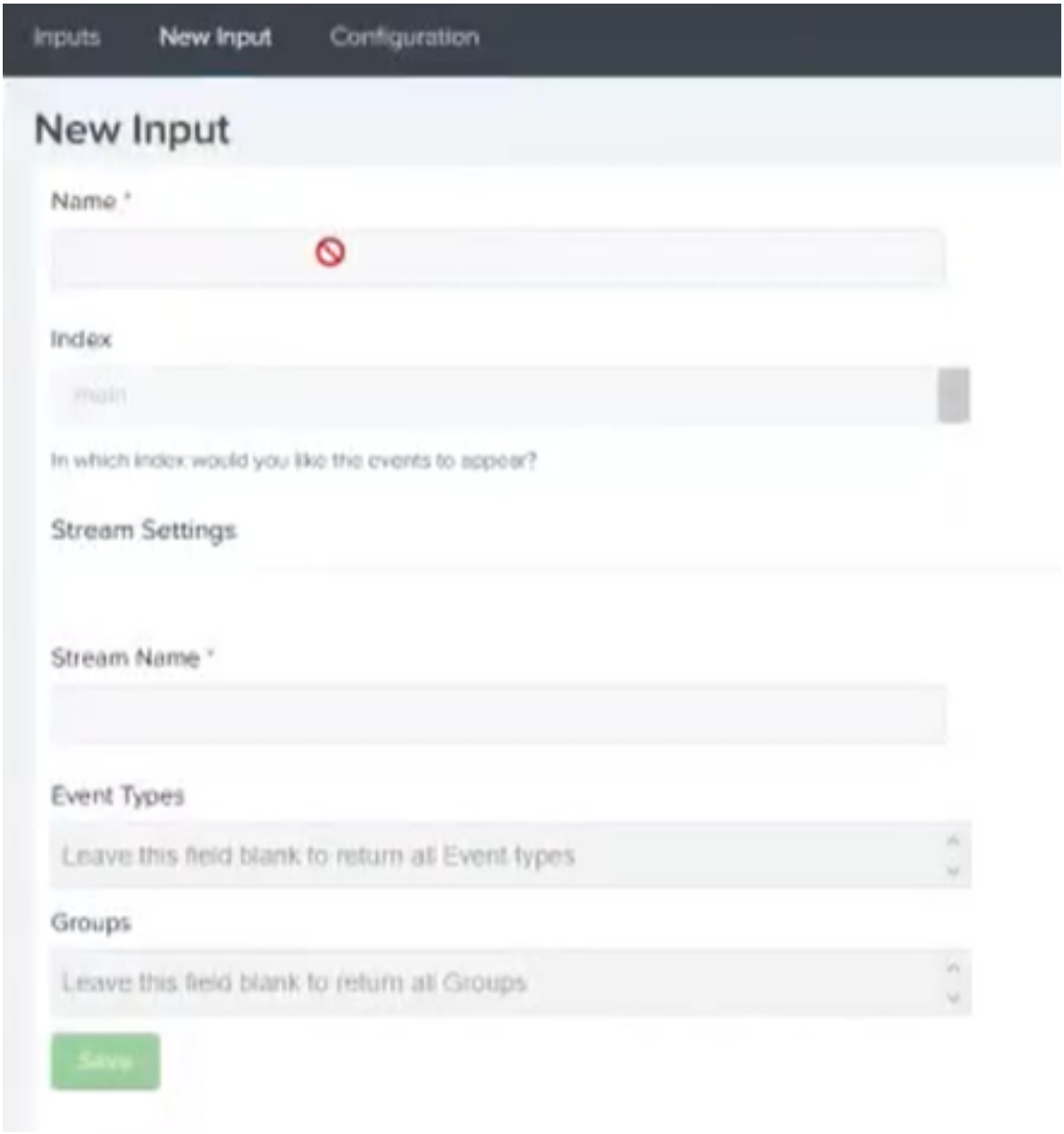
步驟13.確保已成功建立您的輸入。



附註：請記住，此整合未獲得正式支援

疑難排解

如果在建立事件流時，所有欄位都呈灰色顯示，則可能是由於以下某些原因造成的：



1. 連線問題：確保Splunk例項能夠聯絡API主機
2. API主機：根據您的業務所在的位置，確保步驟10中配置的API主機與您的AMP組織相匹配。
3. API憑據：確保API金鑰和客戶端ID與步驟3中配置的金鑰和客戶端ID匹配。
4. 事件流：請確保配置的事件流少於4個。