排除裝置洞察和Umbrella整合故障

目錄

簡介

本文檔介紹配置整合以及對Device Insights和Cisco Umbrella整合進行故障排除的步驟。

必要條件

需求

思科建議您瞭解這些主題。

- SecureX
- Umbrella
- API基礎知識
- Postman API工具

採用元件

本文件中的資訊是以下列軟體和硬體版本為依據.

- SecureX 1.103

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。

背景資訊

SecureX Device Insights提供組織中裝置的統一檢視，並整合來自整合資料來源的清單。

Umbrella自動發現針對當前威脅而轉移的攻擊者基礎設施，並在惡意請求到達組織的網路或終端之前主動阻止它們。通過整合，您可以更早地阻止惡意軟體感染、更快地識別已感染的裝置，並防止資料洩露。該整合提供了對所有位置和使用者的Internet活動的完整可視性，並且允許您通過兩鍵式響應來採取行動來快速阻止域。支援多個Umbrella功能，並通過Umbrella平台中生成的API金鑰連

結這些功能。

如果您想瞭解有關配置的更多資訊，請檢視整合模組詳細資訊。

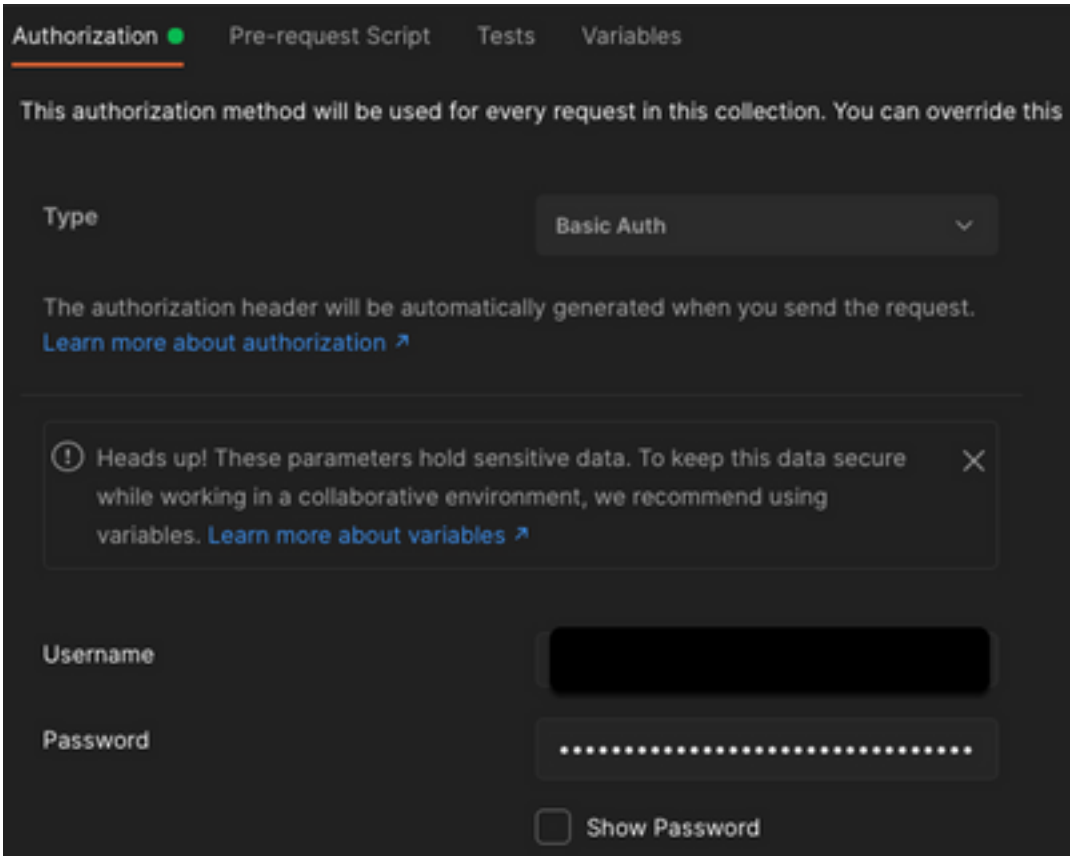
疑難排解

為了解決SecureX和Umbrella整合的常見問題，您可以驗證API的連線和效能。

使用Device Insights和Umbrella進行連線測試

步驟1。您可以選擇**Basic** Authas作為授權方法，因為MobileIron將使用此方法，如下圖所示。

> **附註**：Postman不是思科開發的工具。如果您對Postman工具功能有任何疑問，請聯絡Postman支援。



步驟2.您可以透過此API呼叫取得**協同作業**電腦（預設頁面限製為100個專案）。

```
https://management.api.umbrella.com/v1/organizations/
```

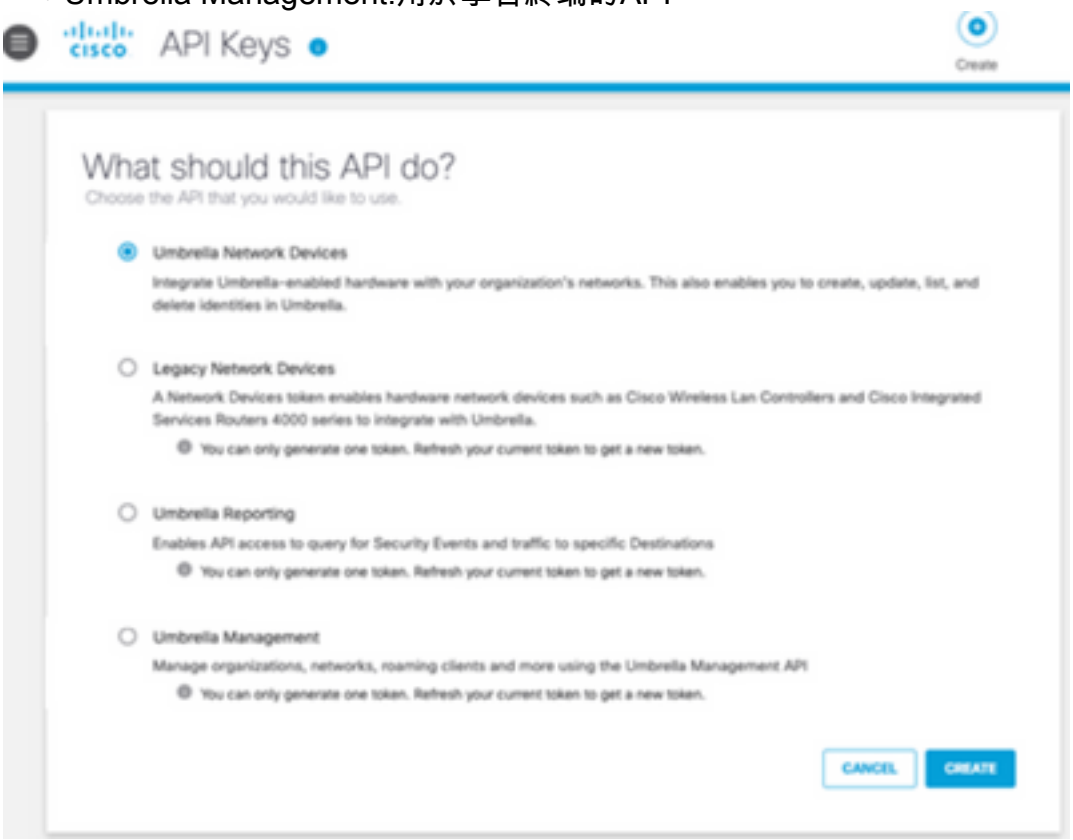
步驟3.響應第一次呼叫，返回對象總數。可以使用Limit和Page引數獲取下一頁。

```
https://management.api.umbrella.com/v1/organizations/
```

金鑰錯誤

Device Insights使用的金鑰與SecureX使用的金鑰不同，因此需要驗證並確認配置為Umbrella API金鑰的金鑰是否正確，如下圖所示。

- Umbrella網路裝置：用於瞭解DNS策略的API
- Umbrella Management:用於學習終端的API



驗證

將Umbrella作為源新增到Device Insights後，您可以看到成功的**REST API連**接狀態。

- 您可以**看到**綠色狀態的REST API連線
- 按一下「**onSync**」，即可觸發初始完全同步，如下圖所示

如果裝置洞察和Umbrella整合問題仍然存在，請參閱本文以從瀏覽器收集HAR日誌，並聯絡TAC支援以執行更深入的分析。

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）。