

排除XDR裝置見解和Umbrella整合故障

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

簡介

本文檔介紹配置整合和排除XDR裝置洞察和Cisco Umbrella整合故障的步驟。

必要條件

需求

思科建議您瞭解這些主題。

- XDR
- 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。

- XDR

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

XDR 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、更快地識別已受感染的裝置，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採取行動，以快速阻止域。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，請檢視整合模組的詳細資訊。

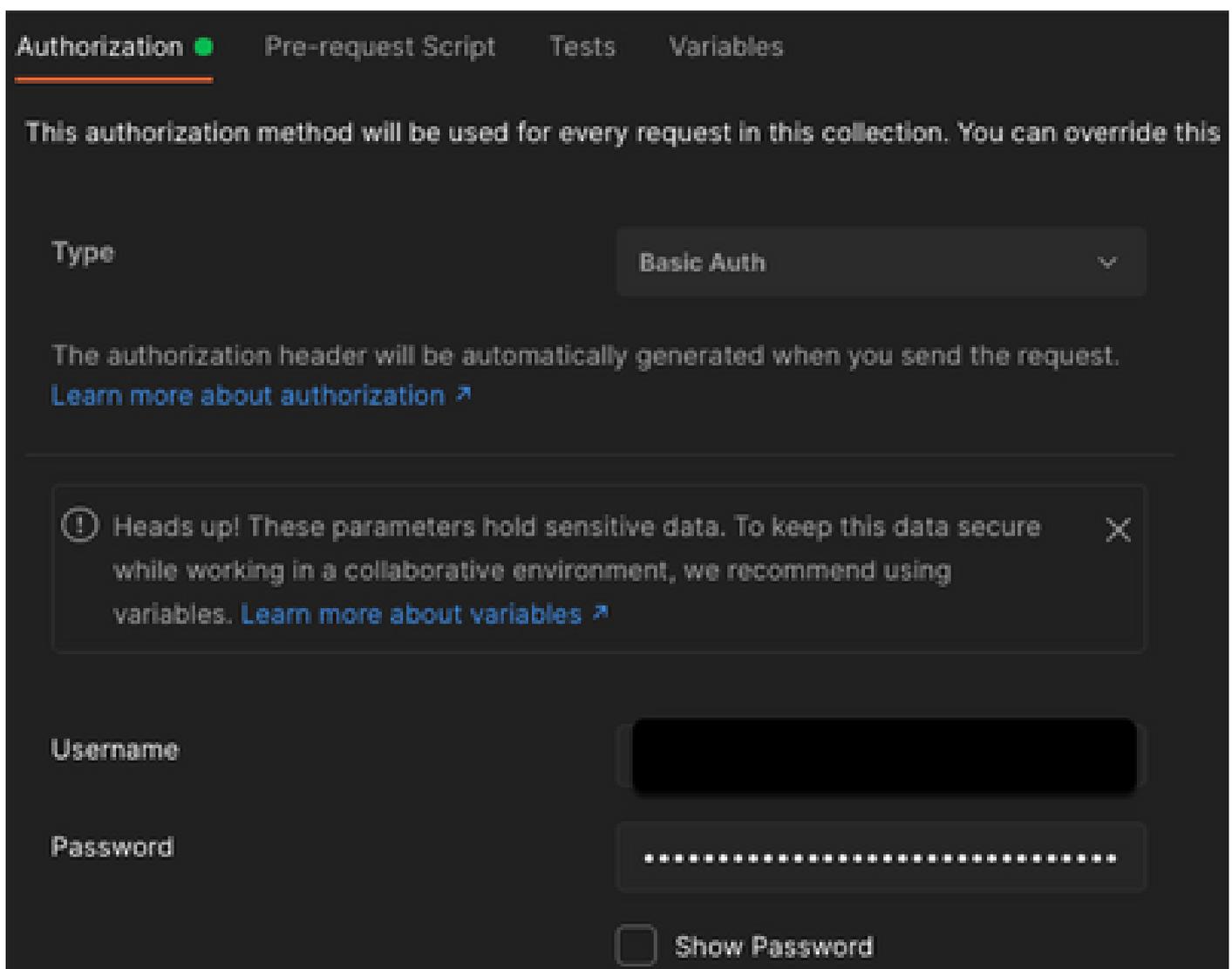
疑難排解

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

使用XDR Device Insights和Umbrella進行連線測試

步驟1.您可以選擇Basic Auths作為授權方法，如下圖所示。

注意: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.您可以使用此API呼叫獲取Roaming電腦（預設頁面限制為100個條目）。

<https://management.api.umbrella.com/v1/organizations/>

/roamingcomputers

步驟3.響應第一個呼叫，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/>

/roamingcomputers?limit=5&page=2

金鑰錯誤

XDR Device Insights使用的金鑰與XDR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

What should this API do?

Choose the API that you would like to use.

Umbrella Network Devices

Integrate Umbrella-enabled hardware with your organization's networks. This also enables you to create, update, list, and delete identities in Umbrella.

Legacy Network Devices

A Network Devices token enables hardware network devices such as Cisco Wireless Lan Controllers and Cisco Integrated Services Routers 4000 series to integrate with Umbrella.

You can only generate one token. Refresh your current token to get a new token.

Umbrella Reporting

Enables API access to query for Security Events and traffic to specific Destinations

You can only generate one token. Refresh your current token to get a new token.

Umbrella Management

Manage organizations, networks, roaming clients and more using the Umbrella Management API

You can only generate one token. Refresh your current token to get a new token.

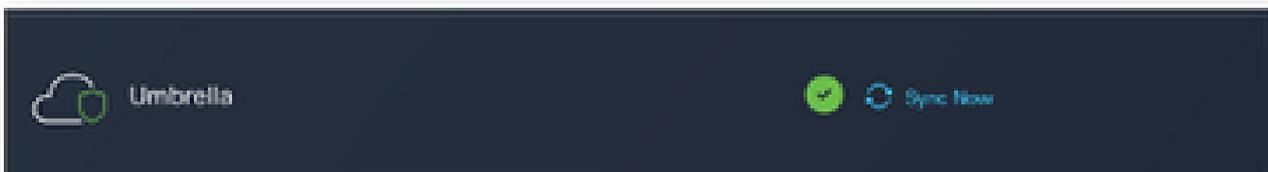
CANCEL

CREATE

驗證

將Umbrella作為XDR裝置洞察的源新增後，您可以看到成功的REST API連接狀態。

- 您可以看到REST API連接處於綠色狀態
- 按一下SYNC NOW以觸發初始完全同步，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）。