

通過Postman使用Umbrella Reporting API

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[概觀](#)

[Umbrella過程](#)

[Postman程式](#)

[響應](#)

簡介

本文檔介紹如何在Postman中使用Cisco Umbrella Reporting API。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據Cisco Umbrella。

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。

概觀

Umbrella API於2022年9月發佈，提供一個使用者友好且安全的平台，使使用者能夠在Umbrella的基礎上構建、擴展和整合。

Umbrella API終端託管在api.umbrella.com上，每個使用案例都有分組的路徑。可以在Umbrella控制面板中的Admin > API keys下管理API金鑰，也可以使用[KeyAdmin API以程式設計方式管理API金鑰](#)。每個金鑰可以細粒度配置，並在五個主要使用案例下分組多個範圍：

- [管理](#)API終端使您能夠調配和管理Umbrella API金鑰和使用者、檢視角色以及管理提供商和託管提供商的客戶。
- [Auth](#) API端點可授權其他服務與Umbrella平台的整合。
- [部署](#)API終端使您能夠調配、監控和管理網路和其他各種實體，並通過在現有Umbrella策略中

配置它們來保護這些實體的安全。

- [策略](#) API端點使您能夠調配和管理目標清單以及每個清單的目標。
- [報告](#) API端點使您能夠讀取和稽核有關部署的即時安全資訊。Umbrella App Discovery API可讓您深入瞭解基於雲的應用程式。

本文演示如何通過API收集活動搜尋報告。

Umbrella過程

1. 從Umbrella控制面板導航到Admin > API Keys。
2. 選擇API Keys > Add。
3. 在金鑰範圍下，選擇Reports，然後選擇Create Key。

Add New API Key

To add this unique API key to Umbrella, select its scope—what it can do—and set an expiry date. The key and secret created here are unique. Deleting, refreshing or modifying this API key may break or interrupt integrations that use this key. For more information, see Umbrella's [Help](#).

API Key Name

API - Reporting

Description (Optional)

Key Scope

Select the appropriate access scopes to define what this API key can do.

- | | |
|---|------|
| ☐ Admin | 4 > |
| ☐ Auth | 1 > |
| ☐ Deployments | 11 > |
| ☐ Policies | 4 > |
| ☒ Reports | 5 > |

1 selected

Remove All

Scope	
Reports	Read / Write 5 X

Expiry Date

☒ Never expire

☐ Expire on Jan 7 2024

Click Refresh to generate a new key and secret.
For more information, see Umbrella's [Help](#).

API Key

[Redacted API Key]

Key Secret

[Redacted Key Secret]

Copy the Key Secret. For security reasons, it is only displayed once. If lost, it cannot be retrieved.

[ACCEPT AND CLOSE](#)

21495050167956

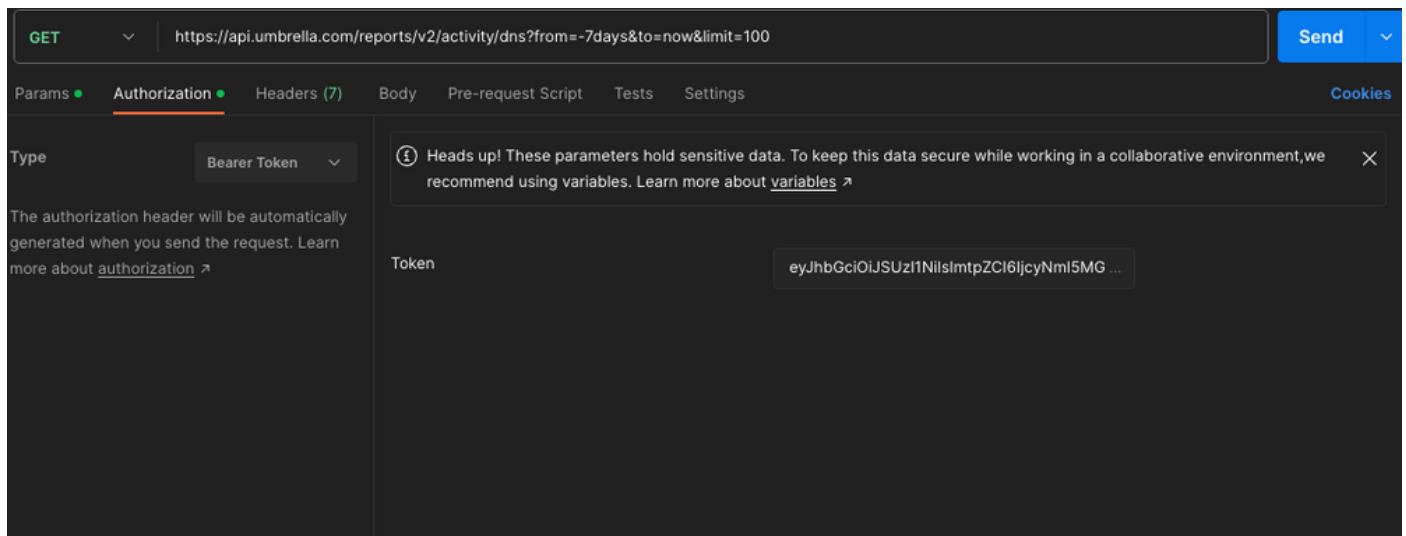
管理員可以根據每個API金鑰的預期用途調整每個作用域的讀/寫和只讀訪問級別，而API金鑰可以配置為在預定義日期過期。在此步驟中，您需要收集API金鑰/金鑰，因為它們當前可見，之後無法顯示。

Postman程式

The screenshot shows the Postman interface for a POST request to `https://api.umbrella.com/auth/v2/token`. The **Authorization** tab is active, displaying **Basic Auth**. A warning message is shown: "Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. Learn more about variables". The **Username** and **Password** fields are visible, with the password field masked with red dots.

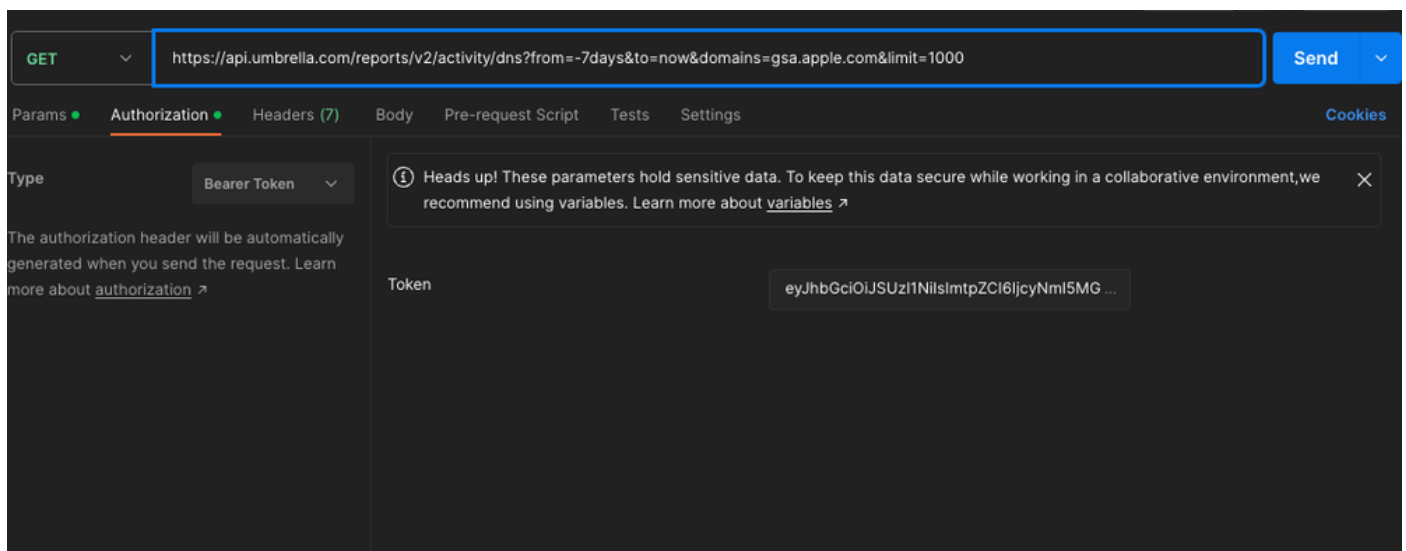
[illegible]

您需要選擇GET方法，並輸入API路徑（包括所需的引數）和訪問令牌。在此示例中，您可以為過去7天的DNS流量從活動搜尋中專門檢索100個報告。



21607952074772

在另一個示例中，您可以嘗試從活動搜尋提取1000個報告，僅針對過去7天的DNS流量，特別是針對「gsa.apple.com」域。



21607927544468

您可以諮詢[請求查詢引數](#)，以發現您可以在API查詢中使用的其他引數。



附註：如果HTTP客戶端請求不是源自Umbrella資料倉儲所在的大洲，則Umbrella伺服器會使用302 Found進行響應。若要自動重定向HTTP請求並保留HTTP授權標頭，可以設定其他標誌或啟用重定向設定。

捲曲:您必須傳遞 — L或 — location和 — location-trusted標誌以重定向捲曲HTTP請求並保留授權標頭。

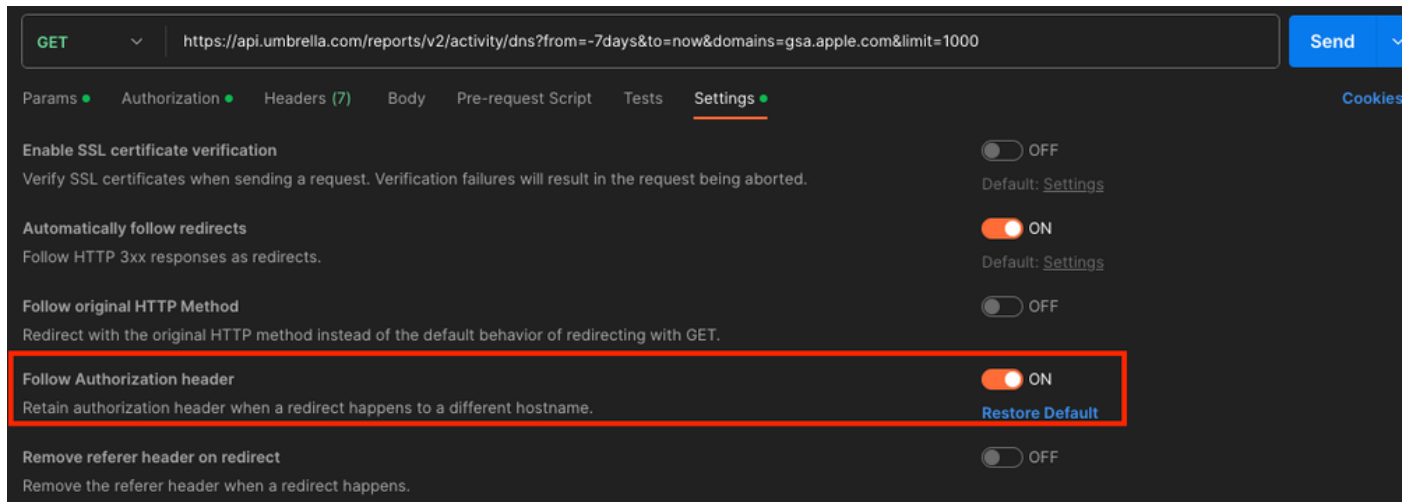
cURL ▾



```
1 curl --location--trusted 'https://api.umbrella.com/reports/v2/activity/dns?from=-7days&to=now&domains=gsa.apple.com&limit=1000' \
```

21608126036628

郵政:在Postman環境中，導航到一個API並選擇一個GET方法。導覽至Settings > Enable Follow Authorization header，以保留重新導向請求的授權標頭。



21608126042388

響應

向URL傳送GET操作後，您可以接收各種狀態代碼：

- 狀態:200:請求已成功獲取您請求的資訊。
- 狀態：400：請求無效。它可能與您傳送查詢的URL相關。一個或多個引數不正確。
- 狀態：401：未授權。缺少授權標頭或令牌未經授權。
- 狀態：403：禁止。令牌無效。

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）。