

# 如何使用AMP API建立事件流

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[驗證](#)

[疑難排解](#)

## 簡介

本文說明如何使用Postman工具在面向終端的AMP ( 高級惡意軟體防護 ) 中配置事件流。

作者：Nancy Pérez、Yeraldin Sánchez、Cisco TAC工程師。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- [對思科終端進階惡意軟體防護](#)
- 來自AMP門戶的API憑證：第三方API客戶端ID和API金鑰，在此連結上您可以找到獲取這些金鑰的步驟：[如何從AMP門戶生成API憑據](#)
- 本文檔中的API處理程式使用Postman工具

### 採用元件

本檔案中的資訊是根據以下軟體和硬體版本：

- 適用於終端的AMP主控台版本5.4.20200107
- Postman 7.16.0版
- [AMP API文檔, v1](#)

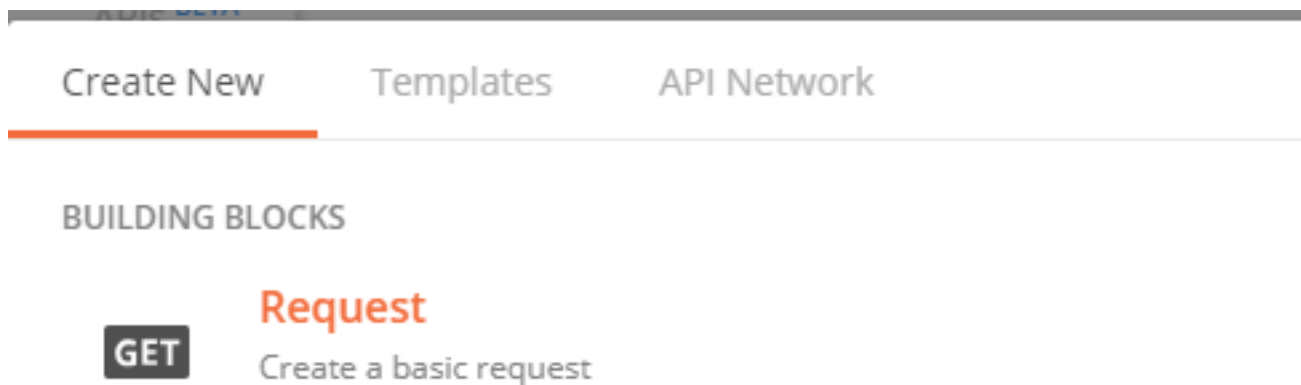
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 ( 預設 ) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

### 背景資訊

思科不支援Postman工具，如果您對此有疑問，請與Postman支援部門聯絡。

## 設定

步驟1。在Postman首頁中，選擇**Create a request**以建立新的事件流，如下圖所示。



步驟2.選擇**POST**並貼上執行查詢所需的URL，如下圖所示。

要鍵入您的第<sup>三</sup>方API客戶端ID和API金鑰，請選擇**基本授權**。

**使用者名稱**=第<sup>三</sup>方API客戶端ID

**密碼**= API金鑰

Launchpad POST https://api.amp.cisco.com/v1/... + ...

### Untitled Request

POST https://api.amp.cisco.com/v1/event\_streams

Params **Auth** Headers Body Pre-req. Tests Settings Cookies Code Resp

**TYPE**

Basic Auth Preview Request

The authorization header will be automatically generated when you send the request. [Learn more about authorization](#)

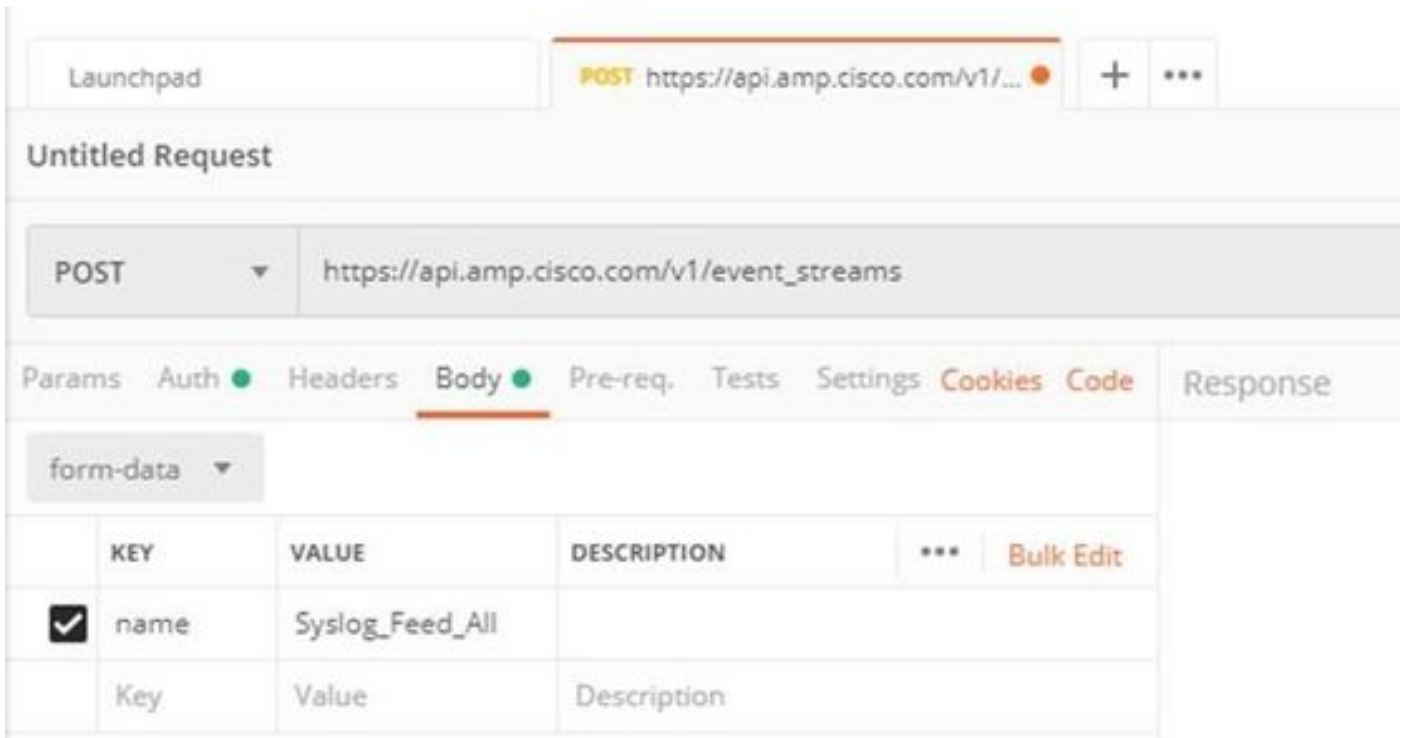
! Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. [Learn more about variables](#)

Username

Password

Show Password

步驟3.在Body部分，選擇form-data。KEY用「name」字填充，VALUE用事件流的名稱填充。確保該行已標籤。



步驟4.此時，您可以點選**Send**按鈕接收事件流。

註：每個組織限制有5個有效資源

## 驗證

使用本節內容，確認您的組態是否正常運作。

生成事件流後，可以使用GET [https://api.amp.cisco.com/v1/event\\_streams](https://api.amp.cisco.com/v1/event_streams) 命令對其進行驗證，該命令顯示在組織上建立的事件流數，如下圖所示。

```
1  {
2      "version": "v1.2.0",
3      "metadata": {
4          "links": {
5              "self": "https://api.amp.cisco.com/v1/event\_streams"
6          },
7          "results": {
8              "total": 5
9          }
10 }
```

在本節中，您可以找到作為ID、名稱和AMP憑據的事件流資訊

若要獲取有關活動事件流的資訊，可以使用GET [https://api.amp.cisco.com/v1/event\\_streams/id](https://api.amp.cisco.com/v1/event_streams/id)

## 疑難排解

目前尚無適用於此組態的具體疑難排解資訊。