

# AMP APIを使用してイベントストリームを作成する方法

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

## 概要

このドキュメントでは、Postmanツールを使用してAMP(Advanced Malware Protection)for Endpointsでイベントストリームを設定する手順について説明します。

著者 : Cisco TACエンジニア、Nancy Perez、Yeraldin Sanchez

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Cisco AMP for Endpointsコンソールへのアクセス
- AMPポータルからのAPIクレデンシャル : サードパーティAPIクライアントIDとAPIキーは、このリンクで取得する手順を参照できます。[AMPポータルからAPIクレデンシャルを生成する方法](#)
- このドキュメントでは、APIハンドラをPostmanツールで使います

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- AMP for Endpointsコンソールバージョン5.4.20200107
- Postmanバージョン7.16.0
- [AMP APIドキュメント、v1](#)

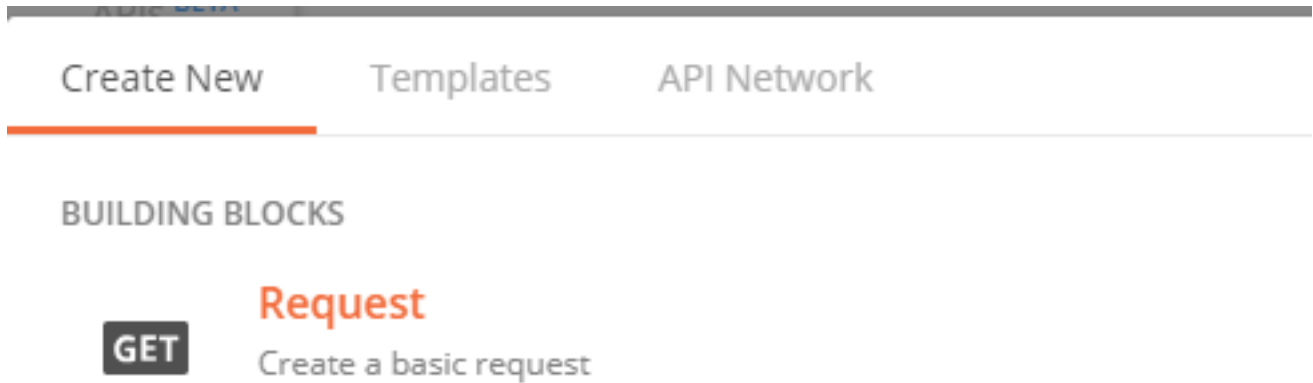
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

### 背景説明

シスコはPostmanツールをサポートしていません。ご質問がございましたら、Postmanサポートにお問い合わせください。

## 設定

ステップ1：図に示すように、Postmanホームページで**Create a request**を選択し、新しいイベントストリームを作成します。



ステップ2：図に示すように、[POST]を選択し、クエリを実行するために必要なURLを貼り付けます。

サードパーティAPIクライアントIDとAPIキーを入力するには、[基本認証]を選択します。

ユーザー名= 3<sup>rd</sup> Party API Client ID

パスワード= APIキー

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

ステップ3:[本文]セクションで、**form-data**を選択します。KEYは「name」という単語で埋められ、VALUEはイベント・ストリームの名前で埋められます。行がマークされていることを確認します。

The screenshot shows a REST client interface with a browser tab labeled "Launchpad" and a "POST" request to "https://api.amp.cisco.com/v1/...". The main area is titled "Untitled Request" and shows a "POST" method to "https://api.amp.cisco.com/v1/event\_streams". The "Body" tab is selected, showing "form-data" as the content type. A table below lists the form data:

	KEY	VALUE	DESCRIPTION	...	Bulk Edit
<input checked="" type="checkbox"/>	name	Syslog_Feed_All			
	Key	Value	Description		

ステップ4：この時点で、[Send]ボタンをクリックしてイベントストリームを受信できます。

注:各組織で有効なリソースの制限は5です。

## 確認

ここでは、設定が正常に機能しているかどうかを確認します。

イベントストリームが生成されたら、GET [https://api.amp.cisco.com/v1/event\\_streams](https://api.amp.cisco.com/v1/event_streams) コマンドを使用して確認できます。このコマンドは、図に示すように、組織で作成されたイベントストリームの数を表示します。

```
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 |   },
```

このセクションでは、ID、名前、およびAMPクレデンシャルとしてイベントストリーム情報を検索できます

アクティブなイベントストリームに関する情報を取得するには、GET [https://api.amp.cisco.com/v1/event\\_streams/id](https://api.amp.cisco.com/v1/event_streams/id) を使用します

# トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。