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

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ツールで使用します

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](#)

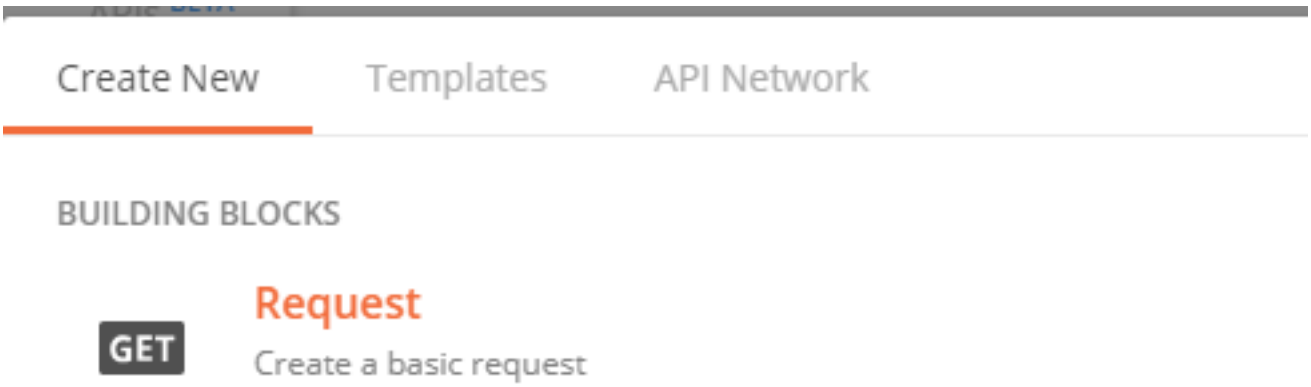
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

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。

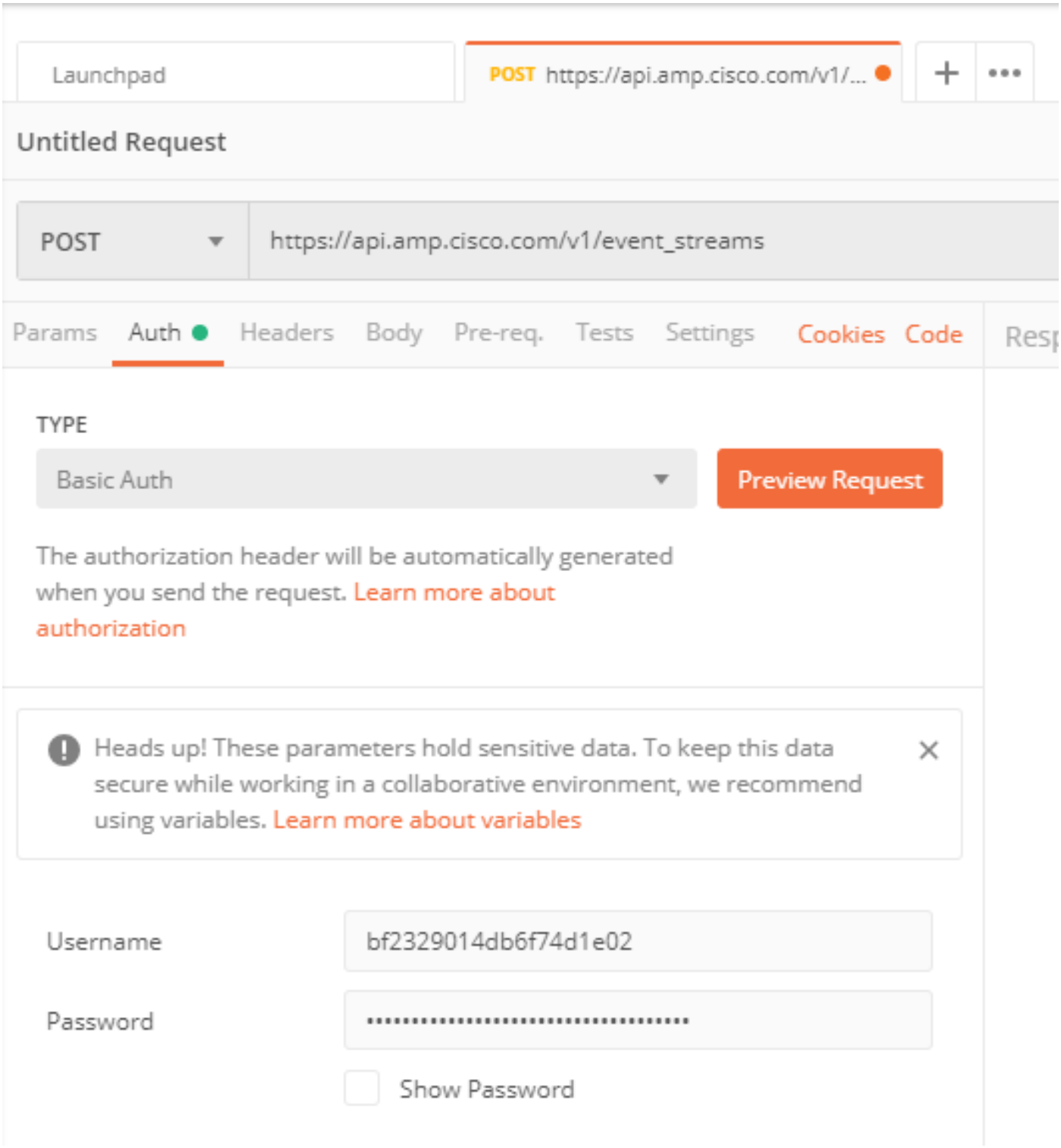


ステップ2：図に示すように、[**POST**]を選択し、クエリを実行するために必要なURLを貼り付けます。

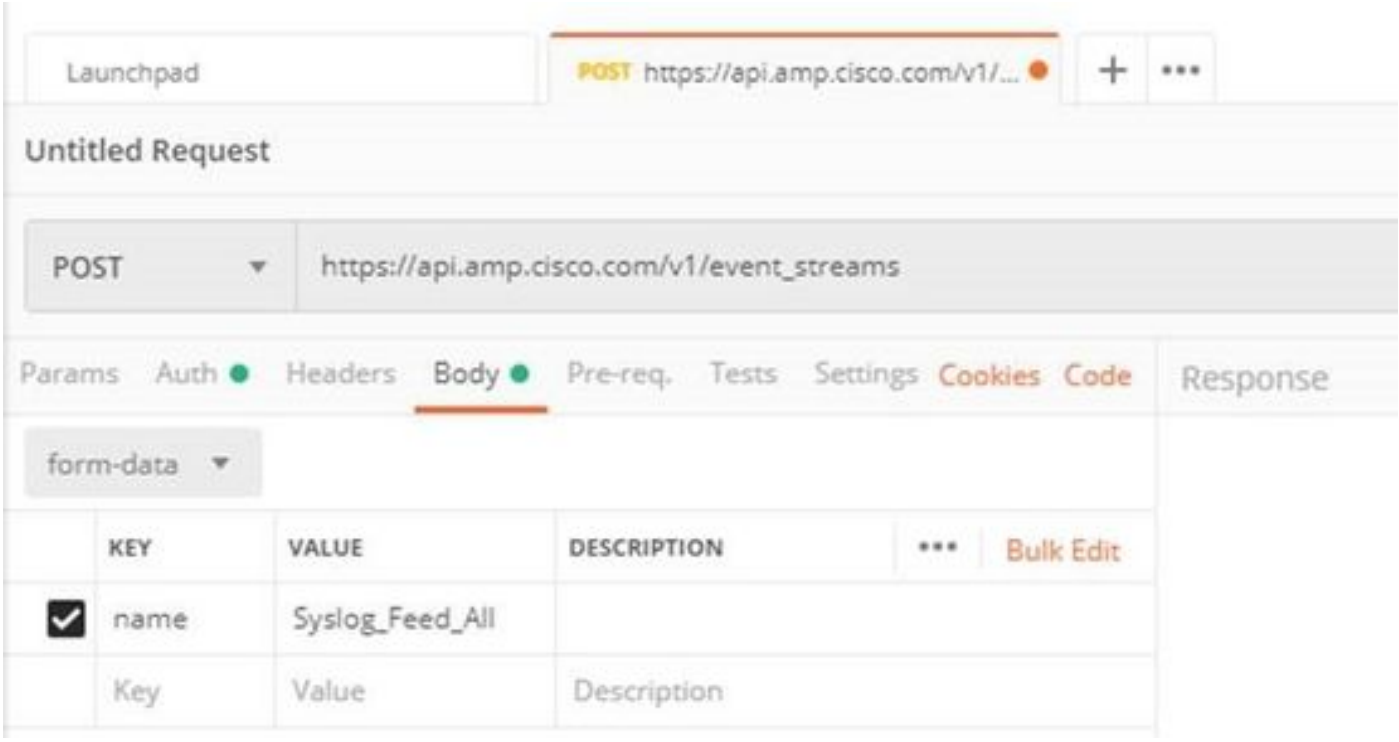
サードパーティAPIクライアントIDとAPIキーを入力するには、[基本認証]を**選択します。**

ユーザ名= 3rd Party API Client ID

パスワード= APIキー



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。



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。

```
{
    "version": "v1.2.0",
    "metadata": {
        "links": {
            "self": "https://api.amp.cisco.com/v1/event_streams"
        },
        "results": {
            "total": 5
        }
    },
```

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"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。