AMP API를 사용하여 이벤트 스트림을 생성하는 방법

목차

소개

이 문서에서는 Postman 툴을 사용한 엔드포인트용 AMP(Advanced Malware Protection)에서 이벤트 스트림을 구성하는 방법에 대해 설명합니다.

기고자: Nancy Pérez, Yeraldin Sánchez, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco AMP for Endpoints 콘솔 액세스
- AMP 포털의 API 자격 증명:이 링크에서 타사 API 클라이언트 ID 및 API 키를 가져오는 단계를 찾을 수 있습니다.AMP 포털에서 API 자격 증명을 생성하는 방법
- 이 문서에서 API 처리기는 Postman 도구로 사용됩니다

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

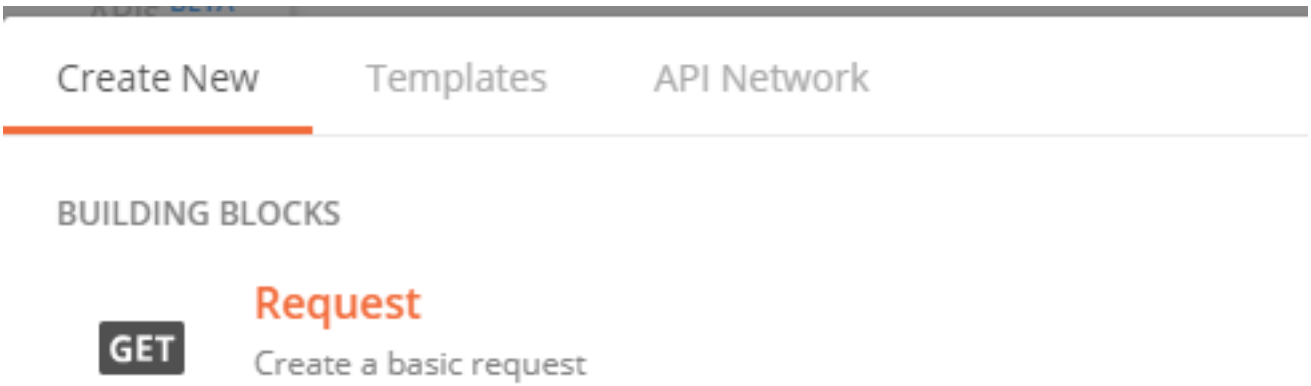
- AMP for Endpoints 콘솔 버전 5.4.20200107
- Postman 버전 7.16.0
- AMP API 설명서, v1

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

구성

1단계. Postman 홈 페이지에서 **Create a request**를 선택하여 새 이벤트 스트림을 생성합니다(이미지에 표시됨).

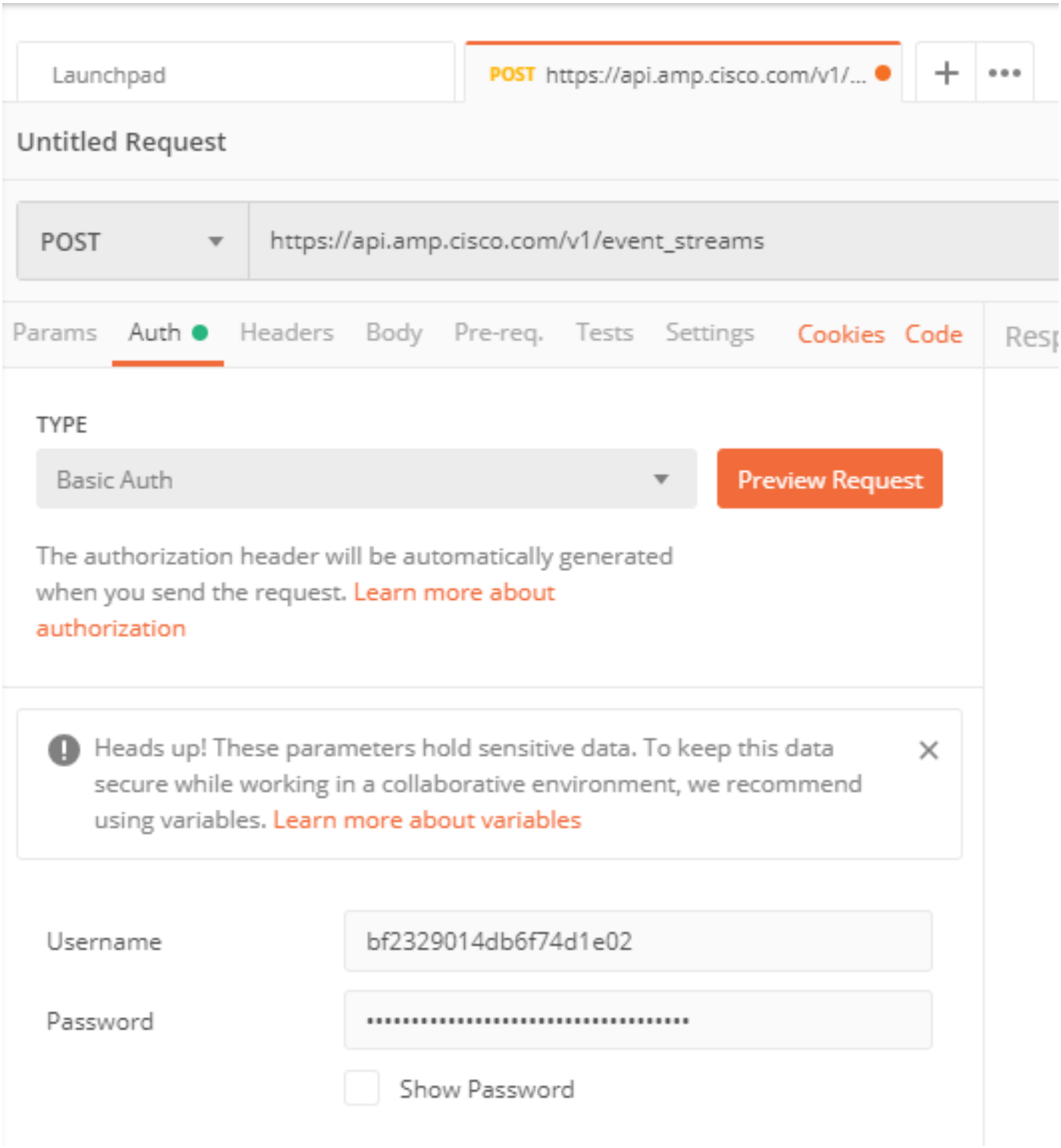


2단계. **POST**를 선택하고 이미지에 표시된 대로 쿼리를 수행하는 데 필요한 URL을 붙여넣습니다.

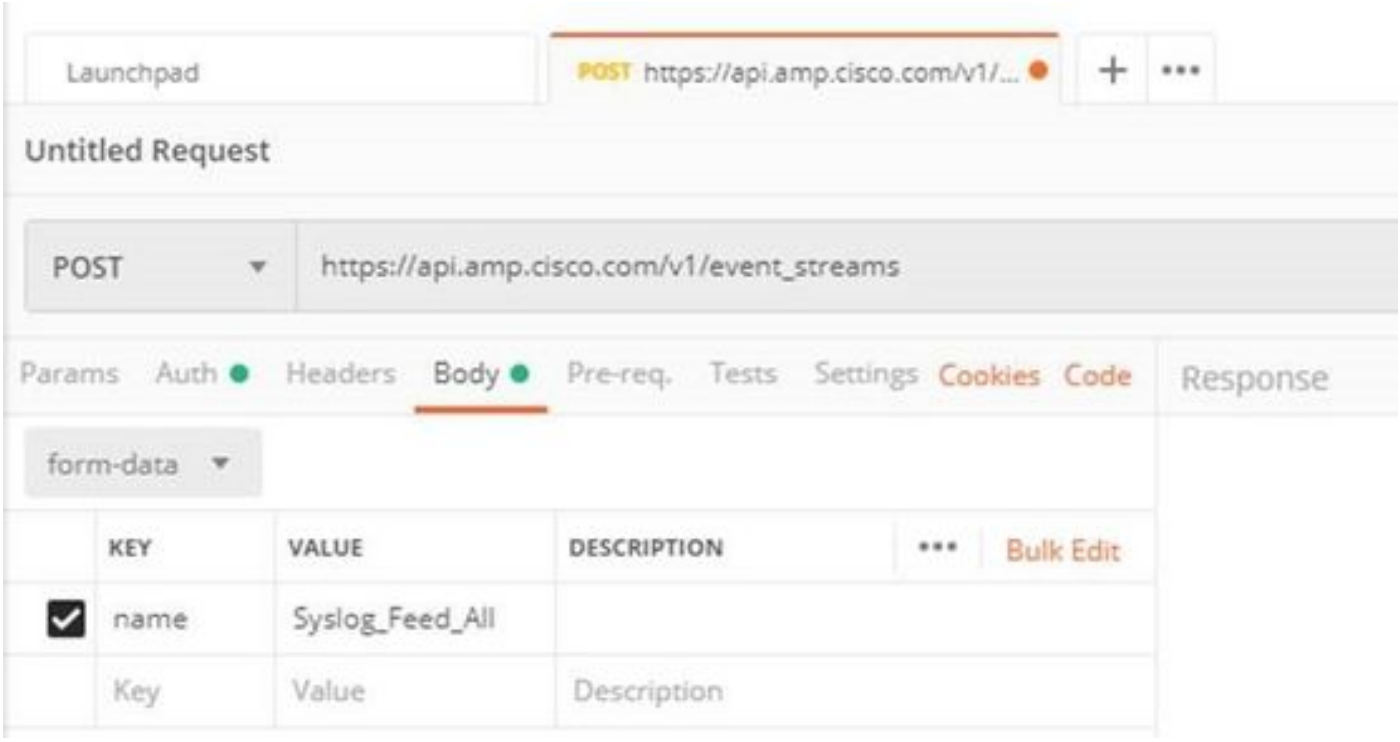
3rd Party API Client ID 및 API Key를 입력하려면 **Basic Authorization**을 선택합니다.

사용자 이름= 3rd Party API 클라이언트 ID

비밀번호= API 키



3단계. **본문** 섹션에서 **양식 데이터를** 선택합니다.**KEY**는 "name" 단어로 채워지고 **VALUE**는 이벤트 스트림 이름으로 채워집니다.행이 표시되어 있는지 확인합니다.



4단계. 이때 **Send** 버튼을 클릭하여 이벤트 스트림을 수신할 수 있습니다.

참고: 각 조직 전체에서 5개의 활성 리소스 제한

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

이벤트 스트림이 생성되면 이미지에 표시된 대로 조직에서 생성된 이벤트 스트림 수를 표시하는 GET https://api.amp.cisco.com/v1/event_streams 명령을 사용하여 이를 확인할 수 있습니다.

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

이 섹션에서는 이벤트 스트림 정보를 ID, 이름 및 AMP 자격 증명으로 찾을 수 있습니다

활성 이벤트 스트림에 대한 정보를 얻으려면 GET https://api.amp.cisco.com/v1/event_streams/"id"를 사용할 수 있습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.