如何使用AMP API创建事件流

目录

简介

本文档介绍如何使用Postman工具在面向终端的AMP（高级恶意软件防护）中配置事件流的步骤。

作者：Nancy Pérez、Yeraldin Sánchez，Cisco TAC工程师。

先决条件

要求

Cisco 建议您了解以下主题：

- 访问面向终端的思科AMP控制台
- 来自AMP门户的API凭证：第3方API客户端ID和API密钥，在此链接上，您可以找到获取这些密钥的步骤：如何从AMP门户生成API凭证
- 本文档中使用的API处理程序是Postman工具

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 面向终端的AMP控制台版本5.4.20200107
- 邮递员版本7.16.0
- AMP API文档，v1

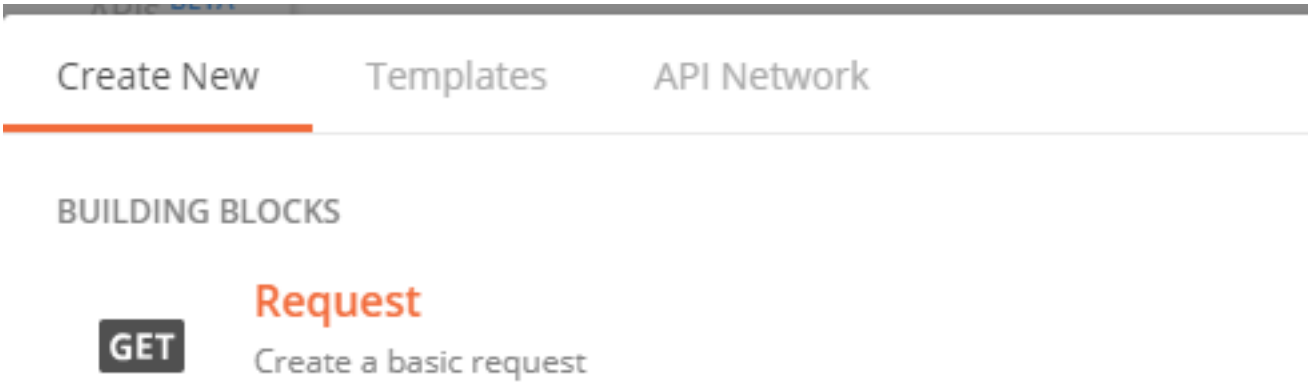
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

思科不支持邮递员工具，如果您对此有疑问，请联系邮递员支持。

配置

步骤1.在Postman主页中，选择**Create a request** 以创建新事件流，如图所示。

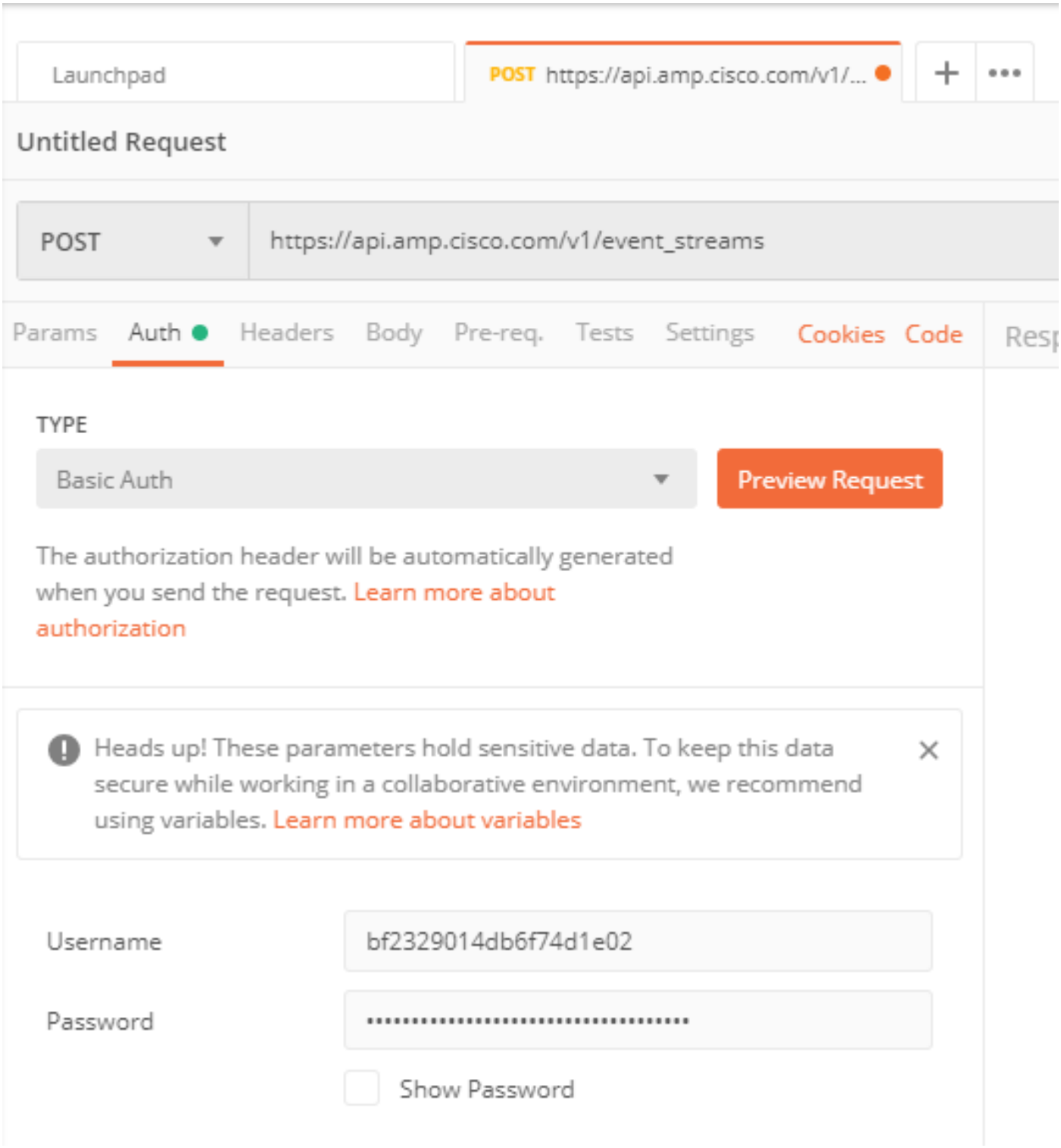


步骤2.选**择POST**并粘贴执行查询所需的URL，如图所示。

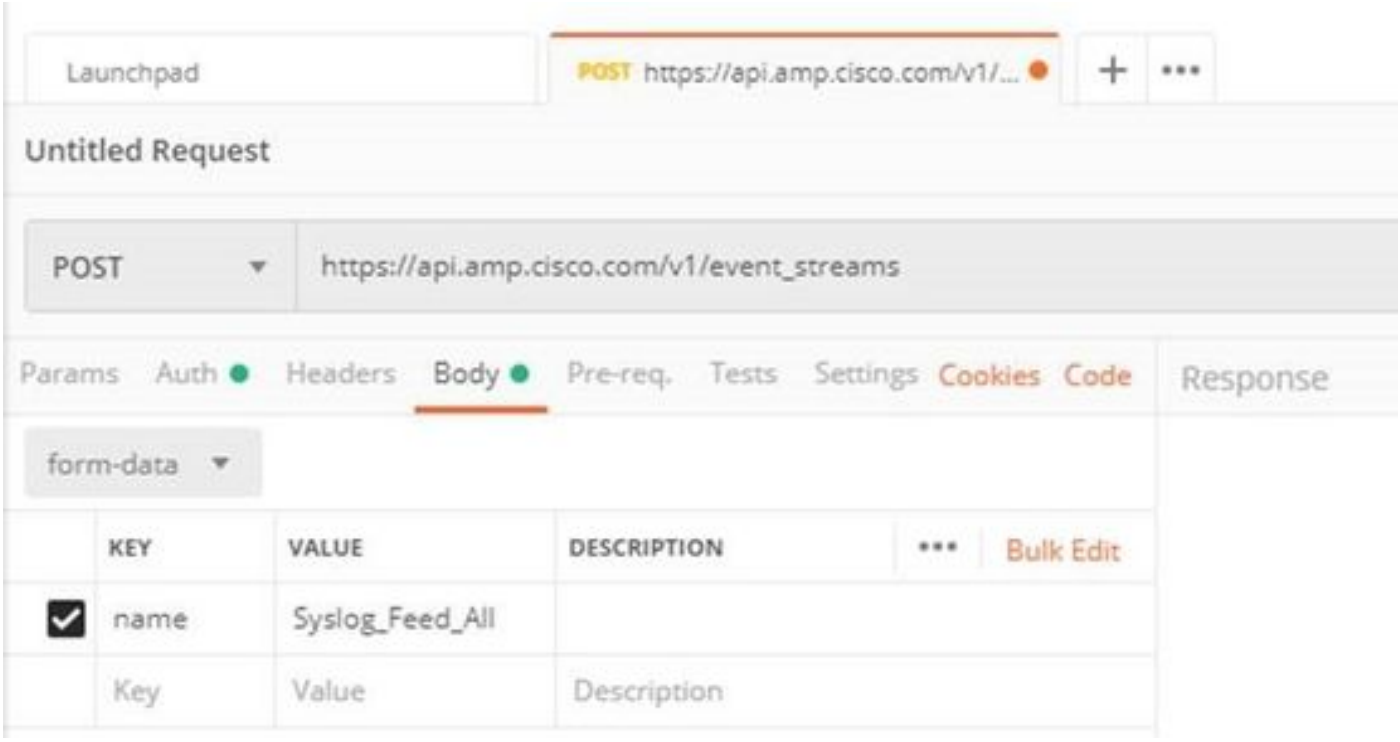
要键入您的第三方API客户端ID和API密钥，请选择**Basic Authorization。**

用户名=第三方API客户端ID

密码= API密钥



步骤3.在“正文”部分，选择**表单数据。KEY**中填入“name”字，**VALUE**中填入事件流的名称。确保已标记该行。



步骤4.此时，您可以单击“发送”**按钮**来接收事件流。

注：每个组织中5个有效资源的限制

验证

使用本部分可确认配置能否正常运行。

生成事件流后，可以使用GET https://api.amp.cisco.com/v1/event_streams命令验证该事件流，该命令显示在组织上创建的事件流数，如图所示。


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


在本节中，您可以找到事件流信息作为ID、名称和AMP凭证

要获取有关活动事件流的信息，可以使用GET https://api.amp.cisco.com/v1/event_streams/"id"

故障排除

目前没有针对此配置的故障排除信息。