Como criar um fluxo de eventos com APIs da AMP

Contents

Introduction

Este documento descreve as etapas de como configurar um fluxo de eventos no AMP (Advanced Malware Protection, Proteção avançada contra malware) para endpoints com a ferramenta Postman.

Contribuído por Nancy Pérez, Yeraldin Sánchez, Engenheiros do TAC da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso ao console Cisco AMP para endpoints
- Credenciais de API do portal AMP: ID do cliente API de terceiros e chave de API, neste link você pode encontrar as etapas para obtê-los: Como gerar uma credencial de API no portal AMP
- Um manipulador de API, neste documento, é usado na ferramenta Postman

Componentes Utilizados

As informações neste documento são baseadas nas seguintes versões de software e hardware:

- AMP for Endpoints console versão 5.4.200107
- Postman versão 7.16.0
- documentação de API AMP, v1

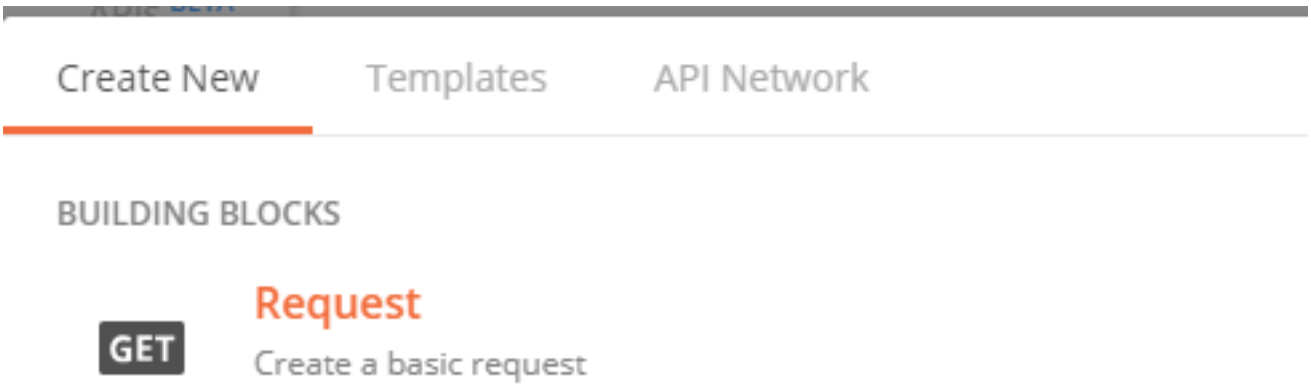
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A Cisco não oferece suporte à ferramenta Postman. Se você tiver alguma dúvida, entre em contato com o suporte do Postman.

Configurar

Etapa 1. Na página inicial do Postman, selecione **Create a request** para criar um novo fluxo de eventos, como mostrado na imagem.

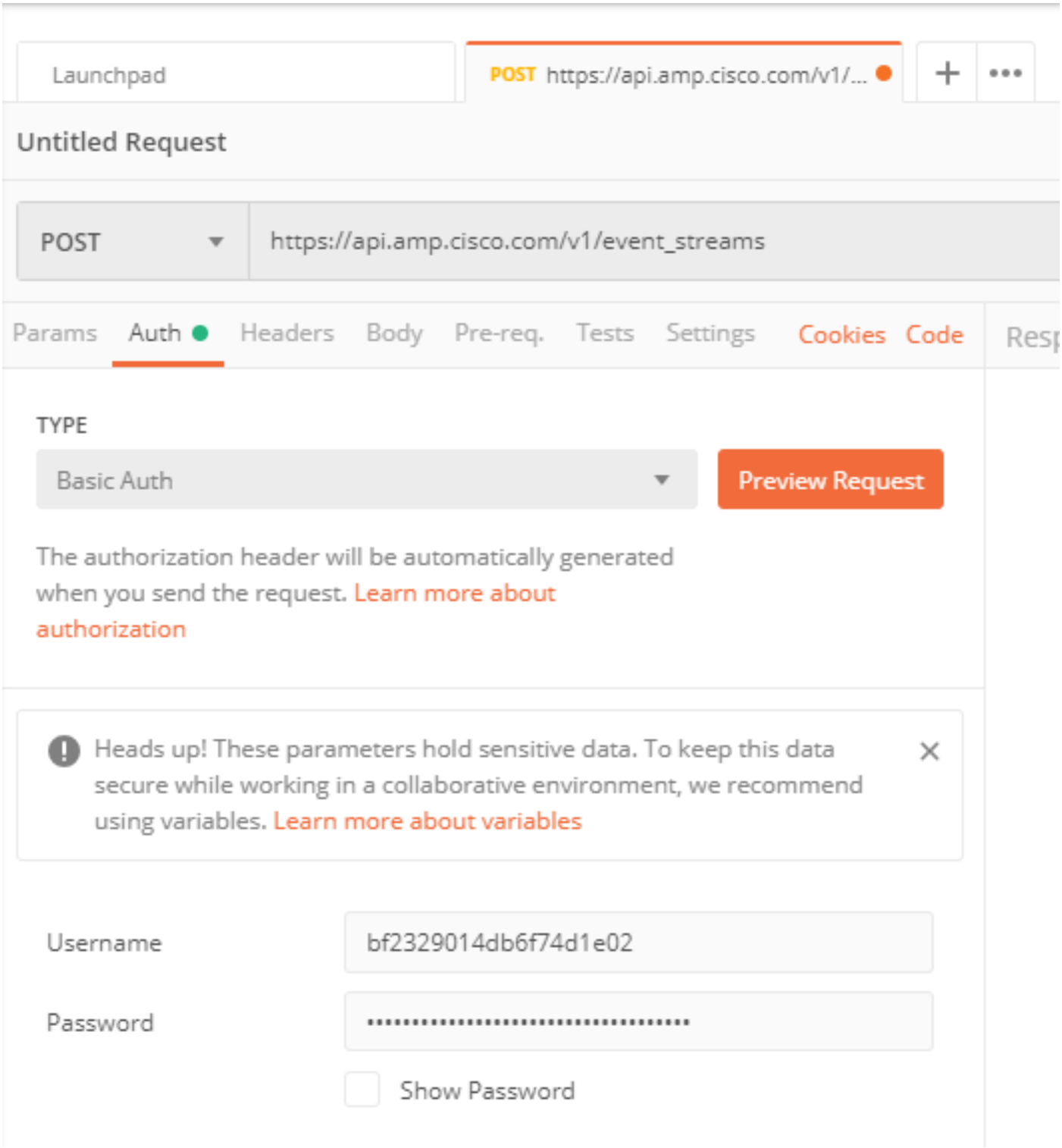


Etapa 2. Selecione **POST** e cole a URL necessária para fazer a consulta, como mostrado na imagem.

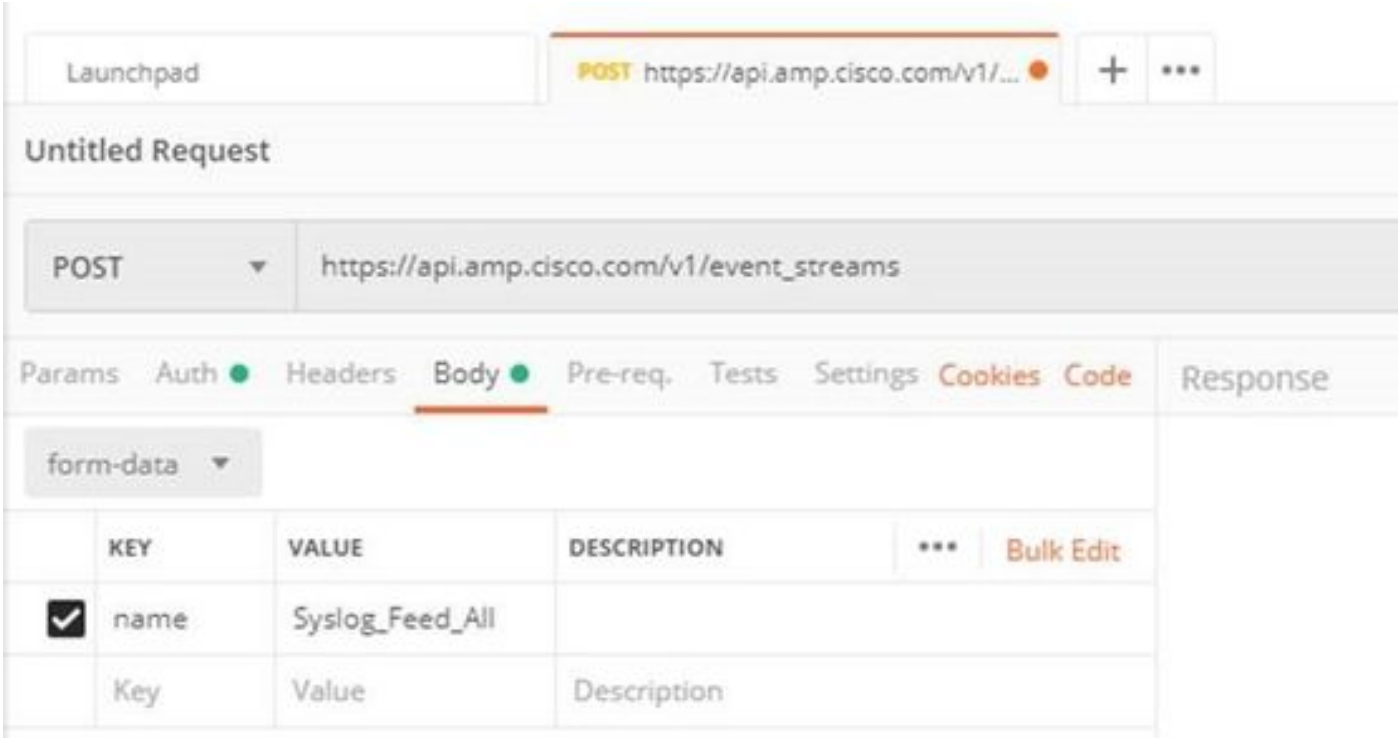
Para digitar sua ID de cliente de API de 3terceiros e chave de API, selecione **Autorização básica.**

Nome de usuário= 3 terceiros ID do cliente da API

Password= API Key



Etapa 3. Na seção **Corpo**, selecione **form-data. A CHAVE** é preenchida com a palavra "nome", **VALUE é** preenchido com o nome do fluxo de eventos. Verifique se a linha está marcada.



Etapa 4. Nesse ponto, você pode clicar no botão **Enviar** para receber o fluxo de eventos.

Observação: limite de 5 recursos ativos em cada organização

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Quando o fluxo de eventos é gerado, você pode verificá-lo com o comando GET https://api.amp.cisco.com/v1/event_streams que exibe o número de fluxos de eventos criados na organização, como mostrado na imagem.


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


Nesta seção, você pode encontrar as informações do fluxo de eventos como a ID, o nome e as credenciais do AMP

Para obter informações sobre o fluxo de eventos ativo, você pode usar GET https://api.amp.cisco.com/v1/event_streams/"id"

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.