Cómo crear un flujo de eventos con las API de AMP

Contenido

Introducción

Este documento describe los pasos para configurar un flujo de eventos en AMP (protección frente a malware avanzado) para terminales con la herramienta Postman.

Colaboración de Nancy Pérez, Yeraldin Sánchez, Ingenieros del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso a la consola de Cisco AMP para terminales
- Credenciales de API del portal de AMP: ID de cliente API y clave API de terceros, en este enlace puede encontrar los pasos para obtenerlos: [Cómo generar una credencial de API desde el portal de AMP](#)
- En este documento, se utiliza un controlador API para la herramienta Postman

Componentes Utilizados

La información de este documento se basa en estas versiones de software y hardware:

- Consola de AMP para terminales, versión 5.4.20200107
- Postman versión 7.16.0
- [documentación de AMP API, v1](#)

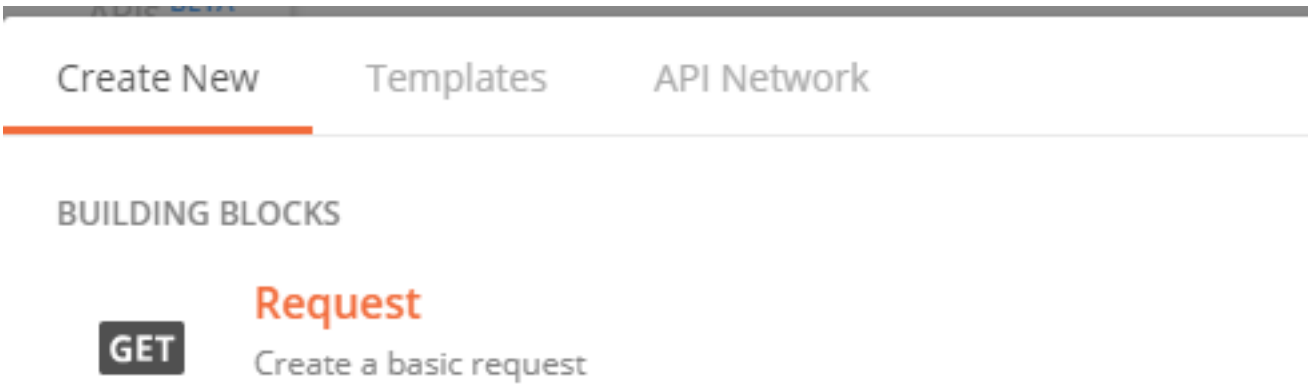
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Cisco no admite la herramienta Postman; si tiene alguna pregunta al respecto, póngase en contacto con el servicio de asistencia técnica de Postman.

Configurar

Paso 1. En la página de inicio de Postman, seleccione **Crear una solicitud** para crear una nueva secuencia de eventos, como se muestra en la imagen.

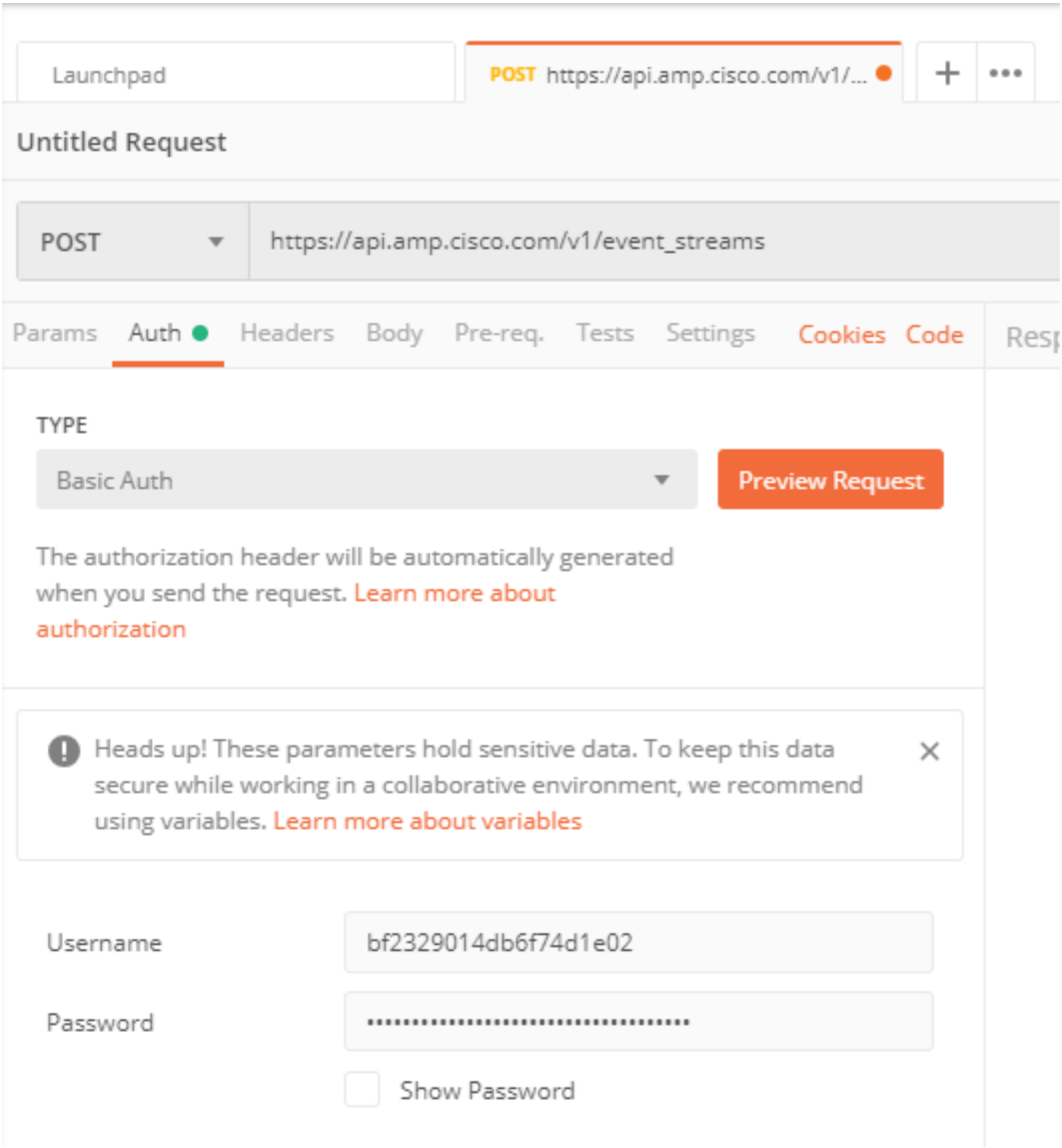


Paso 2. Seleccione **POST** y pegue la URL necesaria para realizar la consulta, como se muestra en la imagen.

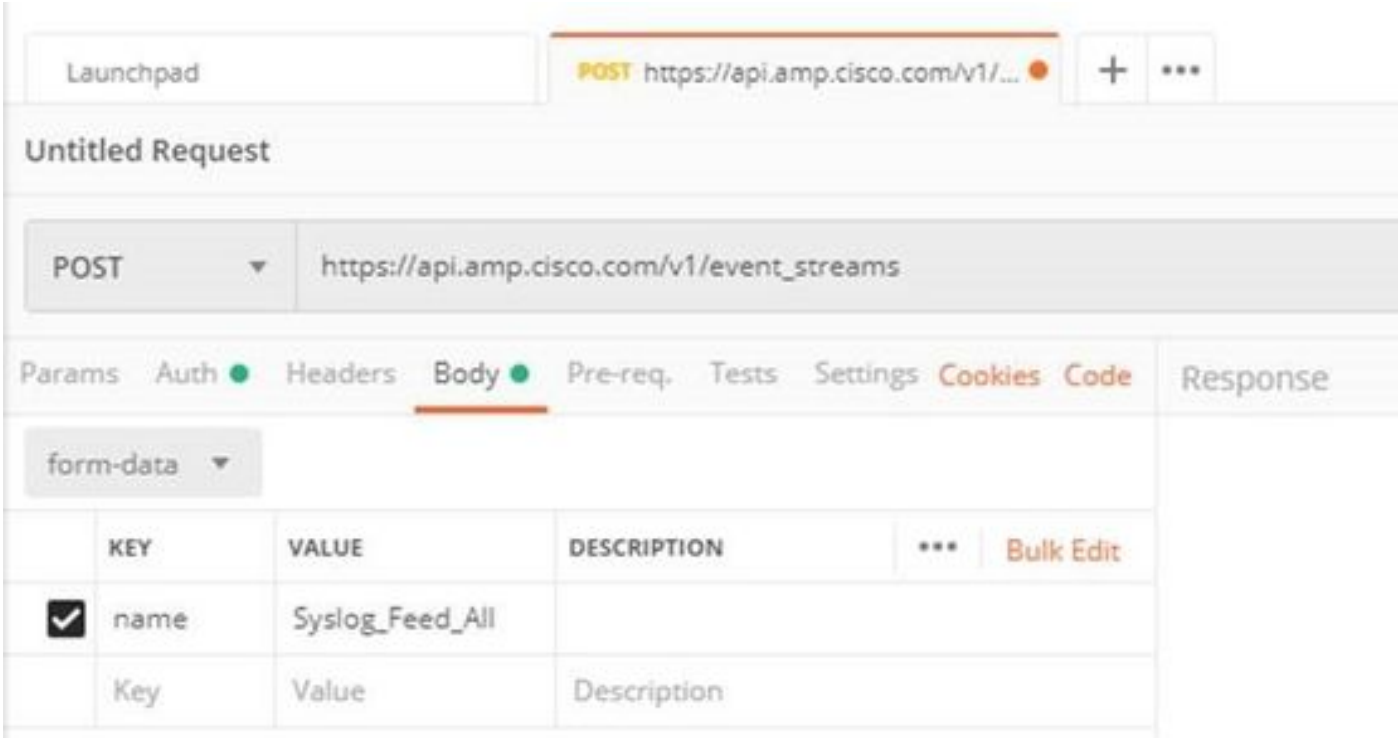
Para escribir su ID de cliente de API y clave de API de 3 terceros, seleccione **Autorización básica.**

Nombre de usuario= 3 ID de cliente de API de terceros

Contraseña= Clave API



Paso 3. En la sección **Cuerpo**, seleccione **form-data. KEY** se rellena con la palabra "name", **VALUE se** rellena con el nombre de la secuencia de eventos. Asegúrese de que la fila está marcada.



Paso 4. En este punto, puede hacer clic en el botón **Enviar** para recibir su flujo de eventos.

Nota: Límite de 5 recursos activos en cada organización

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Una vez que se genera el flujo de eventos, puede verificarlo con el comando GET https://api.amp.cisco.com/v1/event_streams que muestra el número de secuencias de eventos creadas en la organización, como se muestra en la imagen.


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


En esta sección, puede encontrar la información de la secuencia de eventos como la ID, el nombre y las credenciales de AMP

Para obtener información sobre el flujo de eventos activo, puede utilizar GET https://api.amp.cisco.com/v1/event_streams/"id"

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.