How to Create an Event Stream with AMP APIs

Contents

Introduction

This document describes the steps of how to configure an event stream in AMP (Advanced Malware Protection) for Endpoints with Postman tool.

Contributed by Nancy Pérez, Yeraldin Sánchez, Cisco TAC Engineers.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Access to the Cisco AMP for Endpoints console
- API credentials from the AMP portal: 3rd Party API Client ID and API key, on this link you can find the steps to obtain them: [How to Generate an API Credential from the AMP Portal](#)
- An API handler, in this document, is used the Postman tool

Components Used

The information on this document is based on these software and hardware versions:

- AMP for Endpoints console version 5.4.20200107
- Postman version 7.16.0
- [AMP API documentation, v1](#)

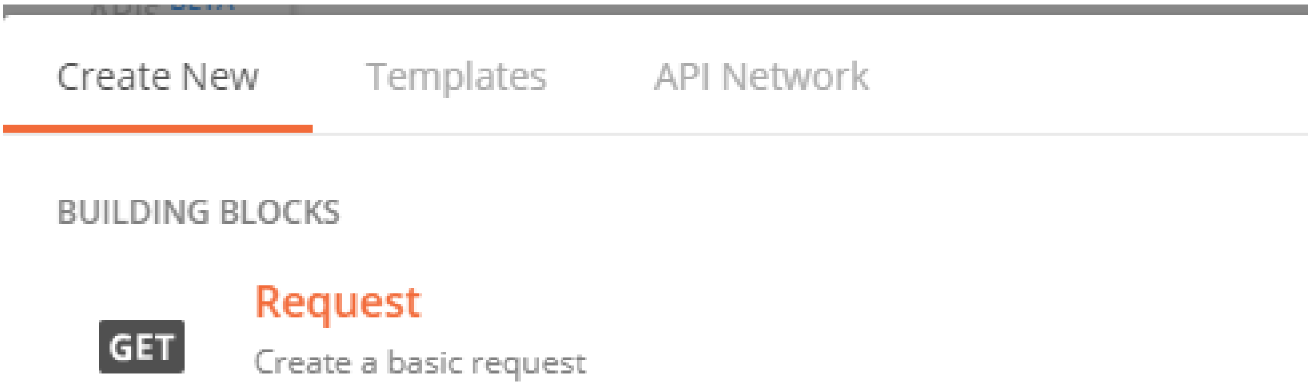
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Cisco does not support the Postman tool, if you have a question about it, please contact the Postman support.

Configure

Step 1. In the Postman home page, select **Create a request** in order to create a new event stream, as shown in the image.

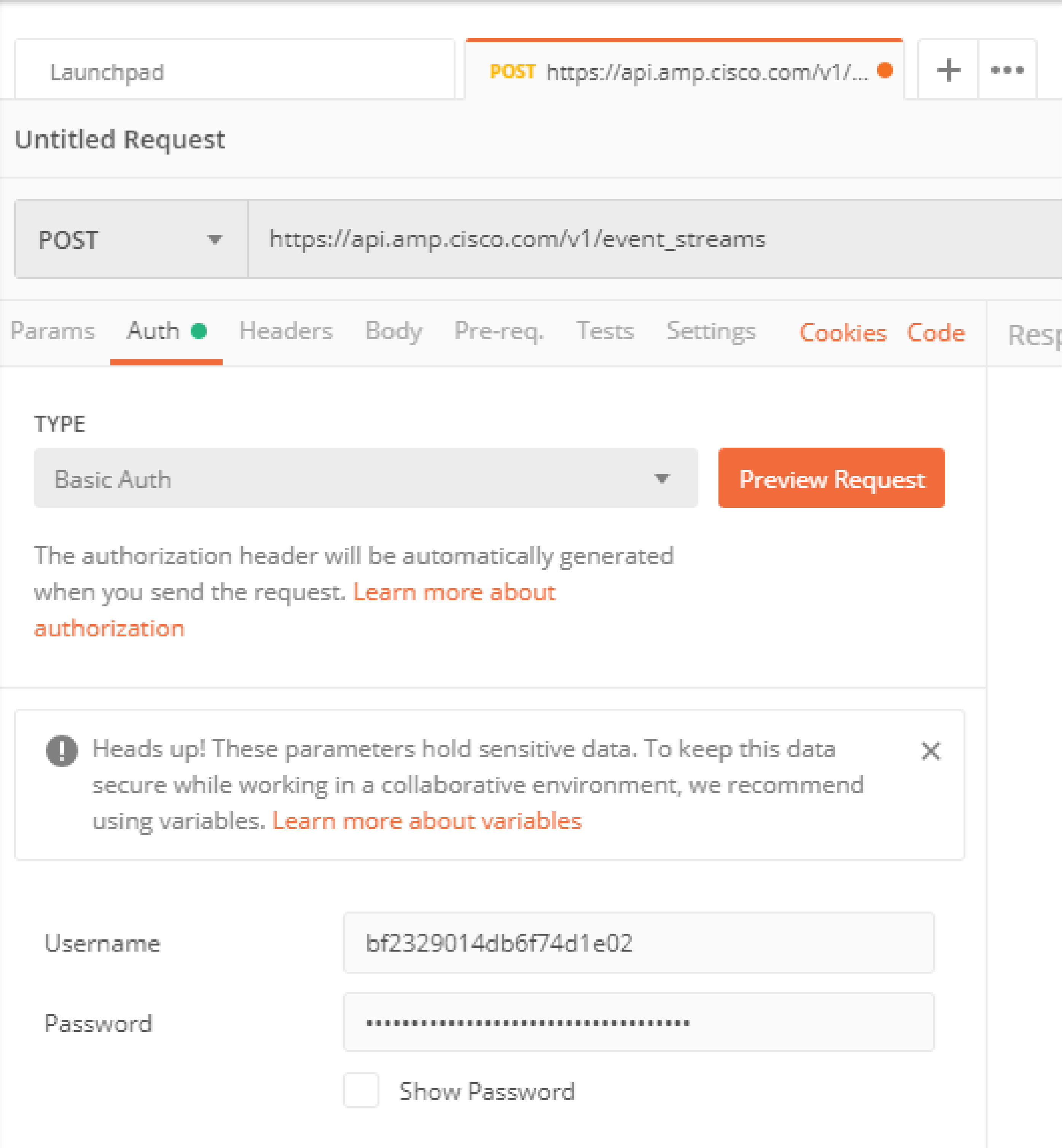


Step 2. Select **POST** and paste the URL needed to do the query, as shown in the image.

To type your 3rd Party API Client ID and API Key, select **Basic Authorization.**

Username= 3rd Party API Client ID

Password= API Key



Untitled Request

POST https://api.amp.cisco.com/v1/event_streams

TYPE

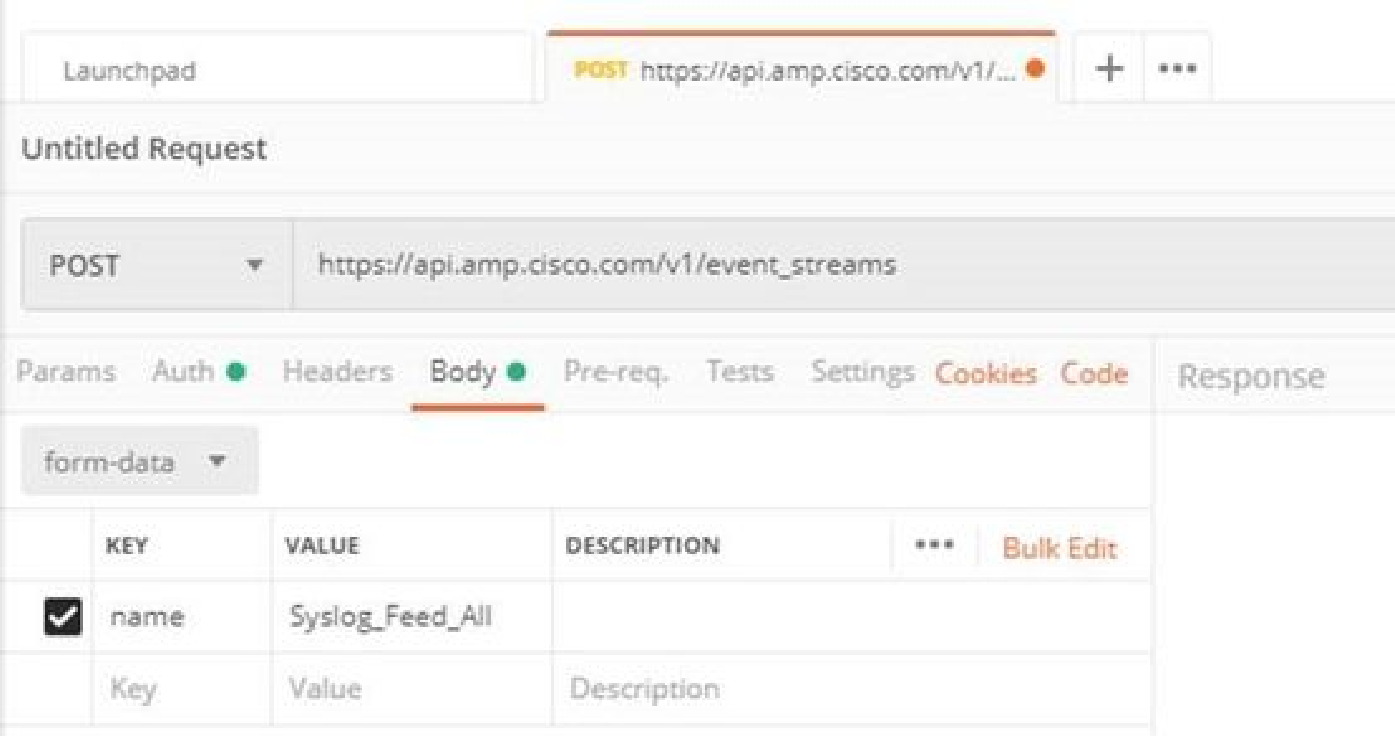
Basic Auth

The authorization header will be automatically generated when you send the request. Learn more about authorization

Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. Learn more about variables

Username	bf2329014db6f74d1e02
Password	••••••••••••••••••••••••••••••••••••••
	□ Show Password

Step 3. In the **Body** section, select **form-data. KEY** is filled with “name” word, **VALUE is** filled with the name of the event stream. Make sure that row is marked.



POST https://api.amp.cisco.com/v1/event_streams

form-data

	KEY	VALUE	DESCRIPTION
☑	name	Syslog_Feed_All	
	Key	Value	Description

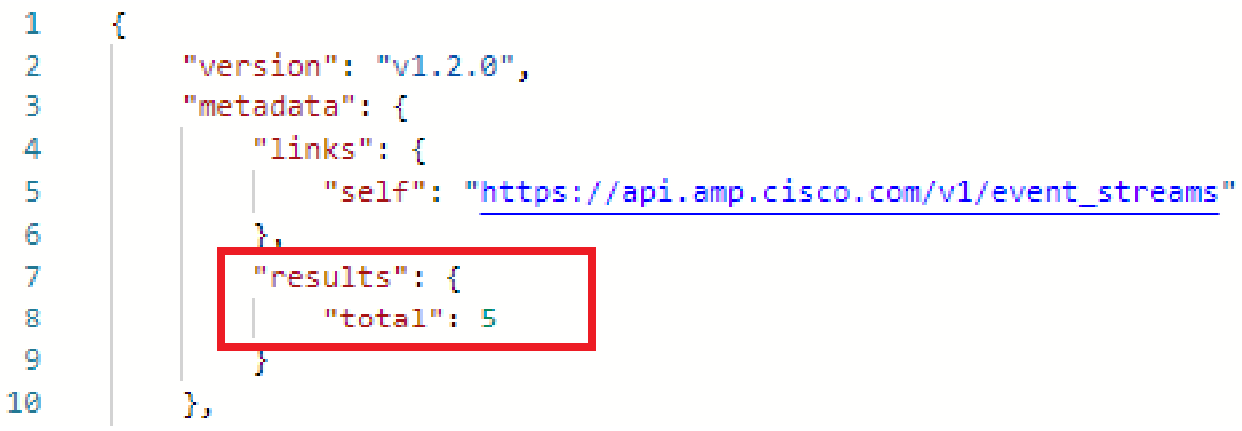
Step 4. At this point, you can click on the **Send** button to receive your event stream.

Note: Limit of 5 active resources across each organization

Verify

Use this section to confirm that your configuration works properly.

Once the event stream is generated, you can verify it with the command GET **https://api.amp.cisco.com/v1/event_streams** which displays the number of event streams created on the organization, as shown in the image.



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

In this section, you can find the event stream information as the ID, name and AMP credentials

In order to obtain information about the active event stream you can use GET **https://api.amp.cisco.com/v1/event_streams/"id"**

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.