Erstellen eines Event Streams mit AMP-APIs

Inhalt

Einführung

Dieses Dokument beschreibt die Schritte zur Konfiguration eines Ereignisstreams in AMP (Advanced Malware Protection) für Endgeräte mit dem Postman-Tool.

Mitarbeiter: Nancy Pérez, Yeraldin Sánchez, Cisco TAC Engineers.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Zugriff auf die Konsole Cisco AMP für Endgeräte
- API-Anmeldeinformationen vom AMP-Portal: API-Client-ID und API-Schlüssel von Drittanbietern. Hier finden Sie die erforderlichen Schritte, um diese zu erhalten: Erstellen einer API-Anmeldeinformationen über das AMP-Portal
- Ein API-Handler wird in diesem Dokument mit dem Postman-Tool verwendet.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- AMP für Endgeräte Konsolenversion 5.4.2020107
- Postman Version 7.16.0
- AMP API-Dokumentation, v1

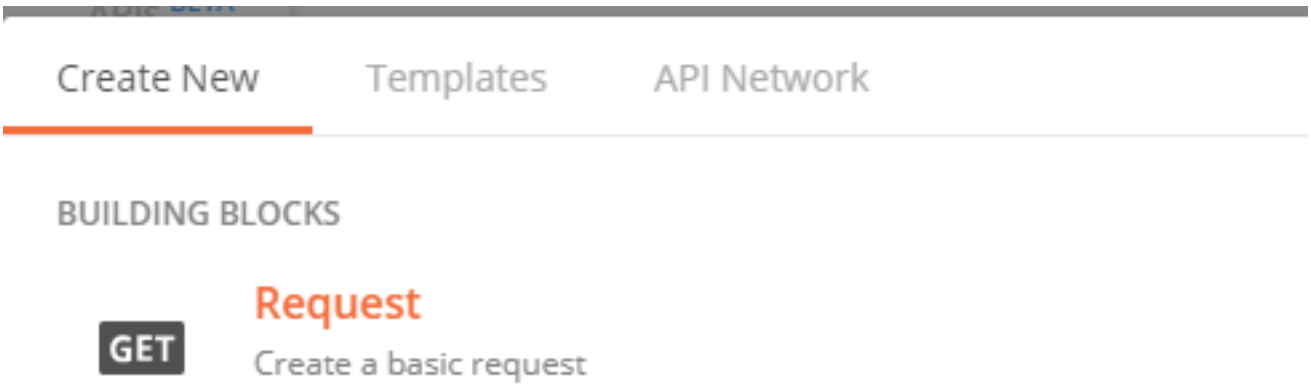
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Cisco unterstützt das Postman-Tool nicht. Wenn Sie Fragen dazu haben, wenden Sie sich bitte an den Postman-Support.

Konfigurieren

Schritt 1: Wählen Sie auf der Postman-Startseite **Anforderung erstellen**, um einen neuen Ereignisstream zu erstellen, wie im Bild gezeigt.

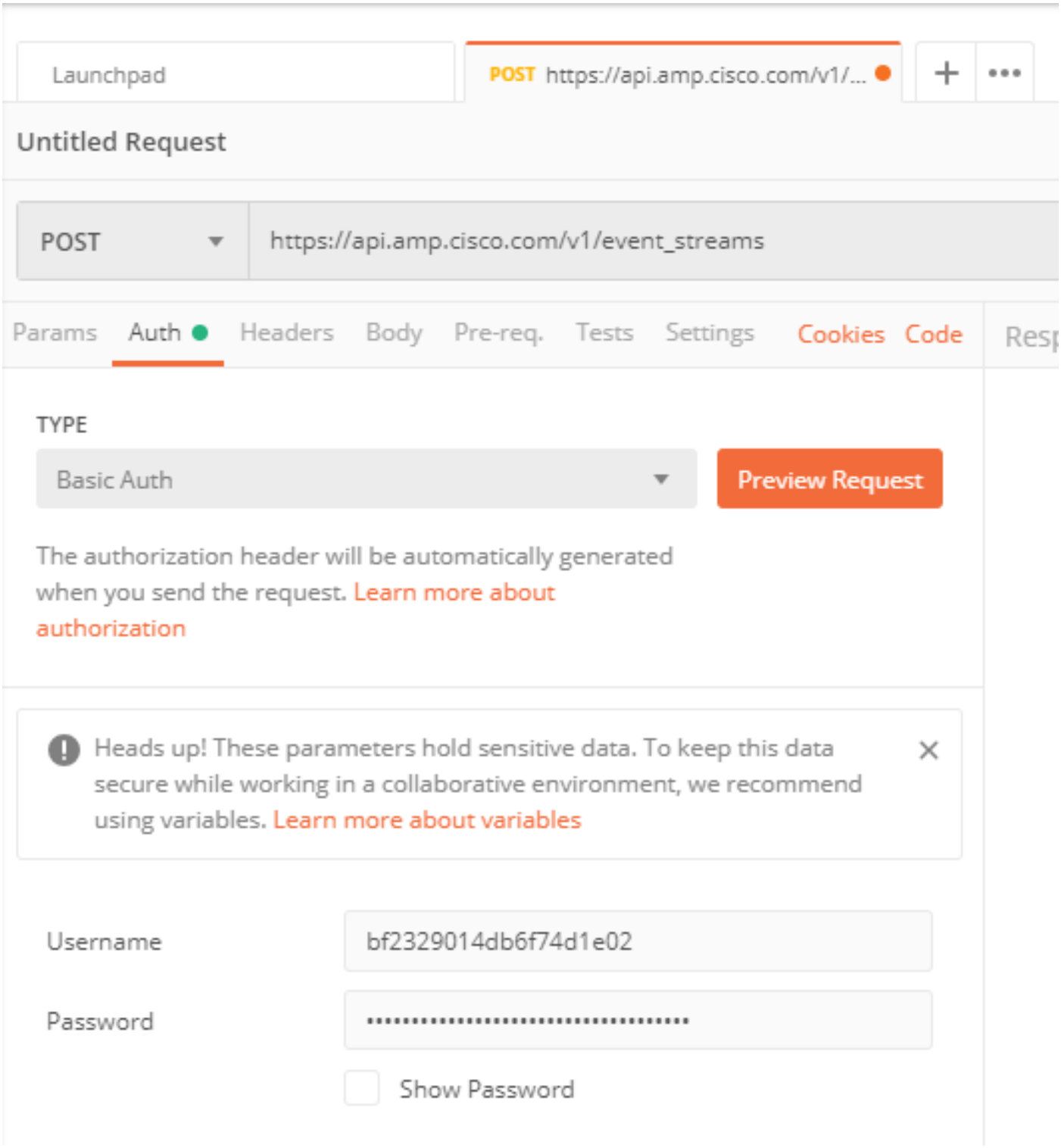


Schritt 2: Wählen Sie **POST** aus, und fügen Sie die URL ein, die für die Abfrage erforderlich ist, wie im Bild gezeigt.

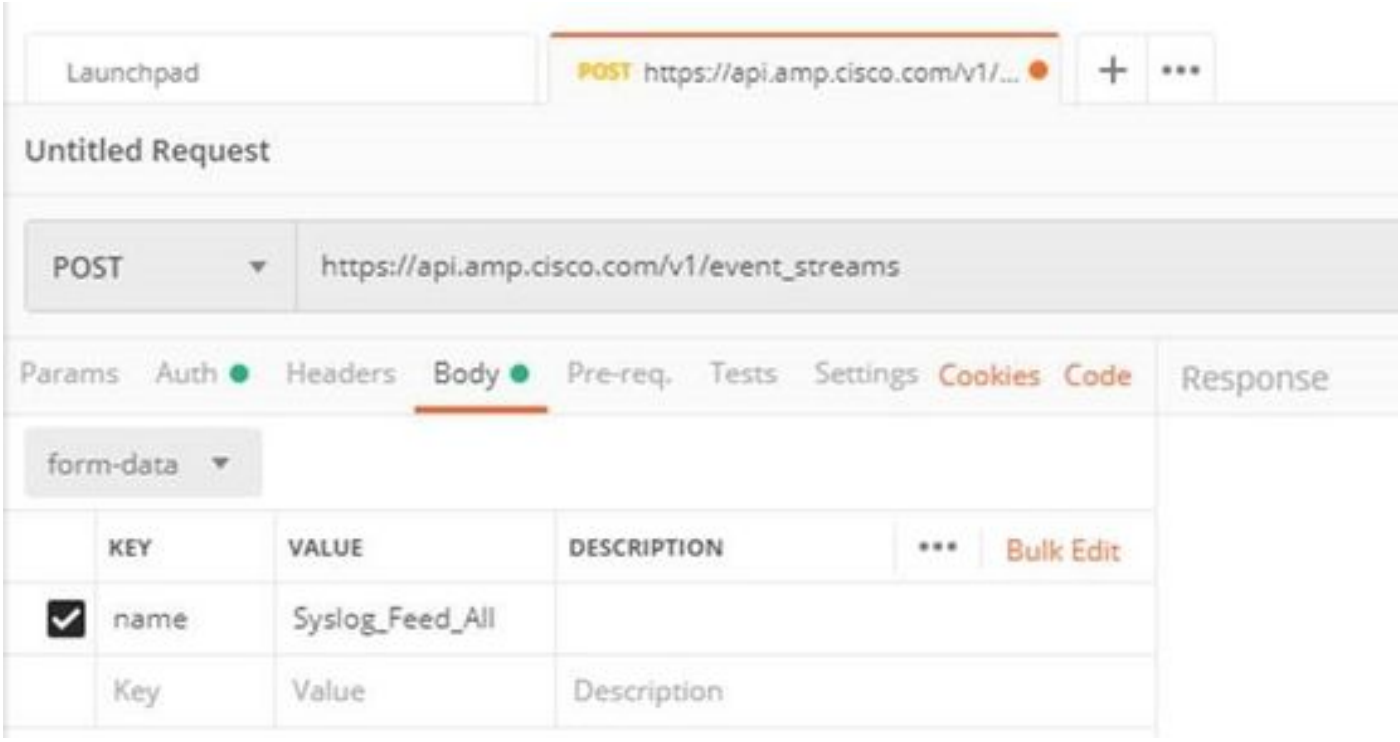
Um Ihre API-Client-ID und Ihren API-Schlüssel von Drittanbietern einzugeben, wählen Sie **Basic Authorization (Basisautorisierung) aus.**

Username= Drittanbieter-API-Client-ID

Password= API-Schlüssel



Schritt 3: Wählen Sie im Bereich **Text** die Option **Formulardaten aus. SCHLÜSSEL** ist mit "name"-Wort gefüllt, **VALUE ist** mit dem Namen des Ereignis-Streams gefüllt. Stellen Sie sicher, dass die Zeile markiert ist.



Schritt 4: An dieser Stelle können Sie auf die Schaltfläche **Senden** klicken, um den Ereignisstream zu empfangen.

> **Hinweis**: Maximal 5 aktive Ressourcen pro Unternehmen

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Nachdem der Ereignisstream generiert wurde, können Sie ihn mit dem Befehl GET https://api.amp.cisco.com/v1/event_streams überprüfen, der die Anzahl der in der Organisation erstellten Ereignisstreams anzeigt, wie im Bild gezeigt.


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


In diesem Abschnitt finden Sie Informationen zum Ereignisstream als ID, Name und AMP-Anmeldeinformationen.

Um Informationen zum aktiven Ereignisstream zu erhalten, können Sie GET https://api.amp.cisco.com/v1/event_streams/"id" verwenden.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.