

# Erstellen eines Event Streams mit AMP-APIs

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Überprüfen](#)

[Fehlerbehebung](#)

## 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:

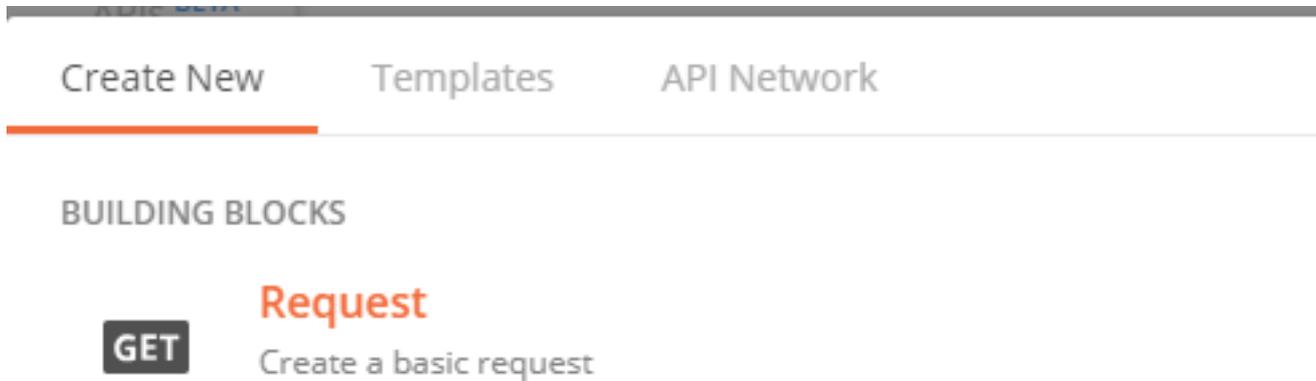
- AMP für Endgeräte Konsolenversion 5.4.2020107
- Postman Version 7.16.0
- [AMP API-Dokumentation, v1](#)

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

## 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 <sup>Drittanbietern</sup> einzugeben, wählen Sie **Basic Authorization (Basisautorisierung)** aus.

**Username=** Drittanbieter-API-Client-ID

**Password=** API-Schlüssel

Launchpad POST https://api.amp.cisco.com/v1/... + ...

### Untitled Request

POST https://api.amp.cisco.com/v1/event\_streams

Params **Auth** Headers Body Pre-req. Tests Settings Cookies Code Resp

**TYPE**

Basic Auth Preview Request

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

Password

Show Password

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.

The screenshot shows a REST client interface with a tab labeled "Launchpad" and a request tab for "POST https://api.amp.cisco.com/v1/...". The request is titled "Untitled Request" and is a POST to "https://api.amp.cisco.com/v1/event\_streams". The body is set to "form-data". A table below shows the form data:

	KEY	VALUE	DESCRIPTION	...	Bulk Edit
<input checked="" type="checkbox"/>	name	Syslog_Feed_All			
	Key	Value	Description		

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](https://api.amp.cisco.com/v1/event_streams) überprüfen, der die Anzahl der in der Organisation erstellten Ereignisstreams anzeigt, wie im Bild gezeigt.

```
1  {
2    "version": "v1.2.0",
3    "metadata": {
4      "links": {
5        "self": "https://api.amp.cisco.com/v1/event\_streams"
6      },
7      "results": {
8        "total": 5
9      }
10  },
```

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](https://api.amp.cisco.com/v1/event_streams/id) verwenden.

# Fehlerbehebung

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