Comment créer un flux d'événements avec des API AMP

Contenu

Introduction

Ce document décrit les étapes de configuration d'un flux d'événements dans AMP (Advanced Malware Protection) for Endpoints with Postman tool.

Contribution de Nancy Pérez, Yeraldin Sánchez, Ingénieurs du TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès à la console Cisco AMP for Endpoints
- Informations d'identification de l'API à partir du portail AMP : ID de client et clé d'API d'API tiers, sur ce lien, vous pouvez trouver les étapes pour les obtenir : Comment générer des informations d'identification d'API à partir du portail AMP
- Un gestionnaire d'API, dans ce document, est utilisé dans l'outil Postman

Components Used

Les informations de ce document sont basées sur les versions logicielles et matérielles suivantes :

- Console AMP for Endpoints version 5.4.20200107
- Postman version 7.16.0
- Documentation de l'API AMP, v1

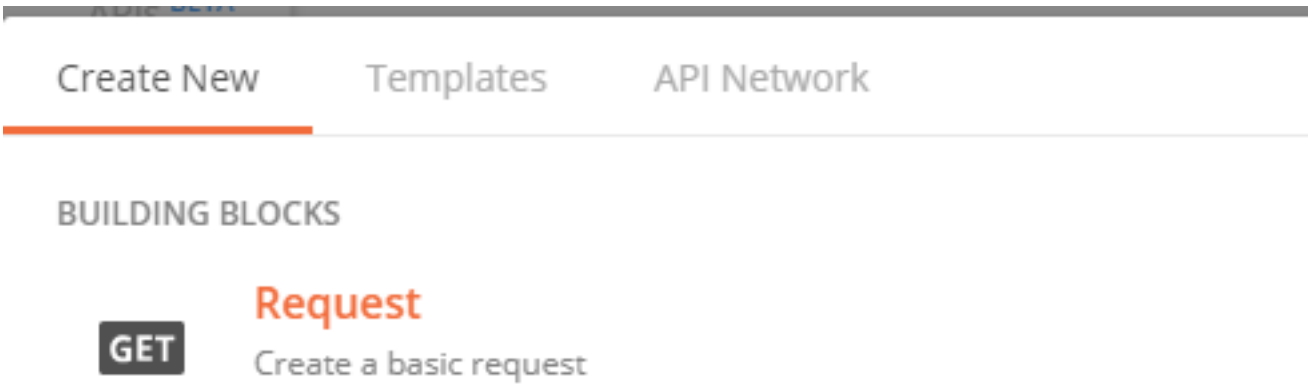
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Cisco ne prend pas en charge l'outil Postman. Si vous avez des questions à ce sujet, contactez le support de Postman.

Configuration

Étape 1. Dans la page d'accueil de Postman, sélectionnez **Créer une demande** afin de créer un nouveau flux d'événements, comme illustré dans l'image.

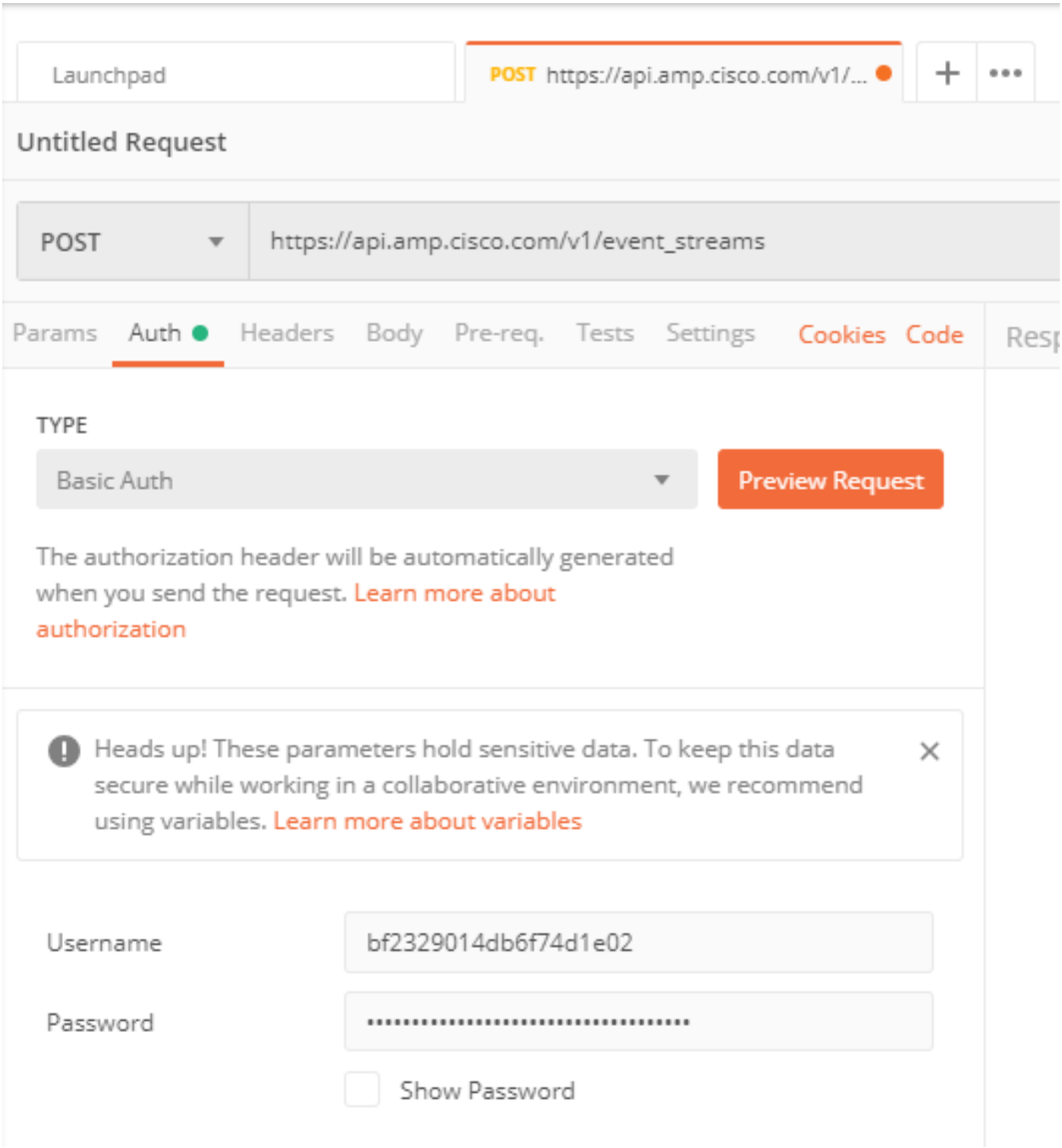


Étape 2. Sélectionnez **POST** et collez l'URL nécessaire pour exécuter la requête, comme indiqué dans l'image.

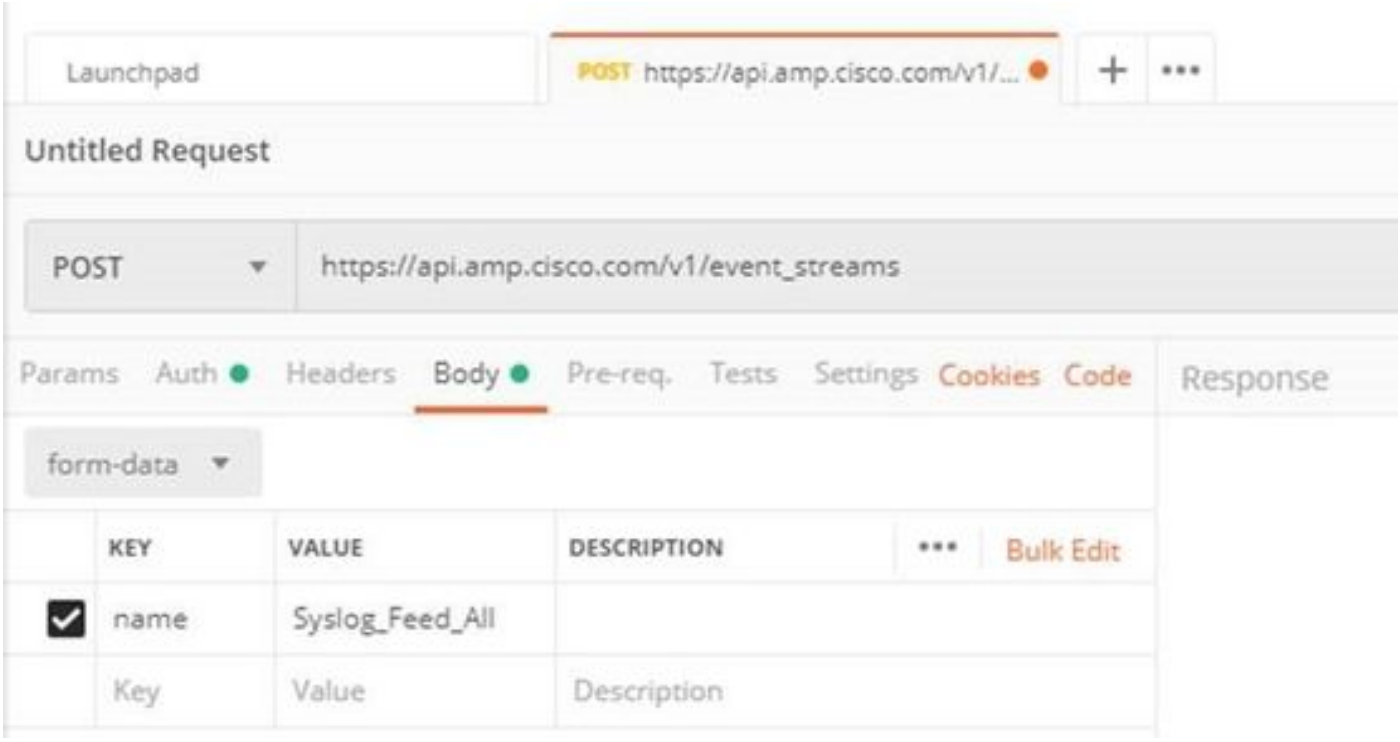
Pour saisir votre ID client et votre clé API tierce 3rd, sélectionnez **Basic Authorization.**

Username= 3rd API ID client

Password= Clé API



Étape 3. Dans la section **Corps**, sélectionnez **form-data. KEY** est rempli de " nom " mot, **VALUE est** rempli du nom du flux d'événements. Assurez-vous que la ligne est marquée.



Étape 4. À ce stade, vous pouvez cliquer sur le bouton **Envoyer** pour recevoir votre flux d'événements.

> **Note** : Limite de 5 ressources actives pour chaque organisation

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Une fois le flux d'événements généré, vous pouvez le vérifier à l'aide de la commande GET https://api.amp.cisco.com/v1/event_streams qui affiche le nombre de flux d'événements créés sur l'organisation, comme illustré dans l'image.

Dans cette section, vous trouverez les informations de flux d'événements comme ID, nom et informations d'identification AMP

Pour obtenir des informations sur le flux d'événements actif, vous pouvez utiliser GET https://api.amp.cisco.com/v1/event_streams/« id"

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.