# Comment créer un flux d'événements avec des API AMP

## Contenu

Introduction Conditions préalables Conditions requises Components Used Informations générales Configuration Vérification Dépannage

## 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 : <u>Comment générer des informations d'identification d'API à partir du portail AMP</u>
- 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.

Create New
Templates

BUILDING BLOCKS

Request

Create a basic request

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= 3<sup>rd</sup> API ID client

Password= Clé API

Launchpad	POST https://api.amp.cisco.com/v1/● + ••	
Untitled Request		
POST v https:/	//api.amp.cisco.com/v1/event_streams	
Params Auth • Headers	Body Pre-req. Tests Settings Cookies Code	Res
ТҮРЕ		
Basic Auth	Preview Request	
The authorization header w when you send the request authorization	vill be automatically generated t. Learn more about	
Heads up! These parameters secure while working in using variables. Learn	meters hold sensitive data. To keep this data X in a collaborative environment, we recommend more about variables	
Username	bf2329014db6f74d1e02	
Password		
	Show Password	

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.

Launchpad		POST	https://api.am	p.cisco.com/v	1/• +	
Untitled Red	luest					
POST	▼ https:/	//api.amp.cisco.com	n/v1/event_st	treams		
Params Aut	h • Headers	Body  Pre-re	q. Tests	Settings Cor	okies Code	Response
Params Aut form-data	h • Headers	Body  Pre-re	eq. Tests	Settings Cor	okies Code	Response
Params Aut form-data ĸey	h  Headers  VALUE	Body Pre-re	iq. Tests	Settings Coo	bkies Code Bulk Edit	Response
Params Aut form-data KEY Name	<ul> <li>Headers</li> <li>VALUE</li> <li>Syslog_F</li> </ul>	Body Pre-re DESCR	eq. Tests	Settings Coo	bkies Code Bulk Edit	Response

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 <u>https://api.amp.cisco.com/v1/event\_streams</u> 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 <u>https://api.amp.cisco.com/v1/event\_streams/« id</u>"

## Dépannage

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