Come creare un flusso di eventi con API AMP

Sommario

Introduzione

In questo documento viene descritto come configurare un flusso di eventi in AMP (Advanced Malware Protection) for Endpoints con lo strumento Postman.

Contributo di Nancy Pérez, Yeraldin Sánchez, Cisco TAC Engineers.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso alla console Cisco AMP for Endpoints
- Credenziali API dal portale AMP: ID client API di terze parti e chiave API, in questo collegamento è possibile trovare i passaggi per ottenerli: [Come generare una credenziale API dal portale AMP](#)
- In questo documento viene utilizzato un gestore API per lo strumento Postman

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- AMP for Endpoints console versione 5.4.2020107
- Postman versione 7.16.0
- [documentazione API AMP, v1](#)

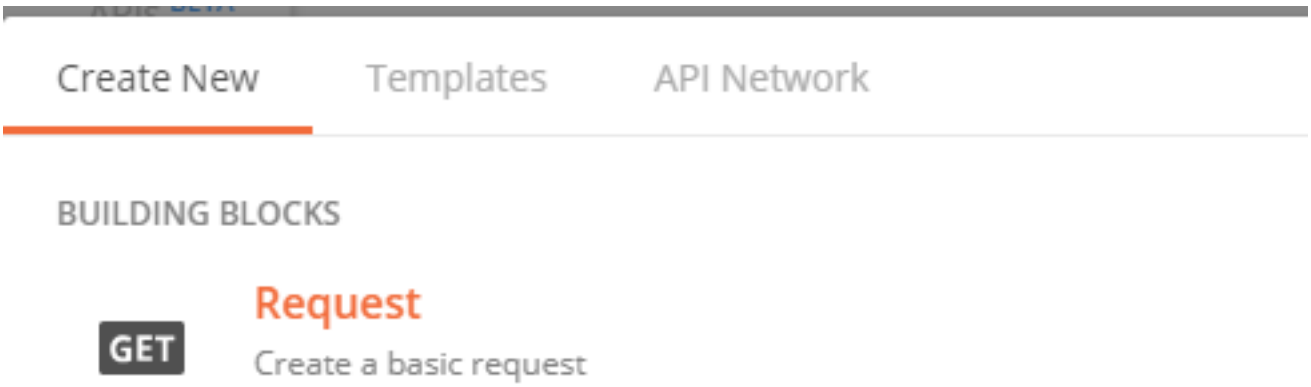
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Cisco non supporta lo strumento Postman. Per qualsiasi domanda, contattare il servizio di assistenza Postman.

Configurazione

Passaggio 1. Nella home page di Postman, selezionare **Crea una richiesta** per creare un nuovo flusso di eventi, come mostrato nell'immagine.

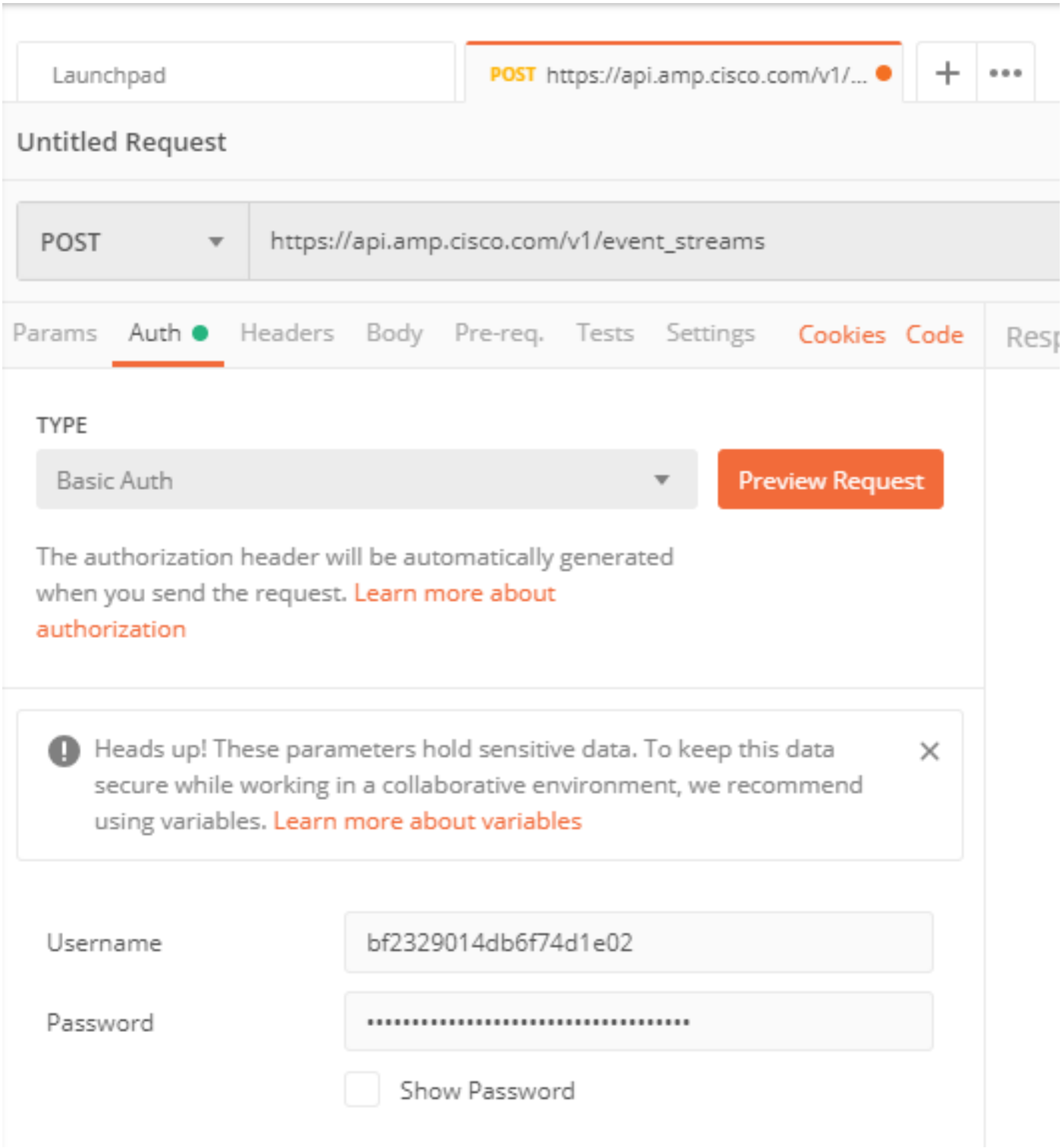


Passaggio 2. Selezionare **POST** e incollare l'URL necessario per eseguire la query, come mostrato nell'immagine.

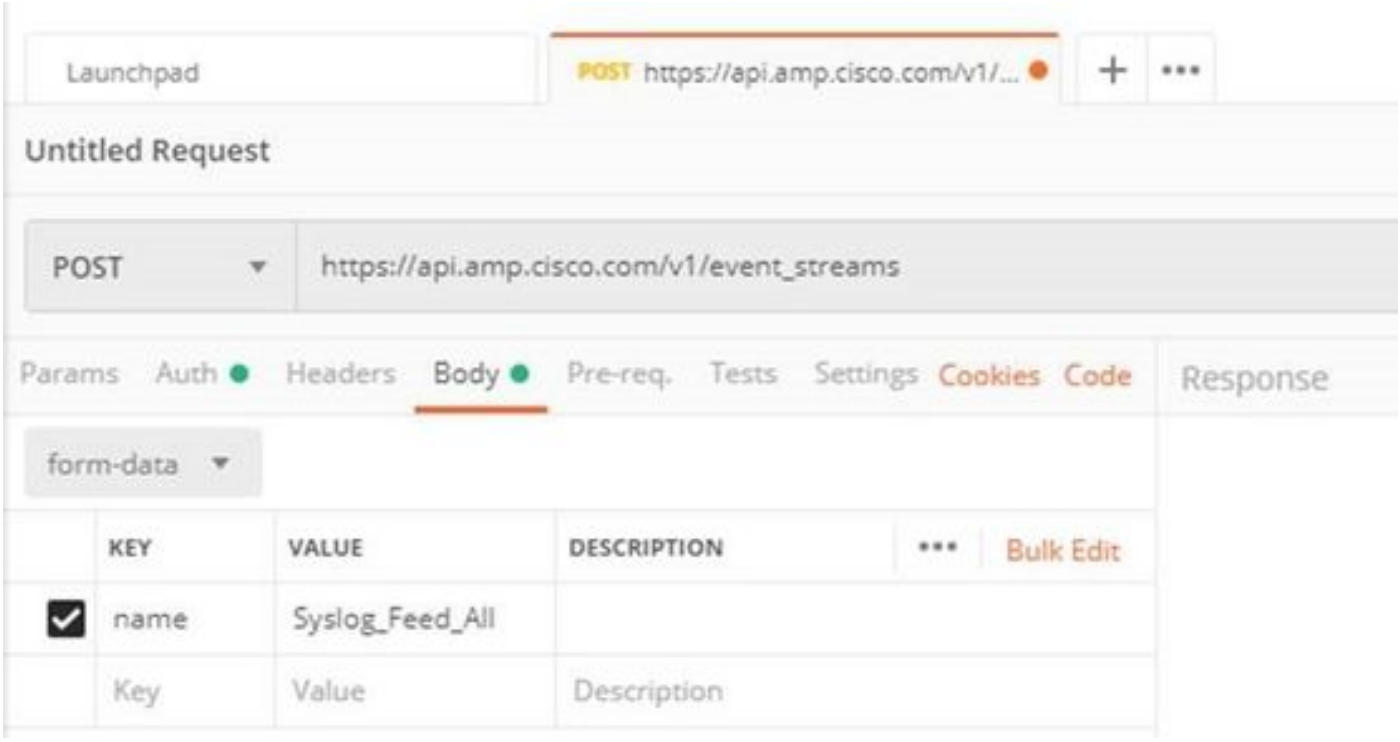
Per digitare l'ID client e la chiave API di terze parti, selezionare **Autorizzazione di base.**

Username= ID client API di terze parti

Password= Chiave API



Passaggio 3. Nella sezione **Body** selezionare **form-data. KEY** viene riempito con la parola "name", **VALUE con** il nome del flusso di eventi. Assicurarsi che la riga sia contrassegnata.



Passaggio 4. A questo punto, è possibile fare clic sul pulsante **Send** per ricevere il flusso di eventi.

> **Nota**: limite di 5 risorse attive in ogni organizzazione

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Una volta generato il flusso di eventi, è possibile verificarlo con il comando GET https://api.amp.cisco.com/v1/event_streams che visualizza il numero di flussi di eventi creati nell'organizzazione, come mostrato nell'immagine.


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


In questa sezione sono riportate le informazioni sul flusso di eventi sotto forma di ID, nome e credenziali AMP

Per ottenere informazioni sul flusso di eventi attivo, è possibile utilizzare GET https://api.amp.cisco.com/v1/event_streams/"id"

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.