Hoe een Event Stream met AMP API's maken

Inhoud

Inleiding

Dit document beschrijft de stappen van hoe u een eventstroom in AMP (Advanced Malware Protection) voor endpoints met Postman kunt configureren.

Bijgedragen door Nancy Pérez, Yeraldin Sánchez, Cisco TAC-engineers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Toegang tot de Cisco Advanced Malware Protection voor endpoints
- API-referenties van het AMP-portaal: API-id en API-toets van derden, op deze link vindt u de stappen om deze te verkrijgen: Hoe kunt u een API-krediet genereren via het AMP-portal
- Een API-geleider, in dit document, wordt gebruikt als postgereedschap

Gebruikte componenten

De informatie op dit document is gebaseerd op deze software- en hardwareversies:

- Advanced Malware Protection voor endpoints, versie 5.4.2001-07
- Post, versie 7.16.0
- AMP API-documentatie, v1

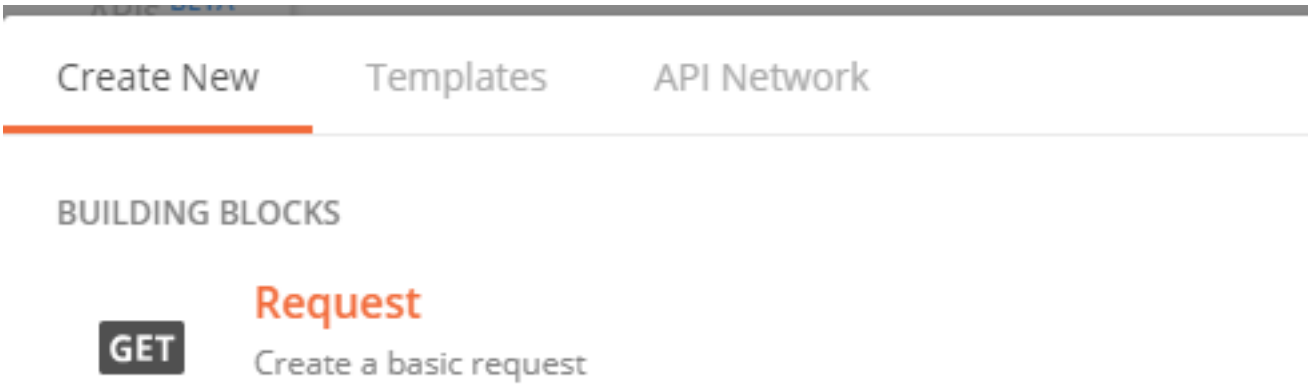
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Cisco ondersteunt het Postman gereedschap niet. Als u een vraag hebt over dit, neem dan contact op met de Postman ondersteuning.

Configureren

Stap 1. Selecteer in de startpagina Postman **een verzoek** maken om een nieuwe eventstroom te creëren, zoals in de afbeelding.

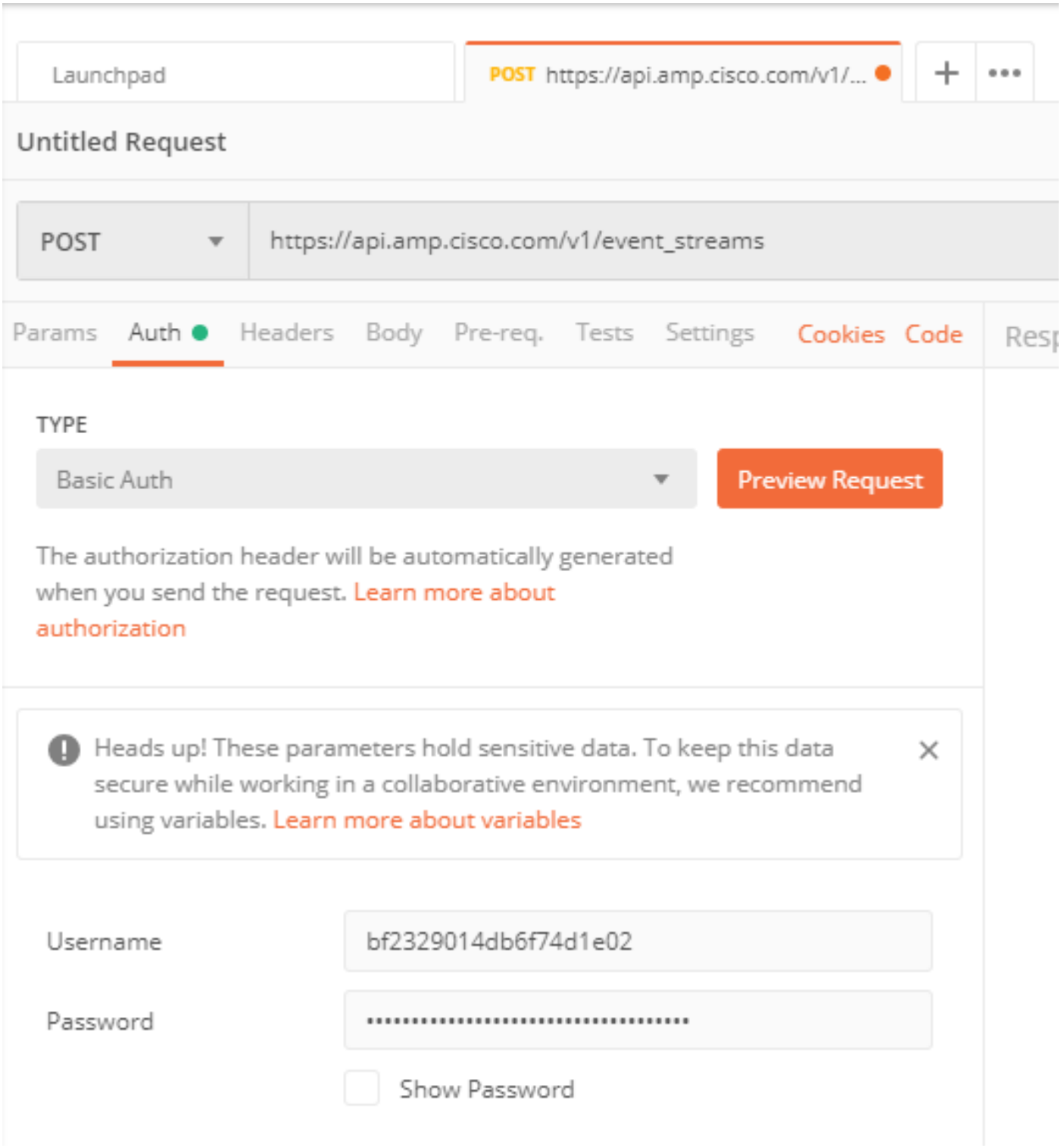


Stap 2. Selecteer **POST** en plak de URL die nodig is om de query uit te voeren, zoals in de afbeelding.

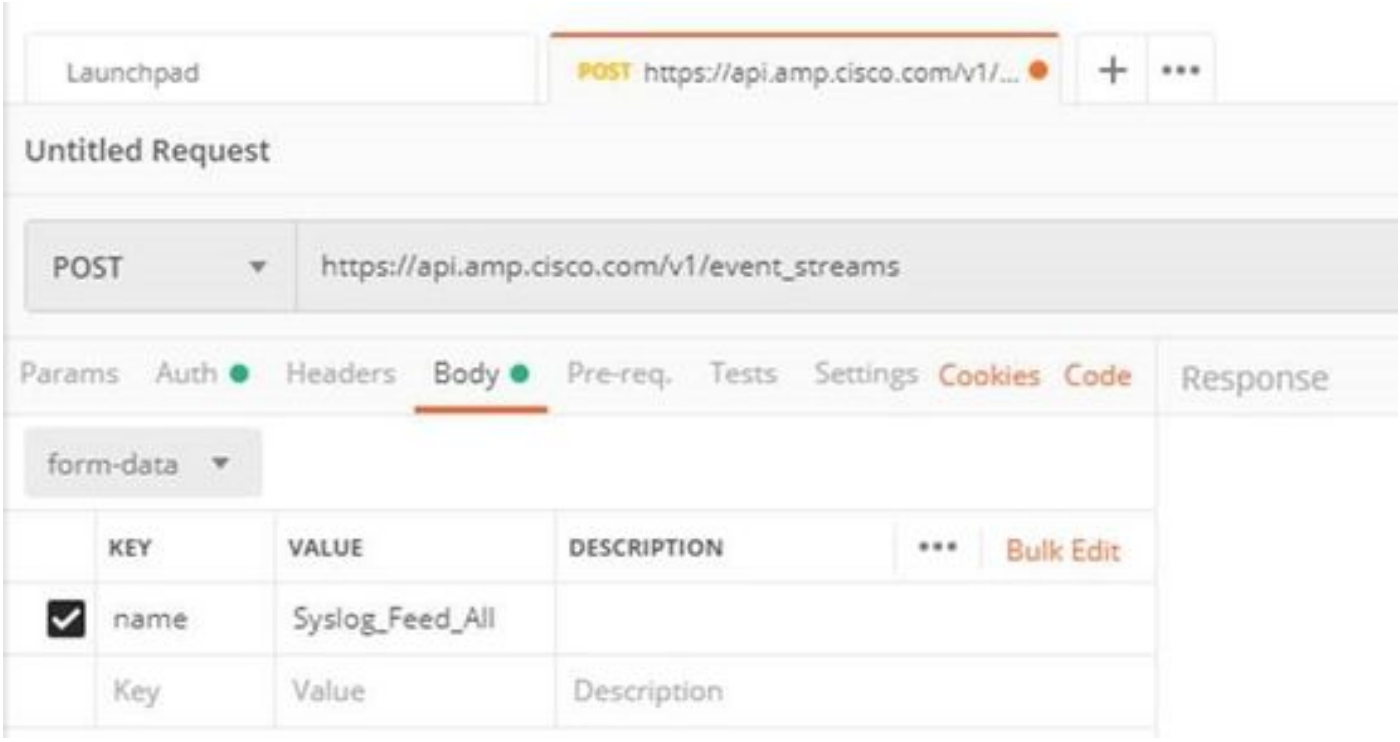
Als u uw 3e-client-API en -toets wilt typen, selecteert u **basisautorisatie.**

Clientid **voor** E**-naam=** 3rd API

Wachtwoord= API-toets



Stap 3. Selecteer in het gedeelte **Tekst de formuliergegevens. SLEUTEL** is ingevuld met het woord "naam", **WAARDE is** ingevuld met de naam van de eventstream. Controleer of de rij is gemarkeerd.



Stap 4. Op dit punt kunt u op de knop **Verzend** klikken om uw eventstroom te ontvangen.

Opmerking: Beperking van 5 actieve middelen per organisatie

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Zodra de gebeurtenis stroom wordt gegenereerd kunt u het met de opdracht GET https://api.amp.cisco.com/v1/event_streams controleren dat het aantal gebeurtenissen dat op de organisatie is gemaakt weergeeft, zoals in het beeld wordt getoond.


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


In deze sectie kunt u de informatie over de eventstream als ID-, naam- en AMP-referenties vinden

U kunt informatie over de actieve eventstroom gebruiken via GET https://api.amp.cisco.com/v1/event_streams/"id"

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.