

# Integração da AMP para endpoints com o Splunk

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Troubleshoot](#)

## Introduction

Este documento descreve o processo de integração entre o Advanced Malware Protection (AMP) e o Splunk.

Contribuído por Uriel Islas e Juventino Macias, editado por Jorge Navarrete, engenheiro do TAC da Cisco.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento de:

- AMP para endpoints
- Interface de programação de aplicativos (API)
- Splunk
- Usuário administrador no Splunk

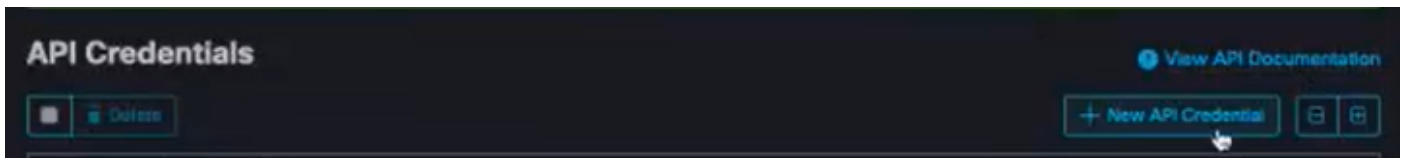
### Componentes Utilizados

- Nuvem pública da AMP
- instância de tronco

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. If your network is live, make sure that you understand the potential impact of any command.

## Configurar

Etapa 1. Navegue até o console AMP (<https://console.amp.cisco.com>) e navegue até **Accounts>API Credentials**, onde você pode criar fluxos de eventos.

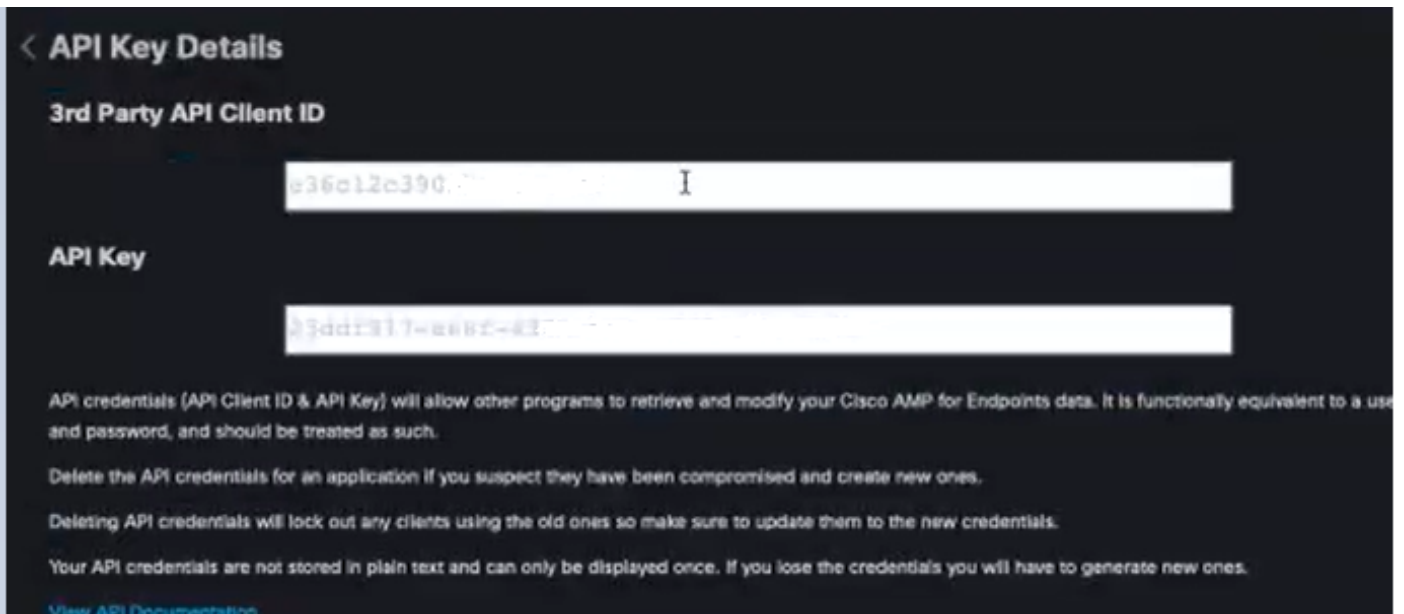


Etapa 2. Para executar essa integração, marque a caixa de seleção **Leitura e gravação** conforme mostrado abaixo:



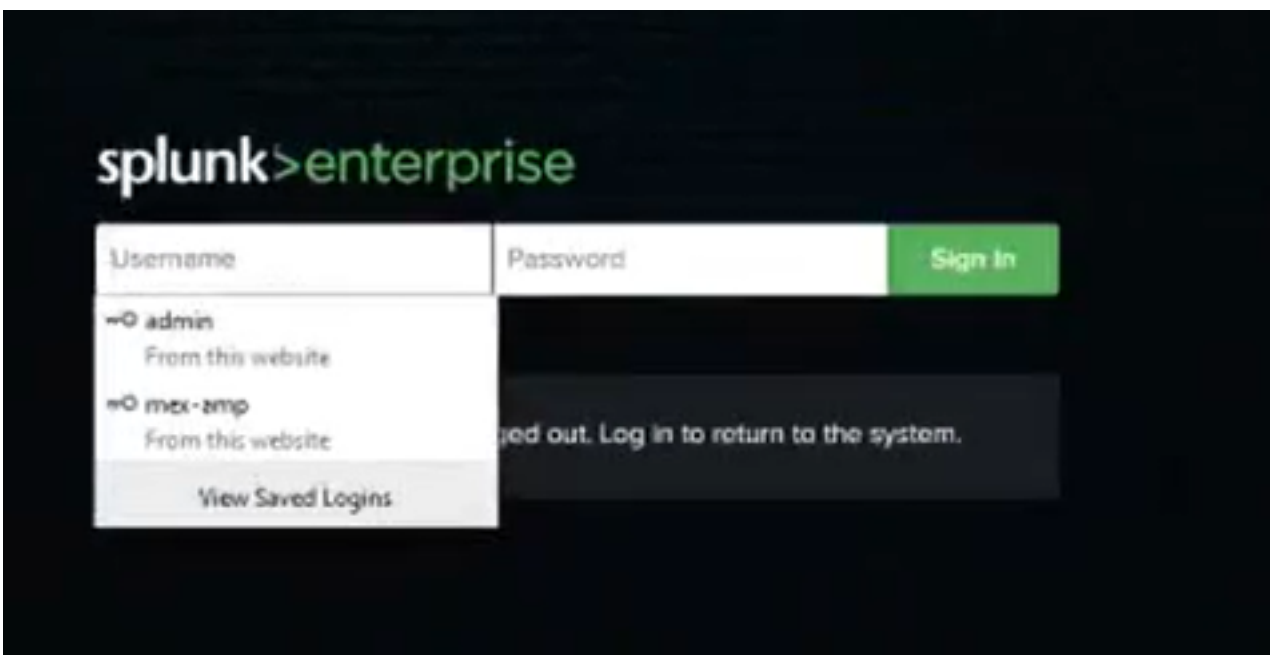
**Note:** Se desejar coletar mais informações sobre os eventos, marque a caixa **Enable Command Line** para obter os Logs de Auditoria gerados do Repositório de Arquivos e marque a caixa **Allow API access to File Repository**.

Etapa 3. Depois de criar o fluxo de eventos, ele exibiria a ID do cliente API e a chave API necessárias no Splunk.

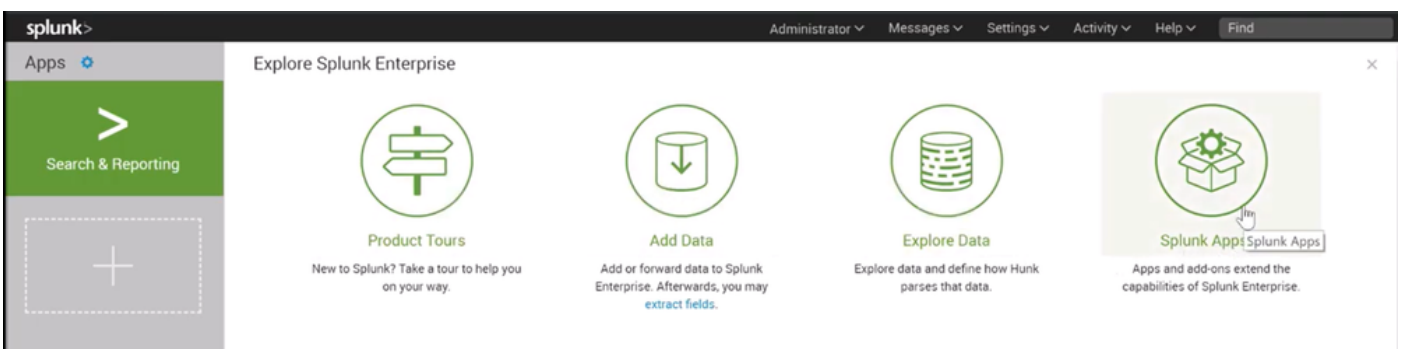


**Cuidado:** essas informações não podem ser recuperadas de nenhuma forma, em caso de perda, uma nova chave API deve ser criada.

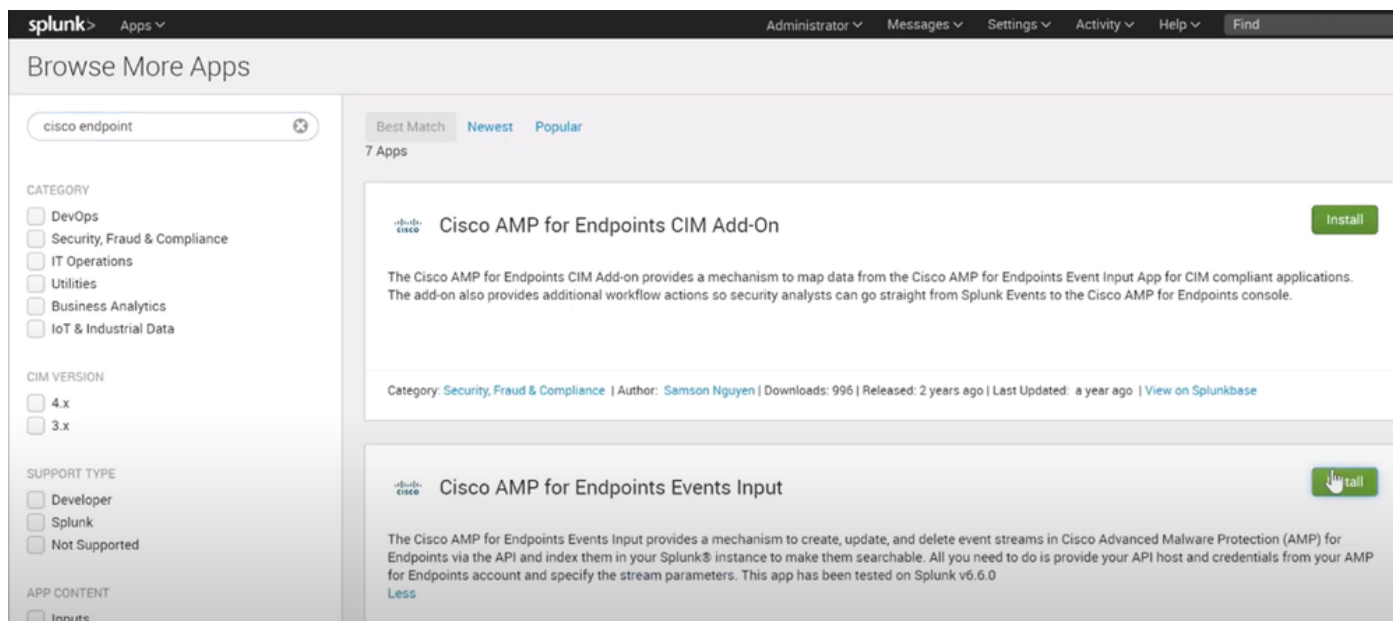
Etapa 4. Para integrar o Splunk com o AMP para endpoints, certifique-se de que o **Admin** da conta existe no Splunk.



Etapa 5. Depois de fazer login no Splunk, continue a fazer o download do AMP de Splunk Apps.



Etapa 6. Procure o Cisco Endpoint no navegador do aplicativo e instale-o (entrada de eventos do Cisco AMP for Endpoints).



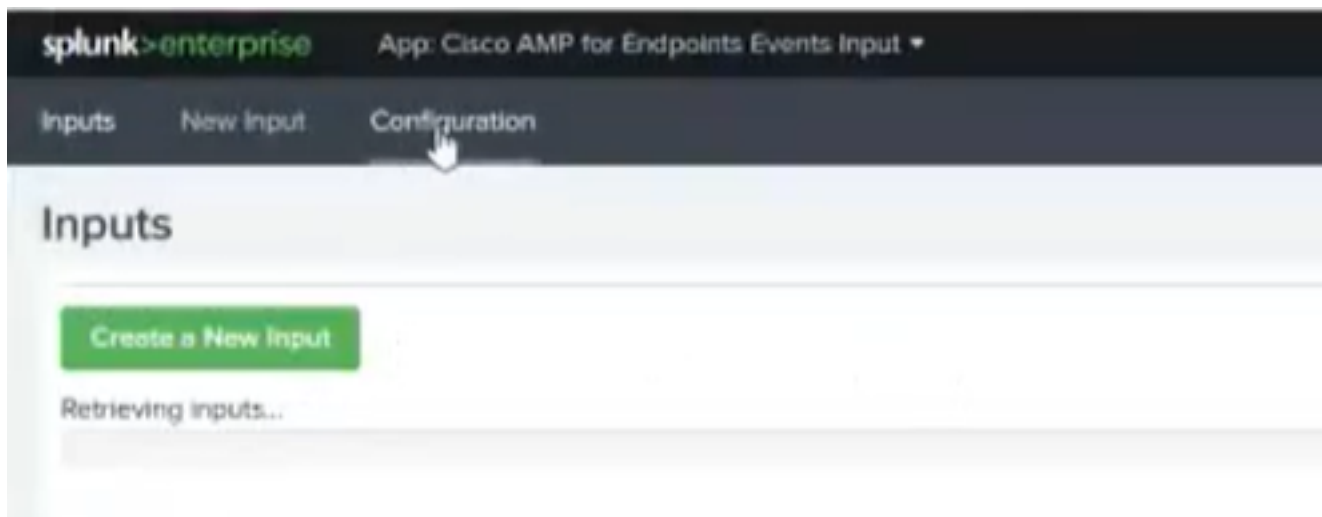
Passo 7. É necessário reiniciar a sessão para concluir a instalação no Splunk.



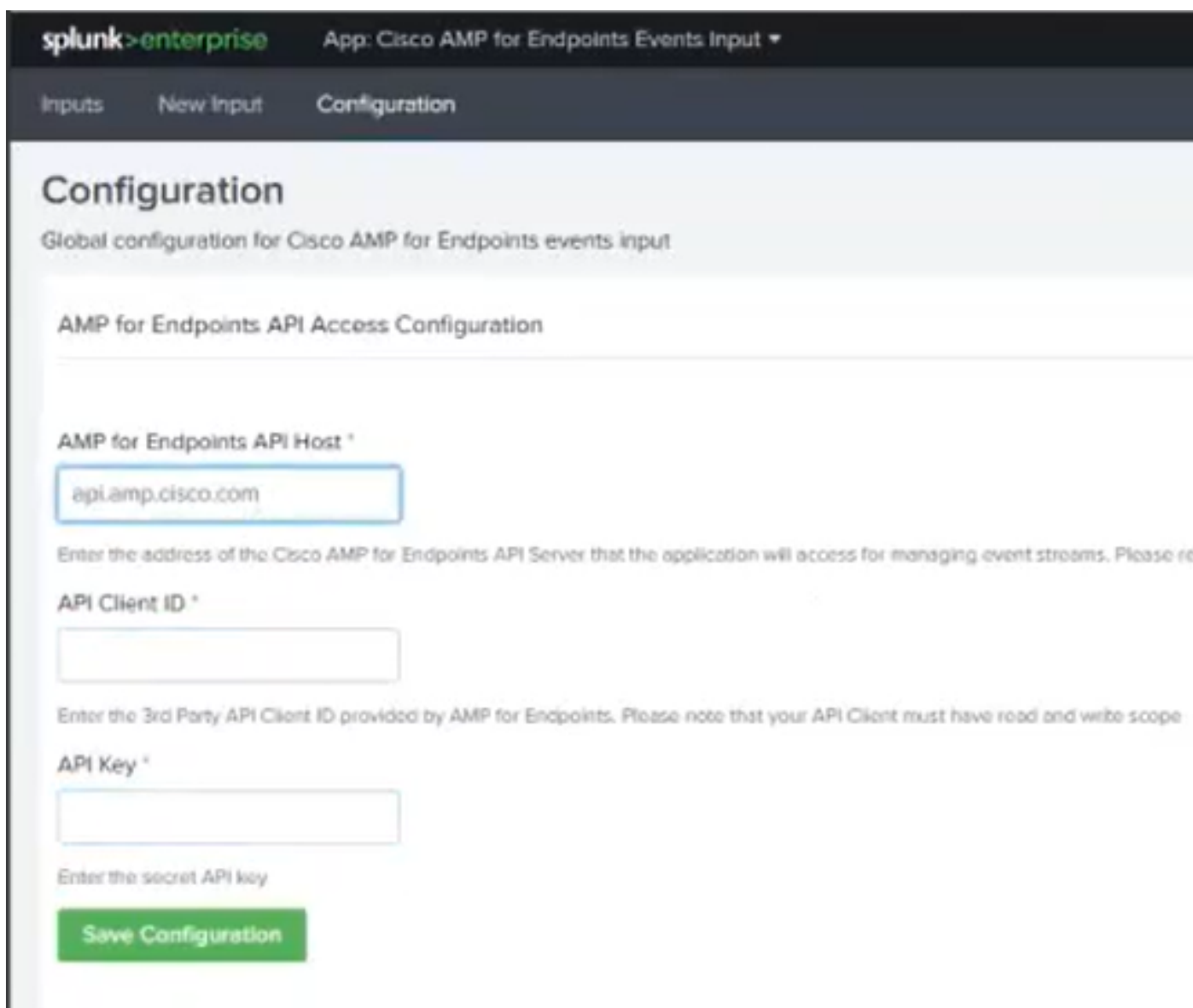
Etapa 8. Depois de fazer login em Splunk, clique em **Cisco AMP For Endpoints** no lado esquerdo da tela.



Etapa 9. Clique na etiqueta **Configuration** na parte superior da tela.



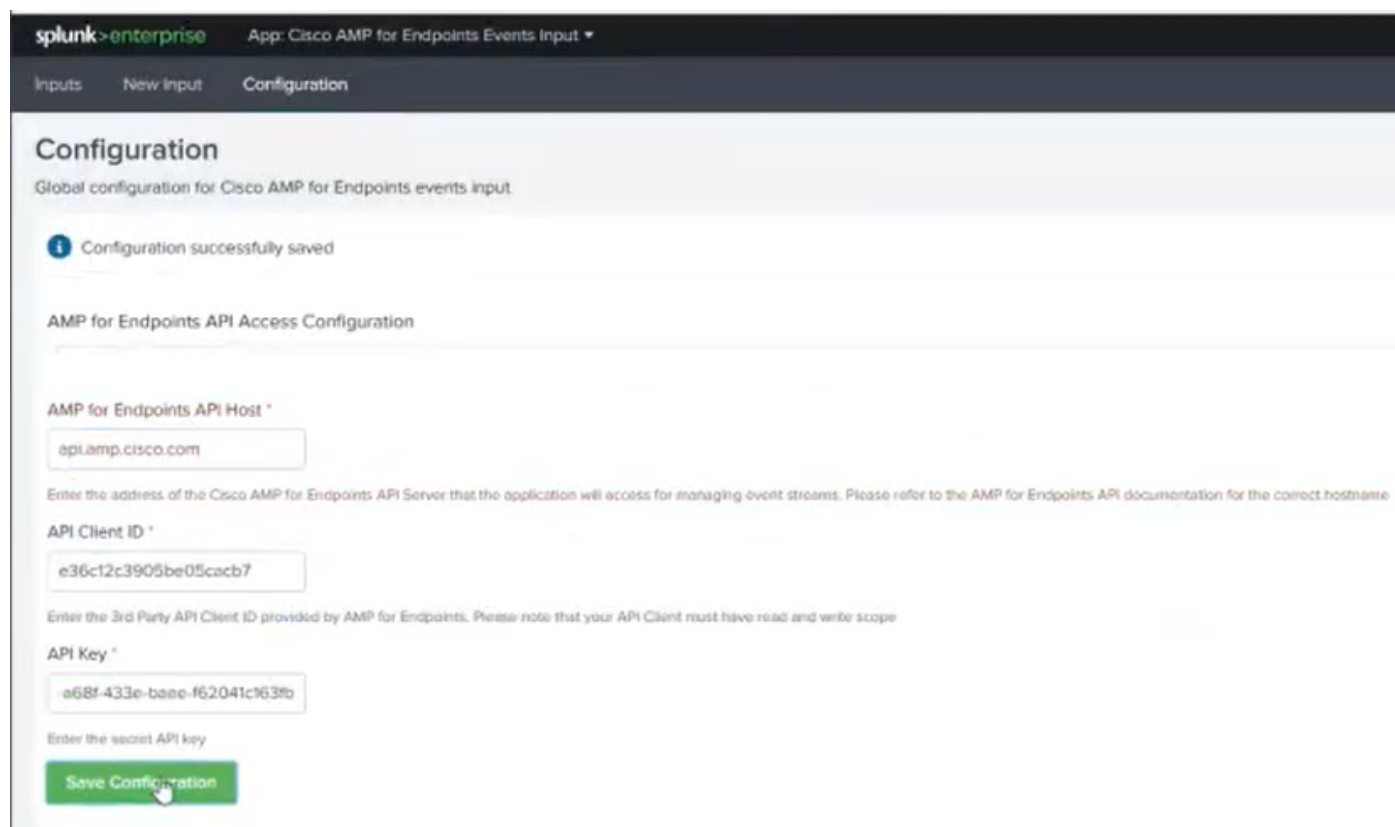
Etapa 10. Digite suas credenciais de API geradas anteriormente no console AMP.



**Note:** O ponto de host da API pode ser diferente com base no data center de nuvem apontado pela sua empresa em:

- América do Norte: `api.amp.cisco.com`
- Europa: `api.eu.amp.cisco.com`
- APJC: `api.apjc.amp.cisco.com`

Etapa 11. Inclua e salve credenciais de API no console Splunk para vinculá-las ao AMP.



The screenshot shows the Splunk configuration interface for the Cisco AMP for Endpoints Events Input app. The page title is "Configuration" and the subtitle is "Global configuration for Cisco AMP for Endpoints events input". A notification at the top indicates "Configuration successfully saved". The main section is titled "AMP for Endpoints API Access Configuration". It contains three input fields: "AMP for Endpoints API Host" with the value "api.amp.cisco.com", "API Client ID" with the value "e36c12c3905be05c0cb7", and "API Key" with the value "a68f433e-ba0e-f62041c163fb". Below the API Key field is a note: "Enter the secret API key". A green "Save Configuration" button is located at the bottom of the form.

splunk > enterprise App: Cisco AMP for Endpoints Events Input

Inputs New Input Configuration

## Configuration

Global configuration for Cisco AMP for Endpoints events input

Configuration successfully saved

### AMP for Endpoints API Access Configuration

AMP for Endpoints API Host \*

Enter the address of the Cisco AMP for Endpoints API Server that the application will access for managing event streams. Please refer to the AMP for Endpoints API documentation for the correct hostname

API Client ID \*

Enter the 3rd Party API Client ID provided by AMP for Endpoints. Please note that your API Client must have read and write scope

API Key \*

Enter the secret API key

Save Configuration

Etapa 12. Volte para **Entrada** para criar o fluxo de eventos.

Inputs   New Input   Configuration

## New Input

Name \*

Index

In which index would you like the events to appear?

### Stream Settings

---

Stream Name \*

Event Types

Groups

**Note:** Se quiser obter todos os eventos de todos os grupos da AMP, deixe os campos **Event Types** e **Groups** em branco.

Etapa 13. Verifique se a entrada foi criada com êxito.

## Inputs

Name	Index
caislas	main

**Note:** Lembre-se de que essa integração não é oficialmente suportada

# Troubleshoot

Se durante a criação de um fluxo de eventos todos os campos estiverem esmaecidos, isso pode ser causado por alguns dos motivos abaixo:

The screenshot shows the 'New Input' configuration page in Splunk. The page has a dark header with three tabs: 'Inputs', 'New Input', and 'Configuration'. The main content area is titled 'New Input'. It contains several form fields: 'Name \*' with a red prohibition icon, 'Index' with 'main' selected, 'Stream Settings' (disabled), 'Stream Name \*' (disabled), 'Event Types' with a dropdown menu, and 'Groups' with a dropdown menu. A green 'Save' button is at the bottom left.

1. Problemas de conectividade: Certifique-se de que a instância Splunk possa entrar em contato com o host da API
2. Host da API: Certifique-se de que o host de API configurado na etapa 10 corresponda à sua organização AMP, com base em onde sua empresa aponta.
3. Credenciais da API: Certifique-se de que a chave API e o ID do cliente correspondam aos configurados na etapa 3.
4. Fluxos de eventos: Verifique se você tem menos de 4 fluxos de eventos configurados.