

# Integración de AMP para terminales con Splunk

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Troubleshoot](#)

## Introducción

Este documento describe el proceso de integración entre la protección frente a malware avanzado (AMP) y Splunk.

Contribuido por Uriel Islas y Juventino Macias, editado por Jorge Navarrete, Ingenieros del TAC de Cisco.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento de:

- AMP para terminales
- Interfaz de programación de aplicaciones (API)
- Splunk
- Usuario administrador en Splunk

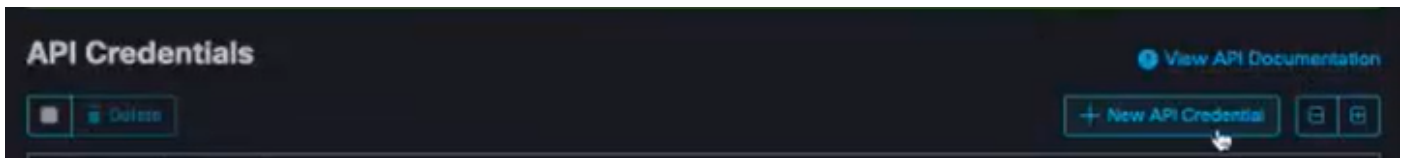
### Componentes Utilizados

- Nube pública AMP
- instancia de Splunk

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

Paso 1. Navegue hasta la consola de AMP (<https://console.amp.cisco.com>) y navegue hasta **Cuentas>Credenciales de API**, donde puede crear secuencias de eventos.

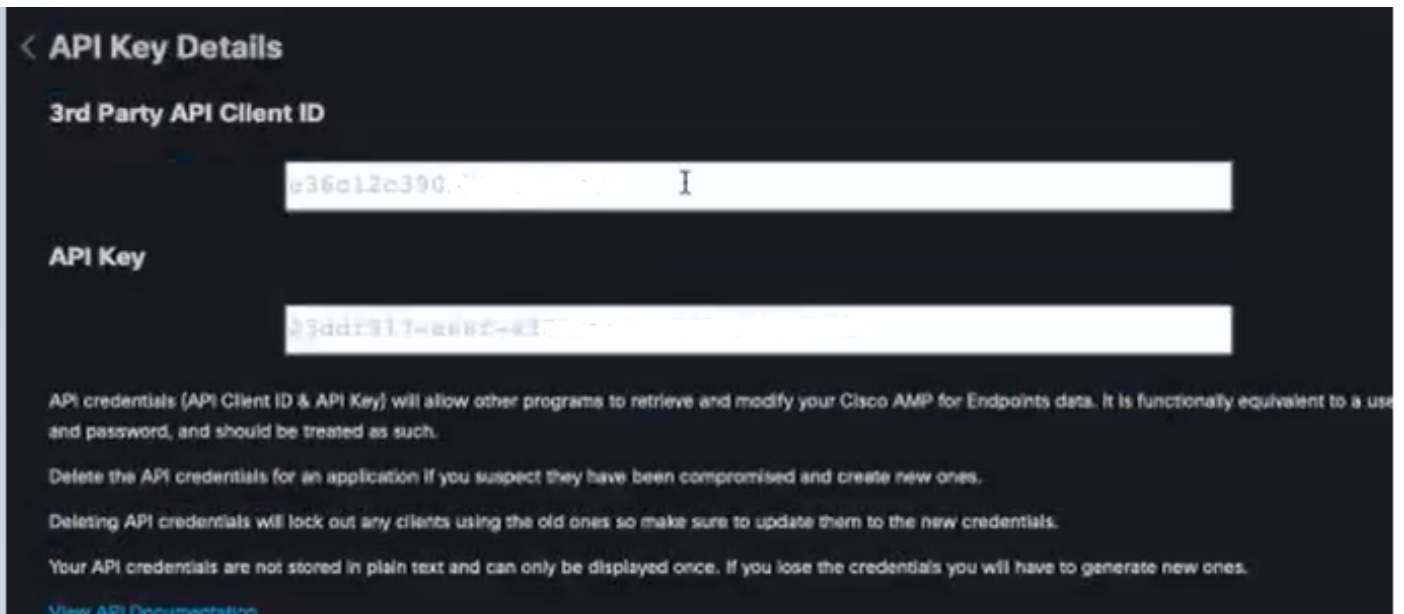


Paso 2. Para realizar esta integración, marque la casilla **Read & Write** como se muestra a continuación:



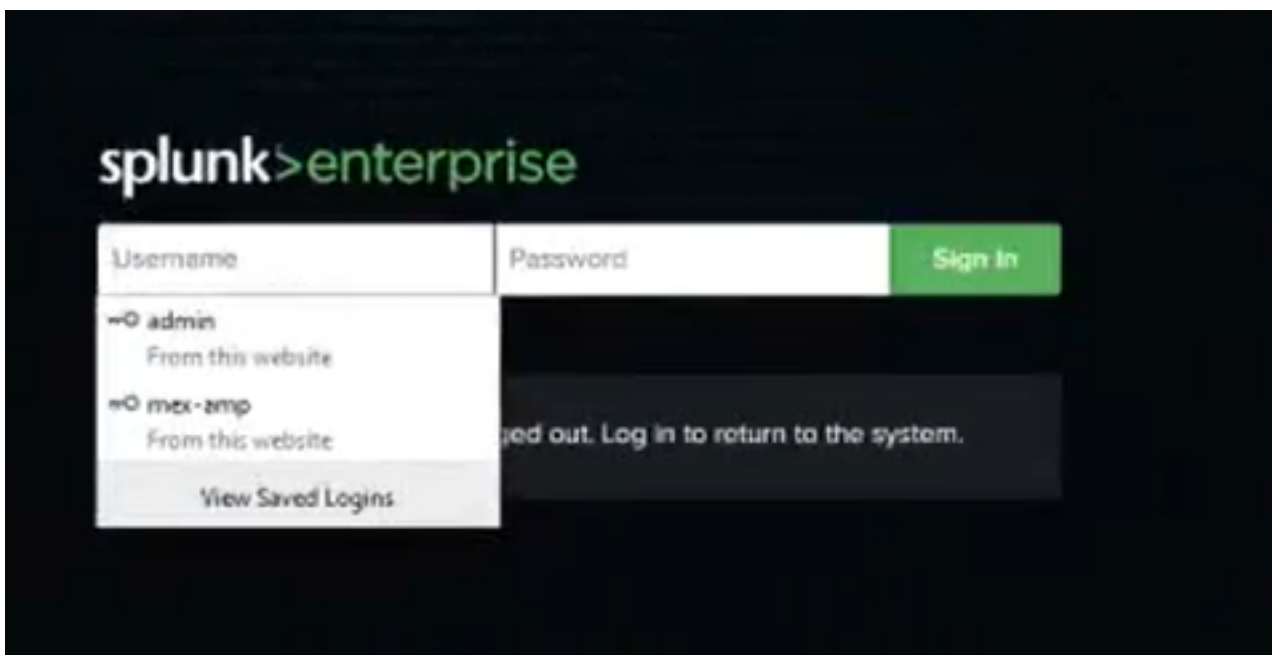
**Nota:** Si desea recopilar más información sobre los eventos, active la casilla **Enable Command Line**, para obtener los registros de auditoría generados desde el repositorio de archivos marque la casilla **Allow API access to File Repository**.

Paso 3. Una vez creada la secuencia de eventos, se mostrarán la ID de cliente API y la clave de API que se requieren en Splunk.

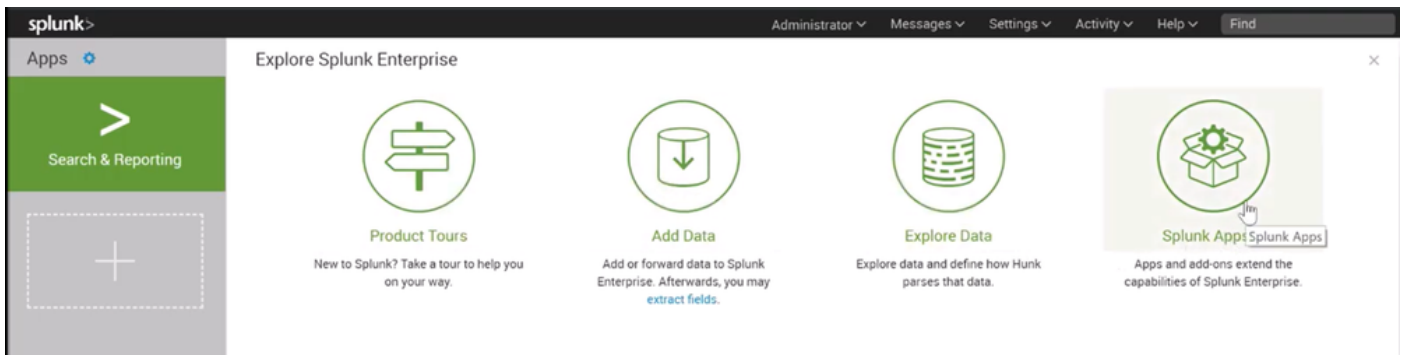


**Precaución:** Esta información no se puede recuperar por ningún medio, en caso de pérdida, se debe crear una nueva clave de API.

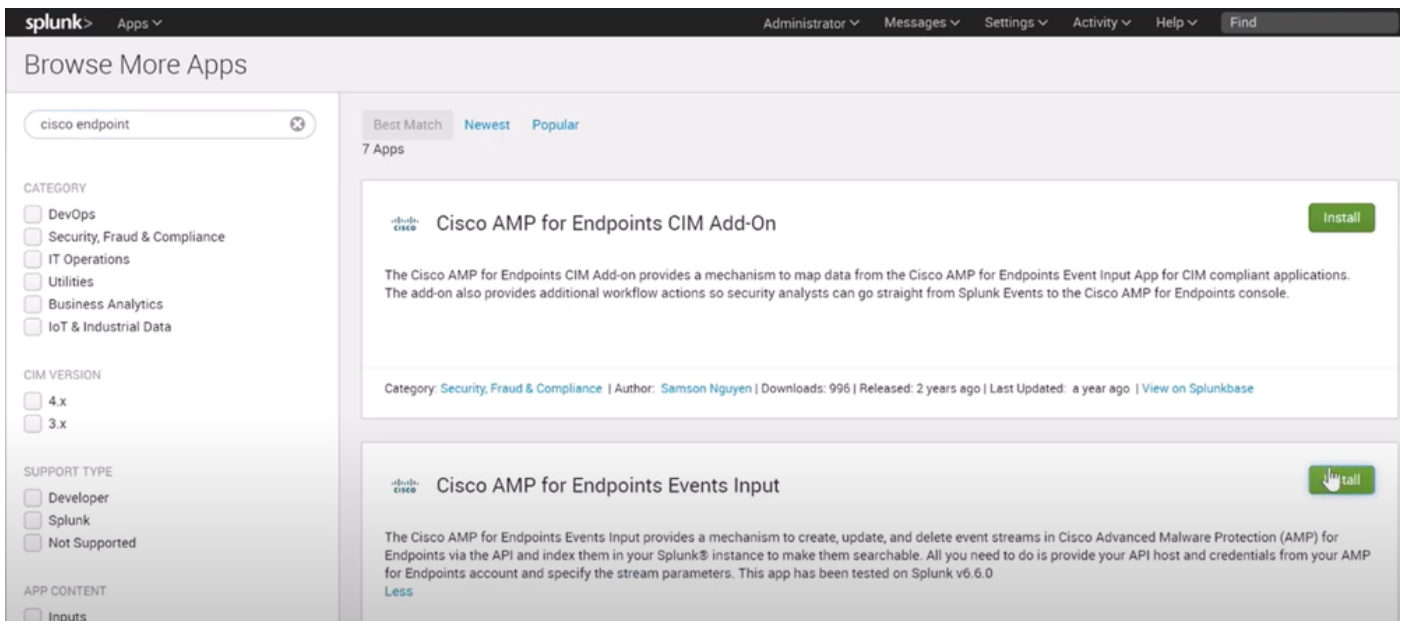
Paso 4. Para integrar Splunk con AMP para terminales, asegúrese de que la cuenta **Admin** exista en Splunk.



Paso 5. Una vez que inicie sesión en Splunk, continúe descargando AMP de las aplicaciones Splunk.



Paso 6. Busque el terminal de Cisco en el navegador de aplicaciones e instálelo (entrada de eventos de Cisco AMP para terminales).



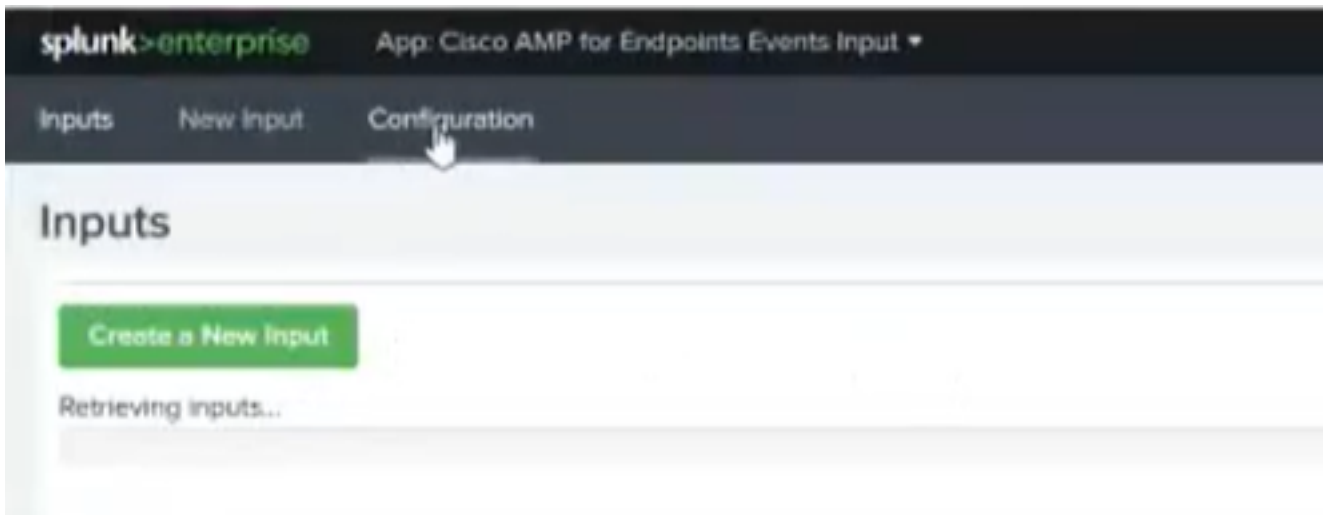
Paso 7. Se requiere un reinicio de la sesión para completar la instalación en Splunk.



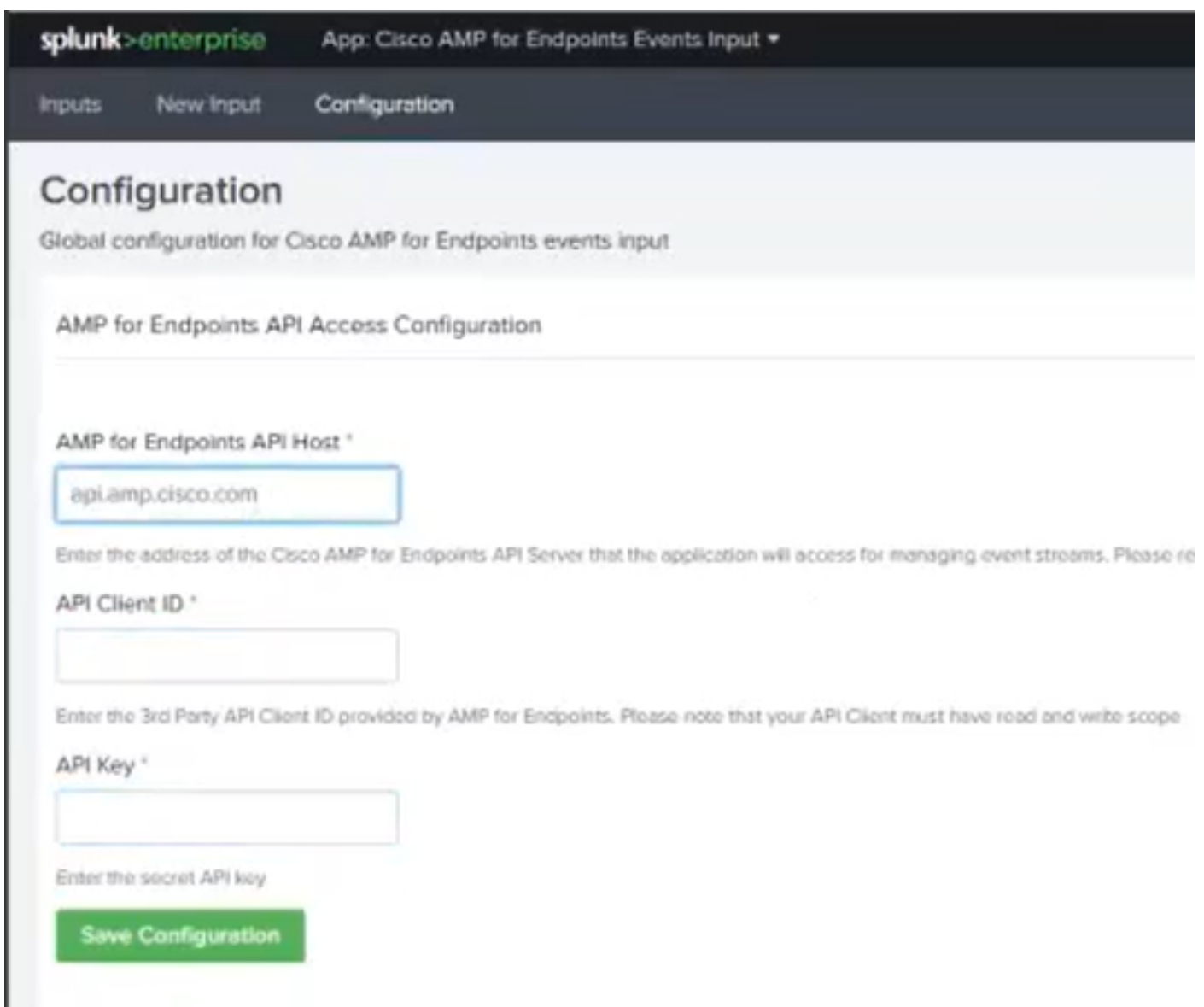
Paso 8. Una vez que inicie sesión en Splunk, haga clic en **Cisco AMP para terminales** en el lado izquierdo de la pantalla.



Paso 9. Haga clic en la etiqueta **Configuration** en la parte superior de la pantalla.



Paso 10. Escriba las credenciales de la API generadas anteriormente desde la consola de AMP.



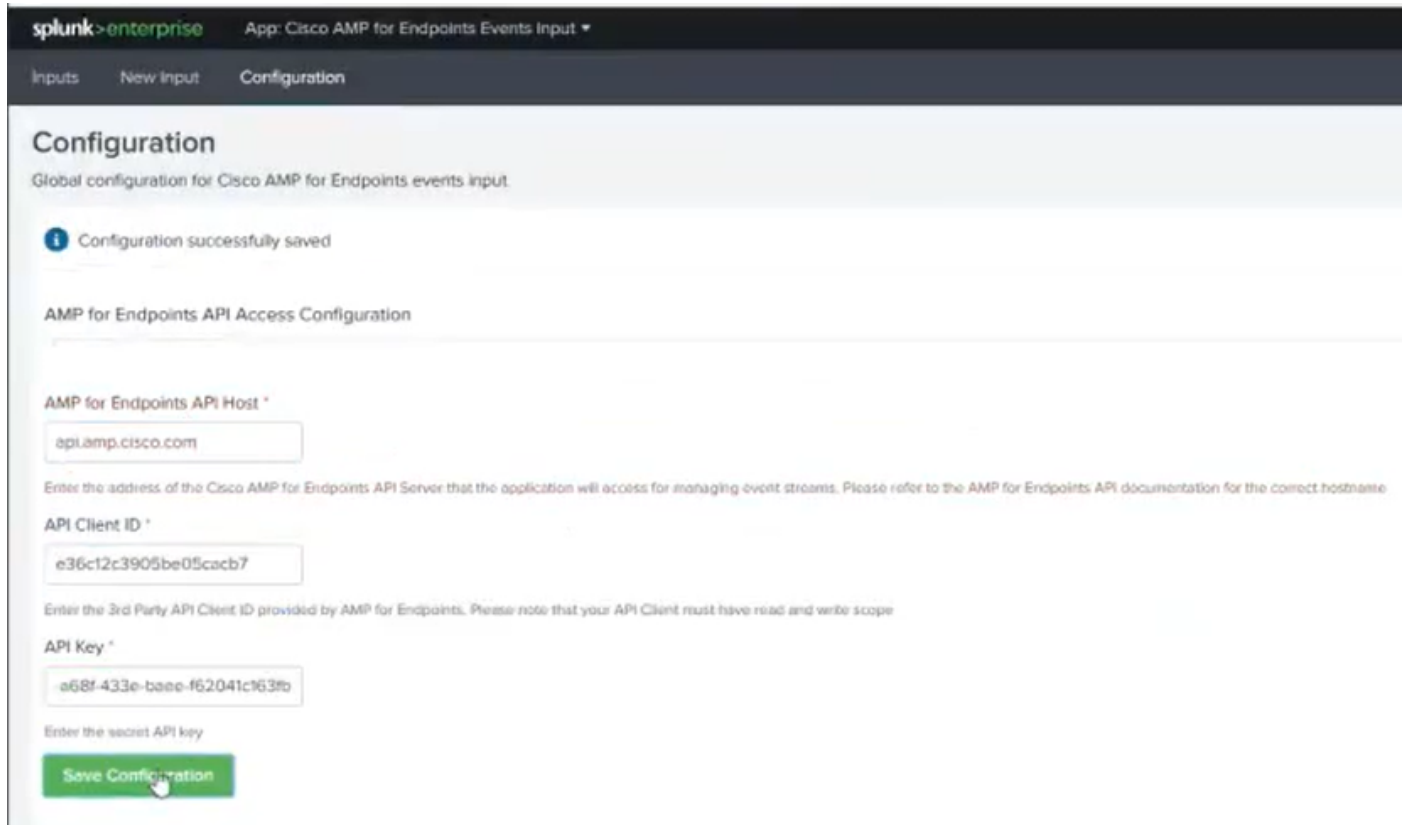
**Nota:** El punto de host de la API puede ser diferente según el Data Center en la nube que su organización señale en:

América del Norte: `api.amp.cisco.com`

Europa: `api.eu.amp.cisco.com`

Asia Pacífico, Japón y China: `api.apjc.amp.cisco.com`

Paso 11. Incluya y guarde las credenciales de la API en la consola de Splunk para vincularlas con AMP.



The screenshot shows the Splunk configuration interface for the 'Cisco AMP for Endpoints Events Input' app. The page title is 'Configuration' and it shows a message 'Configuration successfully saved'. Below this, there is a section for 'AMP for Endpoints API Access Configuration'. The configuration fields are:

- AMP for Endpoints API Host \***: . Below the field is the instruction: '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 \***: . Below the field is the instruction: '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 \***: . Below the field is the instruction: 'Enter the secret API key.'

At the bottom of the configuration section, there is a green button labeled 'Save Configuration'.

Paso 12. Vuelva a Input para crear la secuencia 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

[Save](#)

**Nota:** Si desea obtener de AMP todos los eventos de todos los grupos, deje en blanco los campos **Tipos de eventos** y **Grupos**.

Paso 13. Asegúrese de que la entrada se ha creado correctamente.

## Inputs

[Create a New Input](#)

Name	Index
caistas	main

**Nota:** Tenga en cuenta que esta integración no está oficialmente respaldada

# Troubleshoot

Si al crear una secuencia de eventos se atenúan todos los campos, esto podría deberse a algunos de los motivos siguientes:

The screenshot shows the 'New Input' configuration page in Splunk. The page has a dark header with three tabs: 'Inputs', 'New Input', and 'Configuration'. Below the header, the title 'New Input' is displayed. The form contains several sections: 'Name \*' with a red prohibition icon, 'Index' with a dropdown menu showing 'main', 'Stream Settings' with a sub-section 'Stream Name \*', 'Event Types' with a dropdown menu, and 'Groups' with a dropdown menu. A green 'Save' button is located at the bottom left of the form.

1. Inconvenientes de conectividad: Asegúrese de que la instancia de Splunk pueda ponerse en contacto con el host de la API
2. Host de API: Asegúrese de que el host de la API configurado en el paso 10 coincide con su organización de AMP, según el punto en el que se encuentre su empresa.
3. Credenciales de API: Asegúrese de que la clave API y la ID de cliente coinciden con los configurados en el paso 3.
4. Flujos de eventos: Asegúrese de tener menos de 4 secuencias de eventos configuradas.