AMP for Endpoints Integration with Splunk

Contents

Introduction

This document describes the integration process between Advanced Malware Protection (AMP) and Splunk.

Contributed by Uriel Islas and Juventino Macias, Edited by Jorge Navarrete, Cisco TAC Engineers.

Prerequisites

Requirements

Cisco recommends that you have the knowledge of:

- AMP for Endpoints
- Application Programming Interface (API)
- Splunk
- Admin user on Splunk

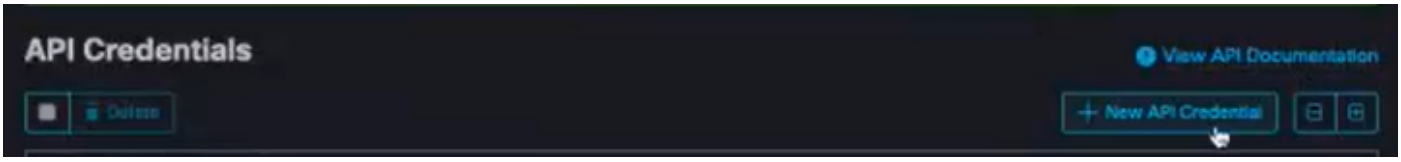
Components Used

- AMP Public Cloud
- Splunk instance

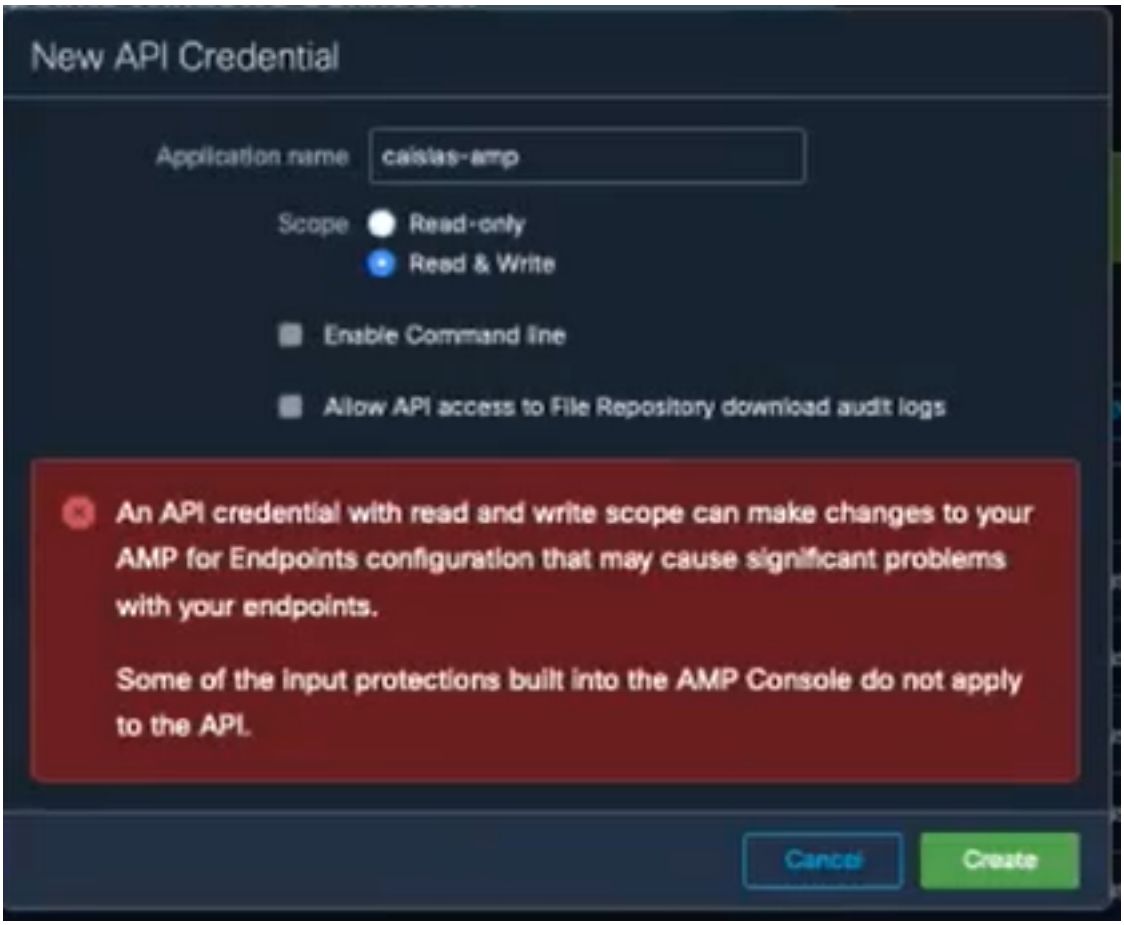
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

Step 1. Navigate to AMP console (https://console.amp.cisco.com) and navigate to **Accounts>API Credentials**, where you can create event streams.

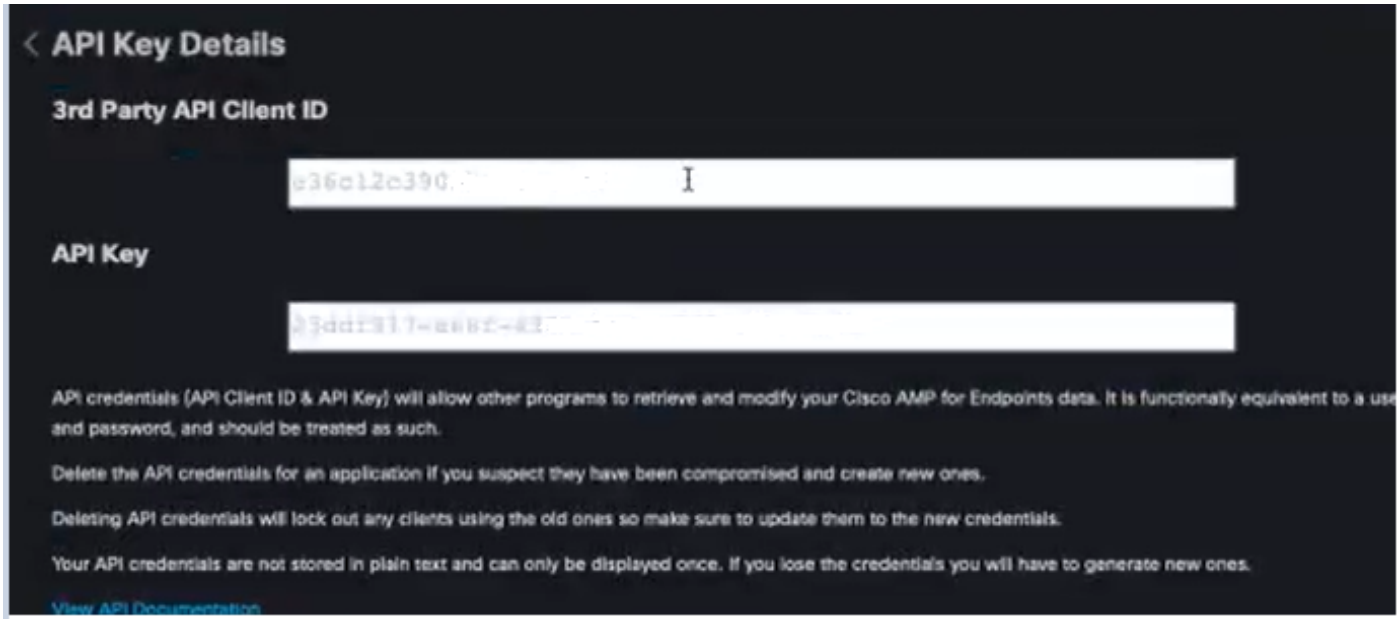


Step 2. In order to perform this integration, mark the **Read & Write** checkbox as shown below:



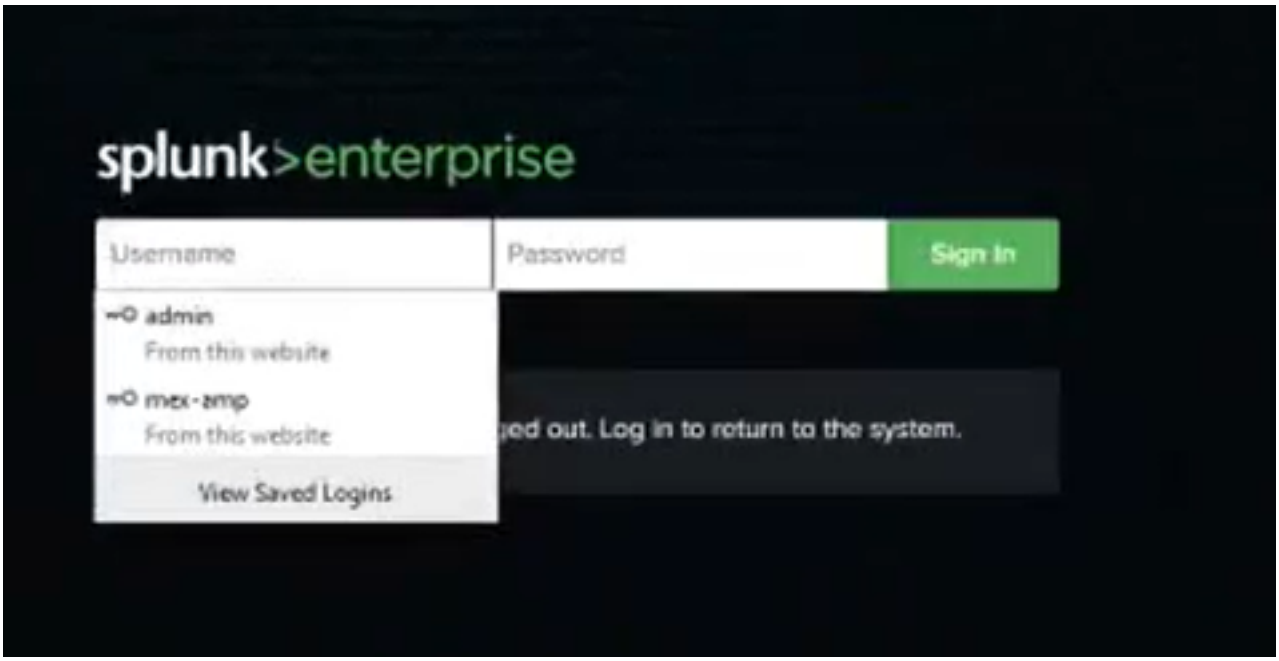
> **Note**: If you would like to collect more information on the events, check the **Enable Command Line** box, to get the Audit Logs generated from the File Repository check the **Allow API access to File Repository** box.

Step 3. Once you create the event stream it would display the API Client ID and API Key which is required on Splunk.

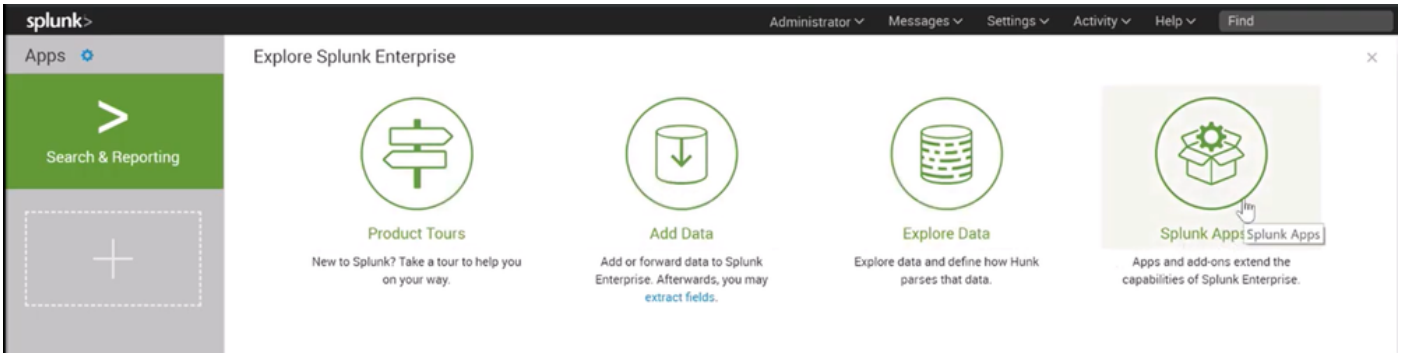


Caution: This information cannot be recovered by any means, in case of loss, a new API Key must be created.

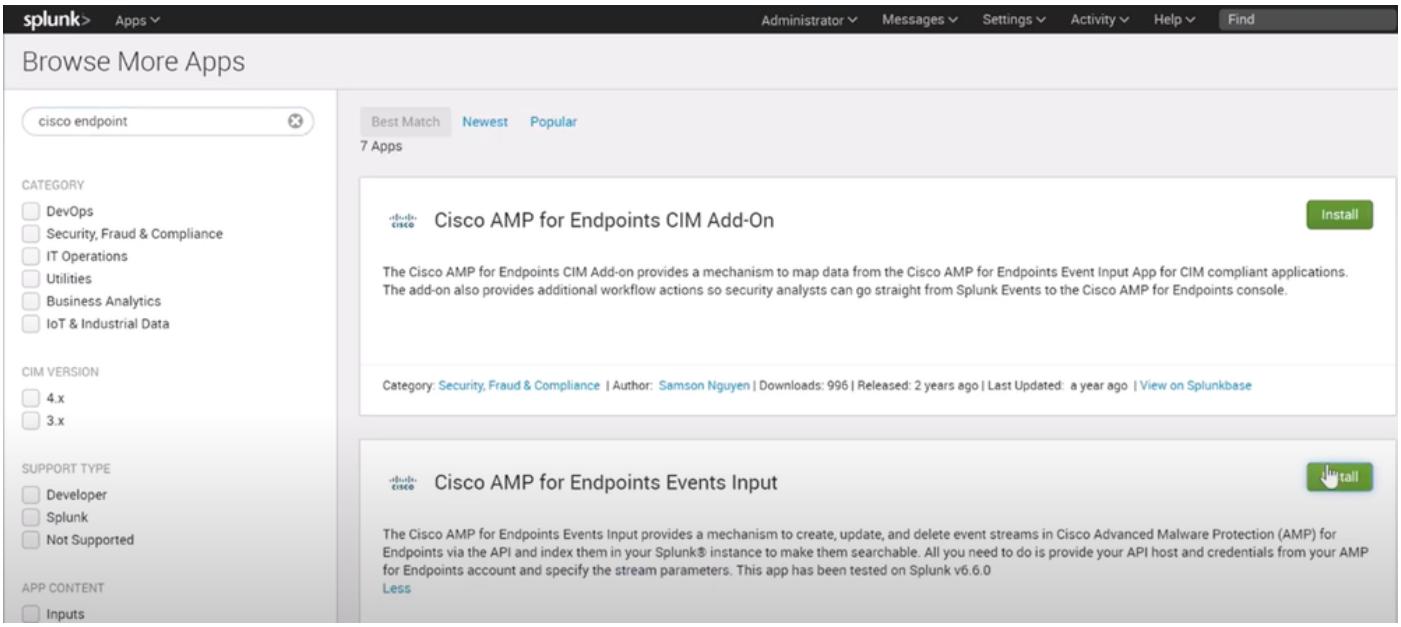
Step 4. In order to integrate Splunk with AMP for endpoints, ensure that the account **Admin** exists on Splunk.



Step 5. Once you log in on Splunk, proceed to download AMP from Splunk Apps.

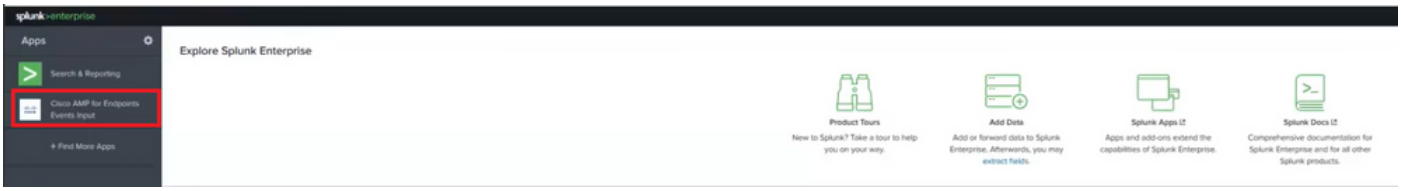


Step 6. Search for Cisco Endpoint on the App browser and install it (Cisco AMP for Endpoints Events Input).

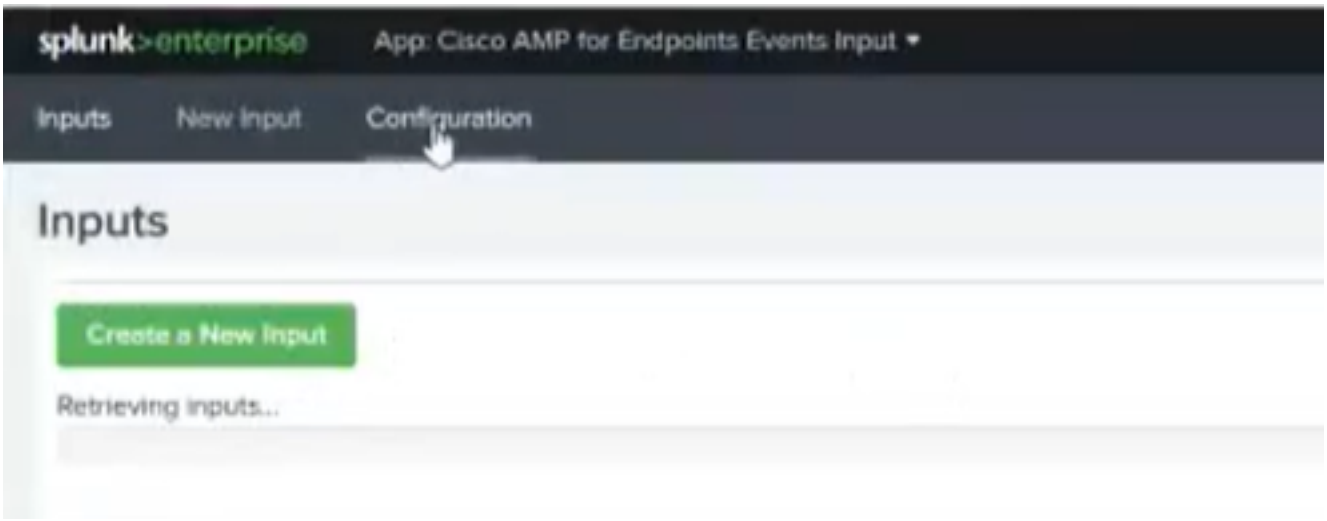


Step 7. A restart of the session is required to complete the installation on Splunk.

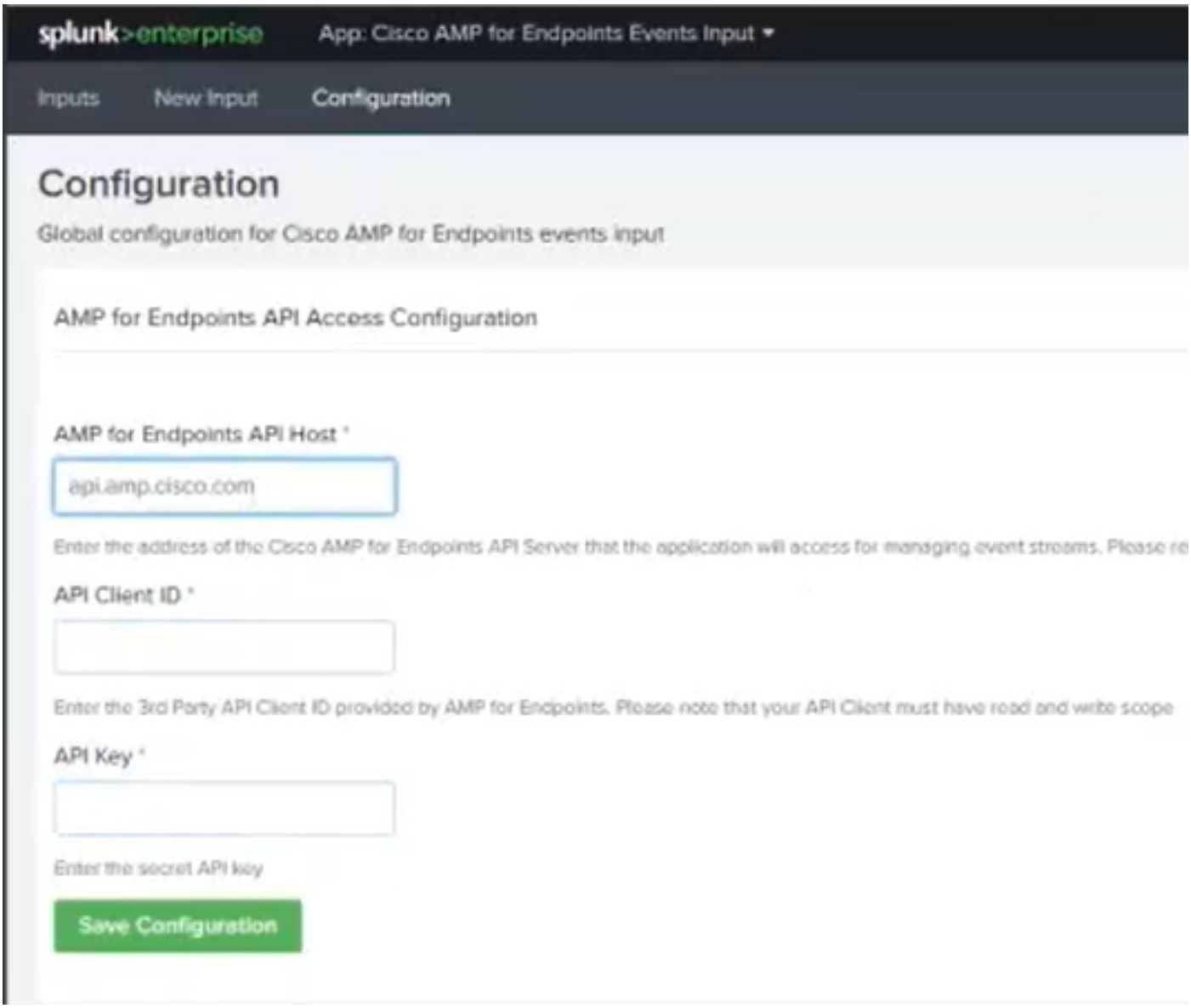
Step 8. Once you log in under Splunk, click on **Cisco AMP For Endpoints** on the left side of the screen.



Step 9. Click on the **Configuration** label at the top of the screen.



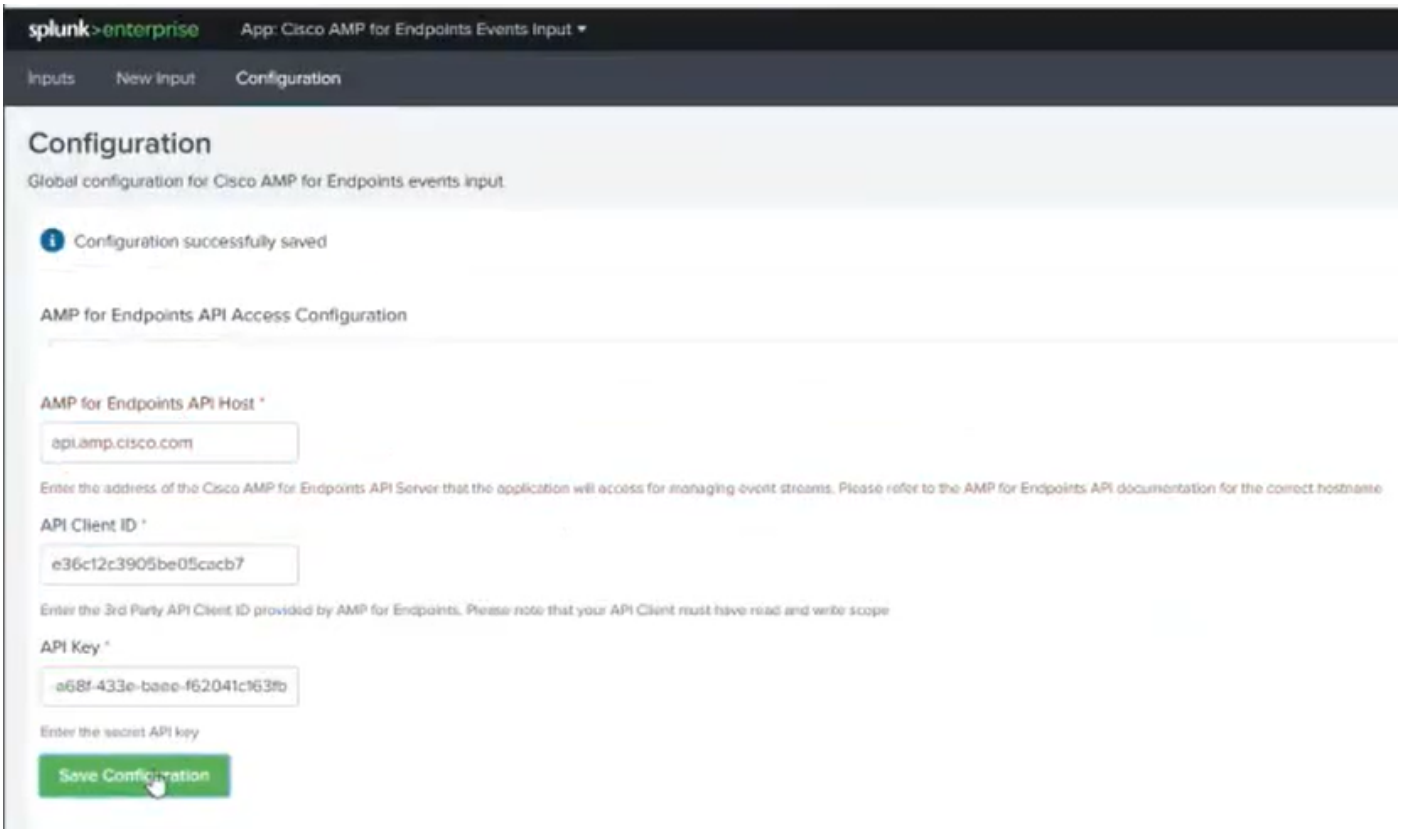
Step 10. Type your API credentials previously generated from the AMP console.



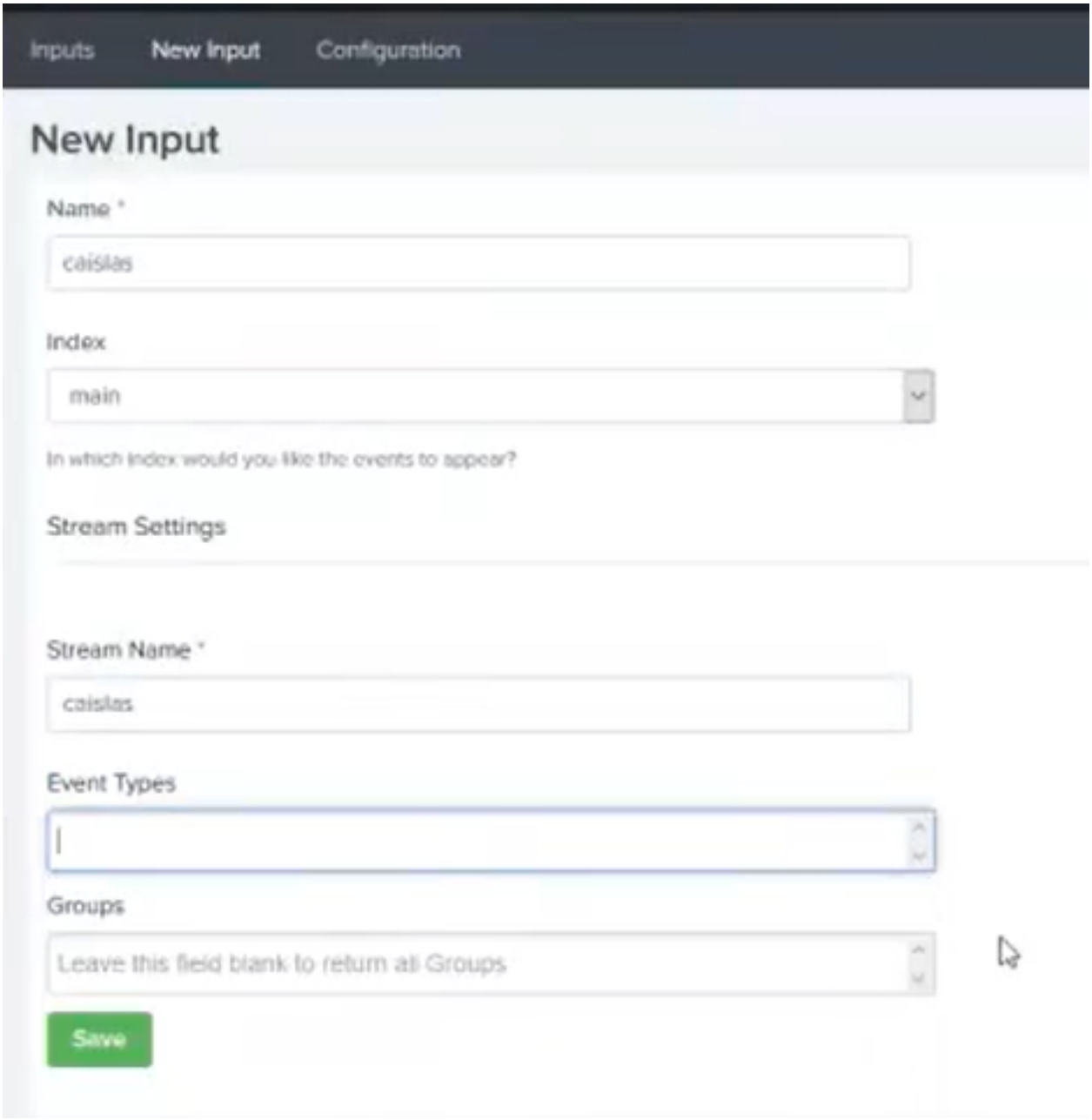
Note: The API Host spot might be different based on the Cloud Data Center that your organization points at:

North America: api.amp.cisco.com
Europe: api.eu.amp.cisco.com
APJC: api.apjc.amp.cisco.com

Step 11. Include and save API credentials on the Splunk console to link them with AMP.

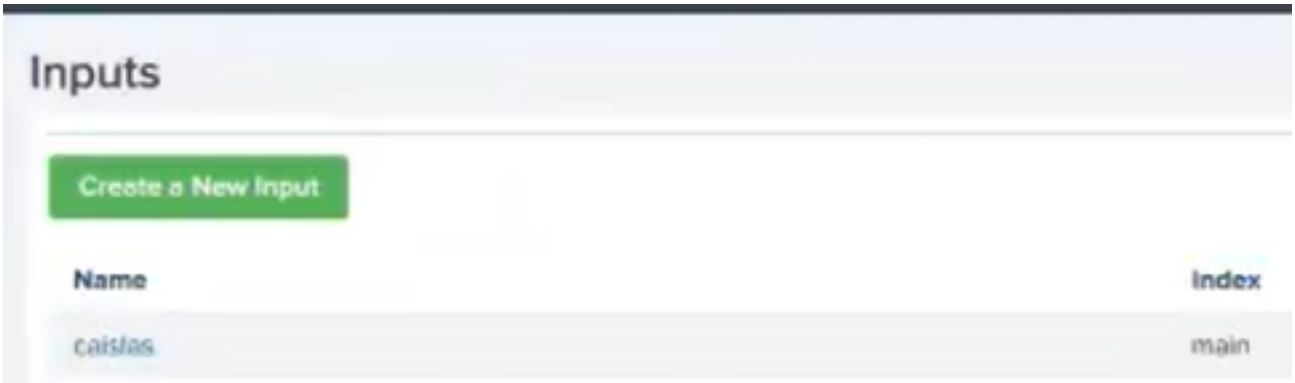


Step 12. Go back to **Input** to get your event stream created.



Note: If you want to get all the events for all the groups from AMP, leave **Event Types** and **Groups** fields blank.

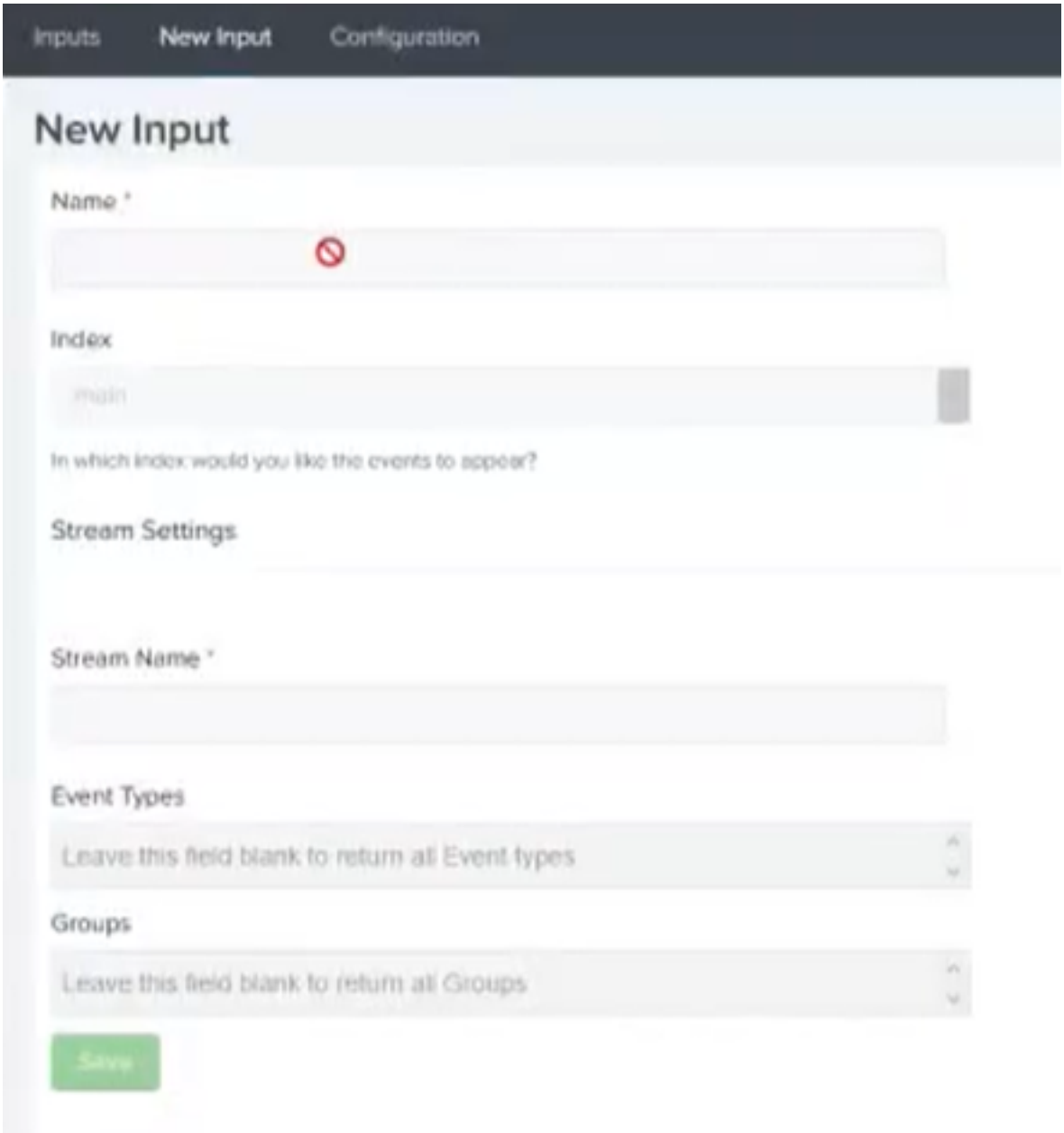
Step 13. Ensure that your input was successfully created.



Note: Please keep on mind that this integration is not officially supported

Troubleshoot

If while you create an event stream all the fields are greyed out, that could be caused for some of the reasons below:



1. Connectivity Issues: Ensure that Splunk instance is able to contact the API host
2. API Host: Ensure that the API host configured on step 10 match with your AMP organization, based on where your business points at.
3. API credentials: Ensure that the API Key and Client ID match with the ones configured on step 3.
4. Event Streams: Ensure that you have less than 4 event streams configured.