面向终端的AMP与Splunk集成

目录

简介

本文档介绍高级恶意软件防护(AMP)与Splunk之间的集成过程。

作者：Uriel Islas和Juventino Macias，编辑者：Jorge Navarrete，思科TAC工程师。

先决条件

要求

思科建议您了解：

- 面向终端的 AMP
- 应用编程接口(API)
- 斯普隆克
- Splunk上的管理员用户

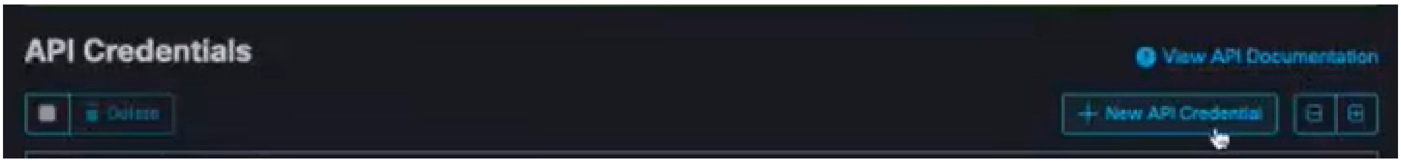
使用的组件

- AMP公共云
- Splunk实例

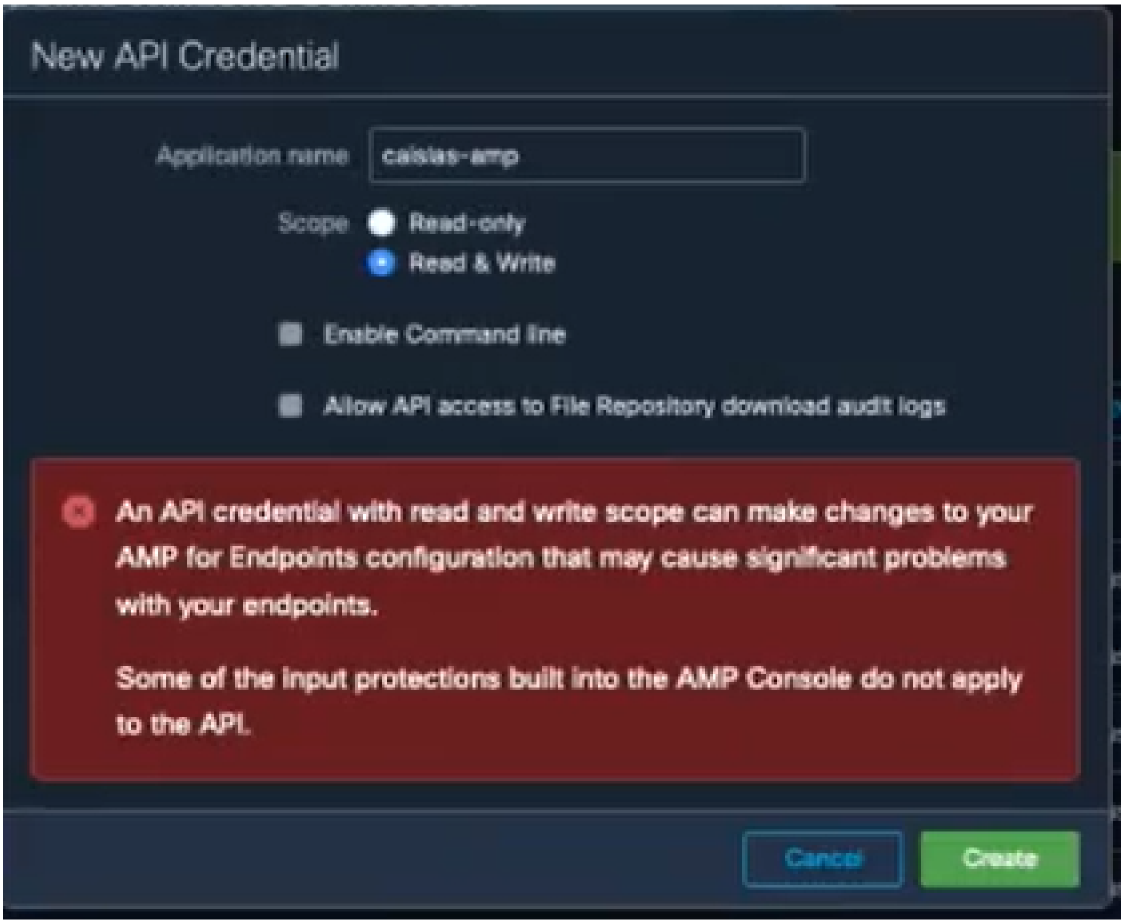
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

步骤1.导航至AMP控制台(https://console.amp.cisco.com)，然后导航**至Accounts>API Credentials**，在其中可以创建事件流。



步骤2.要执行此集成，请勾选“读**写”复**选框，如下所示：



New API Credential

Application name: caisias-amp

Scope ○ Read-only

● Read & Write

□ Enable Command line

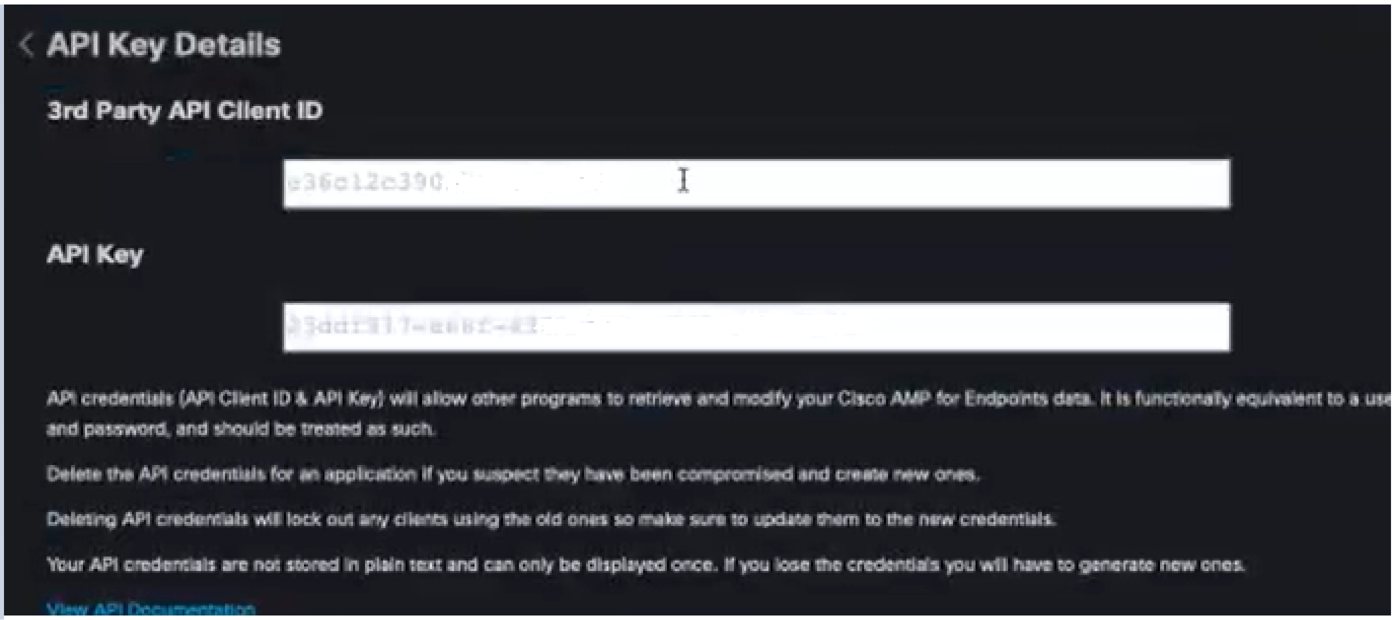
□ Allow API access to File Repository download audit logs

An API credential with read and write scope can make changes to your AMP for Endpoints configuration that may cause significant problems with your endpoints.

Some of the input protections built into the AMP Console do not apply to the API.

注意：如果要收集有关事件的详细信息，请选中**Enable Command Line**框，以获取从文件存储库生成的审核日志，选中**Allow API access to File Repository**框。

步骤3.创建事件流后，它将显示Splunk上所需的API客户端ID和API密钥。



API Key Details

3rd Party API Client ID

e36c12c390[redacted]

API Key

23ddf311-ee8f-42[redacted]

API credentials (API Client ID & API Key) will allow other programs to retrieve and modify your Cisco AMP for Endpoints data. It is functionally equivalent to a use and password, and should be treated as such.

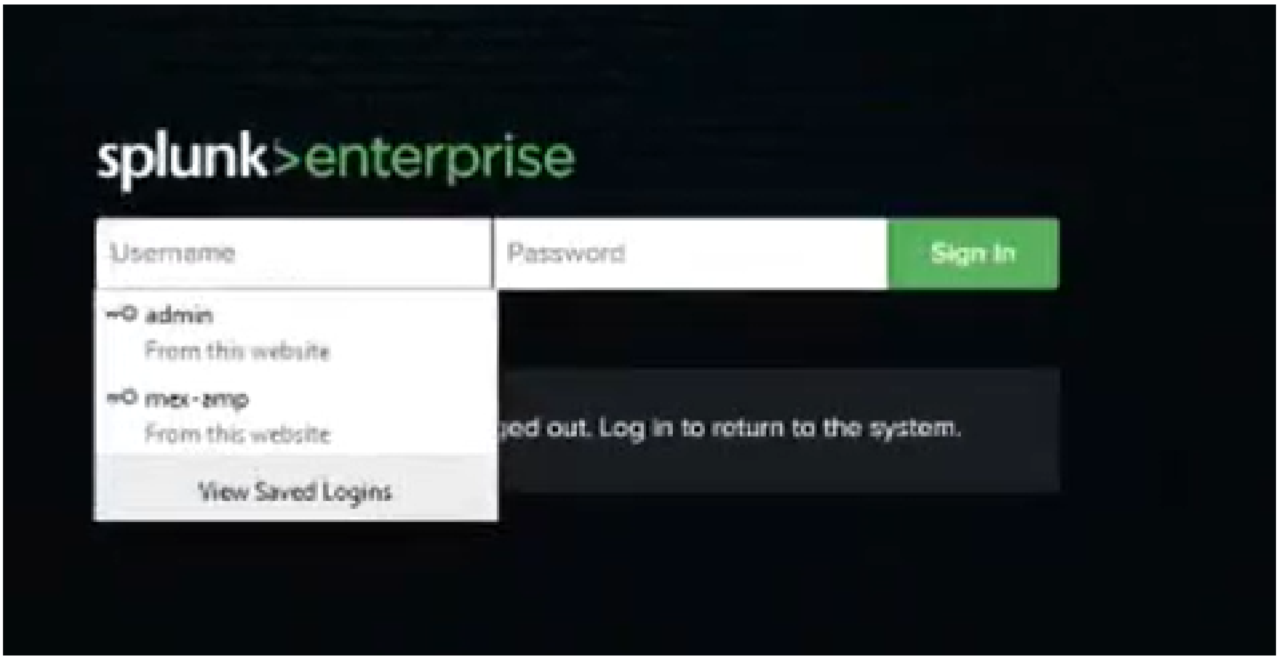
Delete the API credentials for an application if you suspect they have been compromised and create new ones.

Deleting API credentials will lock out any clients using the old ones so make sure to update them to the new credentials.

Your API credentials are not stored in plain text and can only be displayed once. If you lose the credentials you will have to generate new ones.

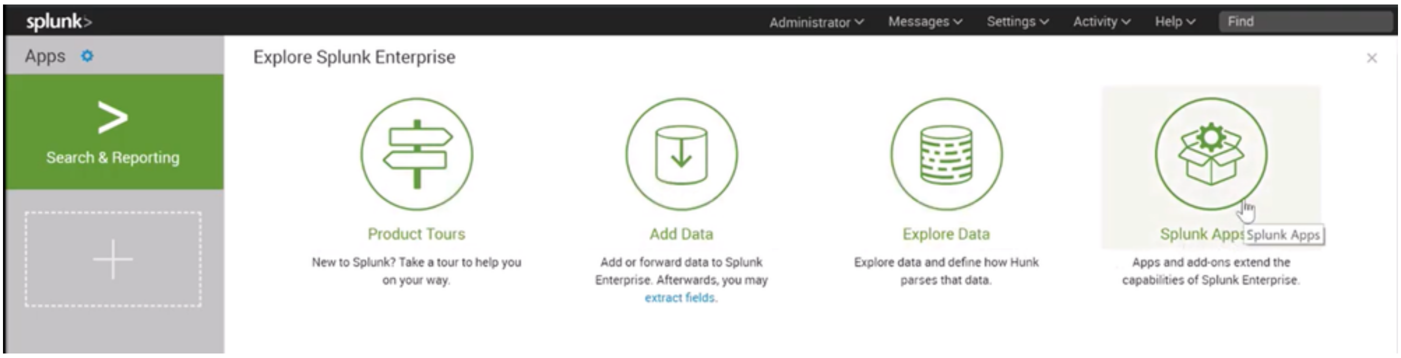
注意：在丢失时，此信息无法通过任何方式恢复，必须创建新的API密钥。

步骤4.为了将Splunk与面向终端的AMP集成，请确保Splunk上存**在帐**户Admin。



ged out. Log in to return to the system.

步骤5.登录Splunk后，继续从Splunk应用下载AMP。



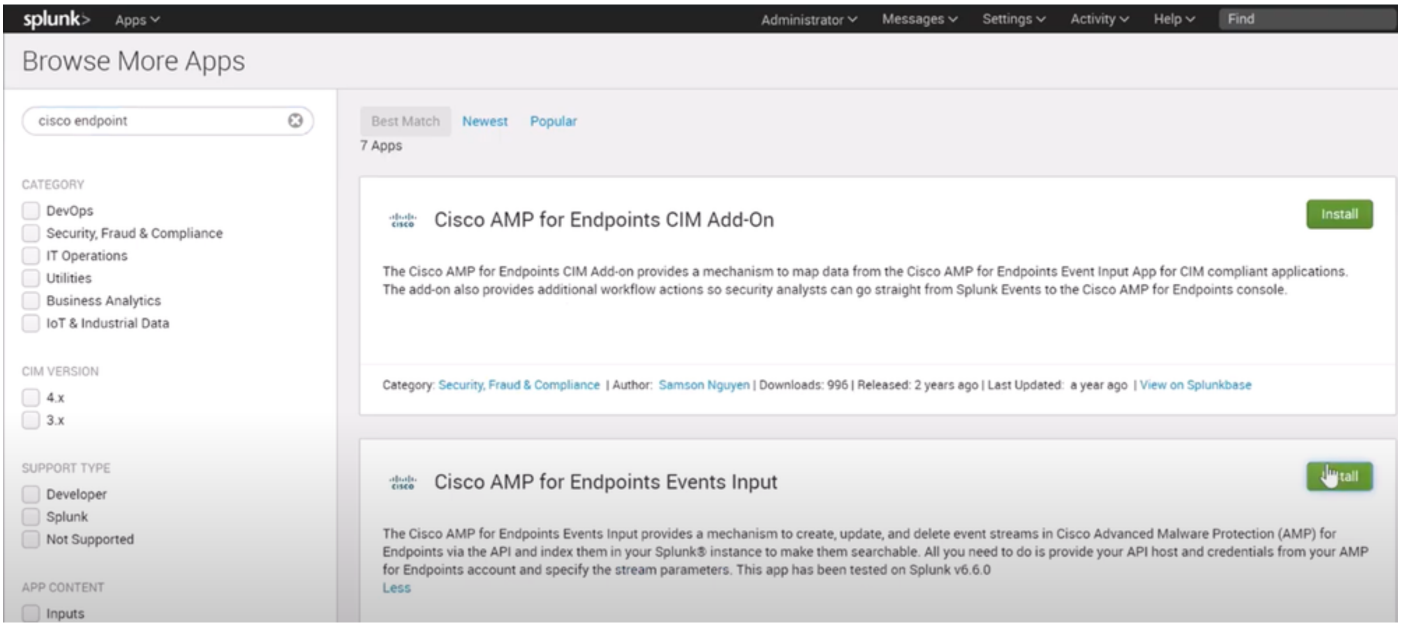
New to Splunk? Take a tour to help you on your way.

Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

Explore data and define how Hunk parses that data.

Apps and add-ons extend the capabilities of Splunk Enterprise.

步骤6.在应用浏览器上搜索并安装思科终端（面向终端的思科AMP事件输入）。



Cisco AMP for Endpoints CIM Add-On

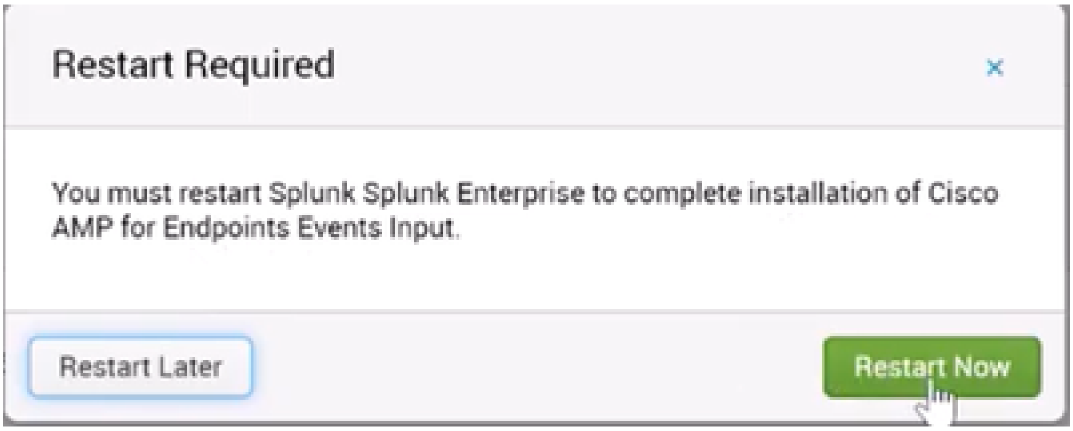
The Cisco AMP for Endpoints CIM Add-on provides a mechanism to map data from the Cisco AMP for Endpoints Event Input App for CIM compliant applications. The add-on also provides additional workflow actions so security analysts can go straight from Splunk Events to the Cisco AMP for Endpoints console.

Category: Security, Fraud & Compliance | Author: Samson Nguyen | Downloads: 996 | Released: 2 years ago | Last Updated: a year ago | View on Splunkbase

Cisco AMP for Endpoints Events Input

The Cisco AMP for Endpoints Events Input provides a mechanism to create, update, and delete event streams in Cisco Advanced Malware Protection (AMP) for Endpoints via the API and index them in your Splunk® instance to make them searchable. All you need to do is provide your API host and credentials from your AMP for Endpoints account and specify the stream parameters. This app has been tested on Splunk v6.6.0
Less

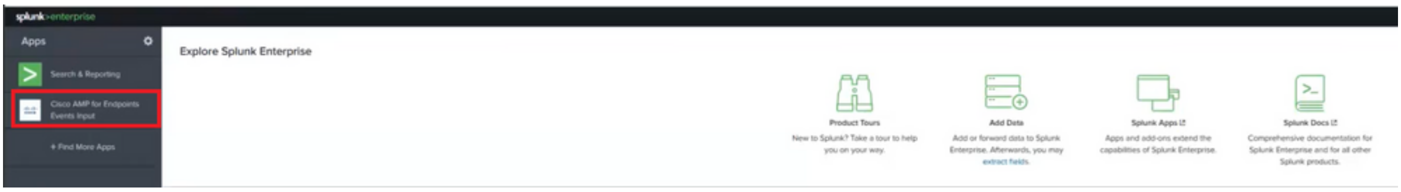
步骤7.要完成Splunk上的安装，需要重新启动会话。



Restart Required

You must restart Splunk Splunk Enterprise to complete installation of Cisco AMP for Endpoints Events Input.

步骤8.在Splunk下登录后，单击屏**幕左侧的**面向终端的思科AMP。



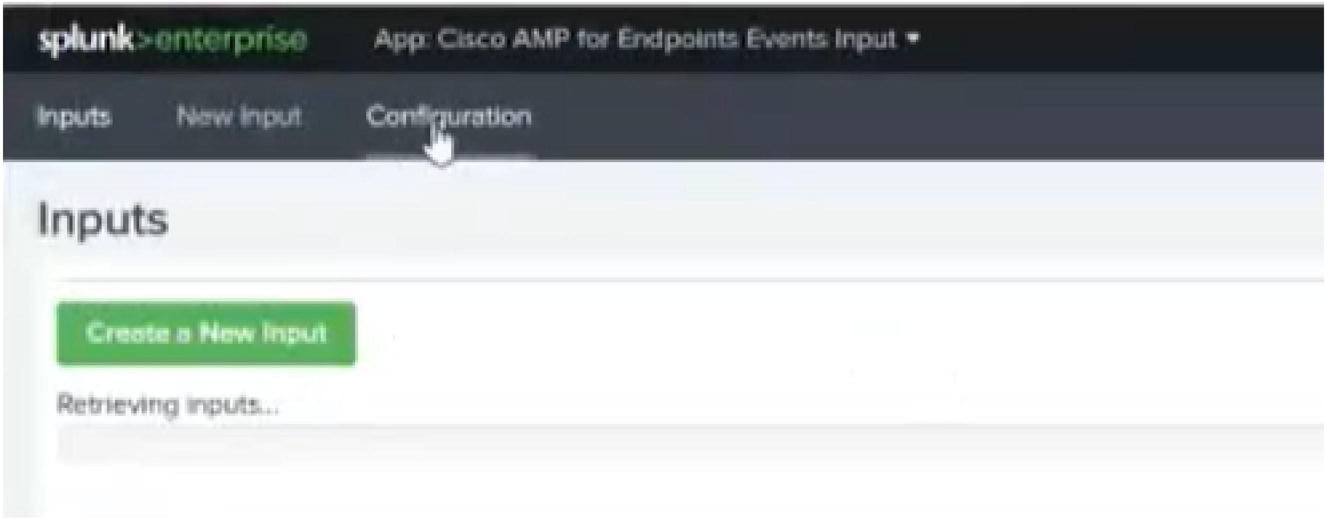
New to Splunk? Take a tour to help you on your way.

Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

Apps and add-ons extend the capabilities of Splunk Enterprise.

Comprehensive documentation for Splunk Enterprise and for all other Splunk products.

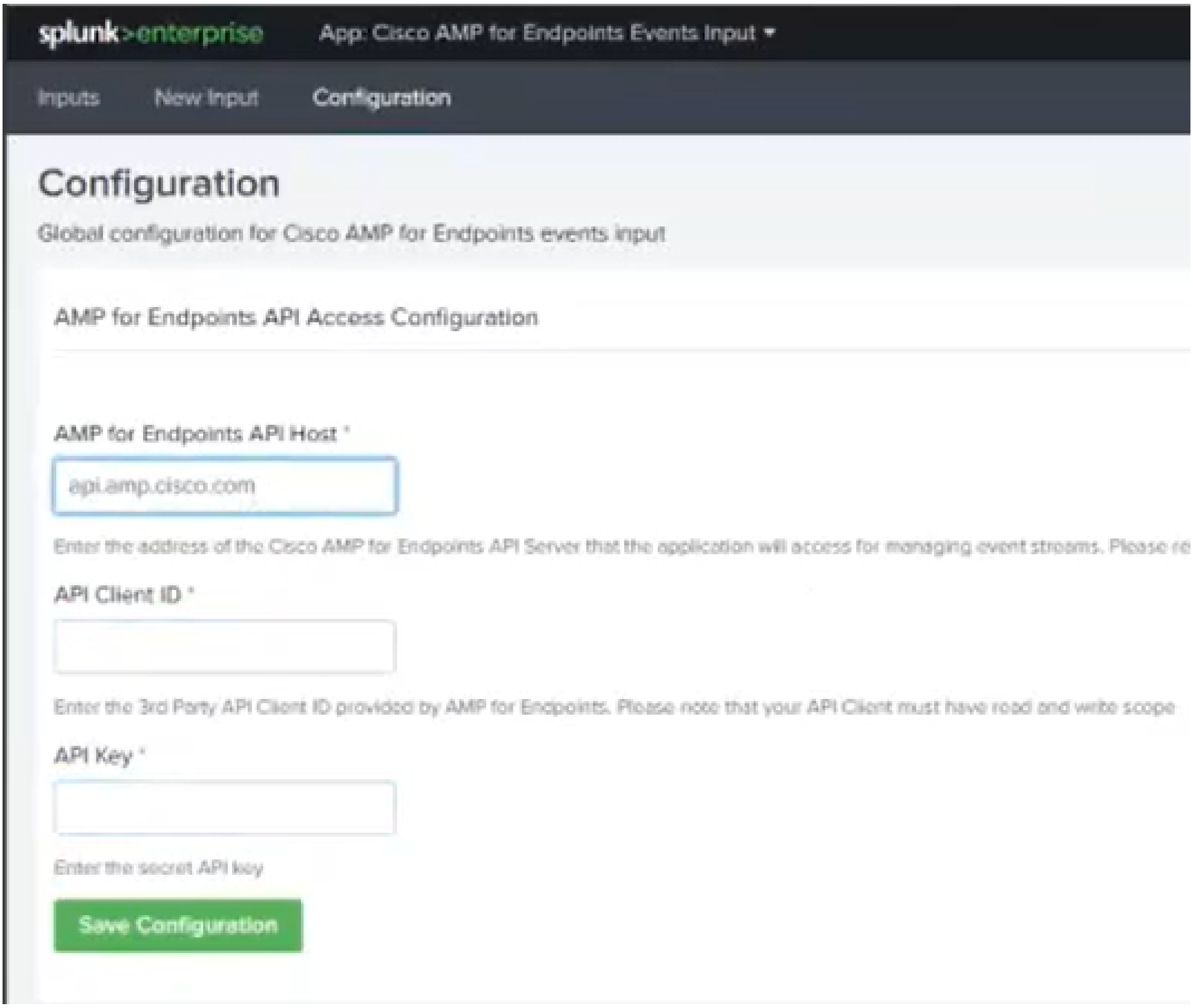
步骤9.单击屏幕顶**部**的“配置”标签。



Inputs

Retrieving inputs...

步骤10.键入之前从AMP控制台生成的API凭证。



Configuration

Global configuration for Cisco AMP for Endpoints events input

AMP for Endpoints API Access Configuration

AMP for Endpoints API Host *

api.amp.cisco.com

Enter the address of the Cisco AMP for Endpoints API Server that the application will access for managing event streams. Please re

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

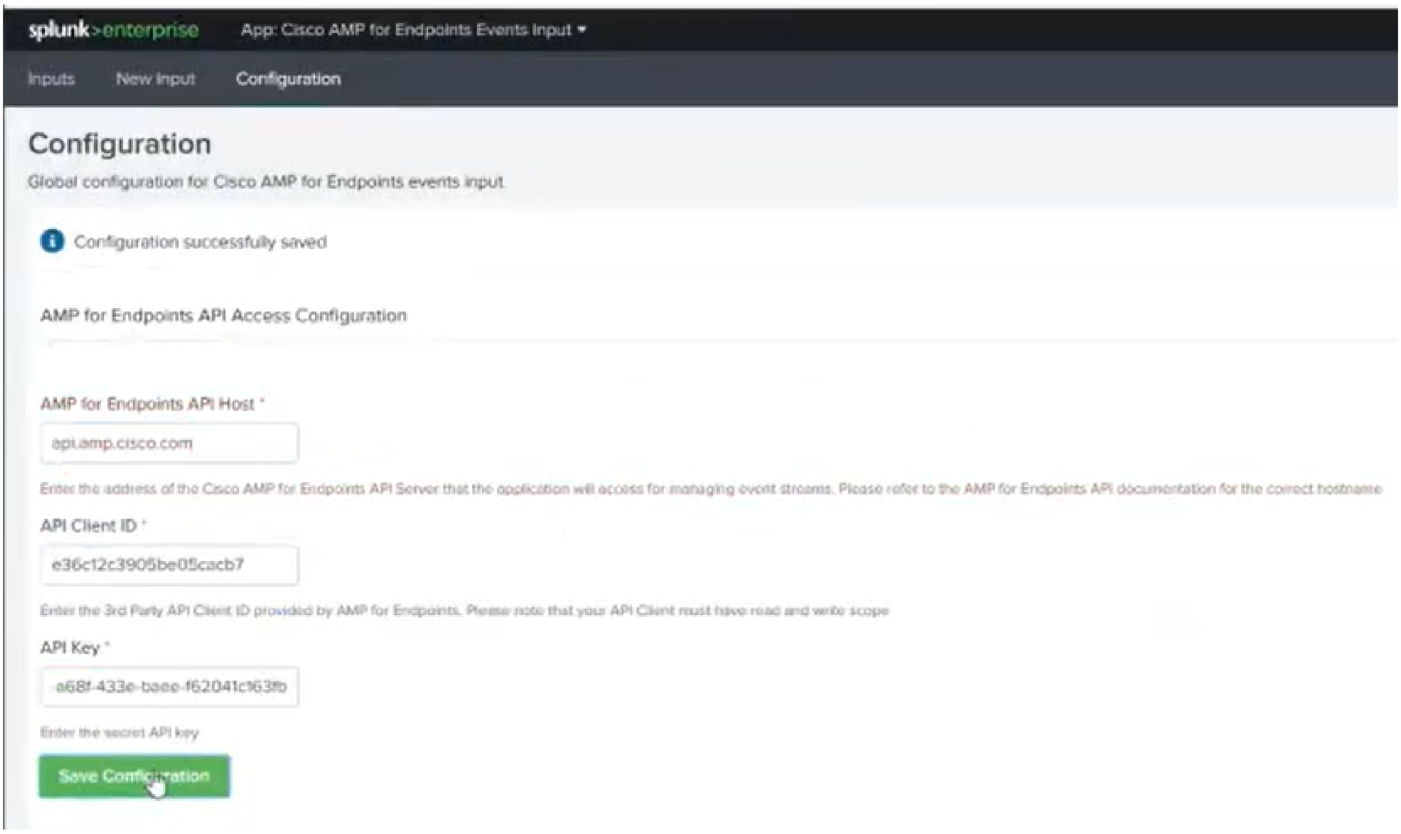
API Key *

Enter the secret API key

注意：API主机位置可能因贵组织指向的云数据中心而异：

北美:api.amp.cisco.com
欧洲:api.eu.am p.cisco.com
亚太地区、日本和中国：api.apjc.amp.cisco.com

步骤11.在Splunk控制台上包含并保存API凭证，以将其与AMP链接。



Configuration

Global configuration for Cisco AMP for Endpoints events input

Configuration successfully saved

AMP for Endpoints API Access Configuration

AMP for Endpoints API Host *

api.amp.cisco.com

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 *

e36c12c3905be05cacb7

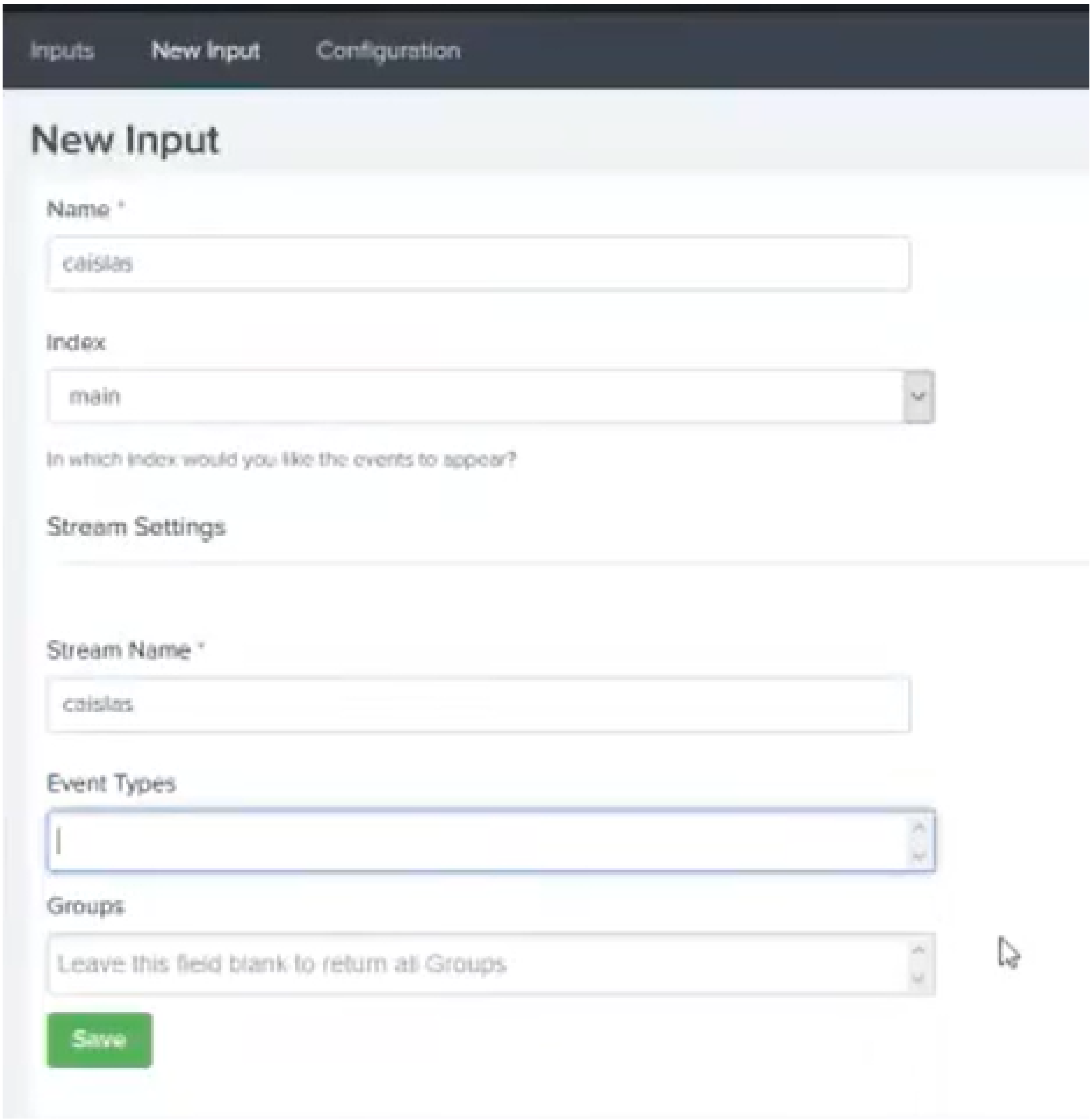
Enter the 3rd Party API Client ID provided by AMP for Endpoints. Please note that your API Client must have read and write scope

API Key *

a68f-433e-baee-f62041c163fb

Enter the secret API key

步骤12.返回“输入”以创建事件流。



New Input

Name *

caislas

Index

main

In which index would you like the events to appear?

Stream Settings

Stream Name *

caislas

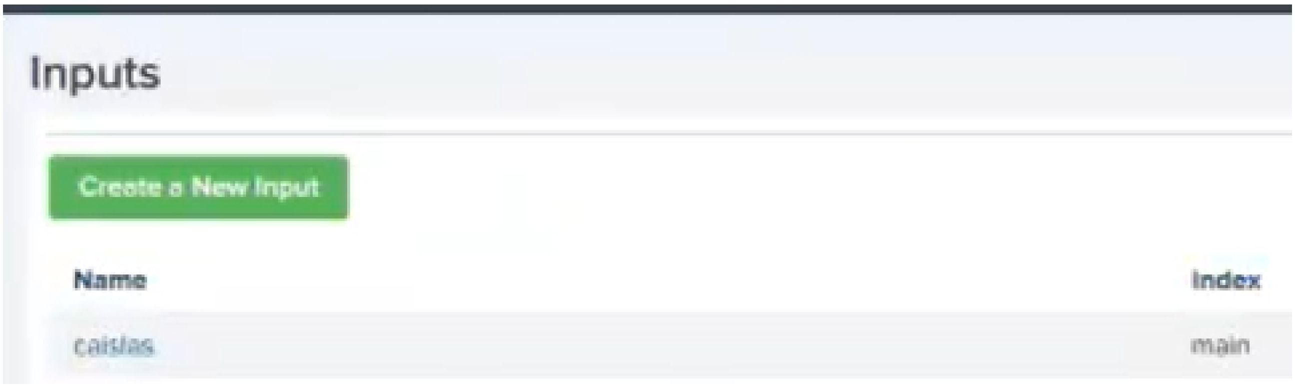
Event Types

Groups

Leave this field blank to return all Groups

注意：如果要从AMP获取所有组的所有事件，请将事件类型和**组字**段留**空**。

步骤13.确保输入已成功创建。



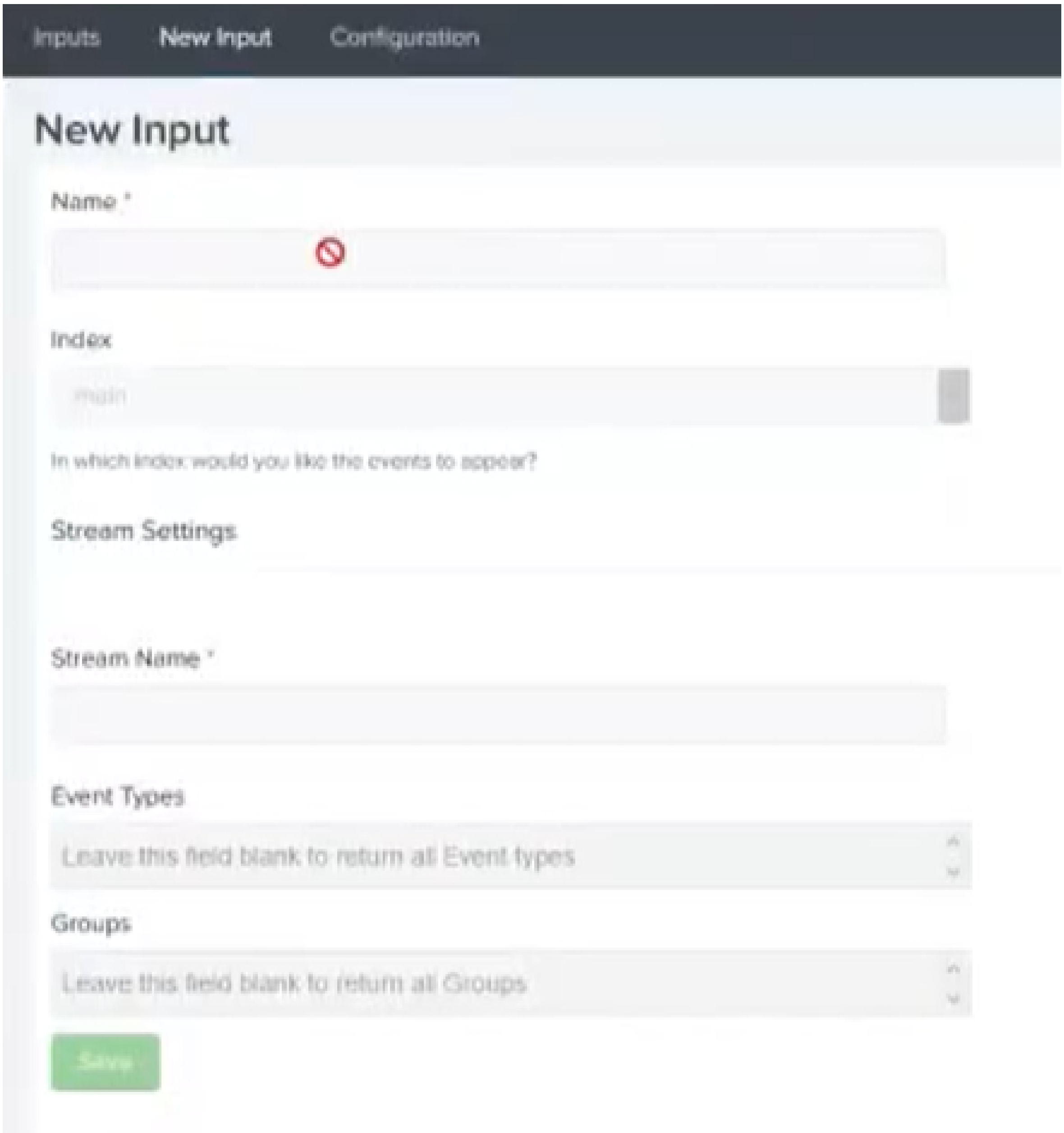
Inputs

Name	Index
caislas	main

注意：请记住，此集成不受正式支持

故障排除

如果在创建事件流时，所有字段都呈灰色显示，则可能是由于以下某些原因导致的：



New Input

Name *

Index

main

In which index would you like the events to appear?

Stream Settings

Stream Name *

Event Types

Leave this field blank to return all Event types

Groups

Leave this field blank to return all Groups

1. 连通性问题：确保Splunk实例能够与API主机联系
2. API主机：确保在步骤10中配置的API主机与AMP组织匹配，具体取决于您的业务所在位置。
3. API凭证：确保API密钥和客户端ID与第3步中配置的API密钥和客户端ID匹配。
4. 事件流：确保配置的事件流少于4个。