

AMP for EndpointsとSplunkの統合

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[トラブルシューティング](#)

概要

このドキュメントでは、高度なマルウェア防御(AMP)とSplunkの統合プロセスについて説明します。

著者 : Cisco TACエンジニア、Jorge Navarrete、Uriel IslasおよびJuventino Macias

前提条件

要件

次の知識があることが推奨されます。

- AMP for Endpoints
- アプリケーションプログラミングインターフェイス(API)
- Splunk
- Splunkの管理者ユーザ

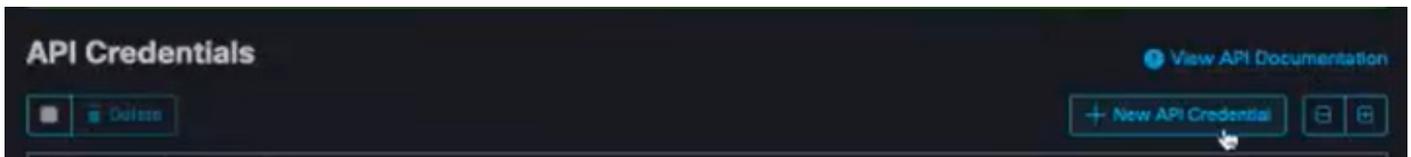
使用するコンポーネント

- AMPパブリッククラウド
- Splunkインスタンス

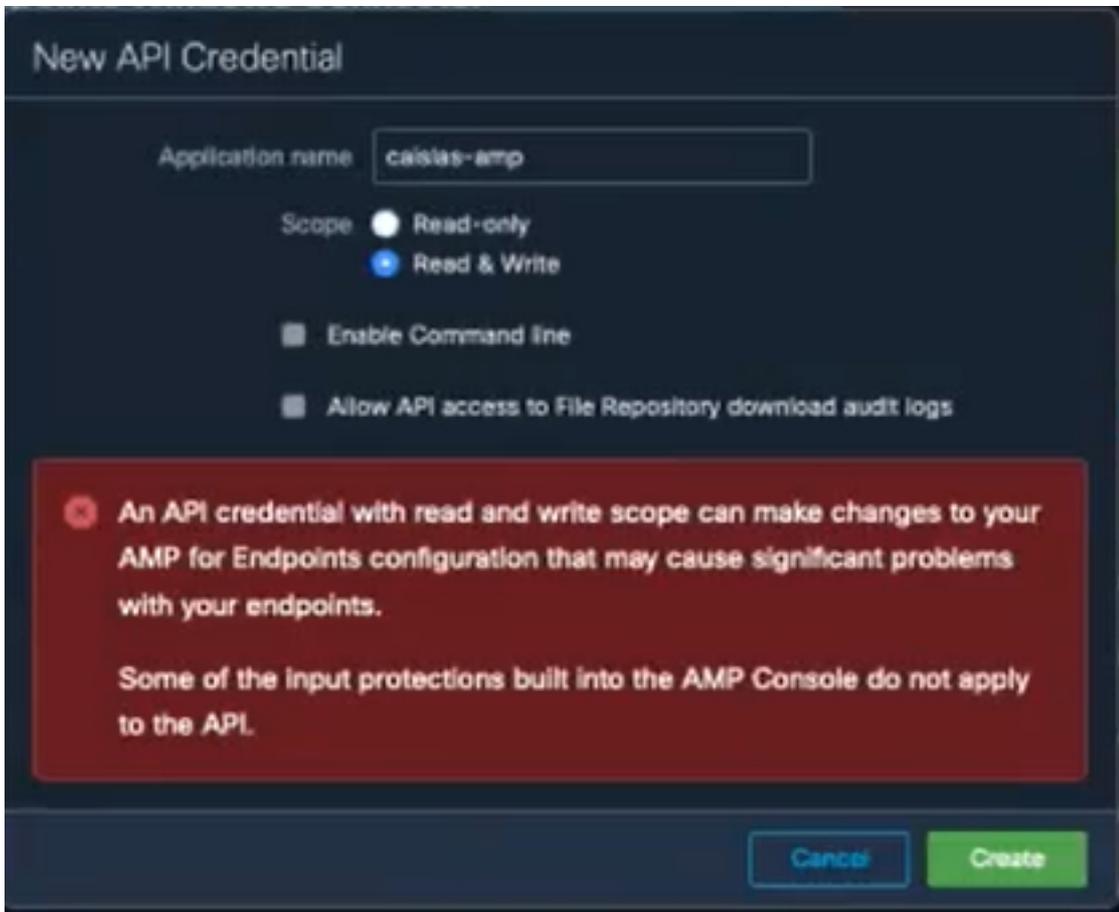
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

設定

ステップ1:AMPコンソール(<https://console.amp.cisco.com>)に移動し、[Accounts] > [API Credentials] に移動して、イベントストリームを作成できます。

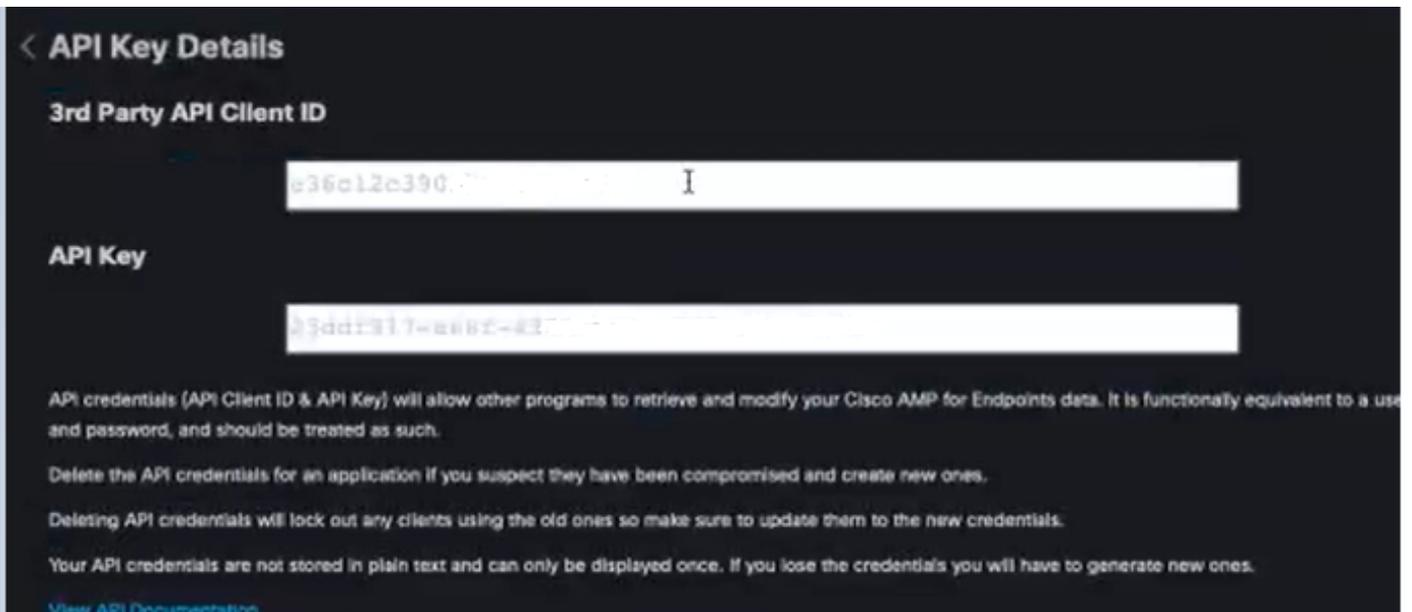


ステップ2：この統合を実行するには、次に示すように[Read & Write]チェックボックスをオンにします。



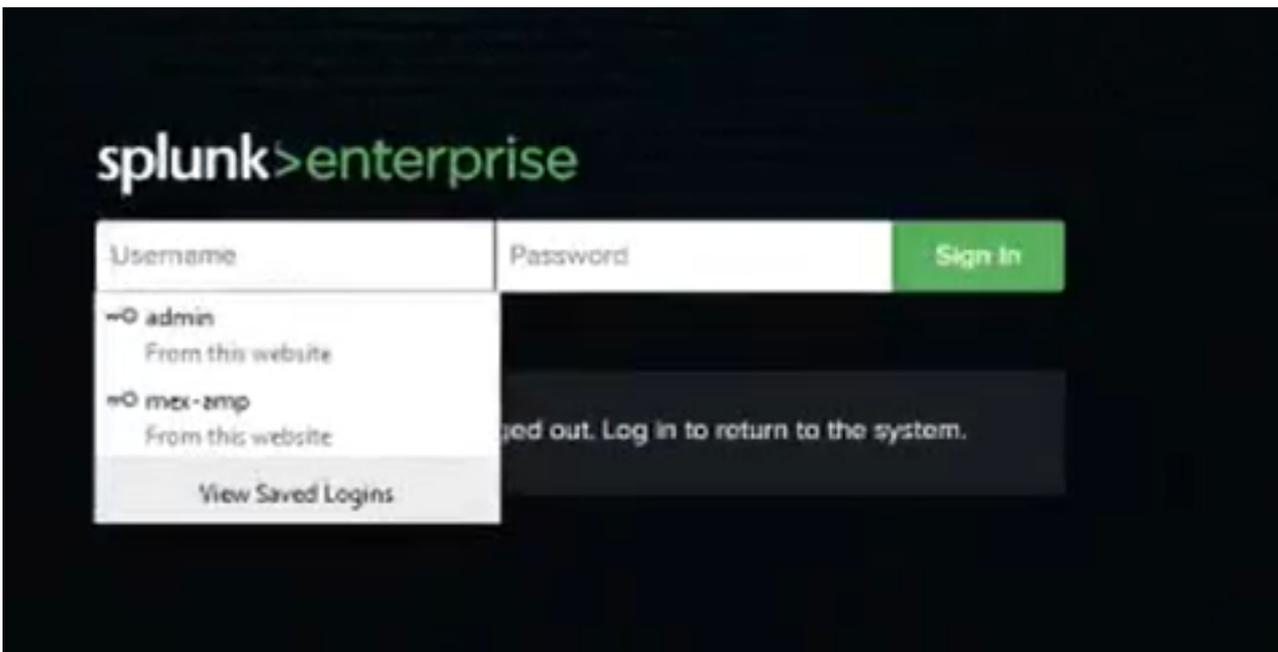
注：イベントに関する詳細情報を収集する場合は、[Enable Command Line]ボックスをオンにし、ファイルリポジトリから生成される監査ログを取得するには、[Allow API access to File Repository]ボックスをオンにします。

ステップ3：イベントストリームを作成すると、Splunkで必要なAPIクライアントIDとAPIキーが表示されます。

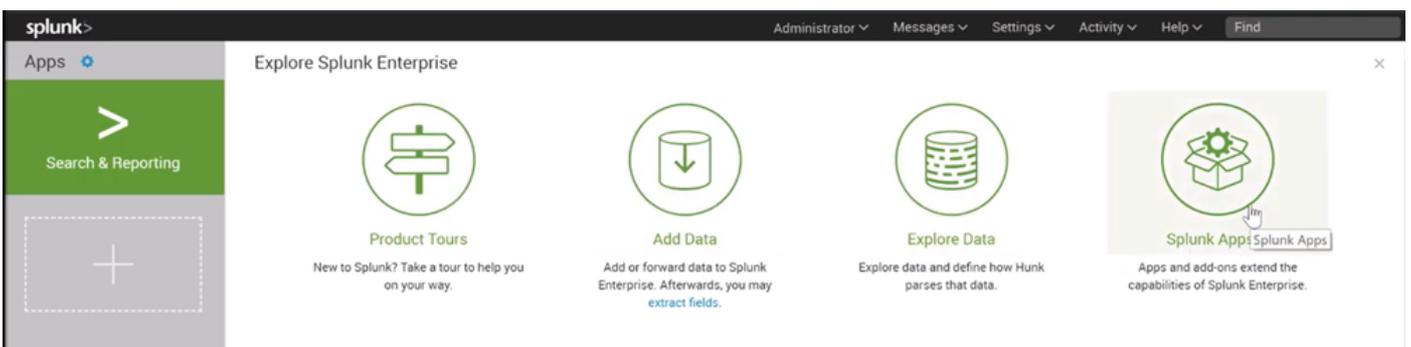


注意：この情報は、損失が発生した場合に新しいAPIキーを作成する必要がある方法で回復することはできません。

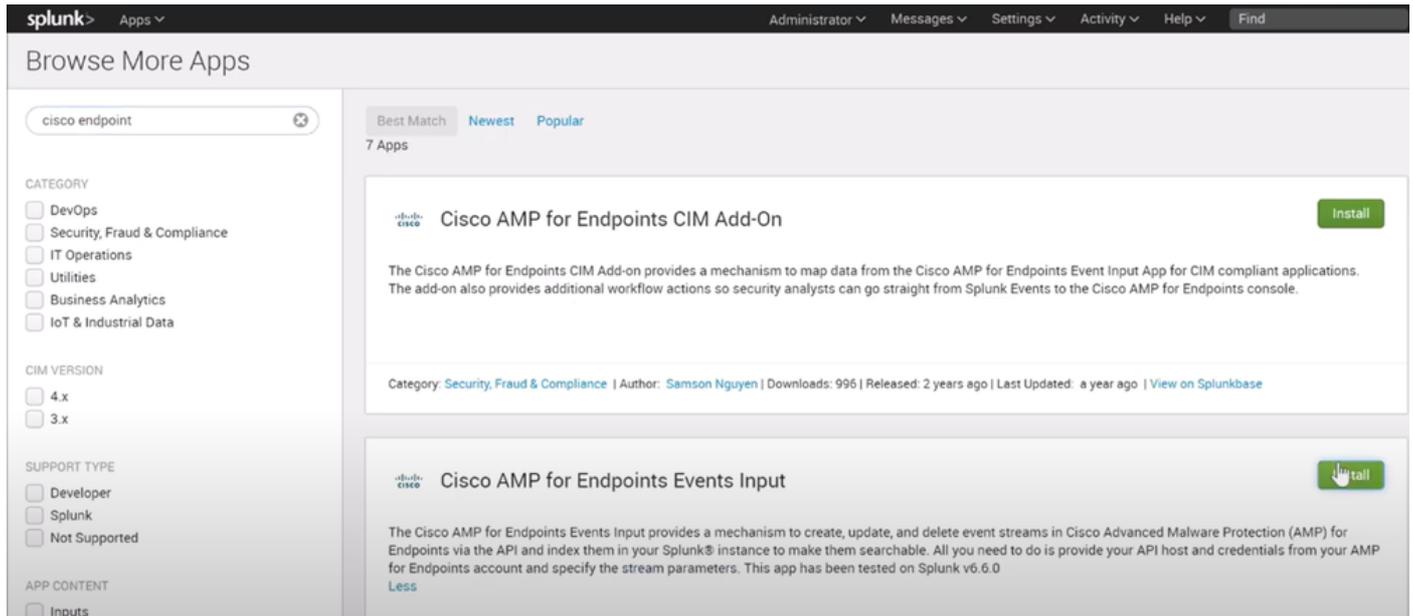
ステップ4: Splunkをエンドポイント用のAMPと統合するには、アカウントAdminがSplunk上に存在することを確認します。



ステップ5: Splunkにログインしたら、Splunk AppsからAMPをダウンロードします。



ステップ6:AppブラウザでCisco Endpointを検索し、インストールします(Cisco AMP for Endpoints Events Input)。



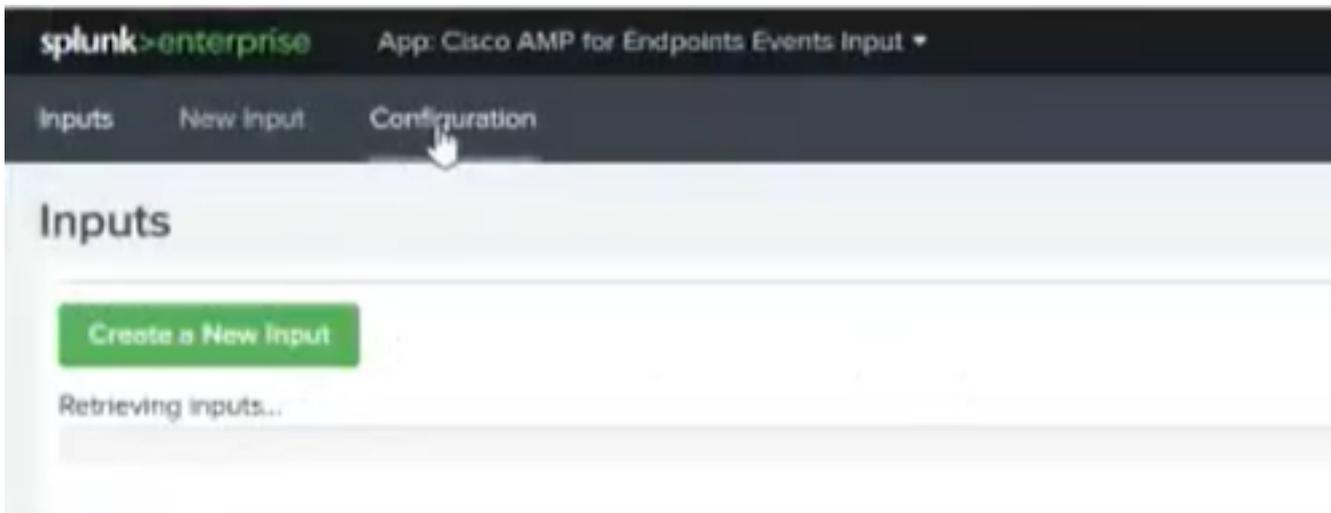
ステップ7: Splunkでのインストールを完了するには、セッションを再起動する必要があります。



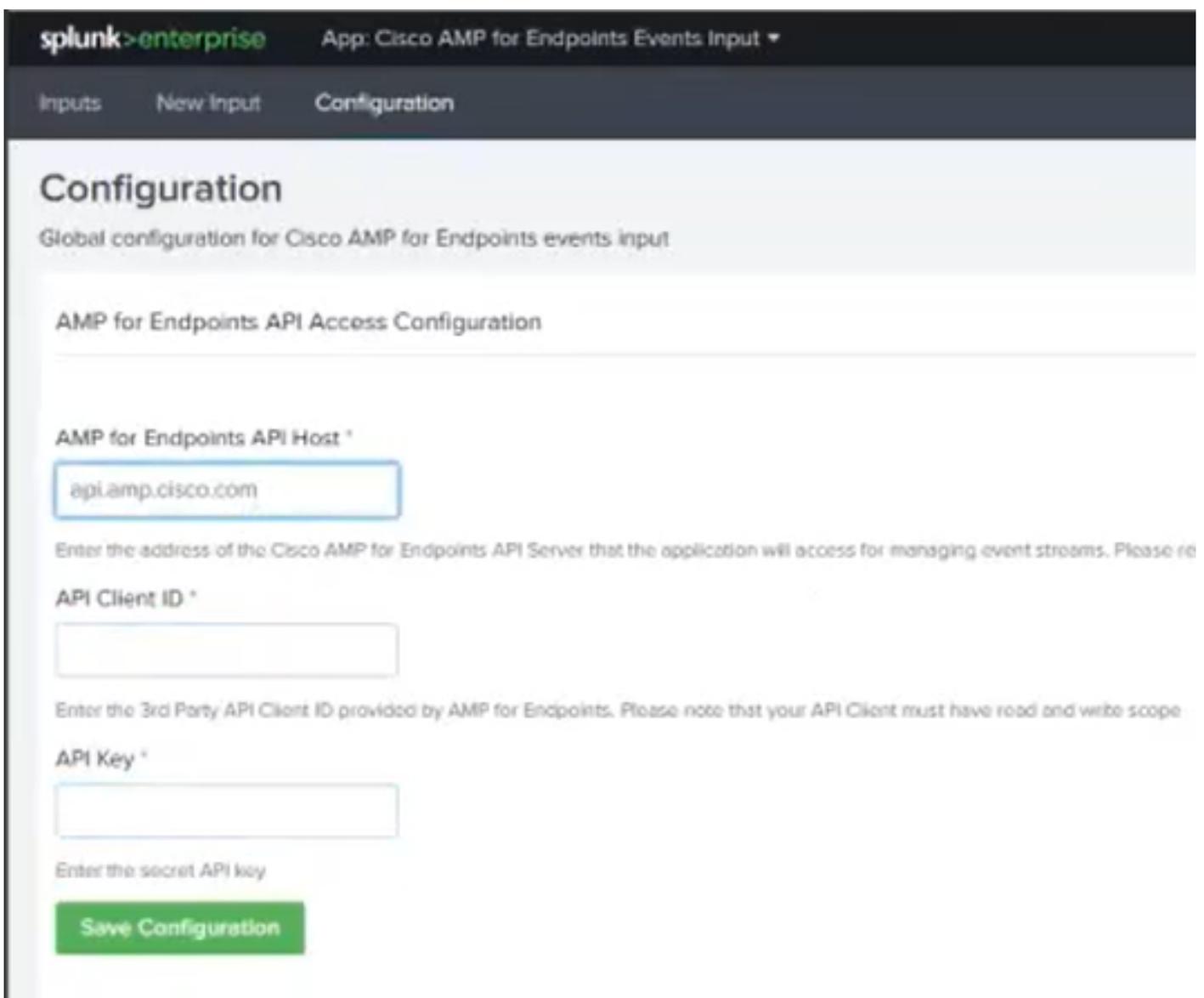
ステップ8: Splunkでログインしたら、画面の左側にあるCisco AMP For Endpointsをクリックします。



ステップ9 : 画面の上部にある[Configuration]ラベルをクリックします。



ステップ10:AMPコンソールから以前に生成したAPIクレデンシャルを入力します。



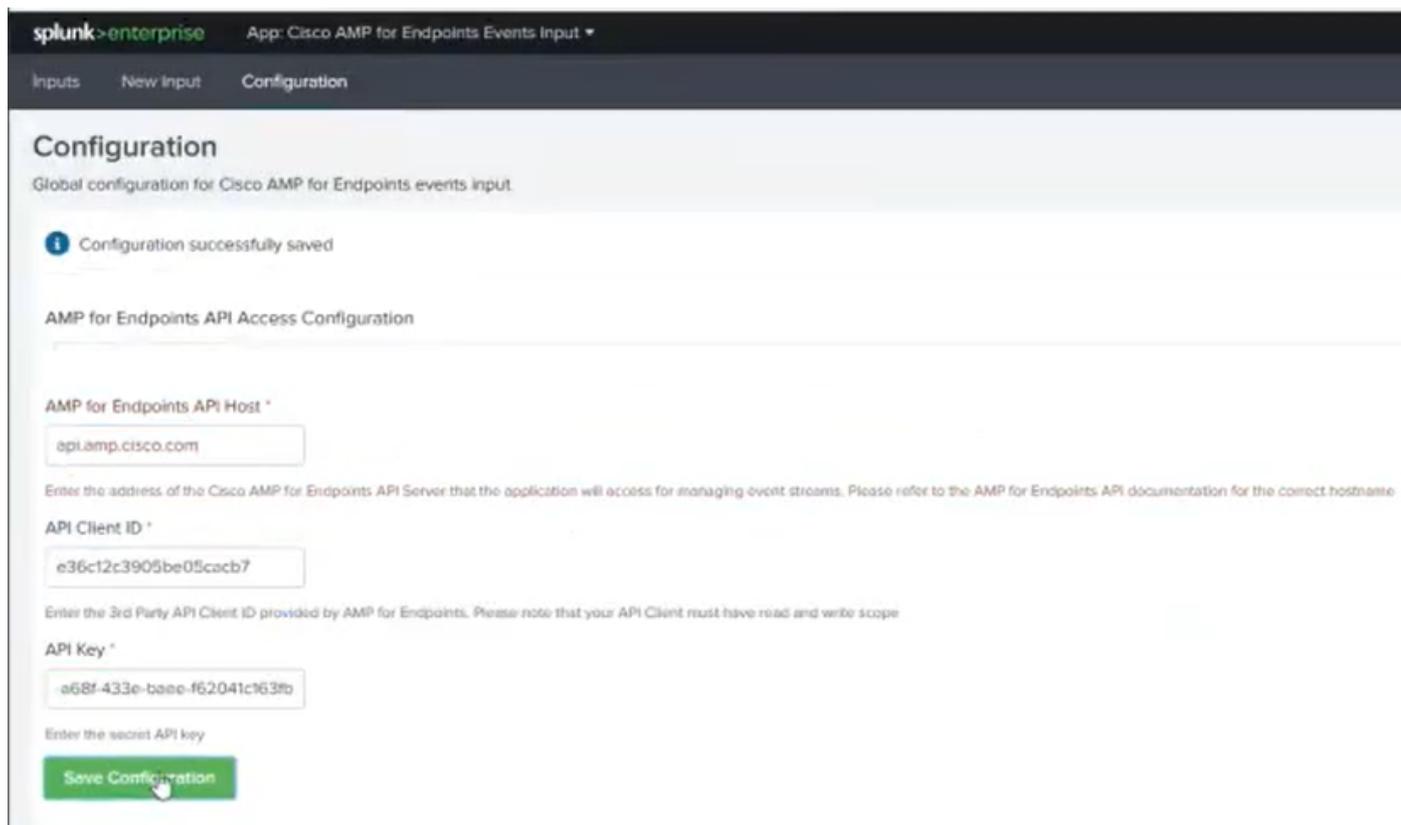
注：APIホストスポットは、組織がポイントするクラウドデータセンターによって異なる場合があります。

北米:api.amp.cisco.com

ヨーロッパ:api.eu.amp.cisco.com

アジア太平洋/日本/中国：api.apjc.amp.cisco.com

ステップ11: SplunkコンソールにAPIクレデンシャルを含めて保存し、それらをAMPにリンクします。



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 'e36c12c3905be05cacb7', and 'API Key' with the value 'a68f433e-baee-f62041c163fb'. Below the API Key field is a green 'Save Configuration' button.

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

ステップ12:[Input]に戻ってイベントストリームを作成します。

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

注：すべてのグループのすべてのイベントをAMPから取得する場合は、[イベントタイプ]フィールドと[グループ]フィールドを空白のままにしてください。

ステップ13：入力が正常に作成されたことを確認します。

Inputs

Name	Index
caistas	main

注：この統合は正式にはサポートされていません

トラブルシューティング

イベントストリームを作成する際に、すべてのフィールドがグレー表示される場合は、次の理由により発生する可能性があります。

The screenshot shows the 'New Input' configuration interface. The 'Name' field is disabled (grayed out) and has a red prohibition sign. The 'Index' field is set to 'main'. The 'Stream Name' field is also disabled. The 'Event Types' and 'Groups' dropdowns are set to 'Leave this field blank to return all Event types' and 'Leave this field blank to return all Groups' respectively. A green 'Save' button is visible at the bottom.

1. 接続性の問題: SplunkインスタンスがAPIホストに接続できることを確認します
2. APIホスト: 手順10で設定したAPIホストが、ビジネスポイントの場所に基づいて、AMP組織と一致していることを確認します。
3. APIクレデンシャル: APIキーとクライアントIDが、ステップ3で設定したものと一致していることを確認します。
4. イベントストリーム: イベントストリームが4つ未満に設定されていることを確認します。