

# Advanced Malware Protection voor endpoints voor integratie met Splunk

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Problemen oplossen](#)

## Inleiding

Dit document beschrijft het integratieproces tussen Advanced Malware Protection (AMP) en Splunk.

Bijgedragen door Uriel Islas en Juventino Macias, bezorgd door Jorge Navarrete, Cisco TAC Engineers.

## Voorwaarden

### Vereisten

Cisco raadt u aan kennis te hebben van:

- Advanced Malware Protection voor endpoints
- Application Programming Interface (API)
- Splunk
- Beheergebruiker op Splunk

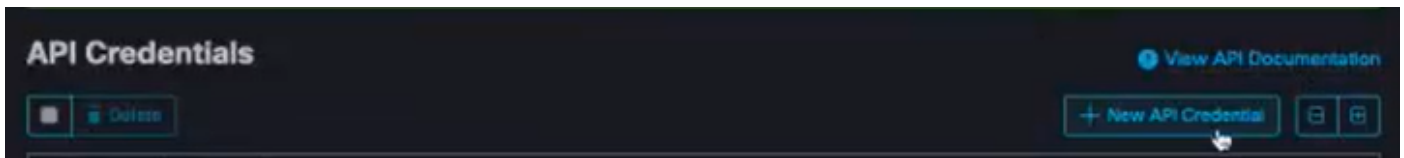
### Gebruikte componenten

- AMP openbare cloud
- Splunk-exemplaar

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

## Configureren

Stap 1. Navigeer naar AMP-console (<https://console.amp.cisco.com>) en navigeer naar **Account>API-Credentials**, waar u eventstromen kunt maken.

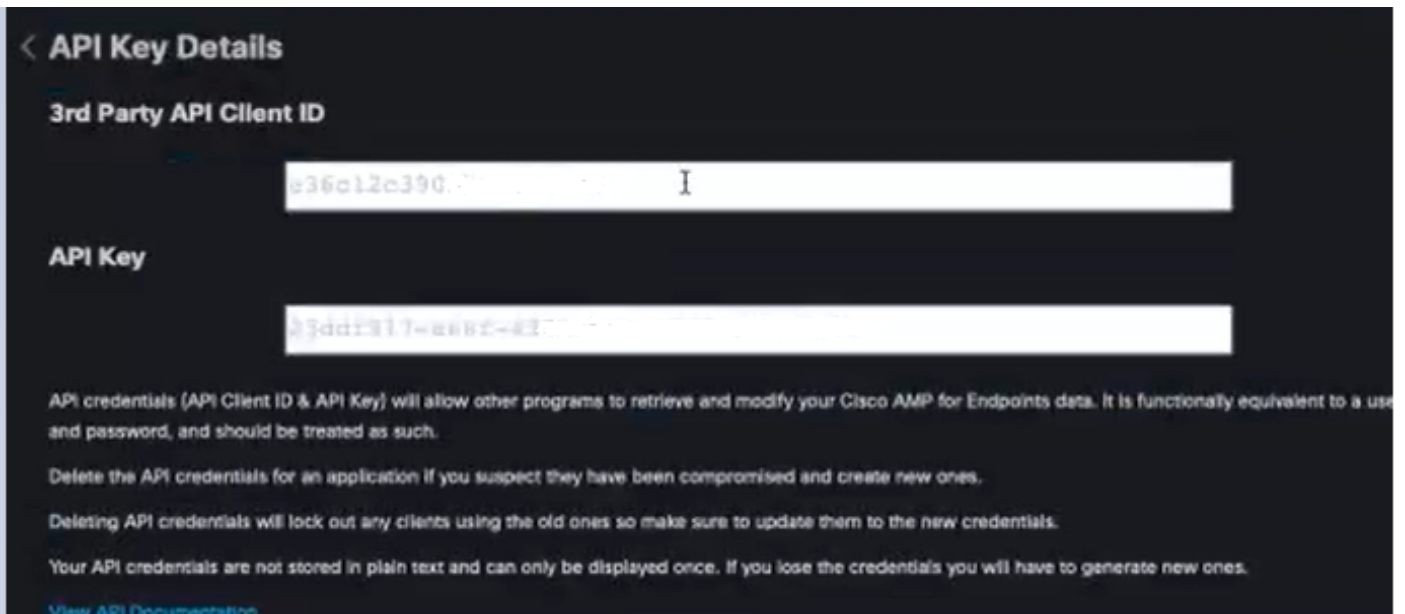


Stap 2. Voor deze integratie markeert u het selectieteken **Lezen en schrijven** zoals hieronder wordt getoond:



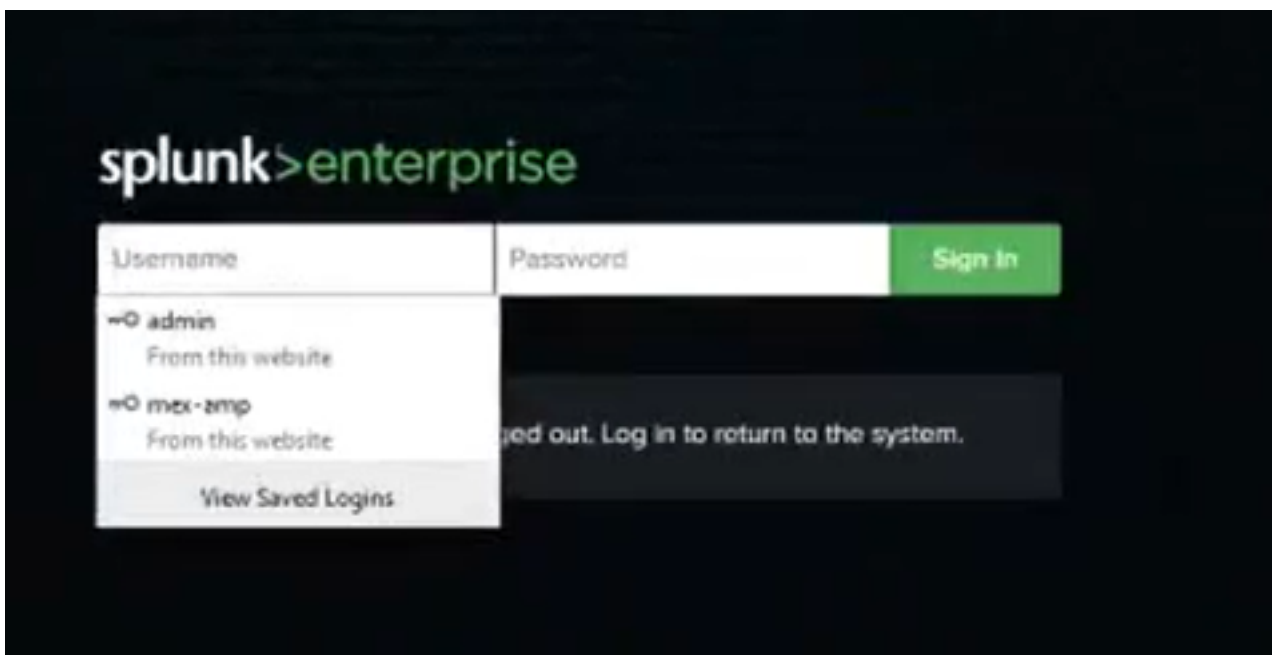
Opmerking: Als u meer informatie over de gebeurtenissen wilt verzamelen, controleert u het vakje **Opdracht inschakelen**, om de Audit Logs te krijgen van de Bestandsopslag van het Bestand te controleren controleer de **API toegang tot het vakje Bestandsopslag toestaan**.

Stap 3. Zodra u de eventstream maakt, wordt de API-client-ID en -API-toets weergegeven die op Splunk vereist is.

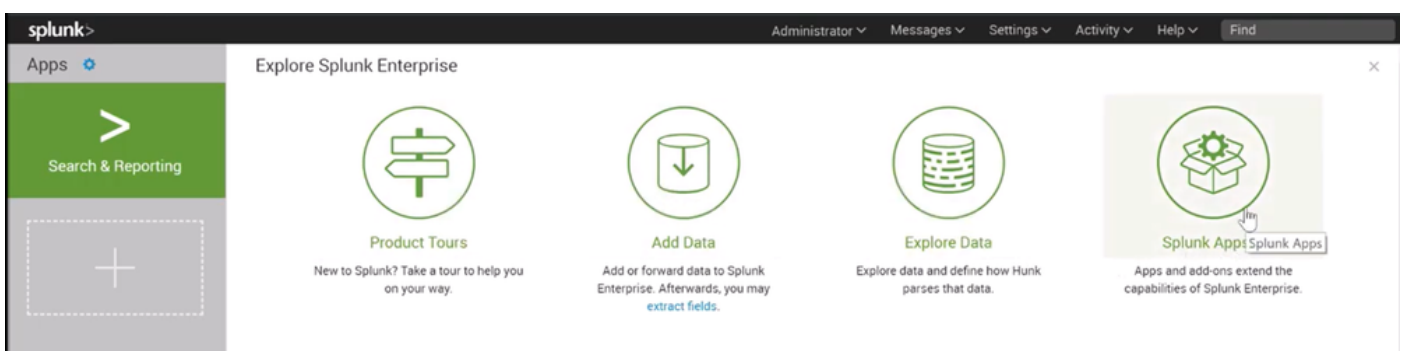


**Waarschuwing:** deze informatie kan op geen enkele manier worden hersteld, in geval van verlies moet een nieuwe API-toets worden gemaakt.

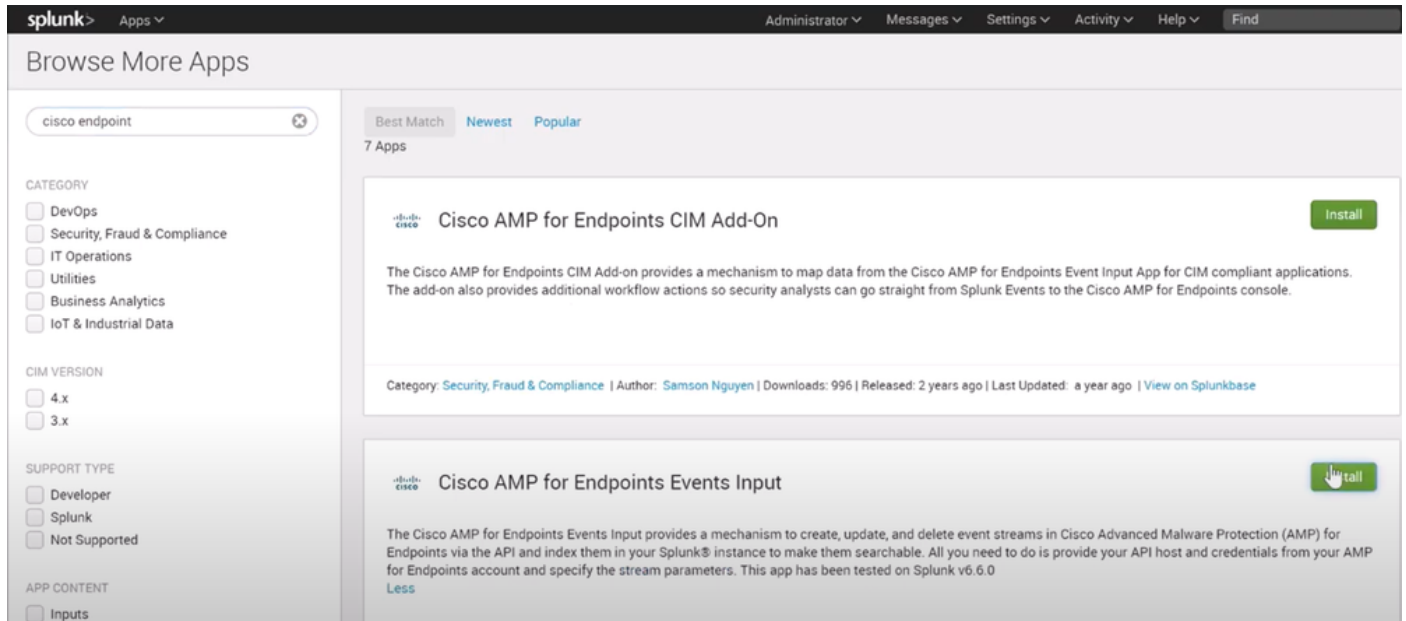
Stap 4. Zorg ervoor dat de account **Admin** op Splunk is geplaatst om Splunk te integreren met de Advanced Malware Protection.



Stap 5. Nadat u op Splunk hebt aangemeld, kunt u AMP downloaden via Splunk Apps.



Stap 6. Zoek naar Cisco Endpoint in de App-browser en installeer het (Cisco Advanced Malware Protection voor Endpoints).



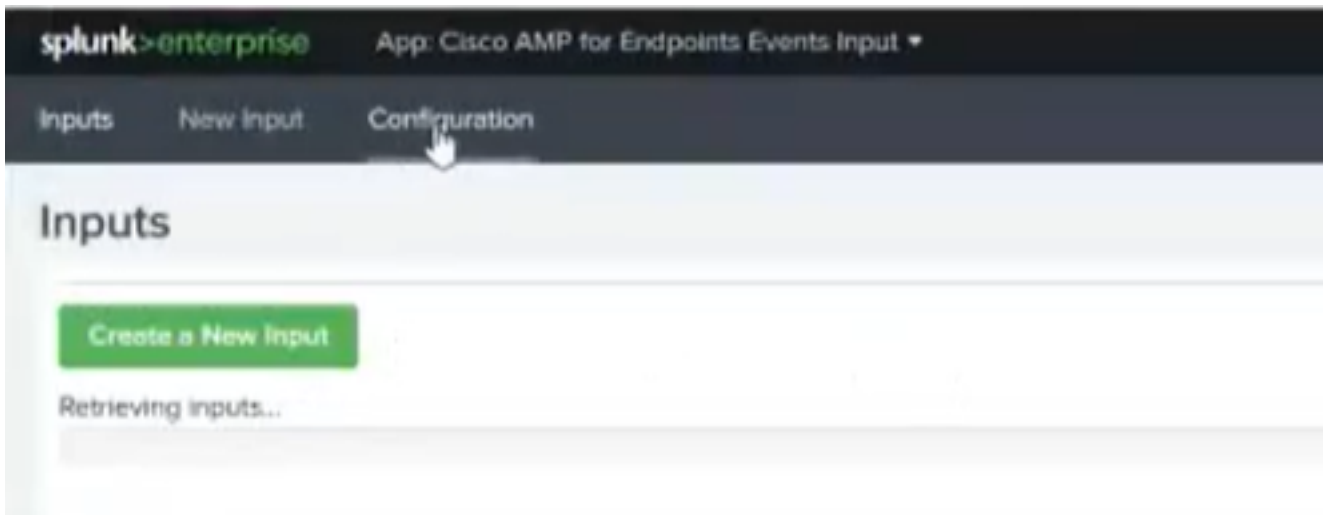
Stap 7. U moet de sessie opnieuw starten om de installatie op Splunk te voltooien.



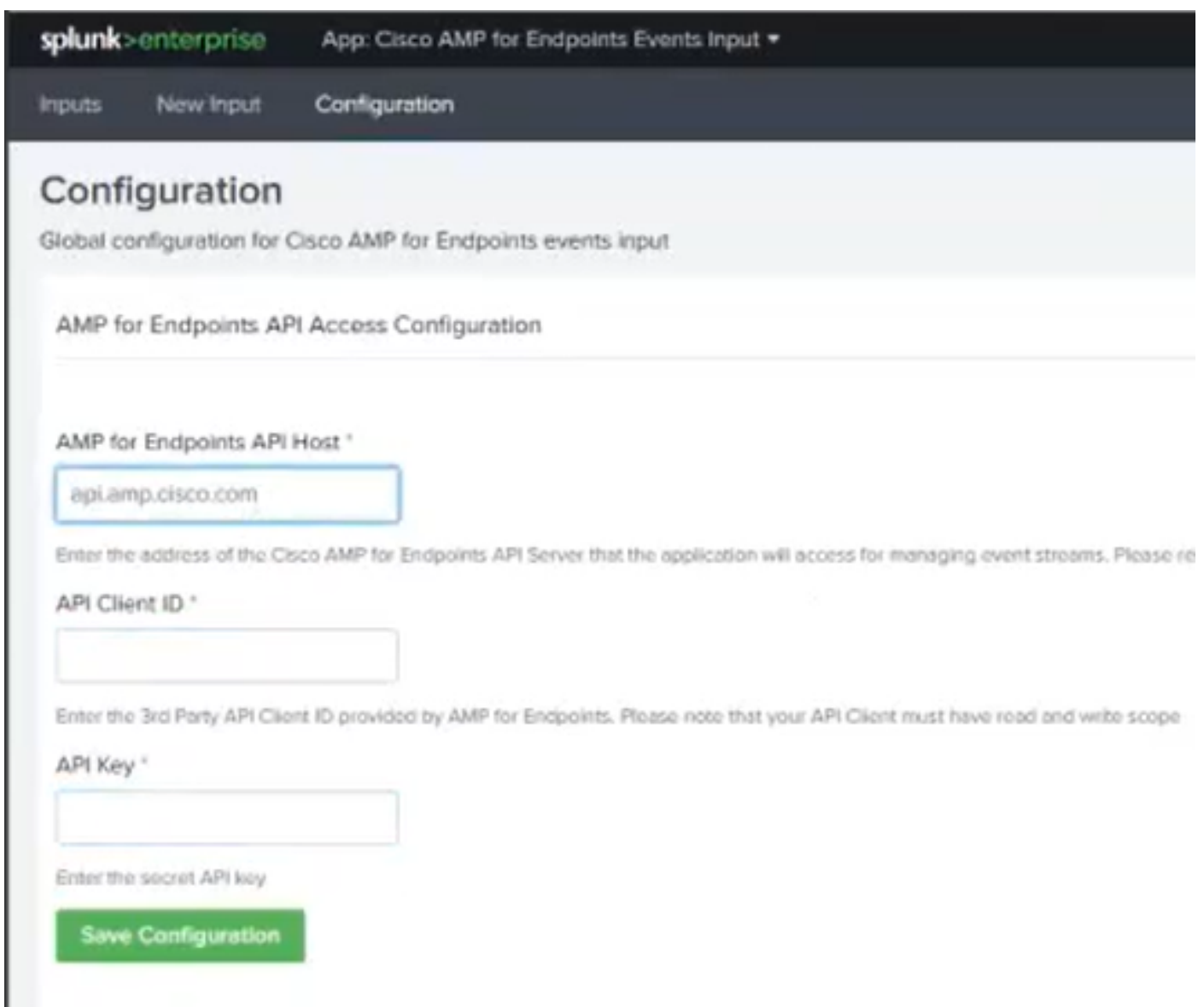
Stap 8. Zodra u bij Splunk hebt ingelogd, klikt u op **Cisco Advanced Malware Protection voor endpoints** aan de linkerkant van het scherm.



Stap 9. Klik op het label **Configuration** boven in het scherm.



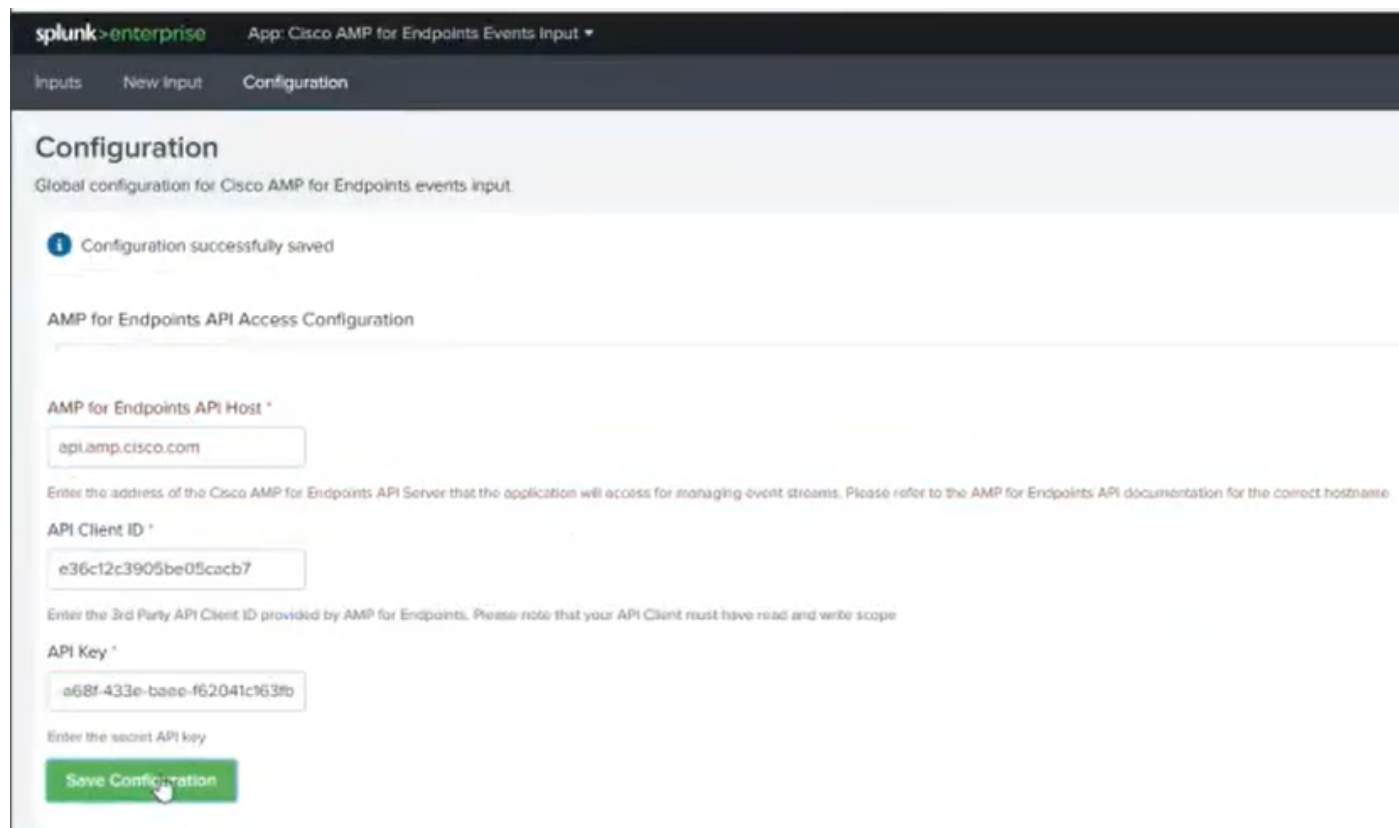
Stap 10. Typ uw API-referenties die eerder uit de AMP-console zijn gegenereerd.



Opmerking: De API Host spot kan verschillend zijn gebaseerd op het Cloud Data Center dat uw organisatie op:

- Noord-Amerika: `api.amp.cisco.com`
- Europa: `api.eu.am.p.cisco.com`
- APJC: `api.apjc.amp.cisco.com`

Stap 1. Voeg API-referenties toe en bewaar deze op de Splunk-console om ze met AMP te verbinden.



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 note: 'Enter the secret API key'. At the bottom, there 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

Stap 12. Ga terug naar **Input** om uw eventstream te creëren.

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

Opmerking: Als u alle gebeurtenissen voor alle groepen wilt opvragen bij AMP, laat u **Event Typen** en **Groepen** velden leeg.

Stap 13. Zorg ervoor dat uw invoer met succes is gemaakt.

## Inputs

| Name    | Index |
|---------|-------|
| caislas | main  |

Opmerking: Houdt u er rekening mee dat deze integratie niet officieel wordt ondersteund

# Problemen oplossen

Als u een eventstream maakt, worden alle velden uit gegraveerd, maar om een of andere van de onderstaande redenen:

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 a dropdown menu showing 'main', a question 'In which index would you like the events to appear?', 'Stream Settings' with a horizontal line, 'Stream Name \*' with an empty text box, 'Event Types' with a dropdown menu showing 'Leave this field blank to return all Event types', 'Groups' with a dropdown menu showing 'Leave this field blank to return all Groups', and a green 'Save' button at the bottom left.

1. Connectiviteitsproblemen: Zorg ervoor dat de instantie Splunk contact kan opnemen met de API-host
2. API-host: Zorg ervoor dat de API host die op stap 10 is ingesteld, overeenkomt met uw AMP-organisatie, gebaseerd op de locatie van uw bedrijf bij.
3. API-referenties: Zorg ervoor dat de API-toets en client-ID overeenkomen met die welke bij stap 3 zijn geconfigureerd.
4. Event Streams: Zorg ervoor dat u minder dan 4 eventstromen hebt geconfigureerd.