AMP für Endgeräte-Integration in Splunk

Inhalt

Einführung

Dieses Dokument beschreibt den Integrationsprozess zwischen Advanced Malware Protection (AMP) und Splunk.

Unterstützt von Uriel Islas und Juventino Macias, herausgegeben von Jorge Navarrete, Cisco TAC Engineers.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- AMP für Endgeräte
- API (Application Programming Interface)
- Splash
- Admin-Benutzer auf Splunk

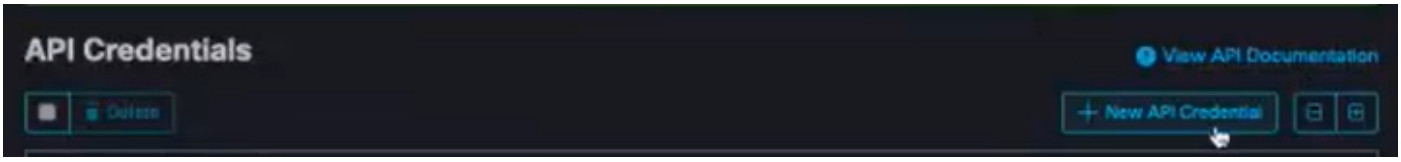
Verwendete Komponenten

- AMP Public Cloud
- Splunk-Instanz

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

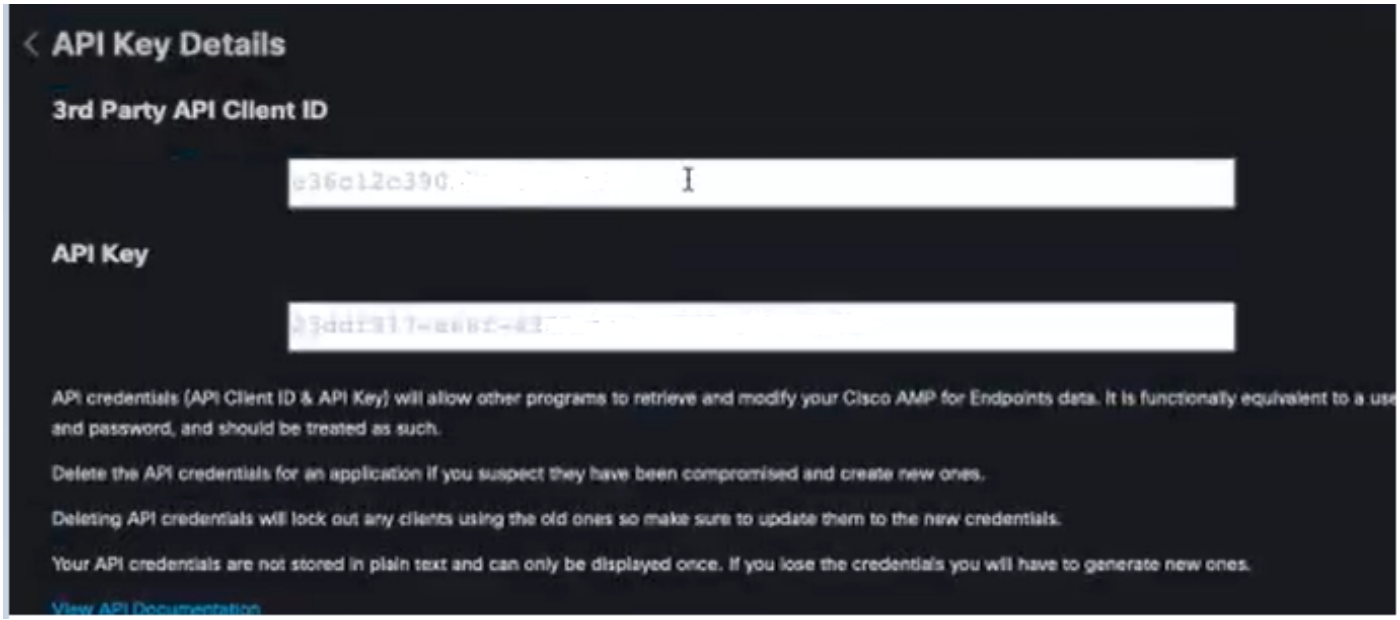
Schritt 1: Navigieren Sie zur AMP-Konsole (https://console.amp.cisco.com), und navigieren Sie zu **Accounts>API Credentials**, wo Sie Ereignisstreams erstellen können.



Schritt 2: Markieren Sie zum Durchführen dieser Integration das Kontrollkästchen **Lesen und Schreiben** wie unten gezeigt:

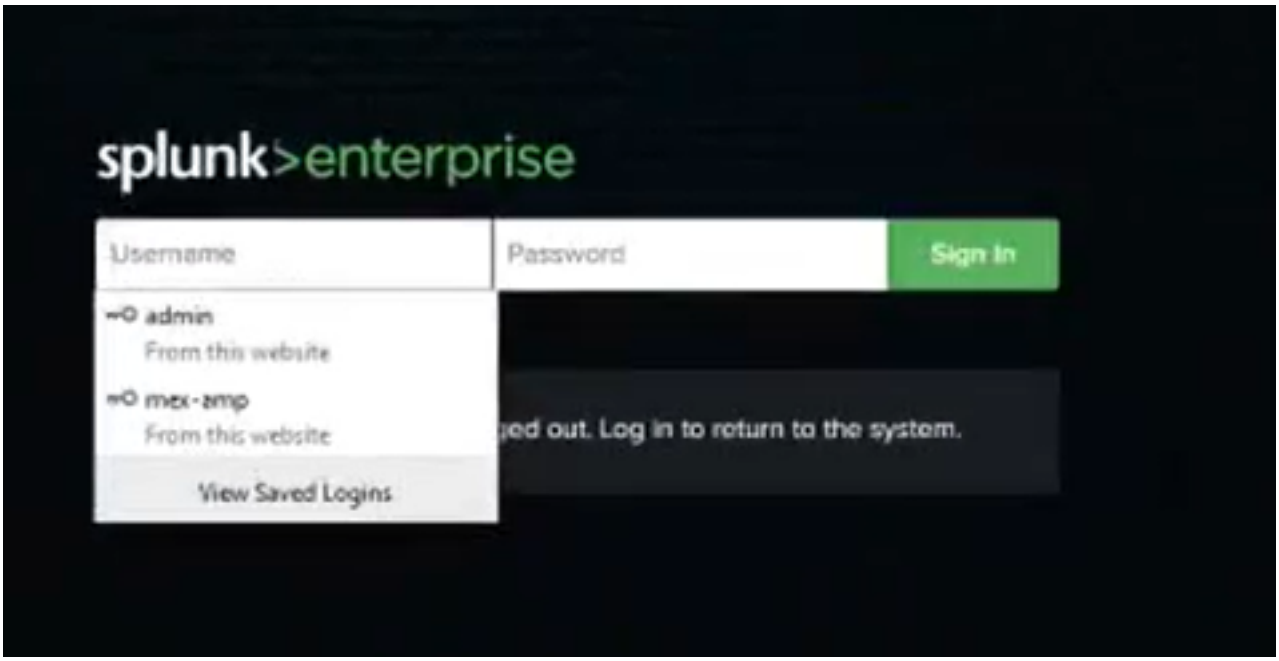
> **Hinweis**: Wenn Sie weitere Informationen zu den Ereignissen sammeln möchten, aktivieren Sie das Kontrollkästchen **Enable Command Line** (Befehlszeile aktivieren), um die im File Repository generierten Audit Logs (Audit-Protokolle) zu erhalten. Aktivieren Sie das Kontrollkästchen **Allow API access to File Repository (API-Zugriff auf Dateispeicher zulassen)**.

Schritt 3: Nach dem Erstellen des Ereignisstreams werden die API-Client-ID und der API-Schlüssel angezeigt, die für Splunk erforderlich sind.

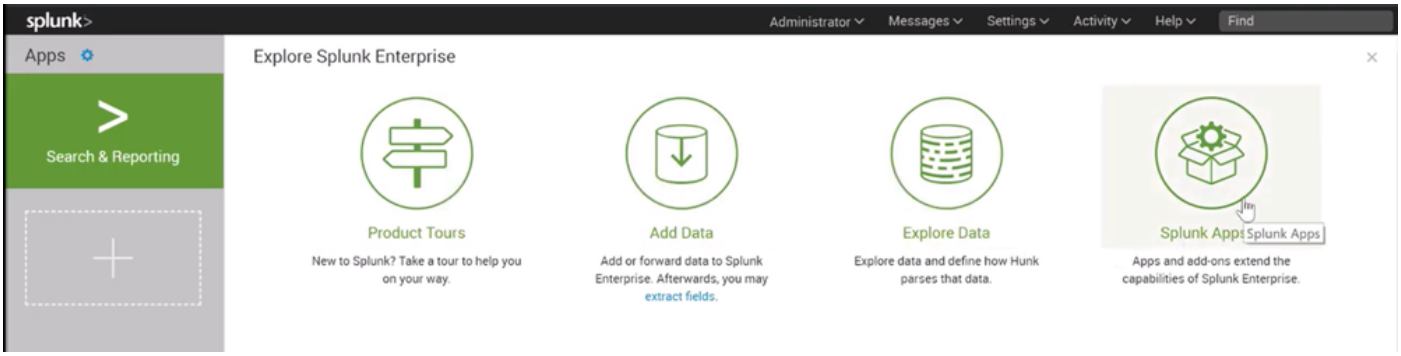


Vorsicht: Diese Informationen können auf keinen Fall wiederhergestellt werden, im Falle eines Verlusts muss ein neuer API-Schlüssel erstellt werden.

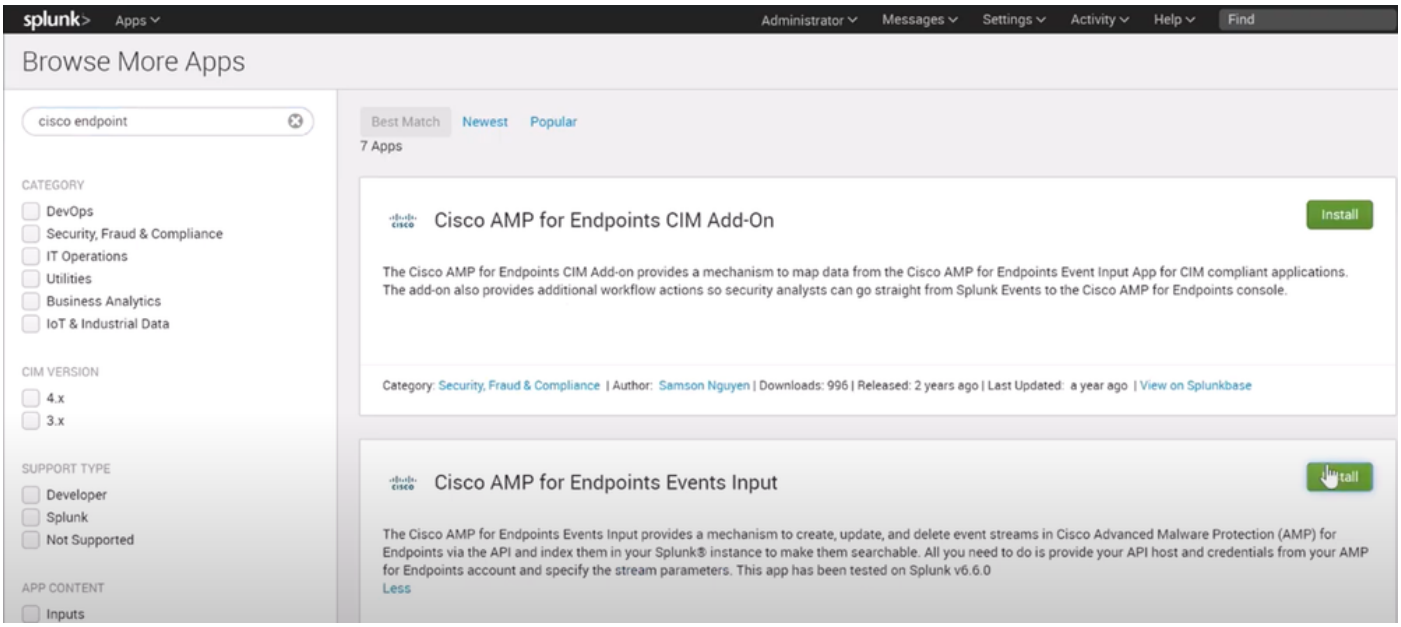
Schritt 4: Um Splunk in AMP für Endgeräte zu integrieren, stellen Sie sicher, dass das Konto **Admin** auf Splunk vorhanden ist.



Schritt 5: Sobald Sie sich bei Splunk angemeldet haben, können Sie AMP von Splunk Apps herunterladen.

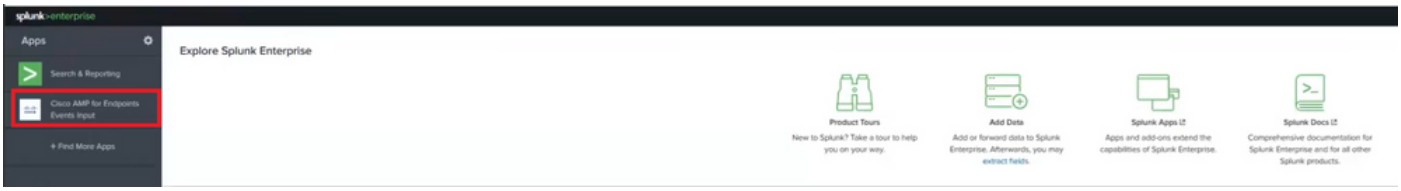


Schritt 6: Suchen Sie im App-Browser nach Cisco Endpoint, und installieren Sie ihn (Eingabe von Cisco AMP für Endgeräte-Ereignissen).

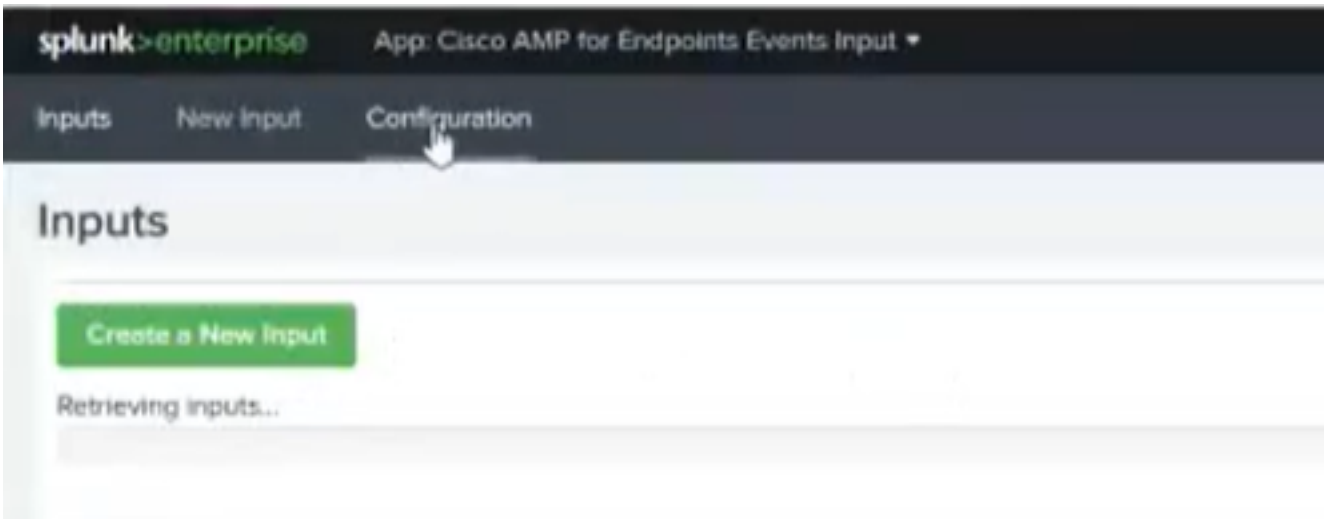


Schritt 7: Um die Installation auf Splunk abzuschließen, ist ein Neustart der Sitzung erforderlich.

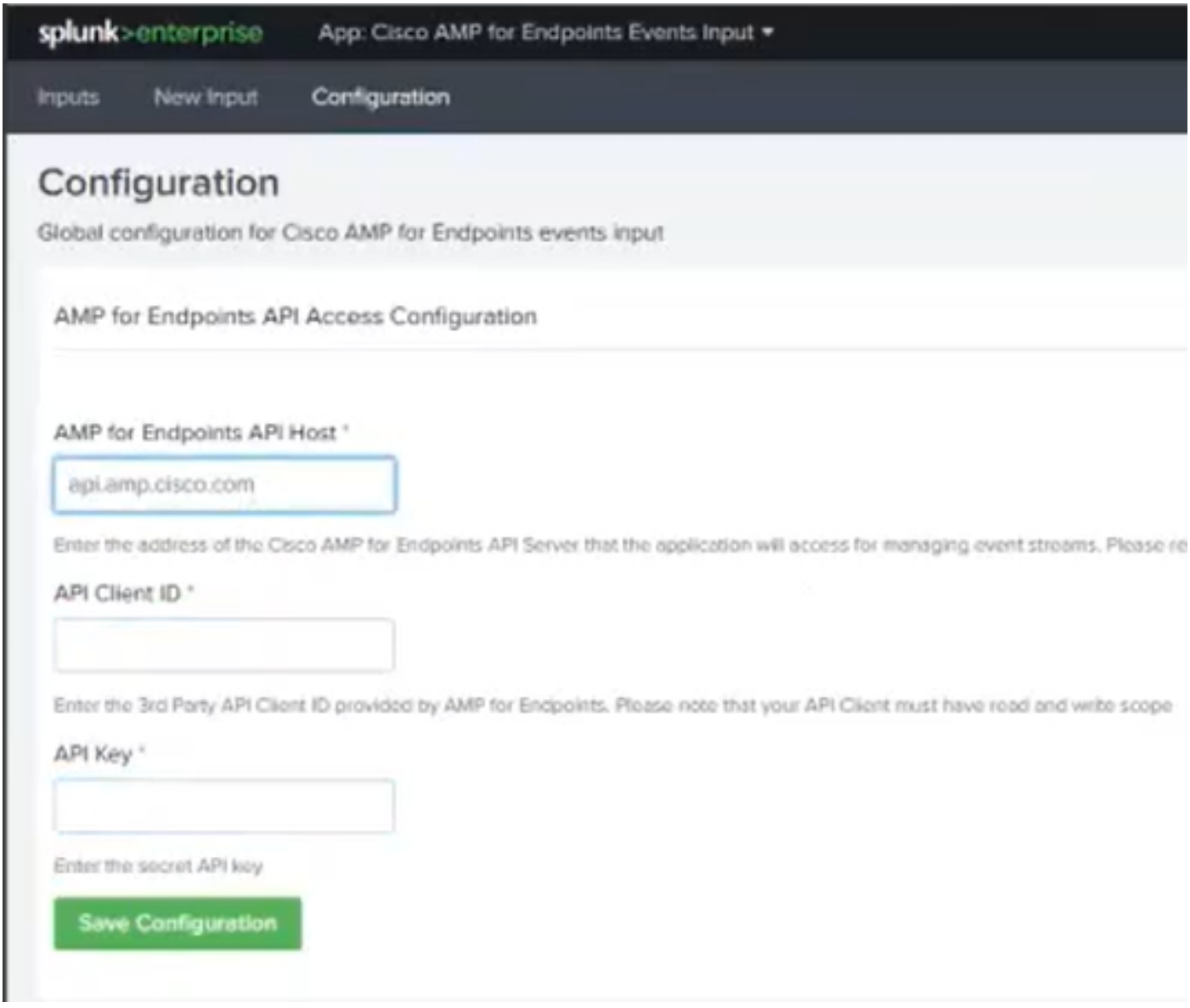
Schritt 8: Wenn Sie sich unter Splunk angemeldet haben, klicken Sie links im Bildschirm auf **Cisco AMP für Endgeräte**.



Schritt 9: Klicken Sie oben im Bildschirm auf die Bezeichnung **Konfiguration**.



Schritt 10: Geben Sie Ihre API-Anmeldeinformationen ein, die zuvor über die AMP-Konsole generiert wurden.

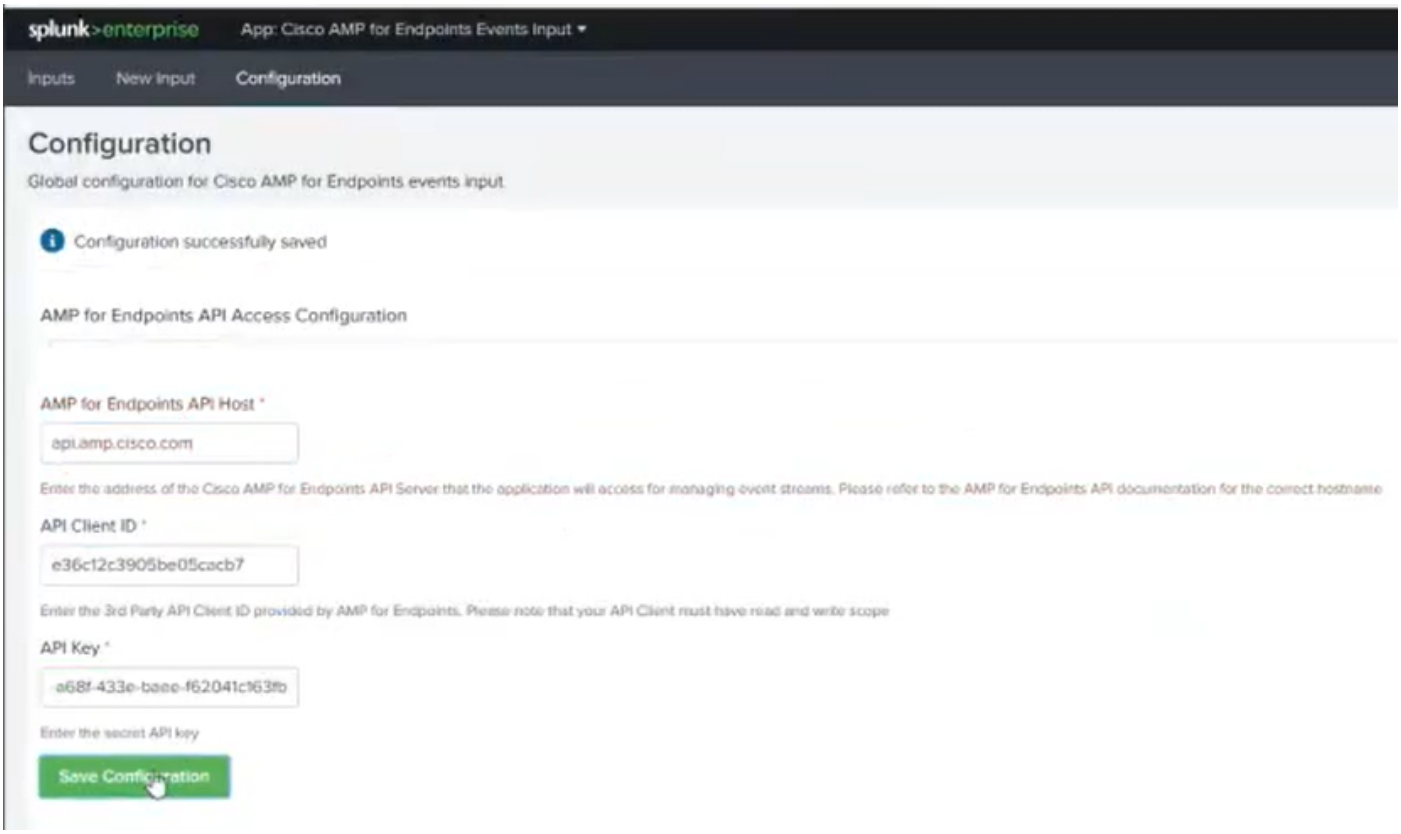


Hinweis: Der API-Host-Spot kann je nach dem Cloud-Rechenzentrum, das Ihr Unternehmen anzeigt, unterschiedlich sein:

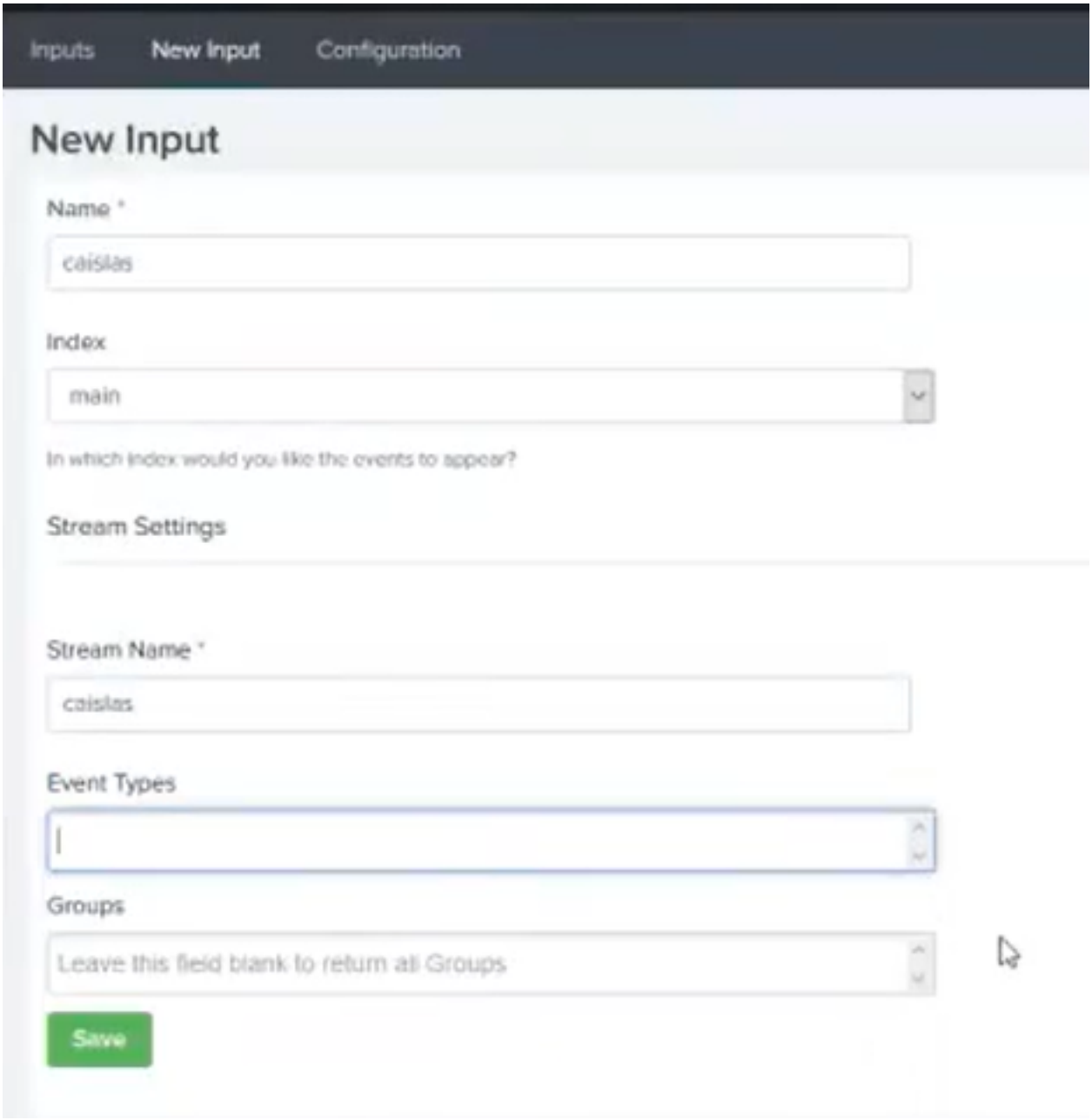
Nordamerika: api.amp.cisco.com
Europa: api.eu.am

APJC: api.apjc.amp.cisco.com

Schritt 11: Integrieren und speichern Sie API-Anmeldeinformationen in der Splunk-Konsole, um diese mit AMP zu verknüpfen.

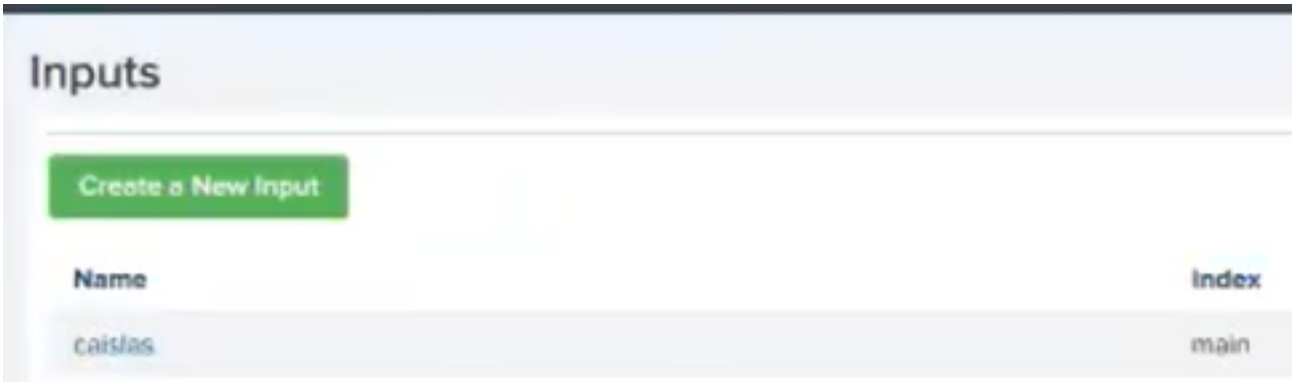


Schritt 12: Wechseln Sie zurück zu **Eingabe**, um den Ereignisstream zu erstellen.



Hinweis: Wenn Sie alle Ereignisse für alle Gruppen aus AMP abrufen möchten, lassen Sie die Felder **Ereignistypen** und **Gruppen** leer.

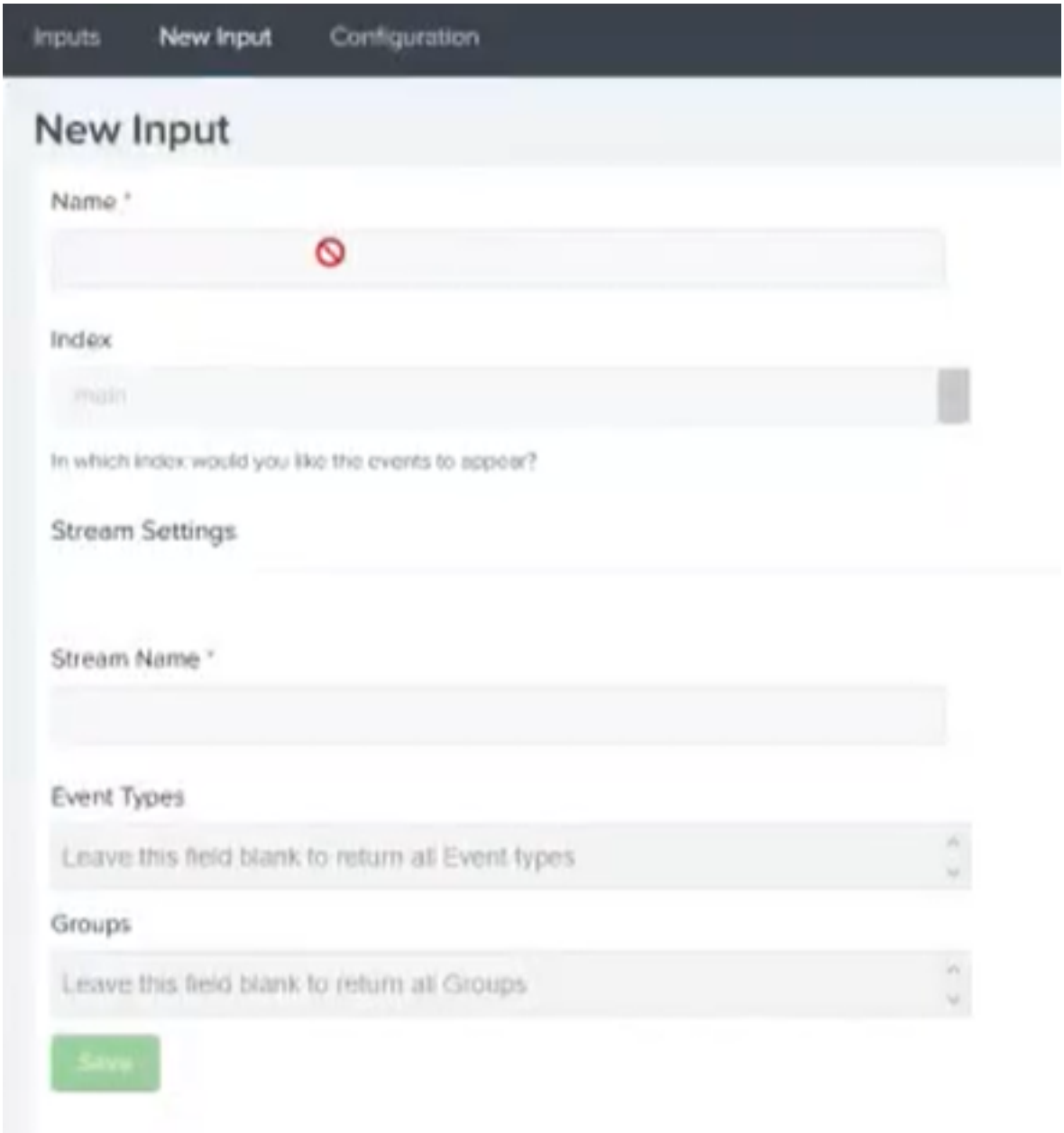
Schritt 13: Stellen Sie sicher, dass Ihre Eingabe erfolgreich erstellt wurde.



Hinweis: Bitte beachten Sie, dass diese Integration nicht offiziell unterstützt wird.

Fehlerbehebung

Wenn beim Erstellen eines Ereignisstreams alle Felder ausgegraut sind, kann dies aus den folgenden Gründen geschehen:



1. Verbindungsprobleme: Stellen Sie sicher, dass die Splunk-Instanz den API-Host kontaktieren kann.
2. API-Host: Stellen Sie sicher, dass der in Schritt 10 konfigurierte API-Host mit Ihrer AMP-Organisation übereinstimmt, je nachdem, wo sich Ihr Unternehmen befindet.
3. API-Anmeldeinformationen: Stellen Sie sicher, dass der API-Schlüssel und die Client-ID mit den in Schritt 3 konfigurierten übereinstimmen.
4. Event-Streams: Stellen Sie sicher, dass weniger als vier Ereignisstreams konfiguriert sind.