Integrazione di AMP for Endpoints con Splunk

Sommario

Introduzione

In questo documento viene descritto il processo di integrazione tra Advanced Malware Protection (AMP) e Splunk.

Contributo di Uriel Islas e Juventino Macias, a cura di Jorge Navarrete, Cisco TAC Engineers.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di:

- AMP for Endpoints
- API (Application Programming Interface)
- Splunk
- Utente amministratore su Splunk

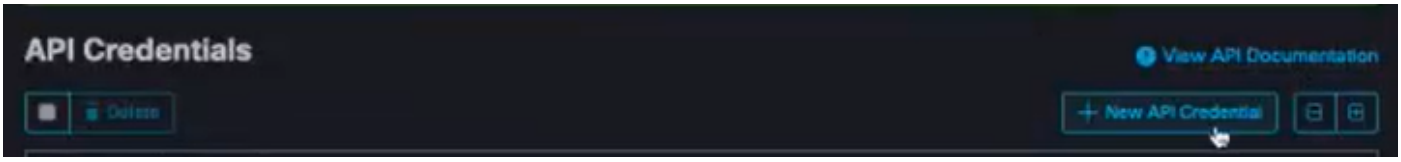
Componenti usati

- AMP Public Cloud
- Istanza Splunk

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

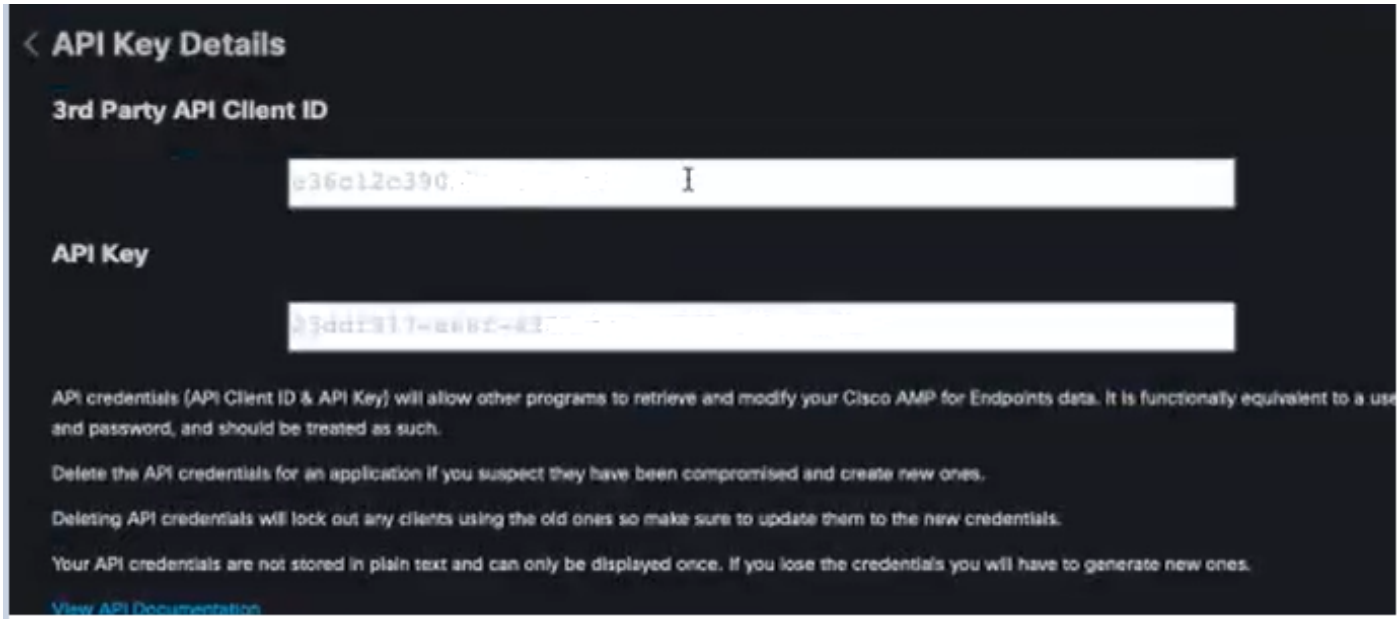
Passaggio 1. Passare alla console AMP (https://console.amp.cisco.com) e selezionare **Account>Credenziali API**, dove è possibile creare flussi di eventi.



Passaggio 2. Per eseguire questa integrazione, selezionare la casella di controllo **Lettura e scrittura** come mostrato di seguito:

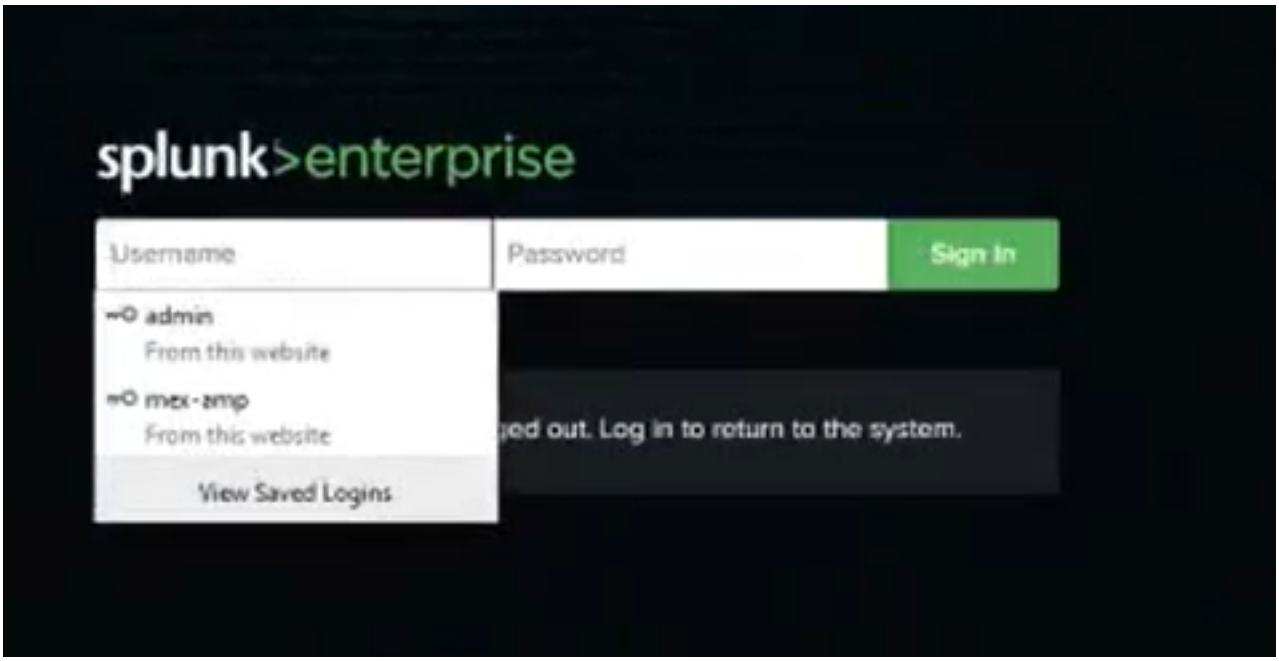
> **Nota:** Se si desidera raccogliere ulteriori informazioni sugli eventi, selezionare la casella **Abilita riga di comando** per ottenere i log di controllo generati dal repository dei file selezionare la casella **Consenti accesso API al repository dei file**.

Passaggio 3. Una volta creato il flusso di eventi, vengono visualizzati l'ID client e la chiave API richiesti in Splunk.

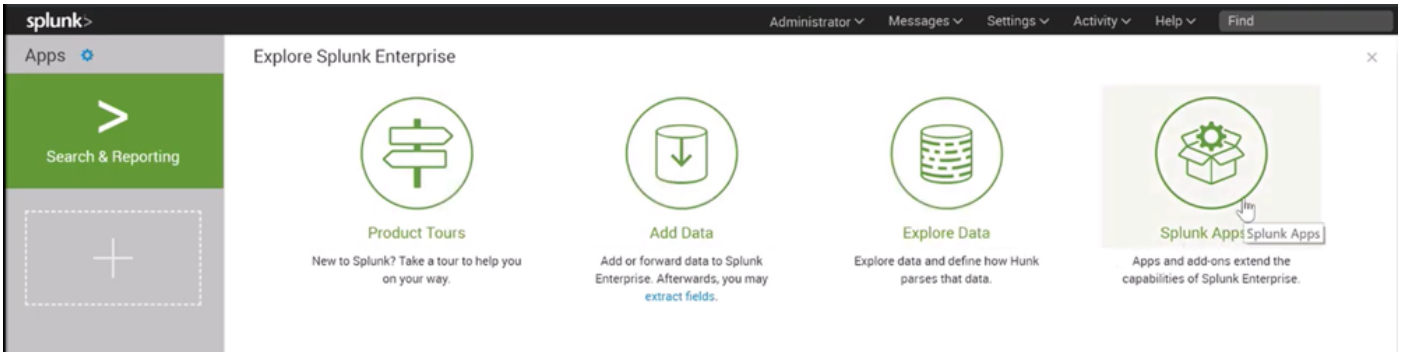


Attenzione: queste informazioni non possono essere recuperate in alcun modo. In caso di perdita, è necessario creare una nuova chiave API.

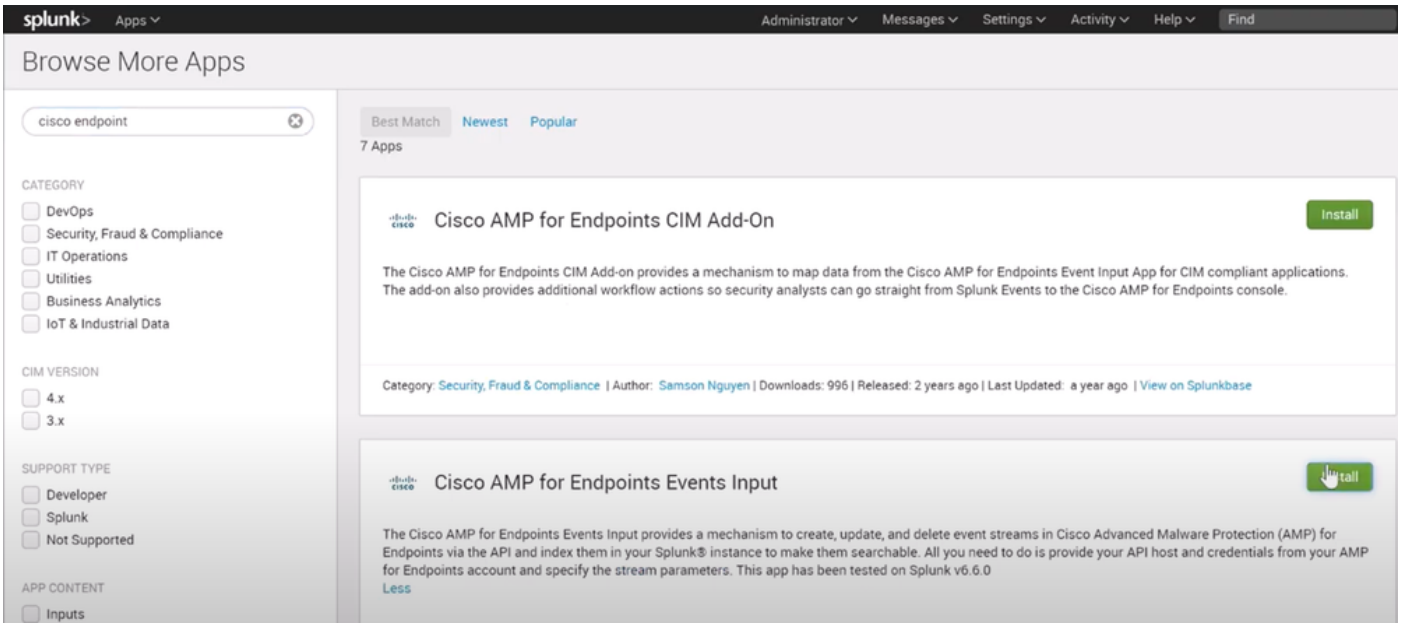
Passaggio 4. Per integrare Splunk con AMP for endpoints, verificare che l'account **Admin** esista in Splunk.



Passaggio 5. Dopo aver eseguito l'accesso a Splunk, procedere al download di AMP da Splunk Apps.

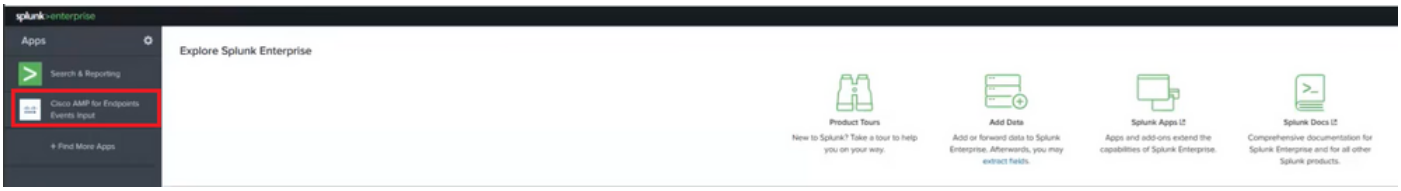


Passaggio 6. Cercare Cisco Endpoint nel browser dell'app e installarlo (Cisco AMP for Endpoints Events Input).

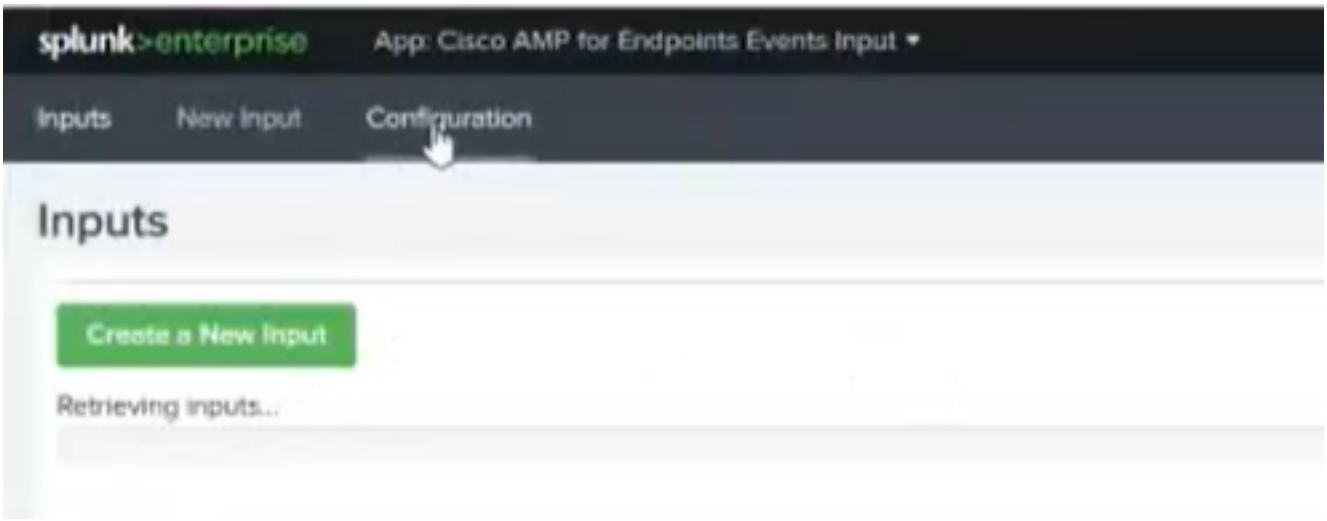


Passaggio 7. Per completare l'installazione su Splunk, è necessario riavviare la sessione.

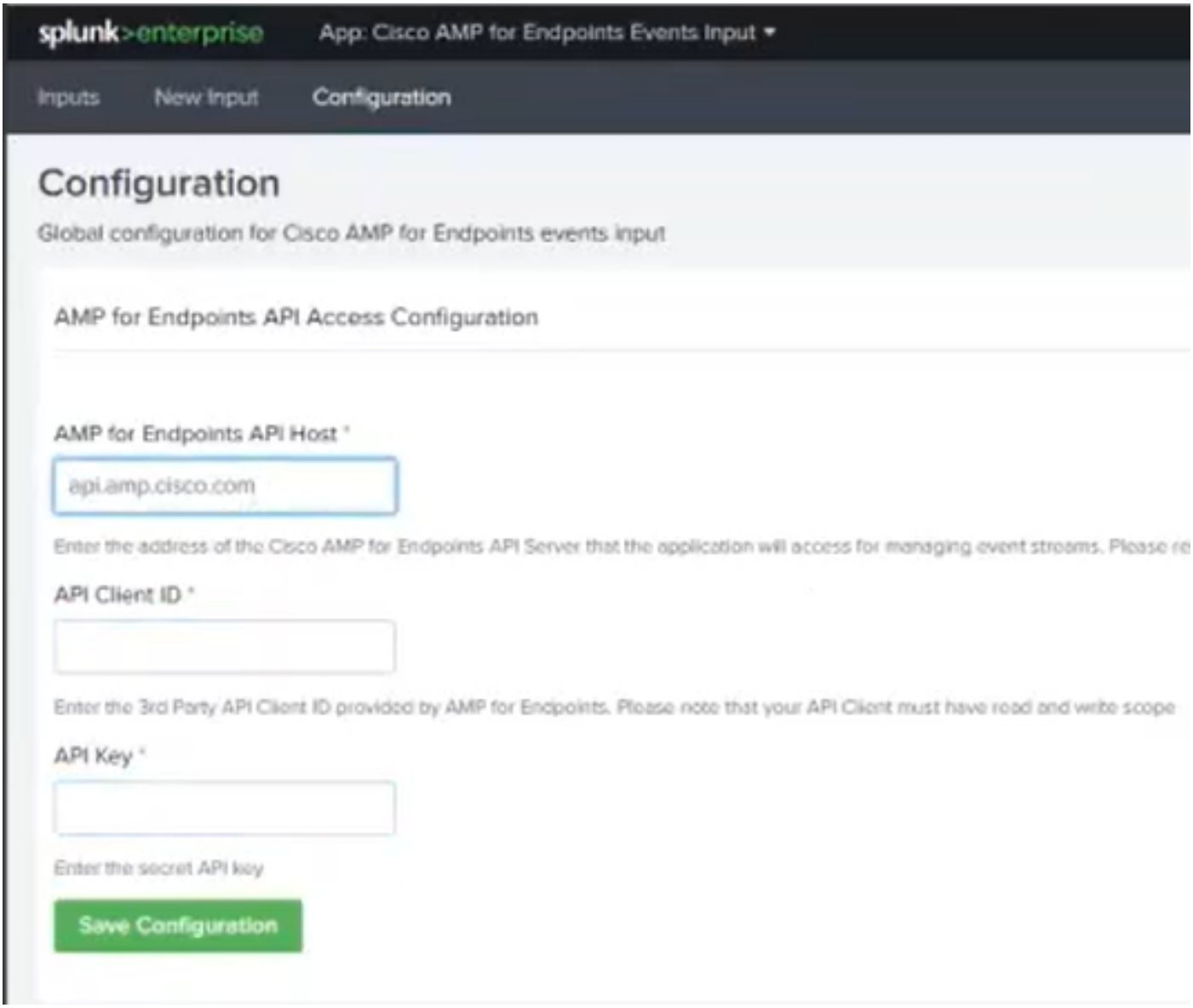
Passaggio 8. Dopo aver effettuato l'accesso in Splunk, fare clic su **Cisco AMP For Endpoints** sul lato sinistro della schermata.



Passaggio 9. Fare clic sull'etichetta **Configuration** nella parte superiore dello schermo.



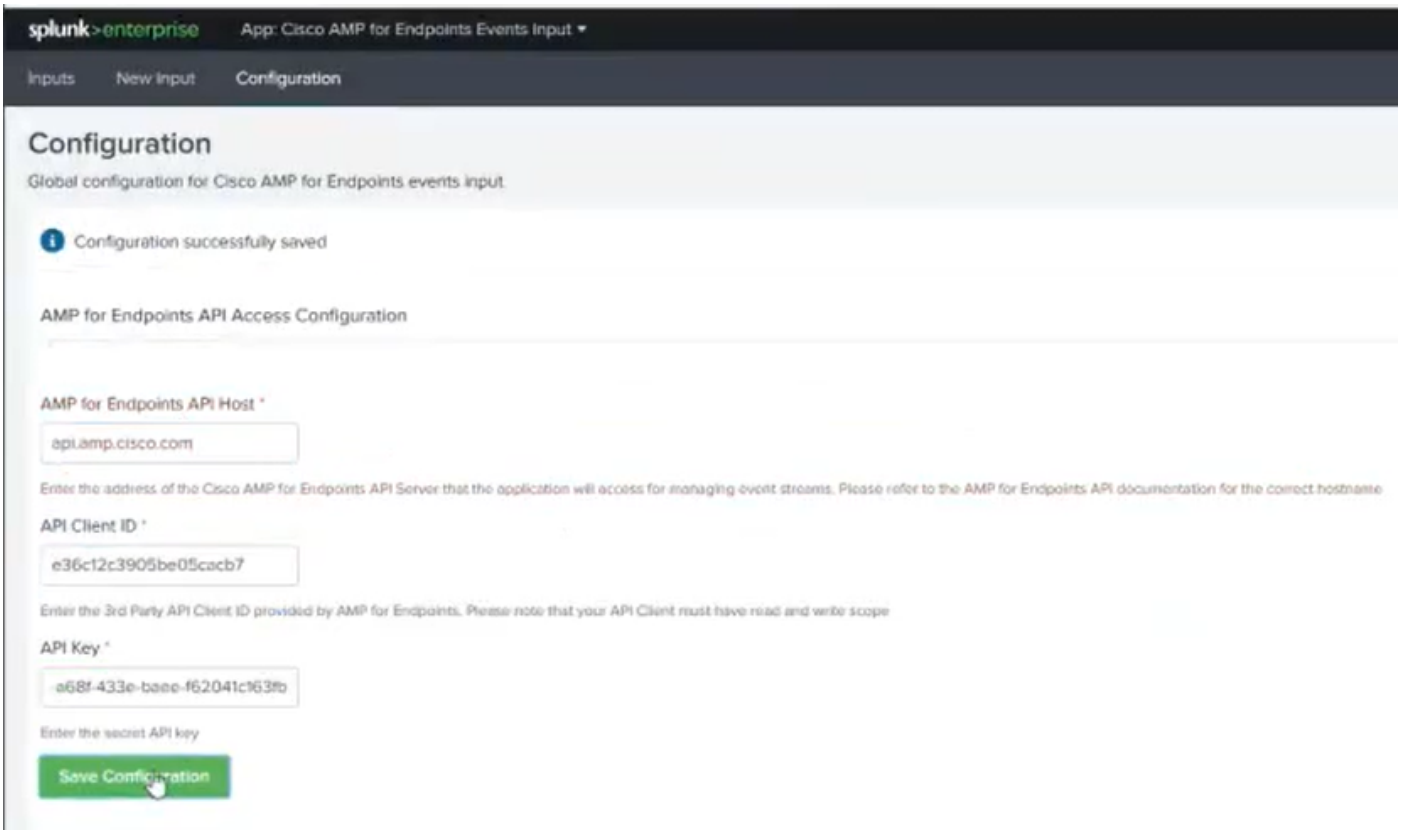
Passaggio 10. Digitare le credenziali API generate in precedenza dalla console AMP.



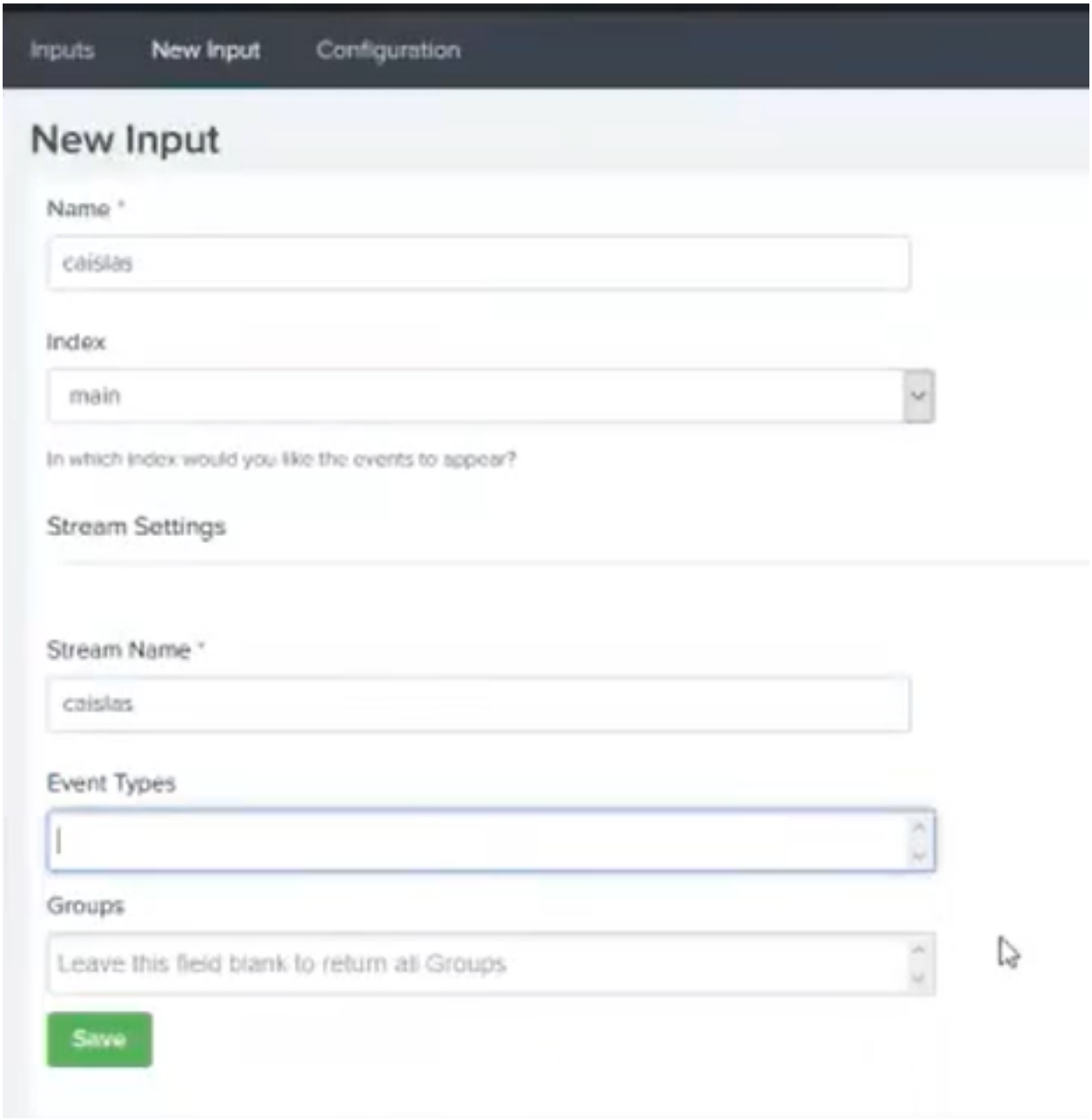
Nota: L'area API Host potrebbe essere diversa in base al centro dati cloud a cui punta l'organizzazione:

- Nord America: api.amp.cisco.com
- Europa: api.eu.amp.cisco.com
- APJC: api.apjc.amp.cisco.com

Passaggio 11. Includere e salvare le credenziali API nella console Splunk per collegarle ad AMP.

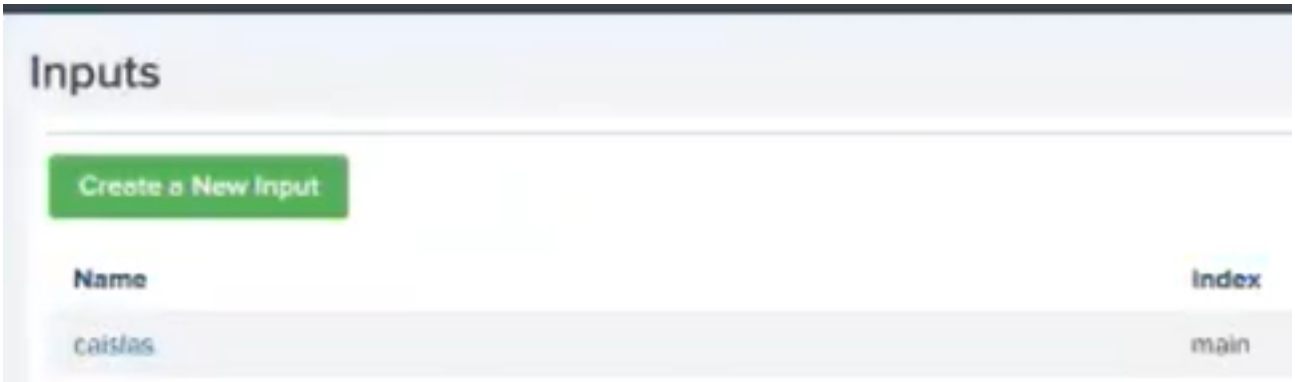


Passaggio 12. Tornare a **Input** per creare il flusso di eventi.



Nota: Se si desidera ottenere tutti gli eventi per tutti i gruppi da AMP, lasciare vuoti i campi **Tipi di evento** e **Gruppi**.

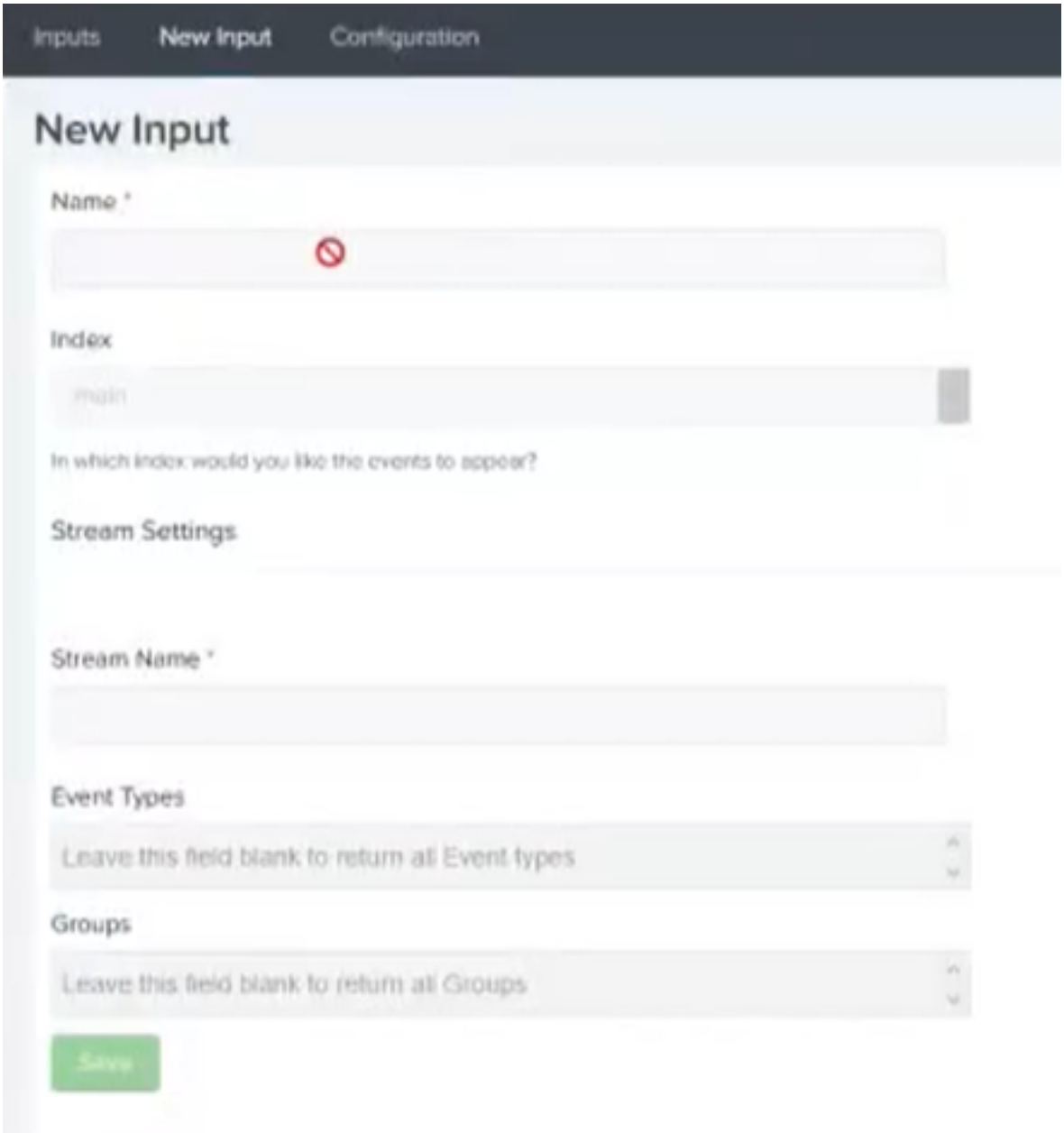
Passaggio 13. Verificare che l'input sia stato creato correttamente.



Nota: Questa integrazione non è ufficialmente supportata

Risoluzione dei problemi

Se durante la creazione di un flusso di eventi tutti i campi sono disattivati, ciò potrebbe essere dovuto ad alcuni dei motivi seguenti:



1. Problemi di connettività: Verificare che l'istanza Splunk sia in grado di contattare l'host API
2. Host API: Verificare che l'host API configurato nel passaggio 10 corrisponda all'organizzazione AMP, in base al punto di riferimento dell'azienda.
3. Credenziali API: Verificare che la chiave API e l'ID client corrispondano a quelli configurati nel passaggio 3.
4. Flussi di eventi: Verificare che siano configurati meno di 4 flussi di eventi.