

# Integrazione di AMP for Endpoints con Splunk

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Risoluzione dei problemi](#)

## 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

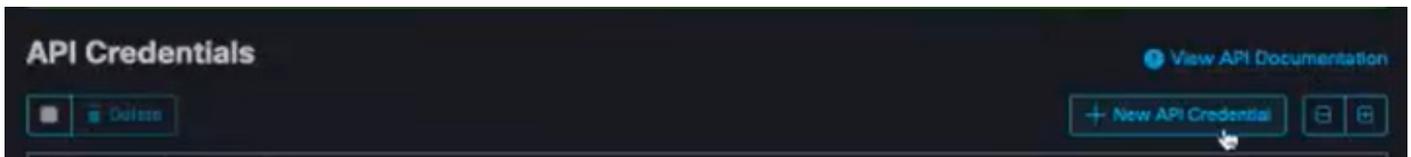
### Componenti usati

- 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.

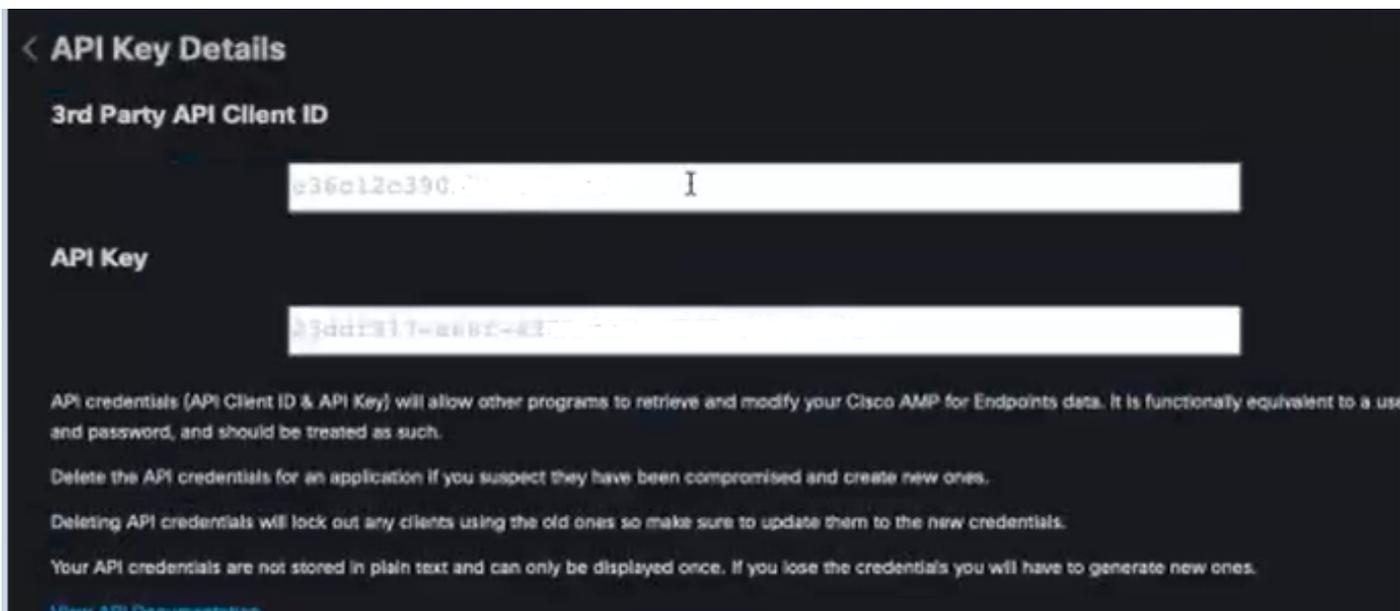


Passaggio 2. Per eseguire questa integrazione, selezionare la casella di controllo **Letture e scrittura** come mostrato di seguito:



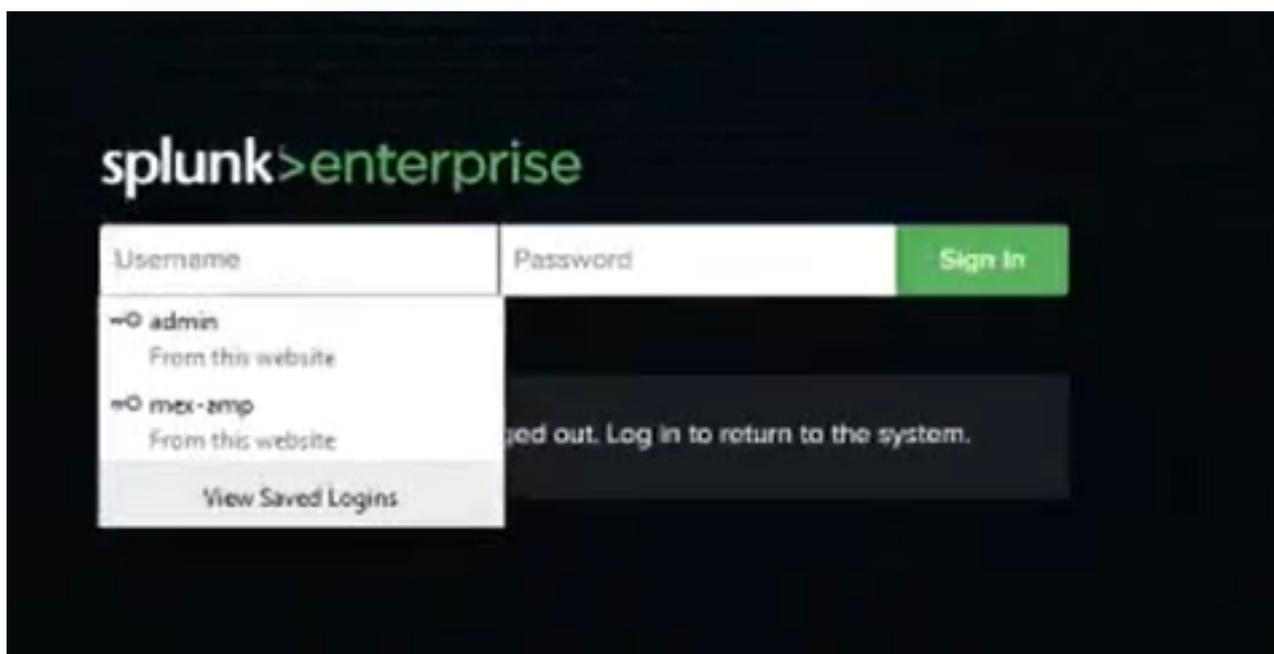
**Nota:** Se si desidera raccogliere ulteriori informazioni sugli eventi, selezionare la casella **Abilita riga di comando** per ottenere i log di controllo generati dal repository dei file selezionare la casella **Consenti accesso API al repository dei file**.

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

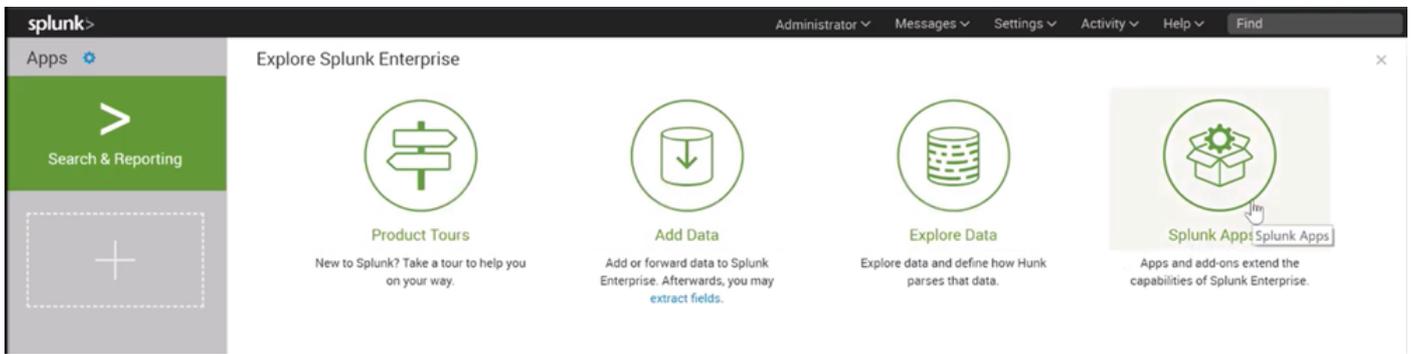


**Attenzione:** queste informazioni non possono essere recuperate in alcun modo. In caso di perdita, è necessario creare una nuova chiave API.

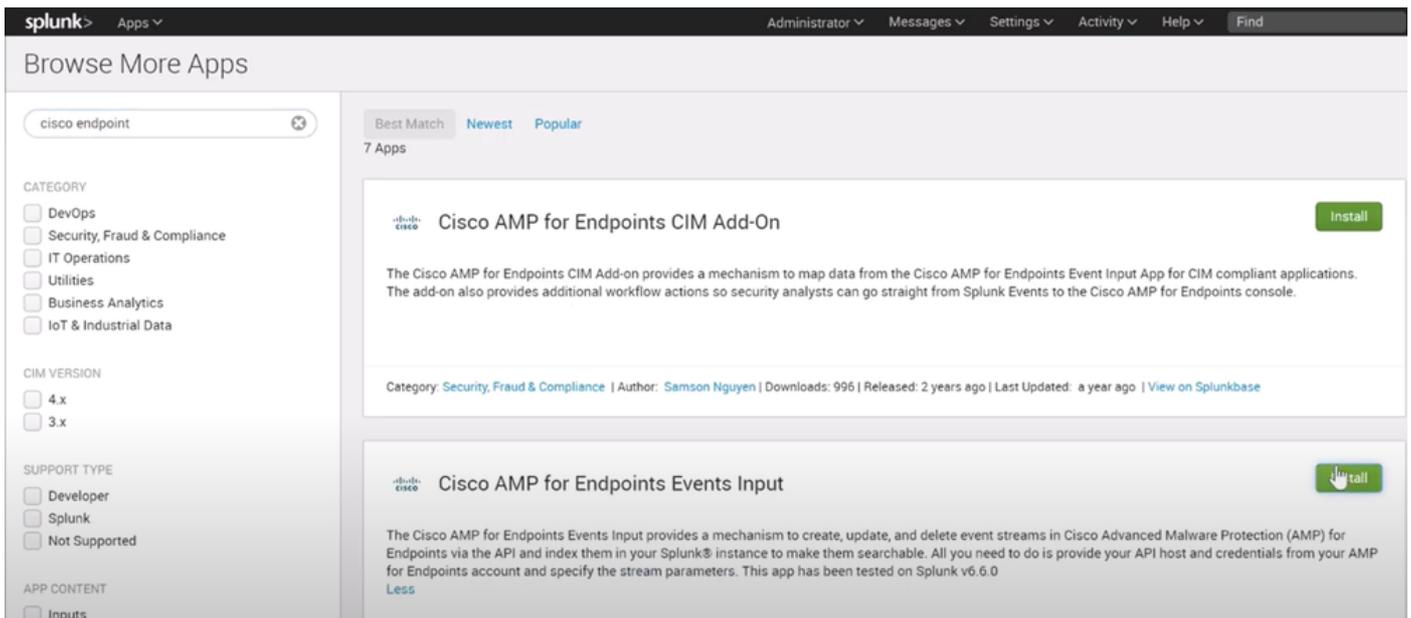
Passaggio 4. Per integrare Splunk con AMP for endpoints, verificare che l'account **Admin** esista in Splunk.



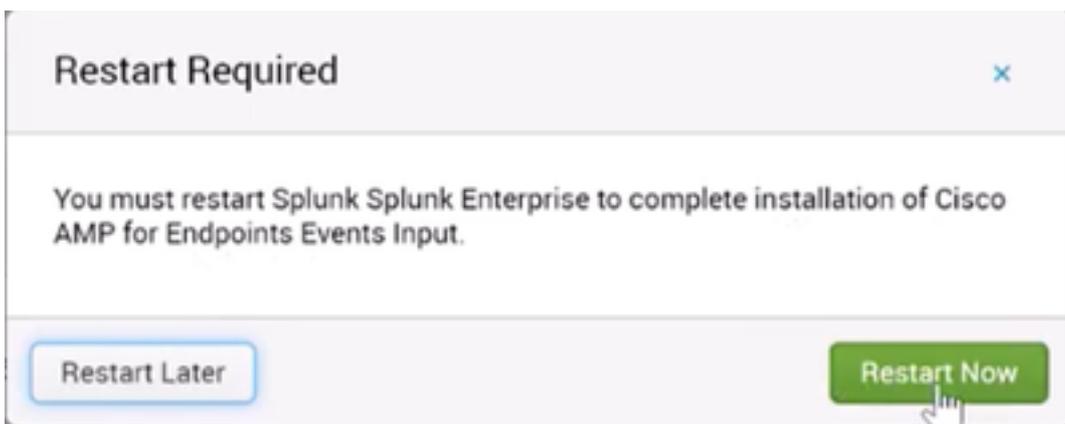
Passaggio 5. Dopo aver eseguito l'accesso a Splunk, procedere al download di AMP da Splunk Apps.



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



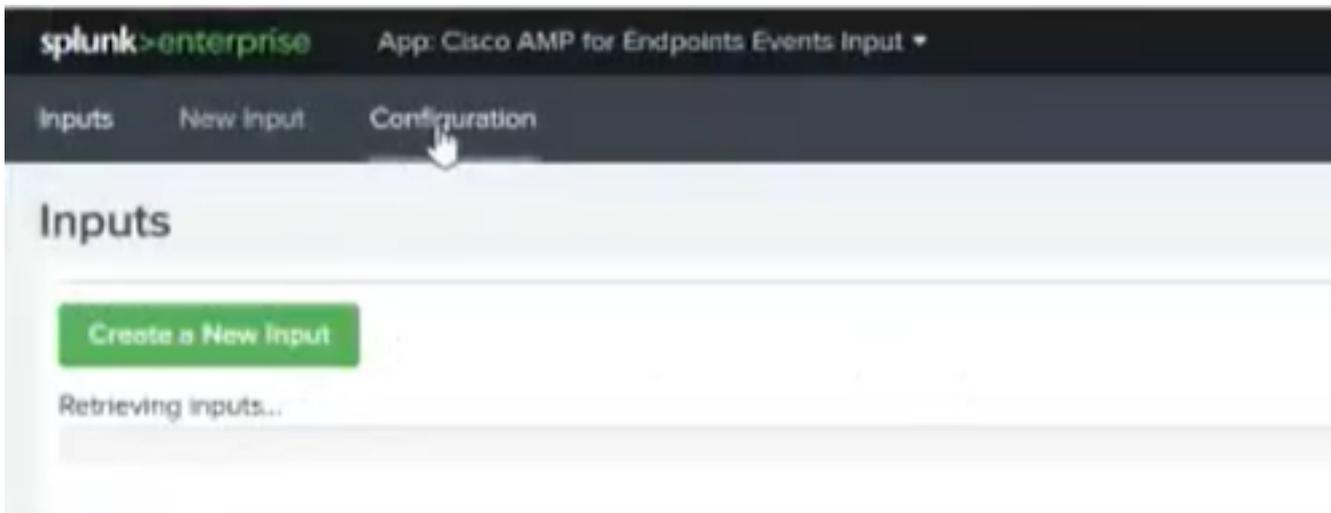
Passaggio 7. Per completare l'installazione su Splunk, è necessario riavviare la sessione.



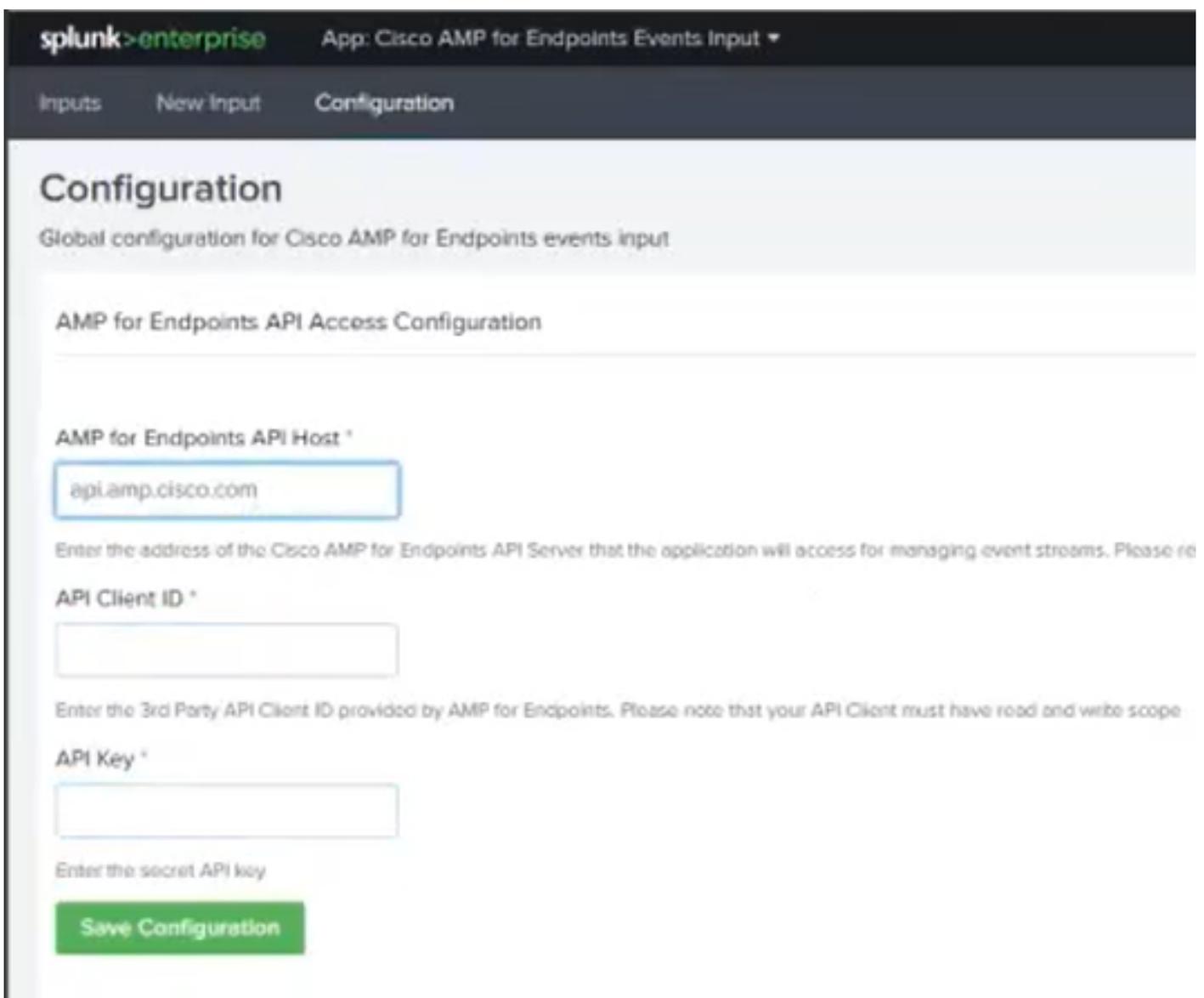
Passaggio 8. Dopo aver effettuato l'accesso in Splunk, fare clic su **Cisco AMP For Endpoints** sul lato sinistro della schermata.



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



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



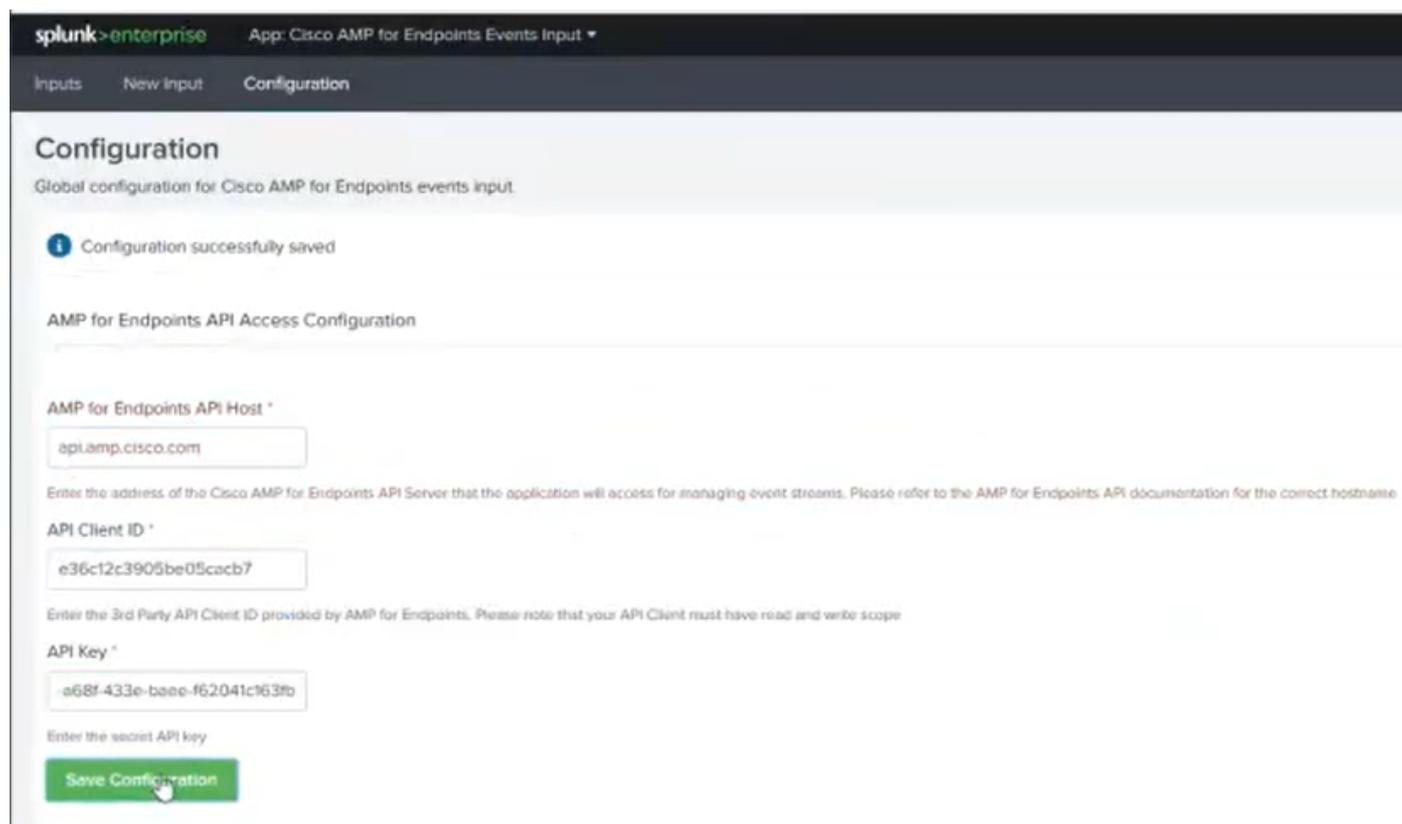
**Nota:** L'area API Host potrebbe essere diversa in base al centro dati cloud a cui punta l'organizzazione:

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.



The screenshot shows the Splunk configuration interface for the 'Cisco AMP for Endpoints Events Input' app. The top navigation bar includes 'splunk > enterprise' and 'App: Cisco AMP for Endpoints Events Input'. Below this, there are tabs for 'Inputs', 'New Input', and 'Configuration'. The main heading is 'Configuration', with a subtitle 'Global configuration for Cisco AMP for Endpoints events input'. A message at the top left states 'Configuration successfully saved'. The 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 'e36c12c3905be05c0cb7', and 'API Key \*' with the value 'a68f433e-ba0e-f62041c163fb'. Each field has a corresponding instruction: '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', 'Enter the 3rd Party API Client ID provided by AMP for Endpoints. Please note that your API Client must have read and write scope', and 'Enter the secret API key'. A green 'Save Configuration' button is located at the bottom left.

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

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

**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.

## Inputs

Name	Index
caislas	main

**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:

The screenshot shows the 'New Input' configuration page in Splunk. The page is divided into sections: 'Name \*', 'Index', 'Stream Settings', 'Stream Name \*', 'Event Types', and 'Groups'. The 'Name \*' field is disabled, indicated by a red prohibition icon. The 'Index' dropdown is set to 'main'. The 'Stream Name \*' field is empty. 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 located at the bottom left of the form.

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.