AMP for Endpoints와 Splunk 통합

목차

소개

이 문서에서는 AMP(Advanced Malware Protection)와 Splunk의 통합 프로세스에 대해 설명합니다.

기고자: Uriel Islas와 Jumentino Macias, Jorge Navarte, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

Cisco는 다음과 같은 정보를 얻을 것을 권장합니다.

- AMP for Endpoints
- API(Application Programming Interface)
- 스펑크
- Splunk의 관리자 사용자

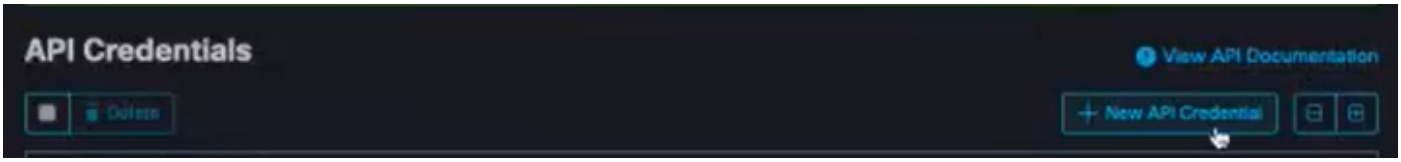
사용되는 구성 요소

- AMP 퍼블릭 클라우드
- Splunk 인스턴스

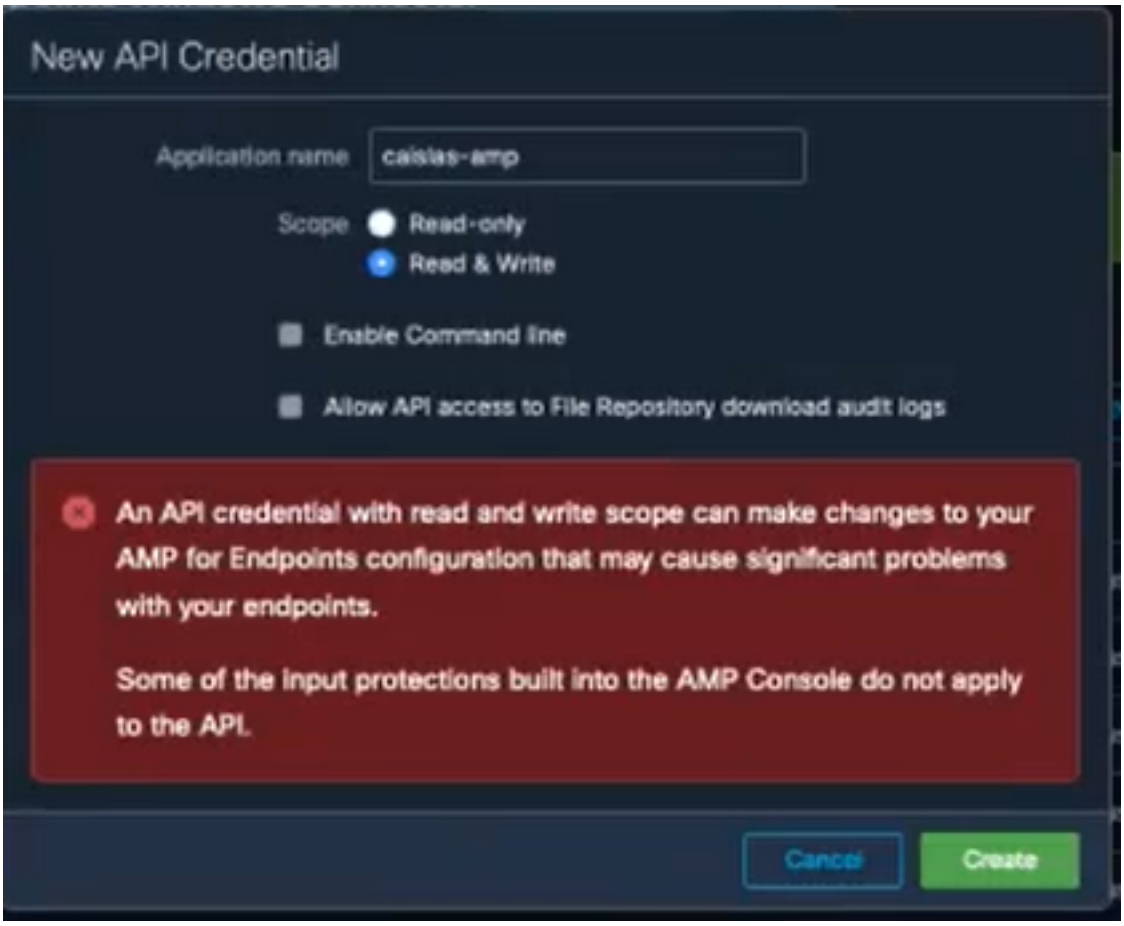
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

1단계. AMP 콘솔(https://console.amp.cisco.com)으로 이동하고 **Accounts>API Credentials(API 자격 증명)**로 이동하여 이벤트 스트림을 생성할 수 있습니다.

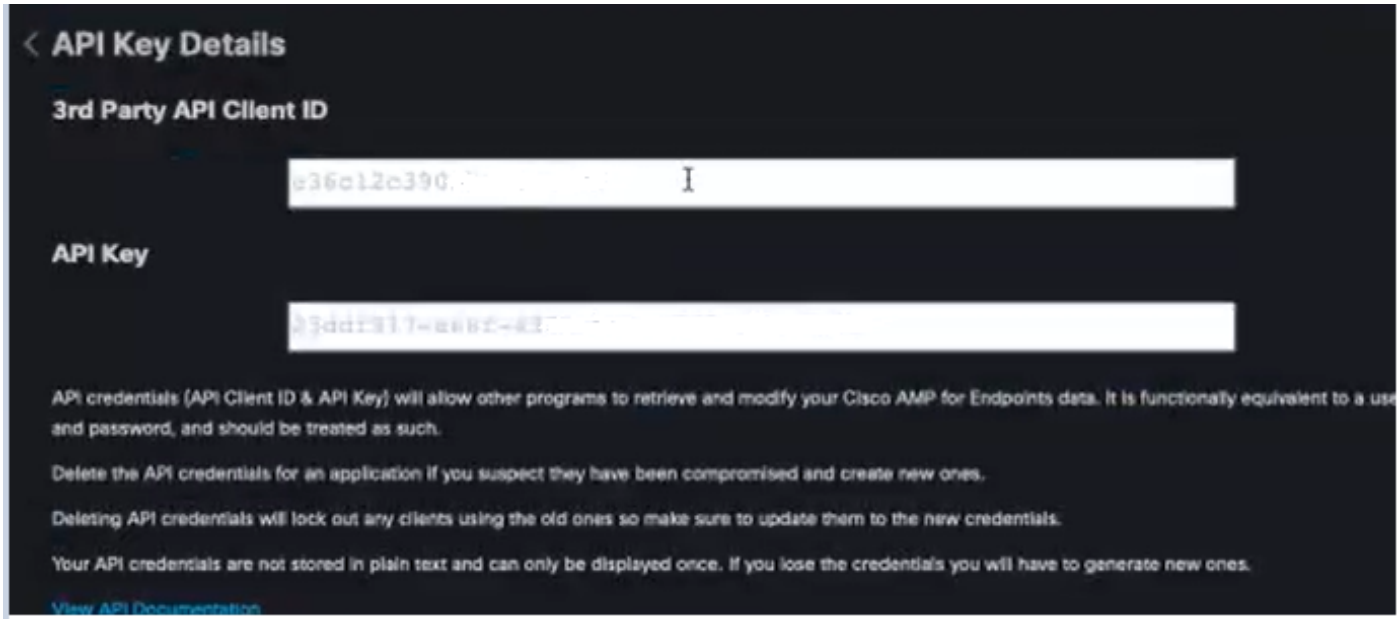


2단계. 이 통합을 수행하려면 아래와 같이 **읽기 및 쓰기** 확인란을 선택합니다.



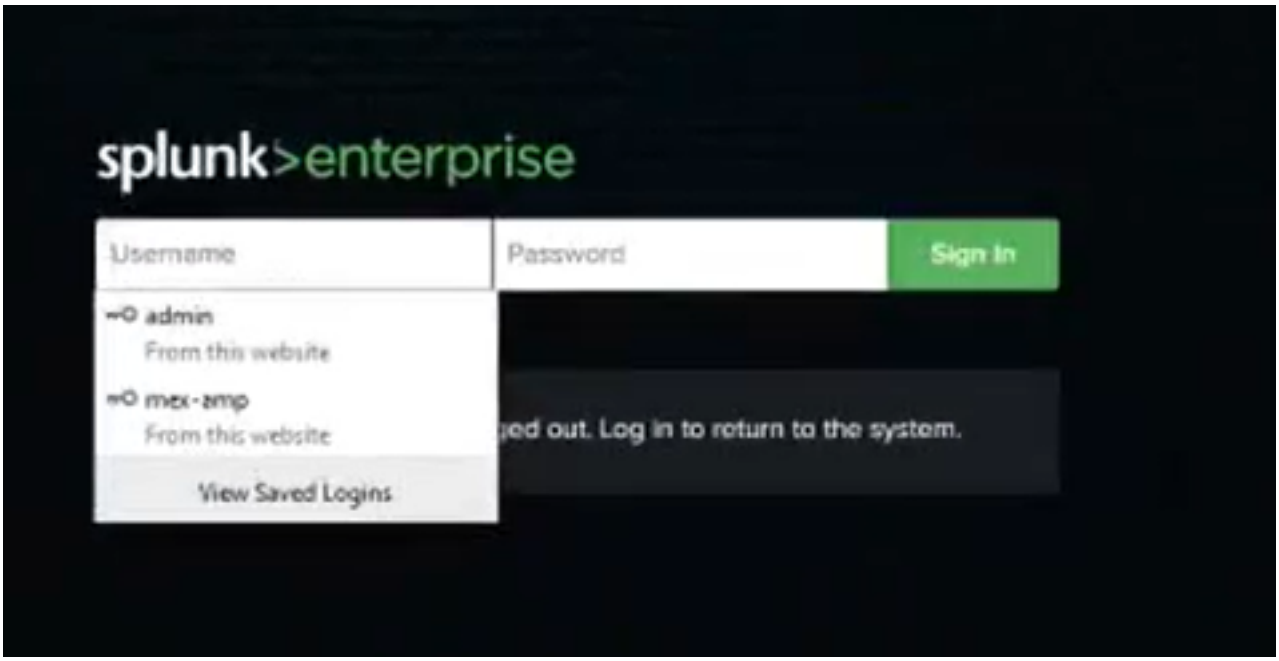
참고:이벤트에 대한 자세한 정보를 수집하려면 **Enable Command Line**(명령줄 활성화) 상자를 선택하여 File Repository(파일 저장소)에서 생성된 Audit Logs(감사 로그)를 가져오고 Allow API access to File Repository(**파일 저장소에 대한 API 액세스 허용**) 상자를 선택합니다.

3단계. 이벤트 스트림을 생성하면 Splunk에 필요한 API 클라이언트 ID 및 API 키가 표시됩니다.

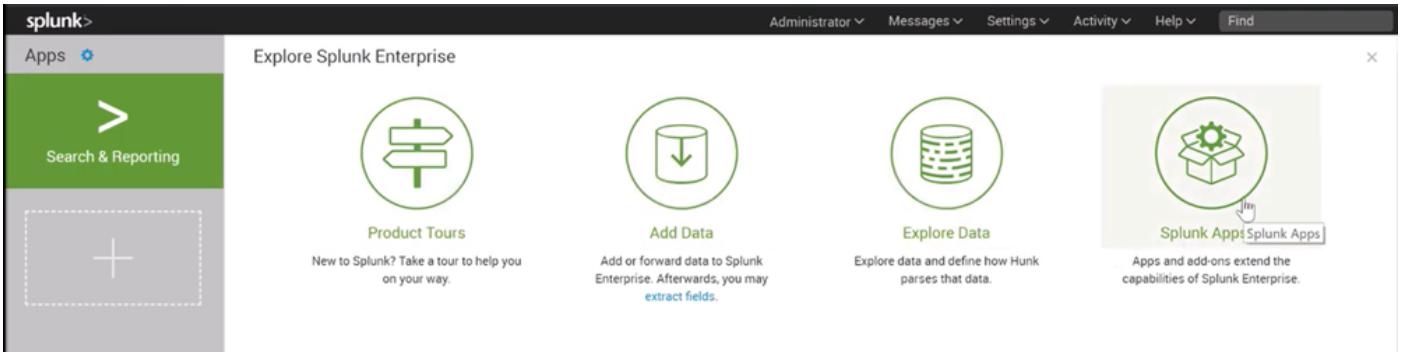


주의: 이 정보는 손실된 경우 새 API 키를 만들어야 하므로 어떤 방법으로도 복구할 수 없습니다.

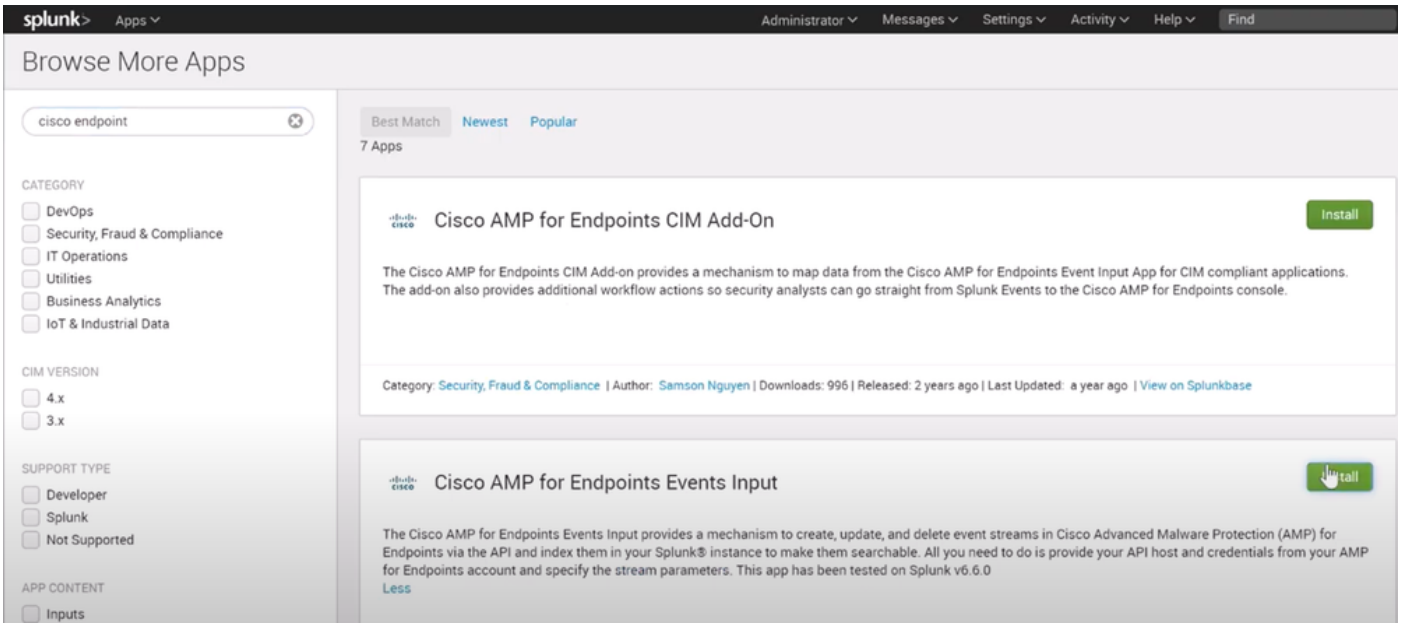
4단계. Splunk를 AMP for endpoints와 통합하려면 Splunk에 **Admin** 어카운트가 있는지 확인합니다.



5단계. Splunk에 로그인하면 Splunk Apps에서 AMP를 다운로드합니다.

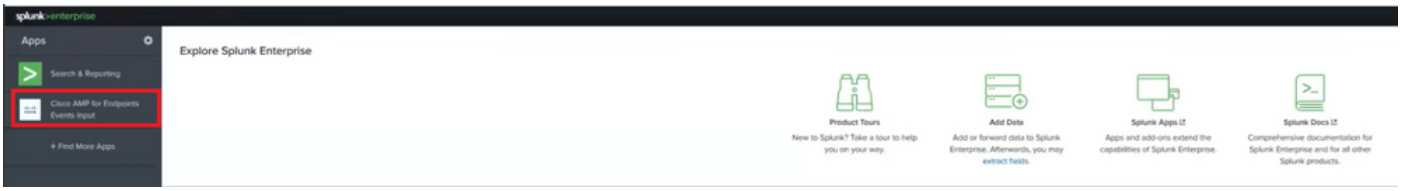


6단계. 앱 브라우저에서 Cisco 엔드포인트를 검색하고 설치합니다(Cisco AMP for Endpoints Events Input).

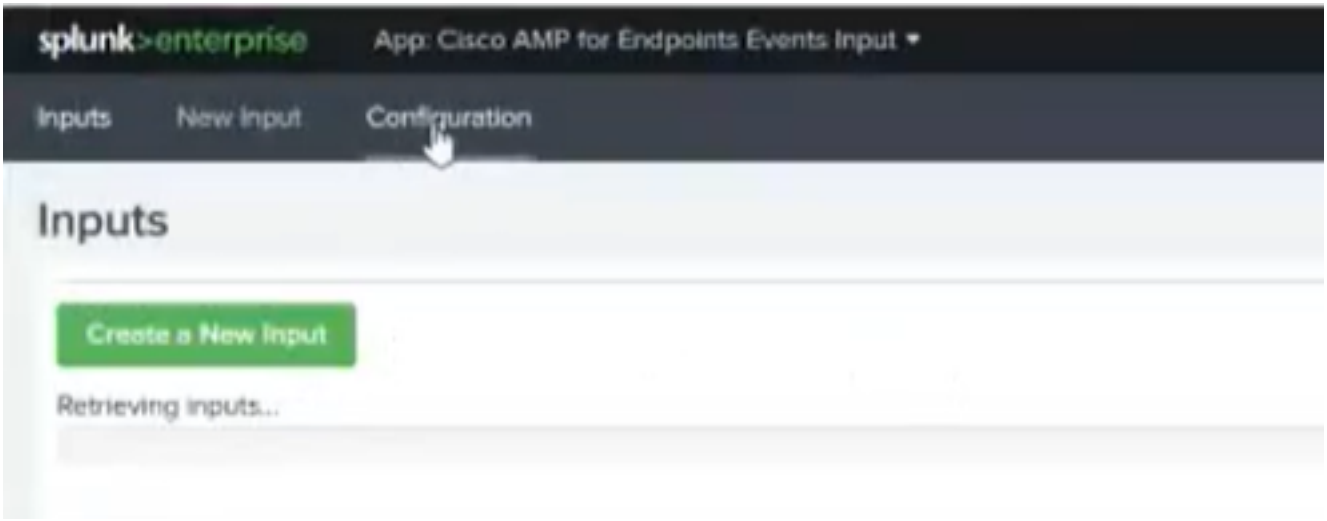


7단계. Splunk에서 설치를 완료하려면 세션을 다시 시작해야 합니다.

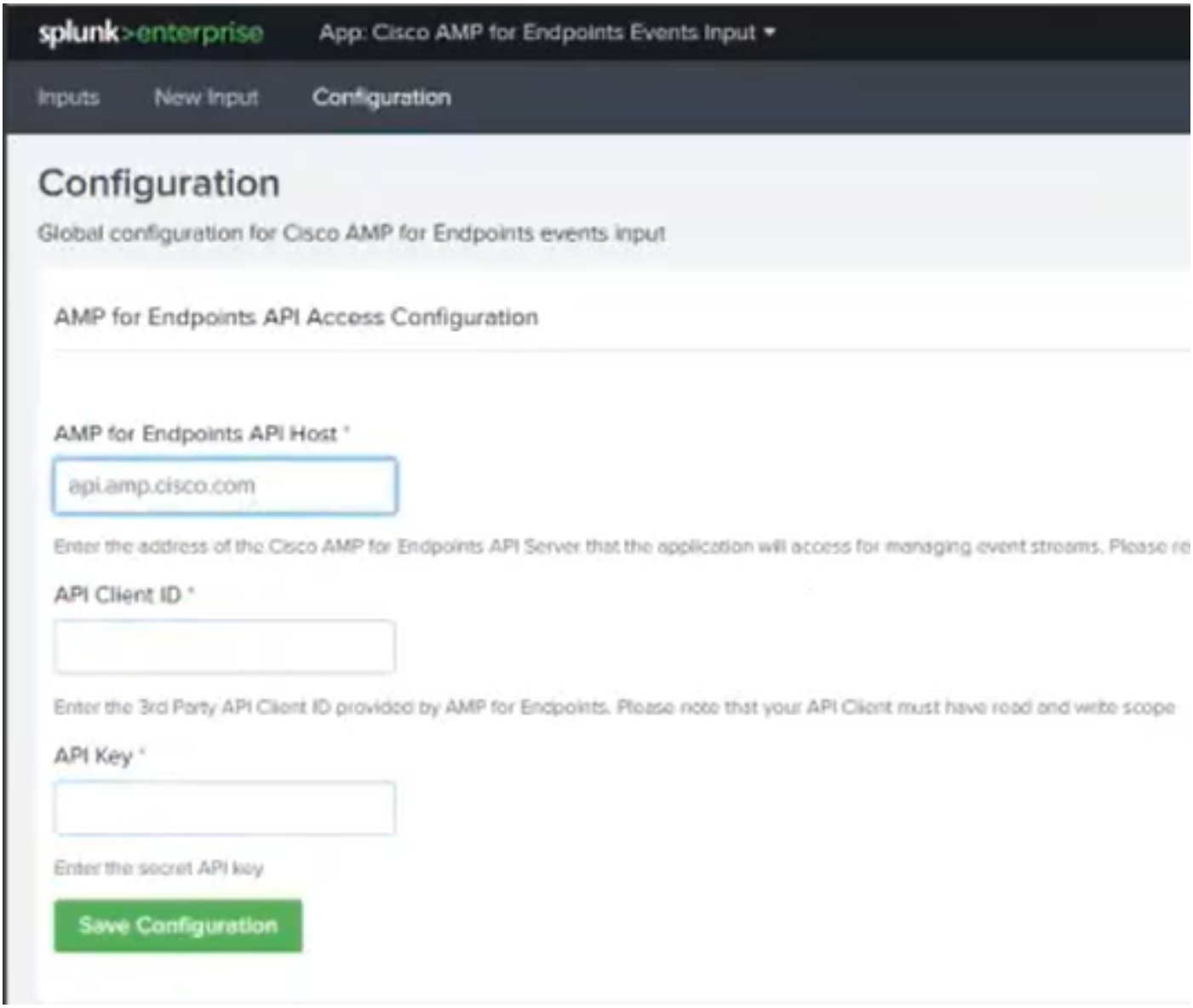
8단계. Splunk에 로그인하면 화면 왼쪽에서 **Cisco AMP For Endpoints**를 클릭합니다.



9단계. 화면 상단의 **Configuration** 레이블을 클릭합니다.

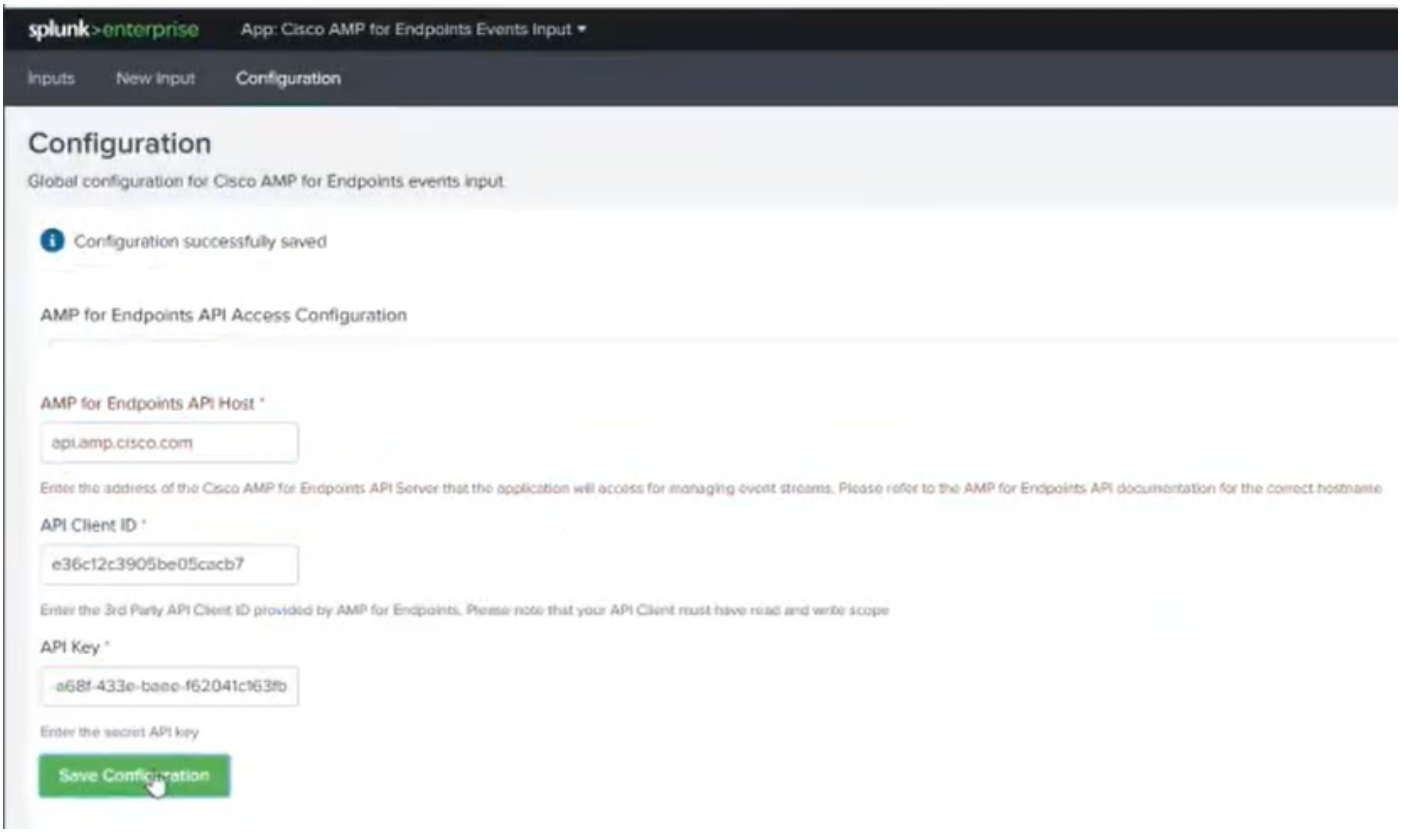


10단계. AMP 콘솔에서 이전에 생성한 API 자격 증명을 입력합니다.

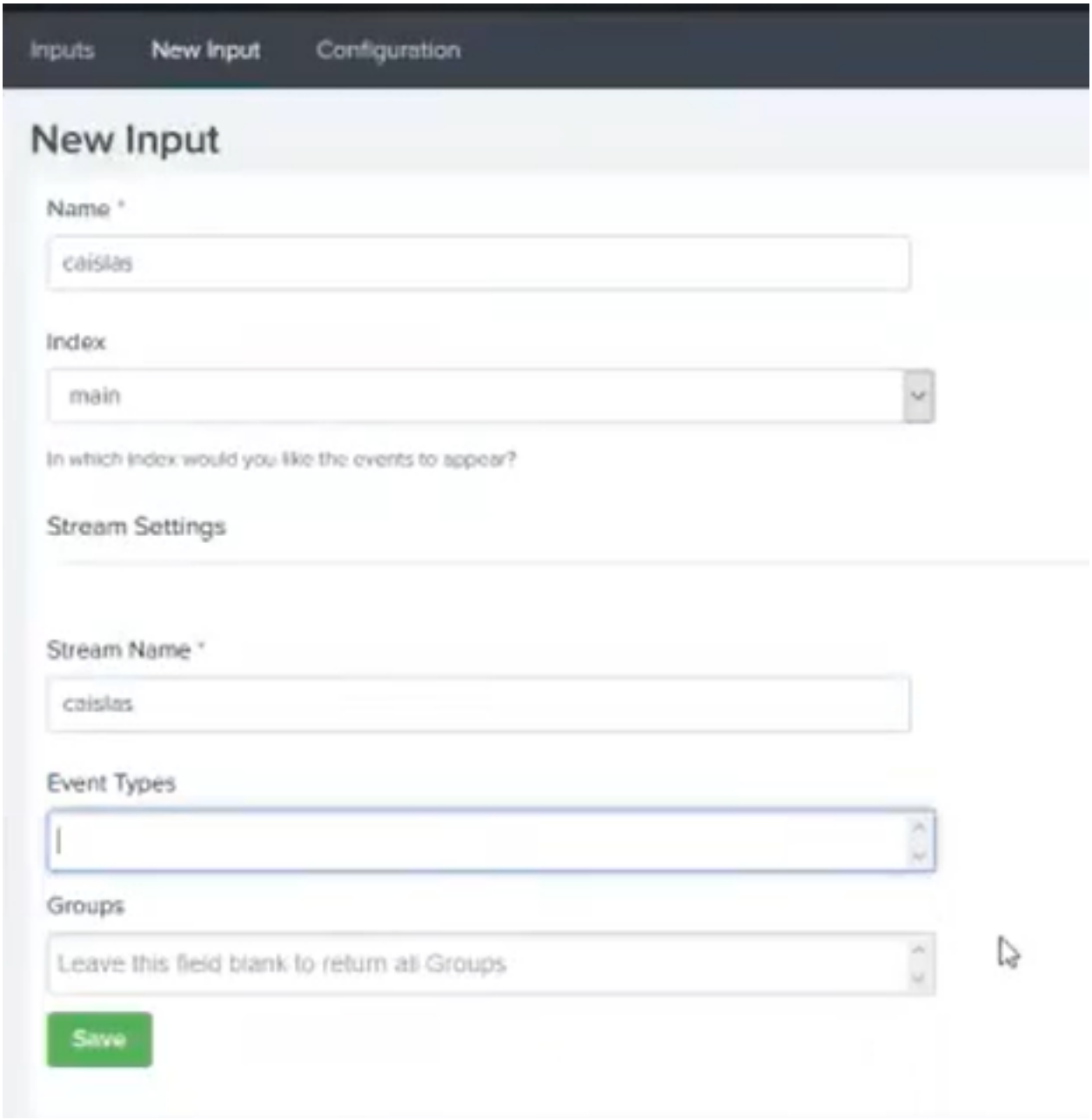


참고:API 호스트 위치는 조직이 가리키는 클라우드 데이터 센터에 따라 다를 수 있습니다.
북미:api.amp.cisco.com
유럽:api.eu.amp.cisco.com
APJC:api.apjc.amp.cisco.com

11단계. API 자격 증명을 Splunk 콘솔에 포함하고 저장하여 AMP와 연결합니다.

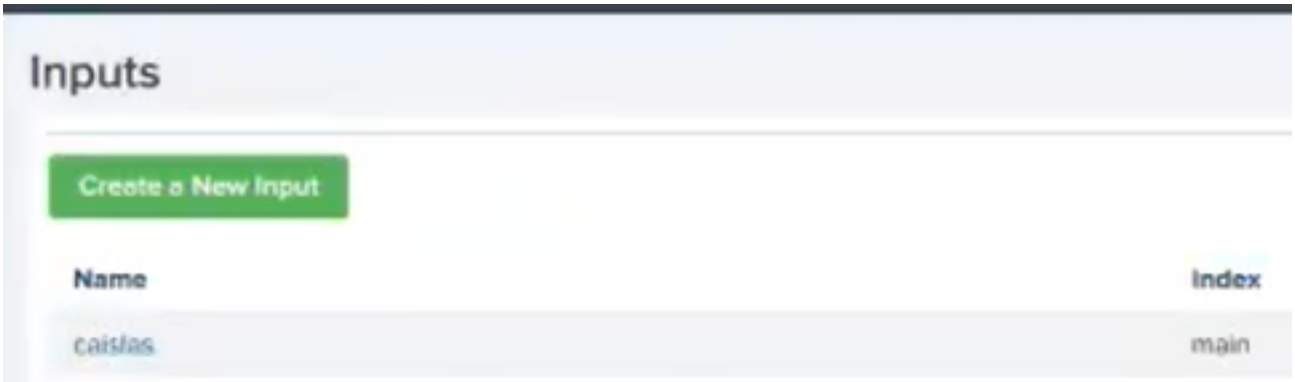


12단계. **입력**으로 돌아가 이벤트 스트림을 생성하십시오.



참고:AMP에서 모든 그룹에 대한 모든 이벤트를 가져오려면 **Event Types** and **Groups** 필드를 비워 둡니다.

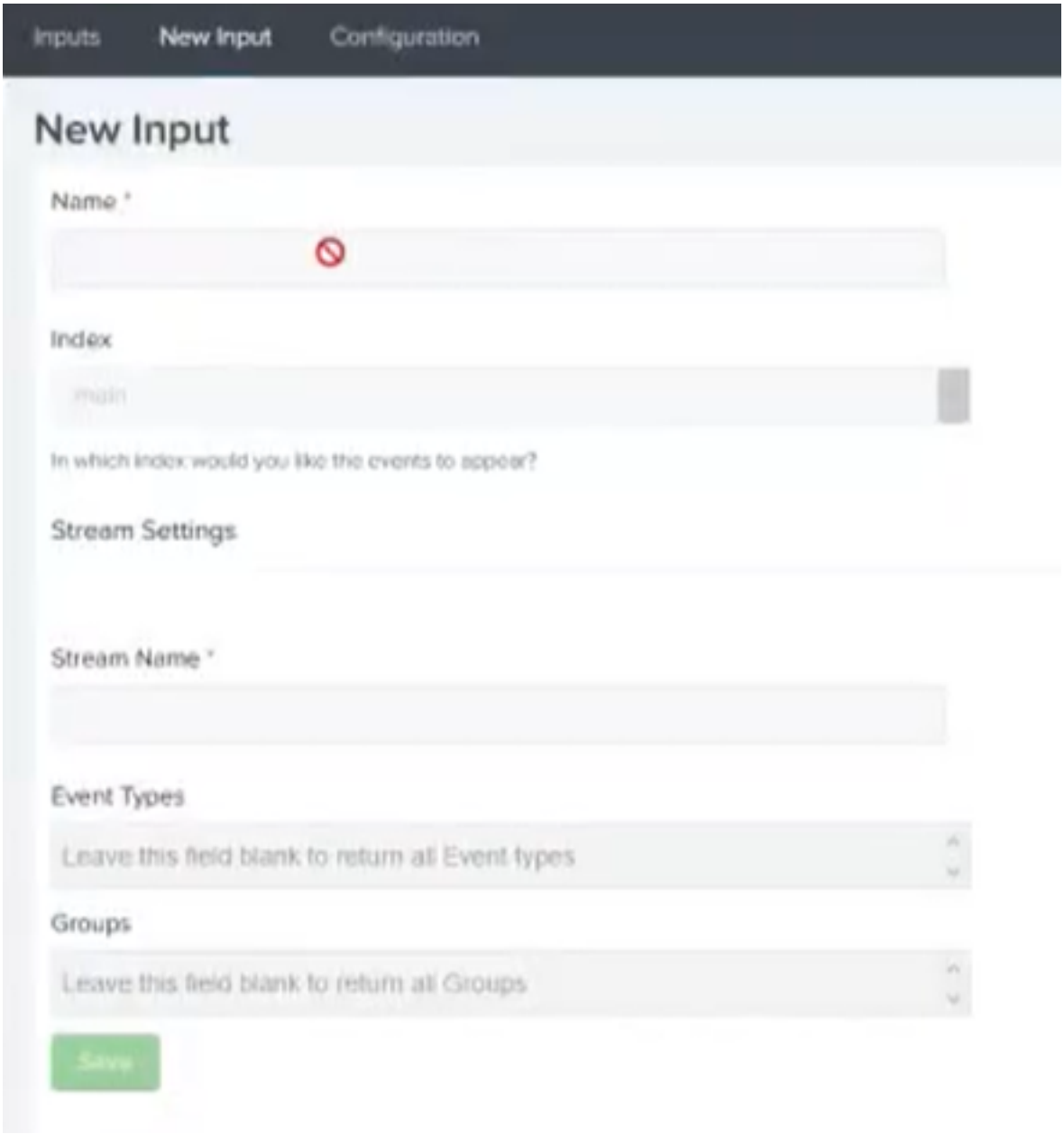
13단계. 입력이 성공적으로 생성되었는지 확인합니다.



참고:이 통합은 공식적으로 지원되지 않습니다.

문제 해결

이벤트 스트림을 생성하는 동안 모든 필드가 회색으로 비활성화된 경우, 이는 다음과 같은 이유로 발생할 수 있습니다.



1. 연결 문제:Splunk 인스턴스가 API 호스트에 연결할 수 있는지 확인합니다.
2. API 호스트:10단계에서 구성된 API 호스트가 AMP 조직과 일치하는지 확인합니다. 이때 비즈니스 포인트가 어디에 있는지 확인합니다.
3. API 자격 증명:API 키 및 클라이언트 ID가 3단계에서 구성된 API와 일치하는지 확인합니다.
4. 이벤트 스트림:구성된 이벤트 스트림이 4개 미만인지 확인합니다.