보안 클라우드 애플리케이션을 사용하여 Splunk에 SNA 통합

목차

소개

이 문서에서는 식별된 위협에 대한 더 신속한 사고 대응을 위해 Cisco Security Cloud를 사용하여 Splunk와 원활하게 SNA를 통합하는 방법에 대해 설명합니다.

사전 요구 사항

Splunk 및 Cisco 장치에 대한 기본 지식

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

Splunk Enterprise

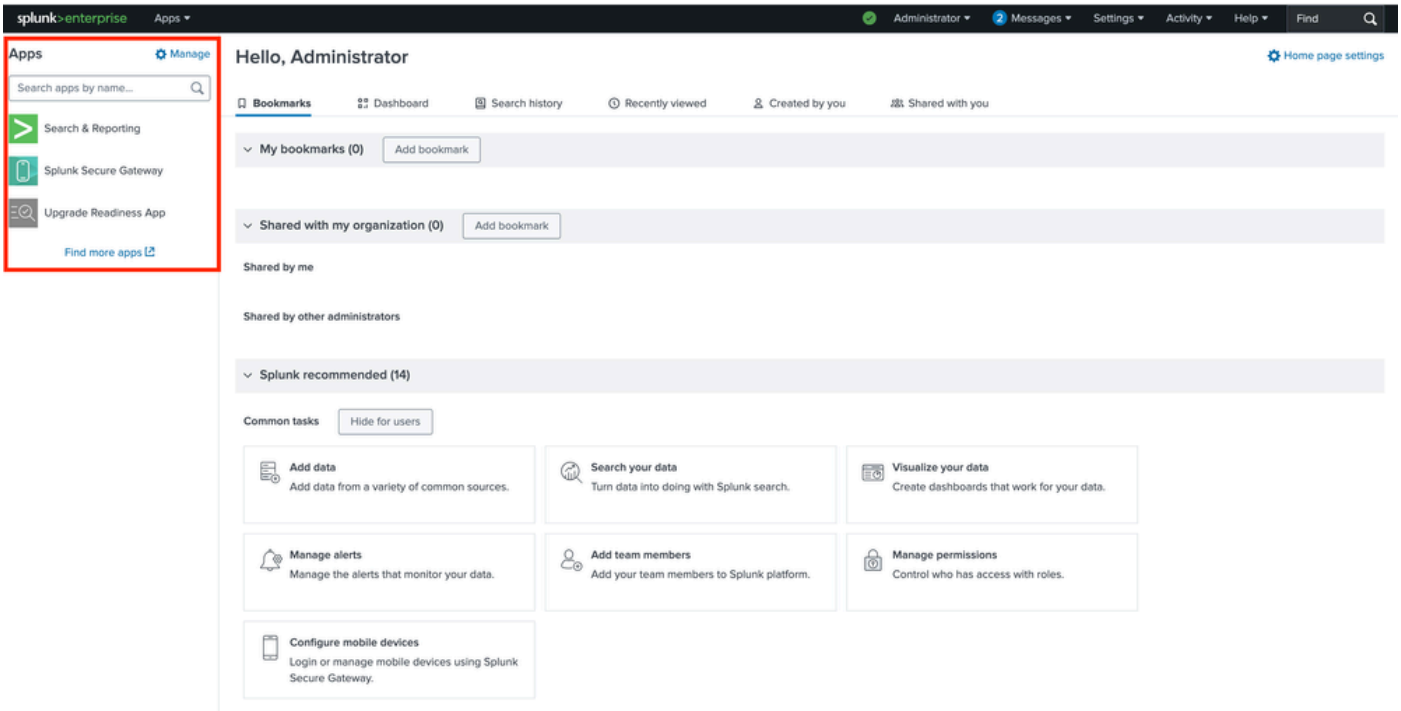
보안 네트워크 분석 v7.5.2.

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

구성

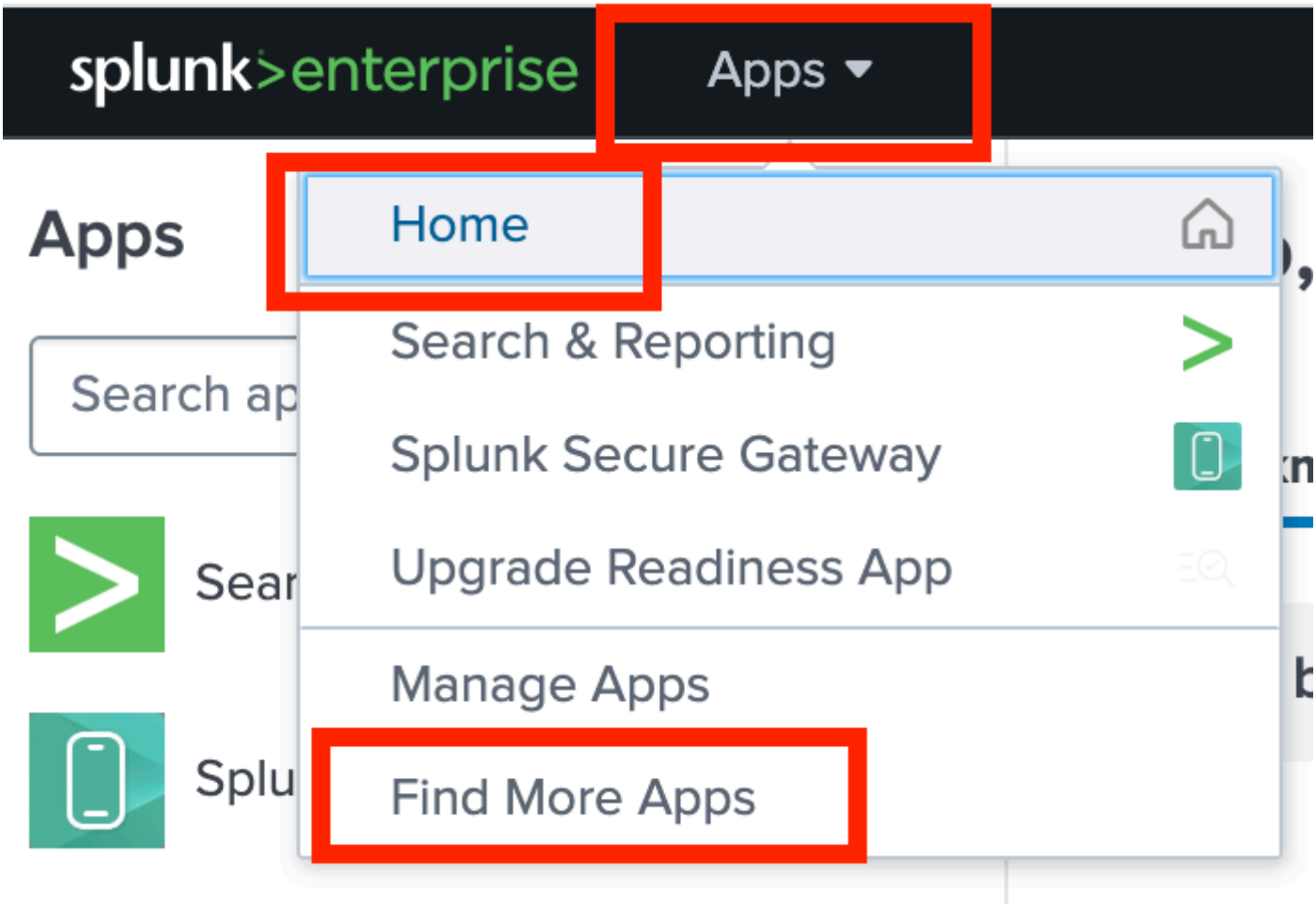
1단계: Splunk 애플리케이션에 액세스하고 Cisco Security Cloud 애플리케이션을 설치합니다.

1. 관리자 자격 증명을 사용하여 Splunk 웹 포털에 로그인하고 성공적으로 로그인하면 App 섹션 아래 왼쪽에 설치된 애플리케이션 목록과 함께 홈 페이지를 볼 수 있습니다.

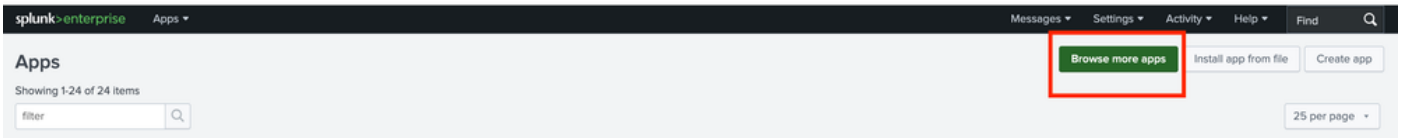


2. SNA를 Splunk와 통합하려면 Cisco Security Cloud Application을 설치해야 합니다. 이 애플리케이션은 다음 방법 중 하나로 구현할 수 있습니다.

1. 드롭다운에서 Find More Apps를 선택합니다.

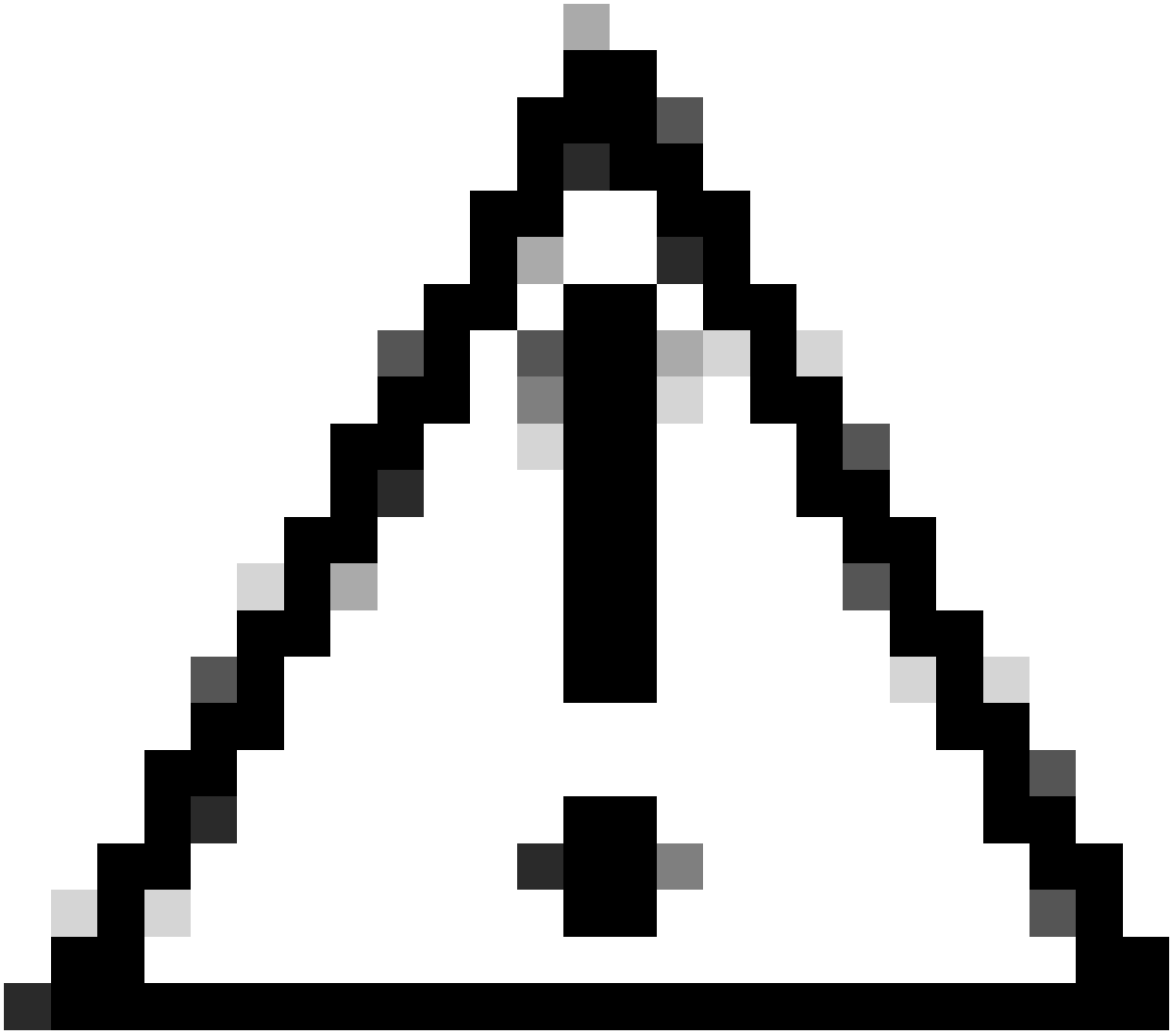


b. 관리자 기어 아이콘 아래에서 더 많은 앱을 탐색합니다.

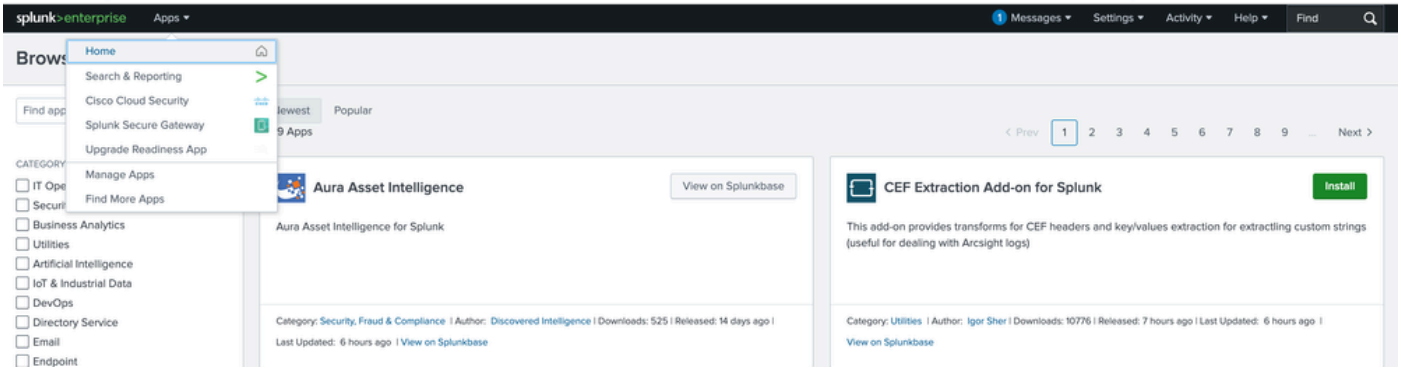


2단계: Cisco Security Cloud Application 설치

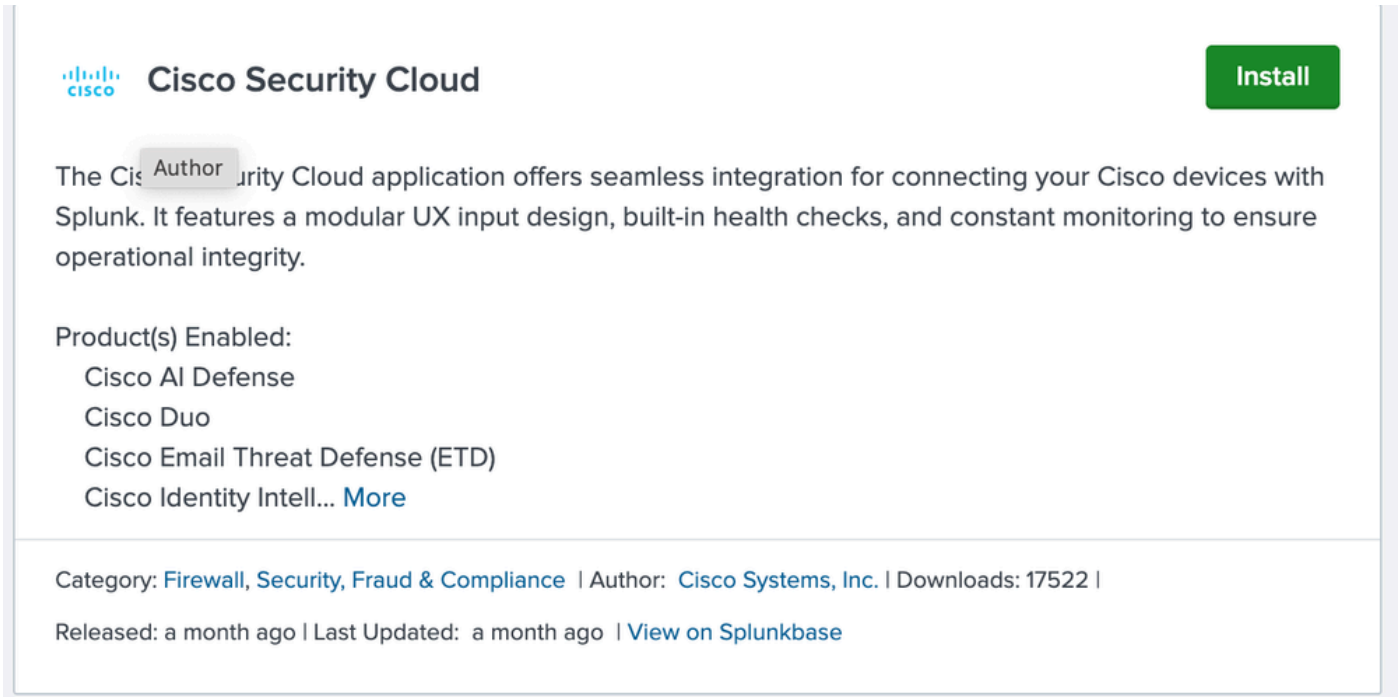
i. Cisco Security Cloud Application을 찾습니다. 이제 앱을 찾을 때까지 아래로 스크롤하거나 cisco 보안 클라우드를 검색합니다.



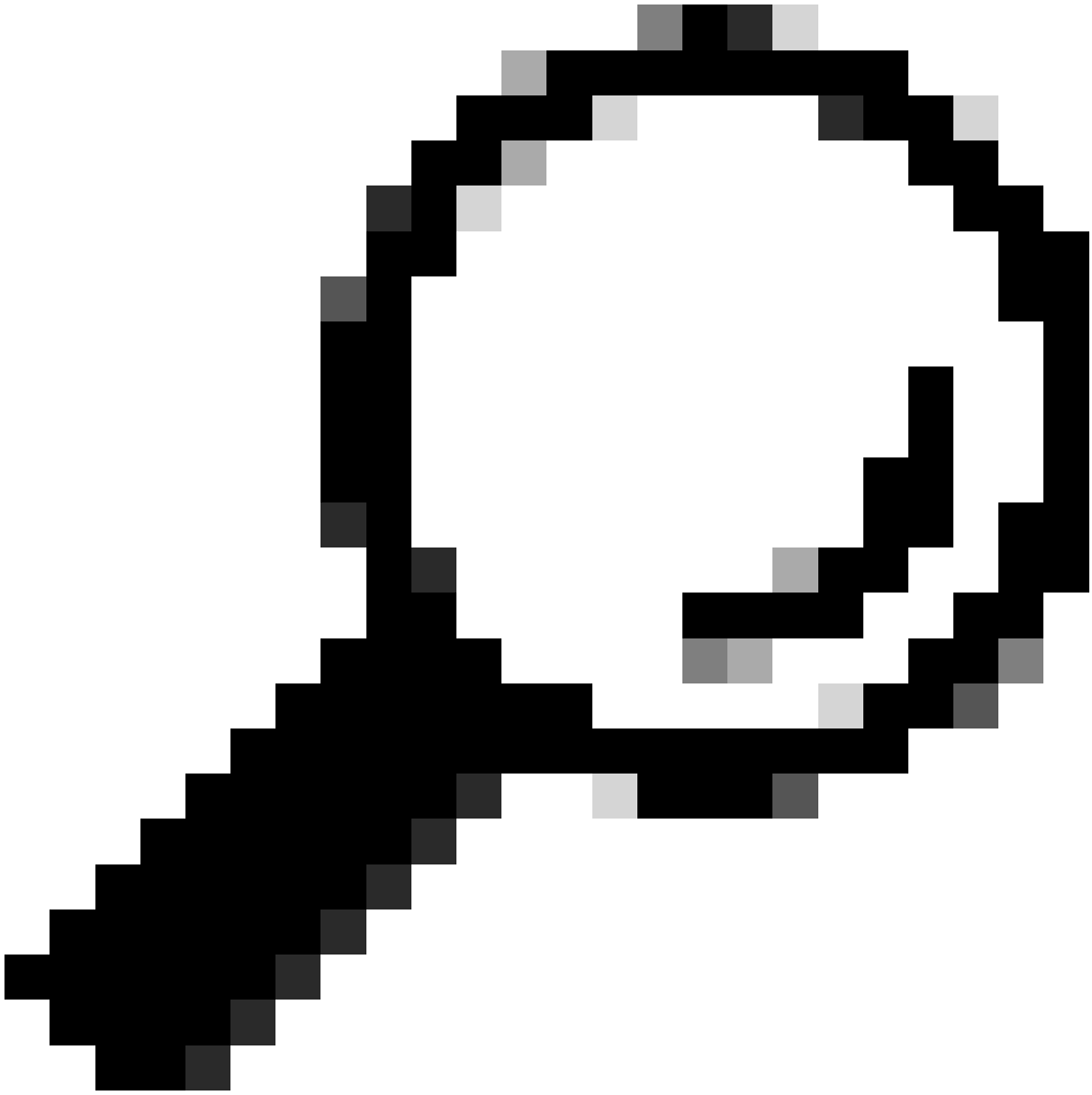
주의: Cisco Cloud Security 앱과 혼동하지 마십시오.



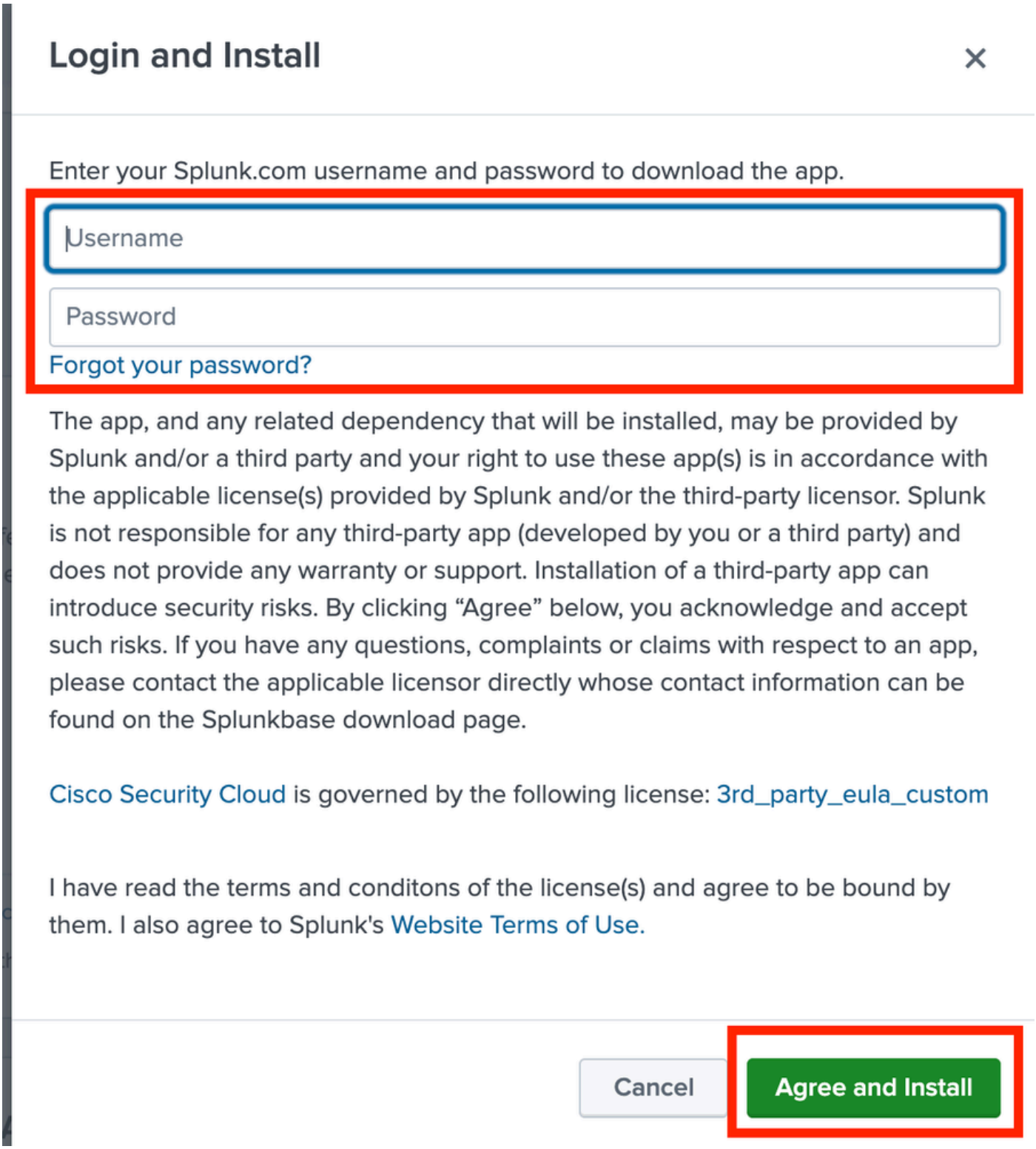
i. Install(설치) 버튼을 클릭하여 애플리케이션을 설치합니다.



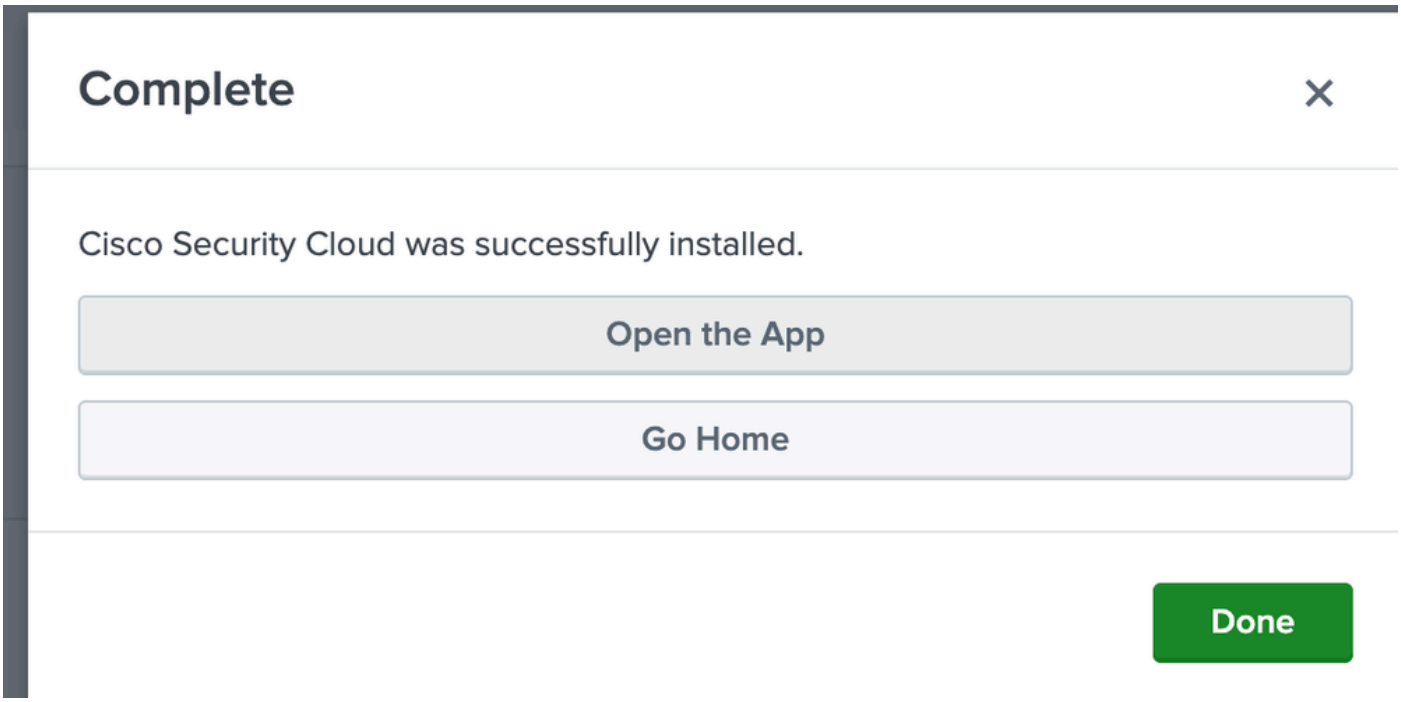
나. 설치 버튼을 클릭하면 애플리케이션을 설치하기 전에 Splunk 어카운트의 자격 증명을 묻는 창이 나타납니다. 자격 증명을 입력하고 Agree and Install을 클릭하여 계속 진행합니다.



팁: 로그인 시 Splunk 엔터프라이즈 애플리케이션에 사용되는 관리자 자격 증명이 아니라 Splunk 포털에 액세스하는 데 사용되는 자격 증명을 제공합니다.

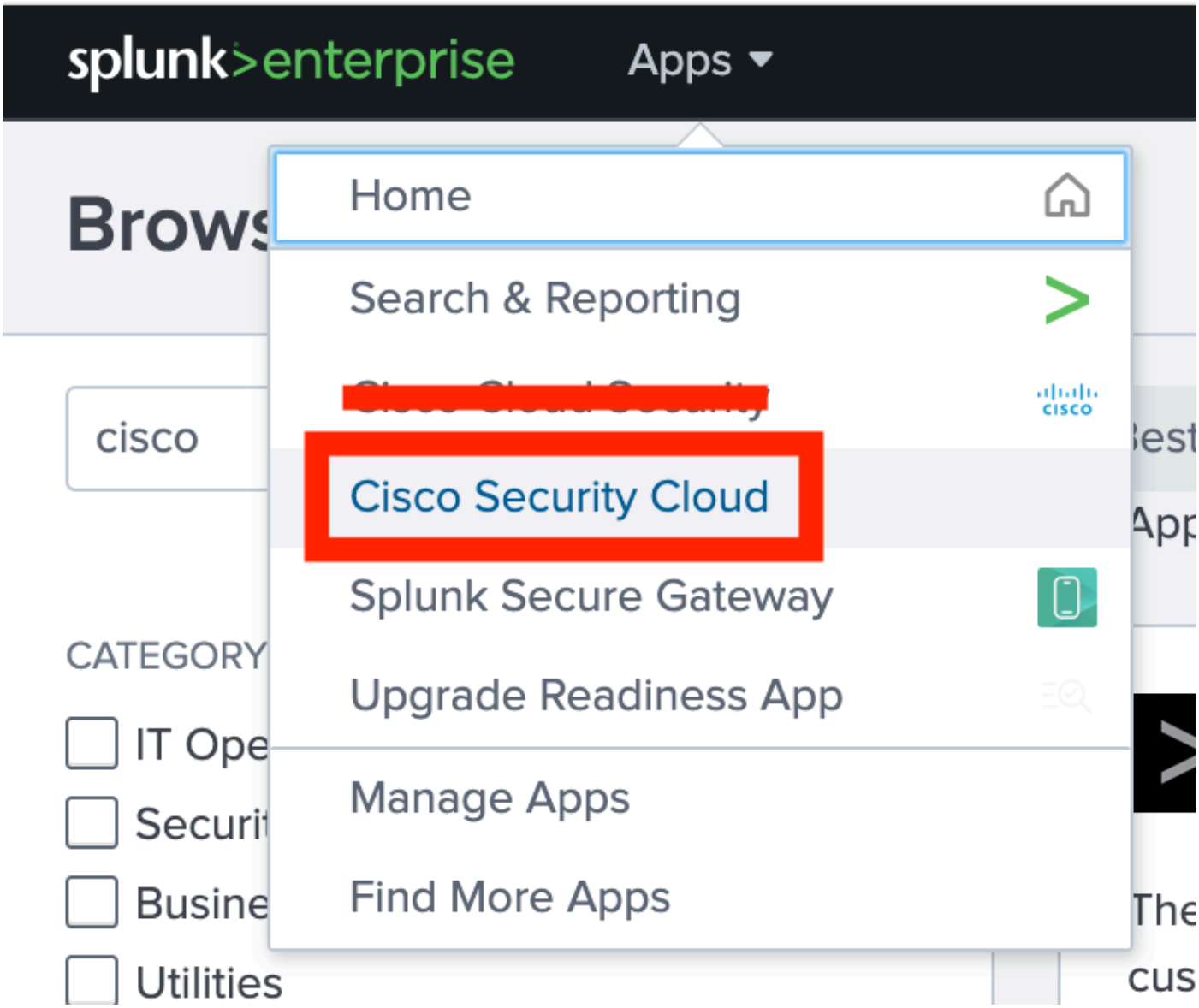


iii. 애플리케이션의 성공적인 설치에 대한 메시지가 표시된 대로 팝업됩니다. 완료를 클릭합니다.

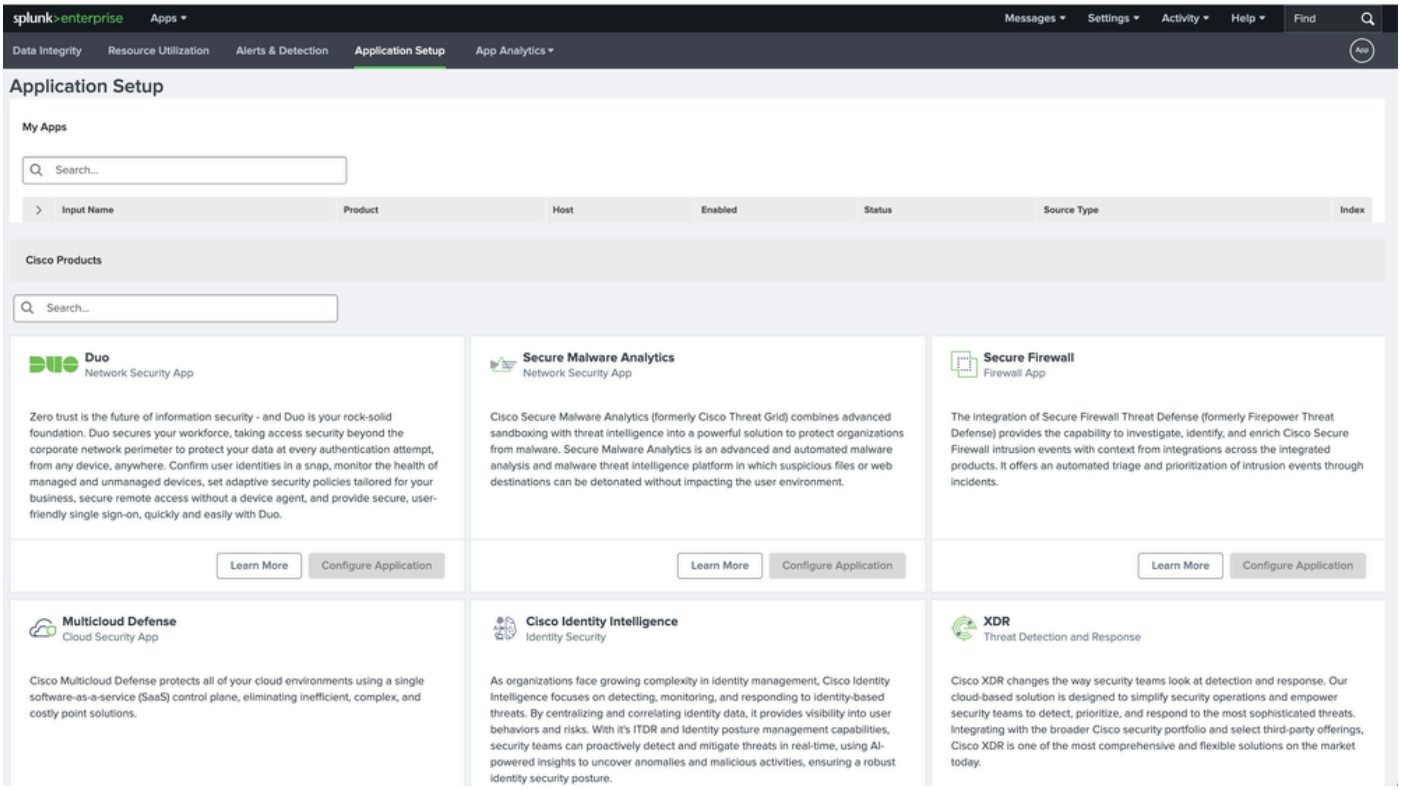


3단계: Cisco Security Cloud Application 설치 확인

i. Apps(앱) 드롭다운 옵션을 클릭하면 설치가 완료된 후 앱이 목록에 표시됩니다.



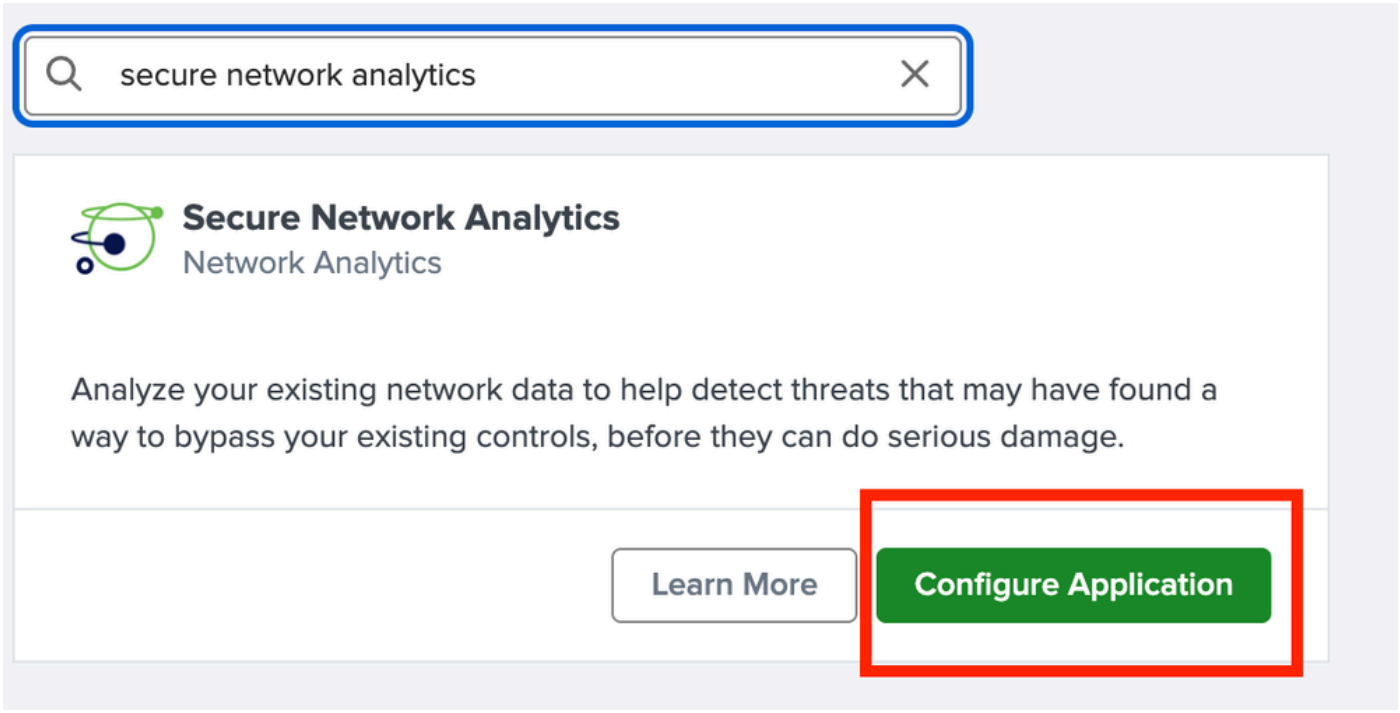
ii. Cisco Security Cloud(Cisco 보안 클라우드)를 클릭하여 선택합니다. 사용 가능한 모든 Cisco Cloud Security 제품을 찾을 수 있는 애플리케이션 설정 페이지로 리디렉션됩니다.



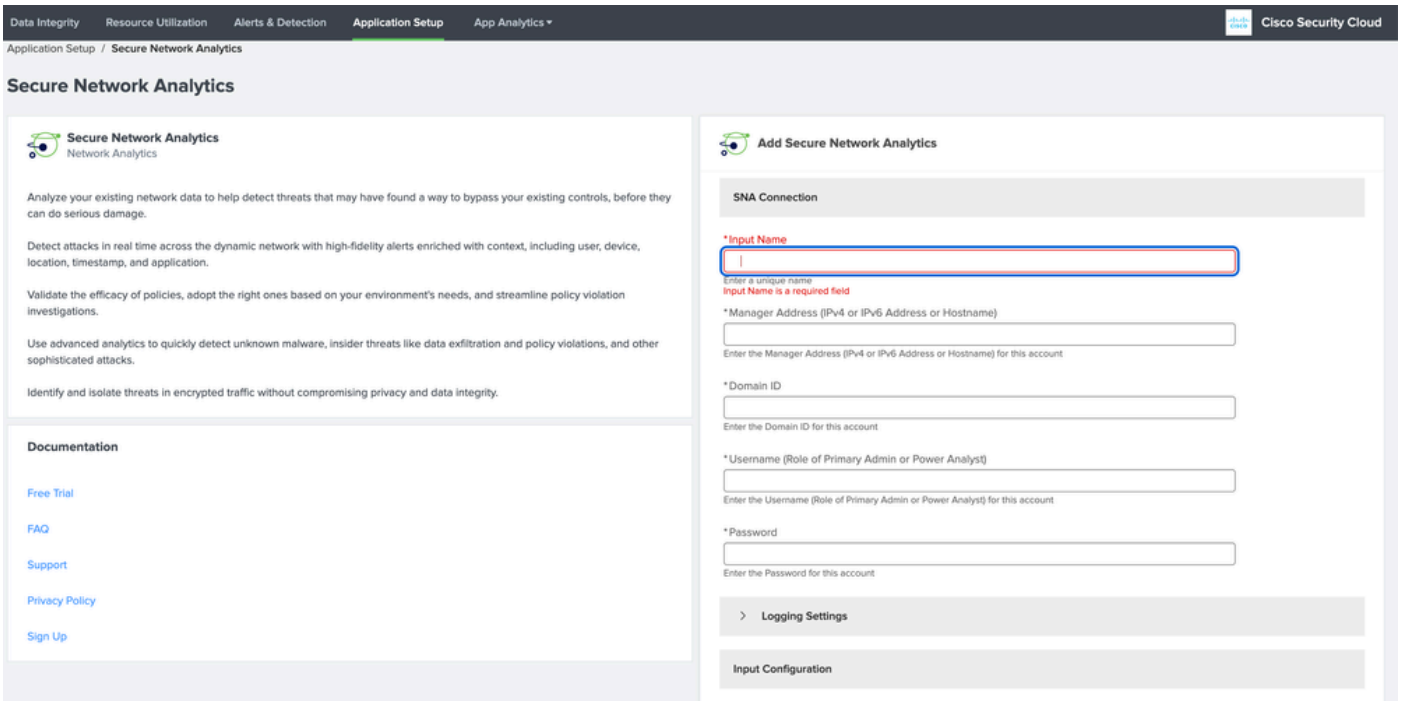
4단계: SNA(Secure Network Analytics)와의 통합.

이 문서의 목적은 SNA(Secure Network Analytics)를 통한 Splunk의 설치 단계를 강조하는 것입니다.

i. Secure Network Analytics를 검색하고, 해당 항목이 나타나면 Configure Application(애플리케이션 구성)을 선택하십시오.

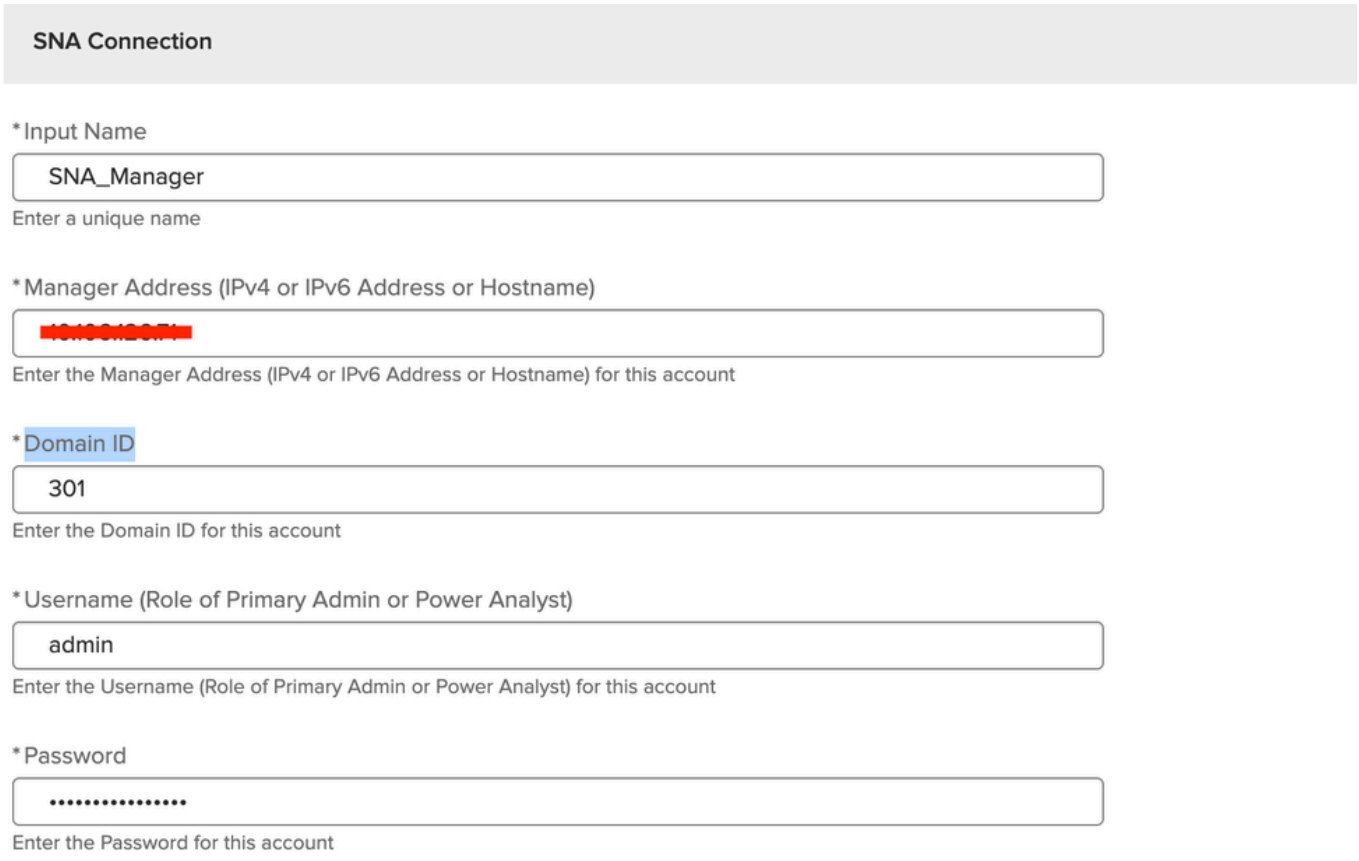


나. 구성 옵션을 선택하면 추가할 세부 정보에 대한 컨피그레이션 페이지가 팝업됩니다.

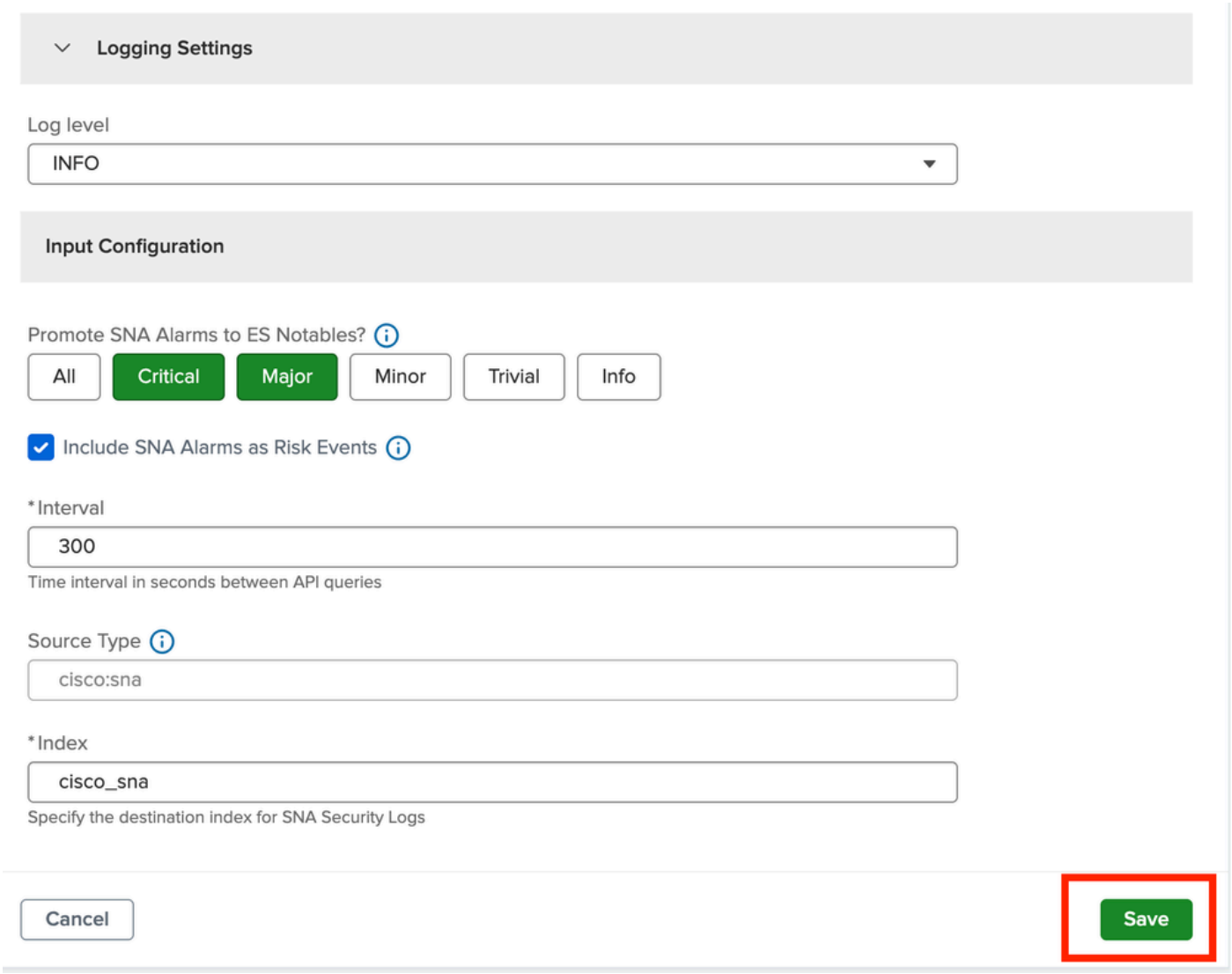


iii. SNA Connection Details(SNA 연결 세부사항)에 대해 언급된 모든 필수 세부사항을 입력합니다.

1. 입력 이름: SNA의 고유한 이름
2. 관리자 주소(IPv4 또는 IPv6 주소 또는 호스트 이름): 기본 SNA Manager의 관리 IP
3. 도메인 ID: domain_ID에 대한 값을 입력합니다(예: 301).
4. 사용자 이름: 기본 관리자의 사용자 이름(예: admin)
5. 암호: 기본 관리자 사용자의 비밀번호



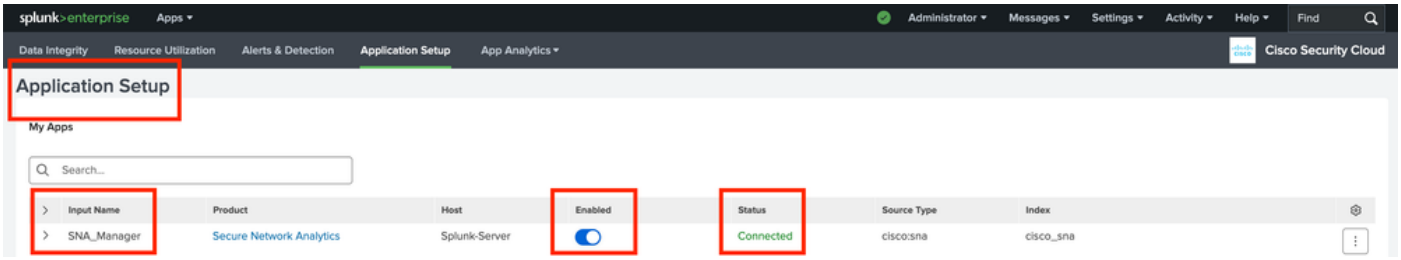
iv. 나머지 설정을 기본값으로 두거나 필요에 따라 수정한 다음 Save를 클릭합니다. 완료 후 성공 메시지가 화면에 팝업됩니다.



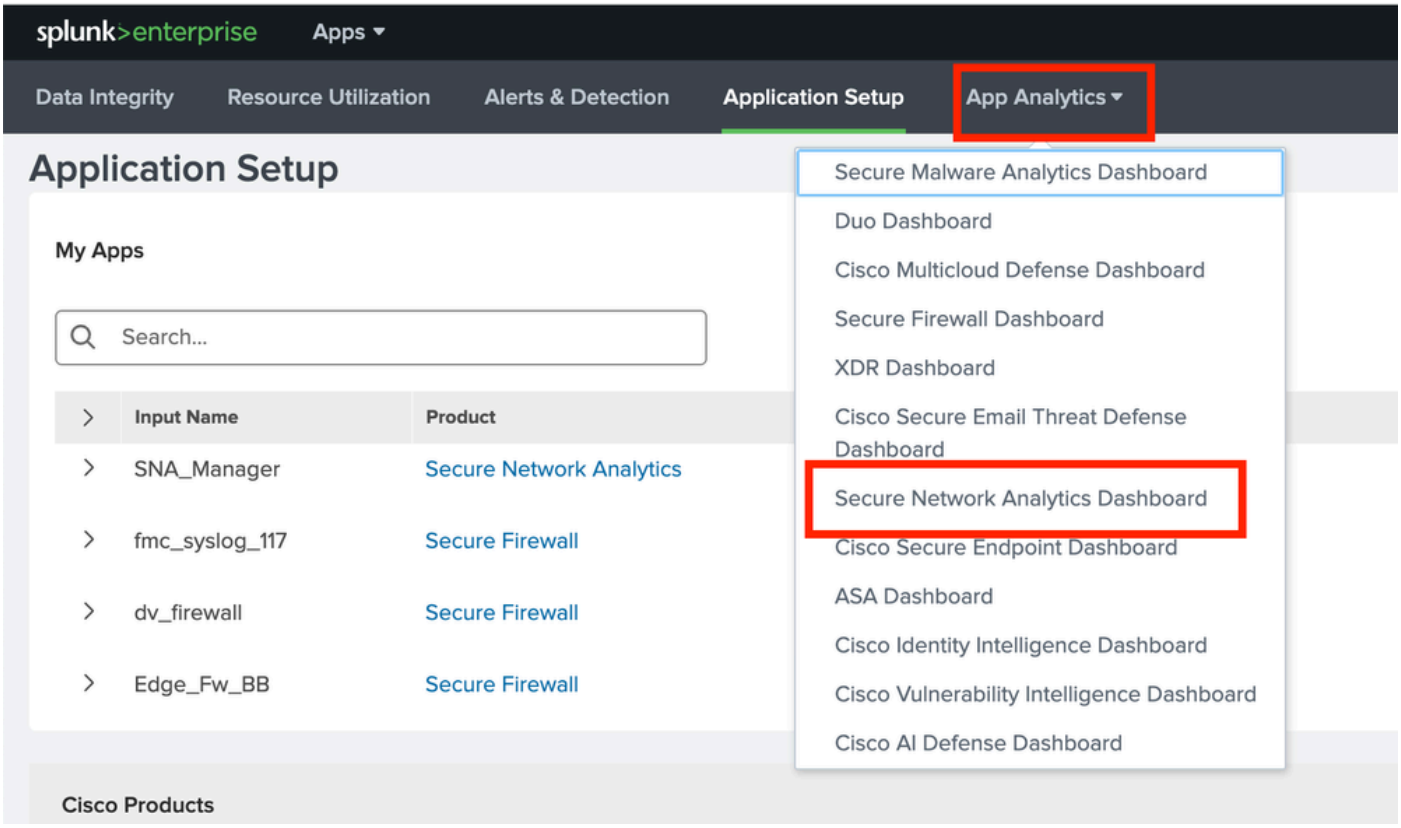
5단계: 통합 확인.

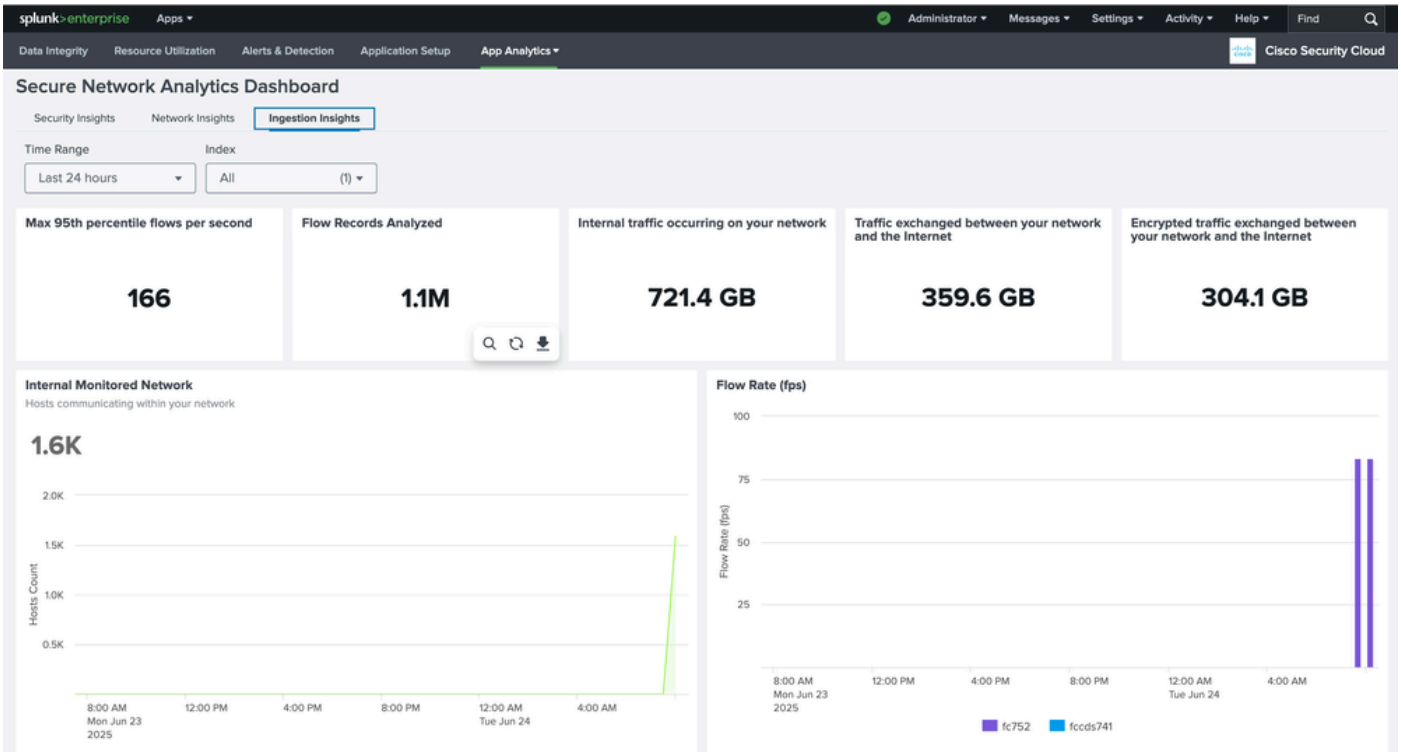
이는 이전 단계에서 실행한 통합이 성공적으로 완료되었는지 여부를 확인해야 하는 중요한 단계입니다.

i. 입력의 연결 상태는 Application Setup(애플리케이션 설정) 탭에서 Connected(연결됨)여야 하며, 기본값은 Input(입력) 필드의 올바른 이름에 대해 Enabled(활성화됨)여야 합니다.



ii. 드롭다운에서 Secure Network Analytics Dashboard(보안 네트워크 분석 대시보드)를 선택하면 최종적으로 대시보드에 통계가 반영되기 시작합니다.





FAQ

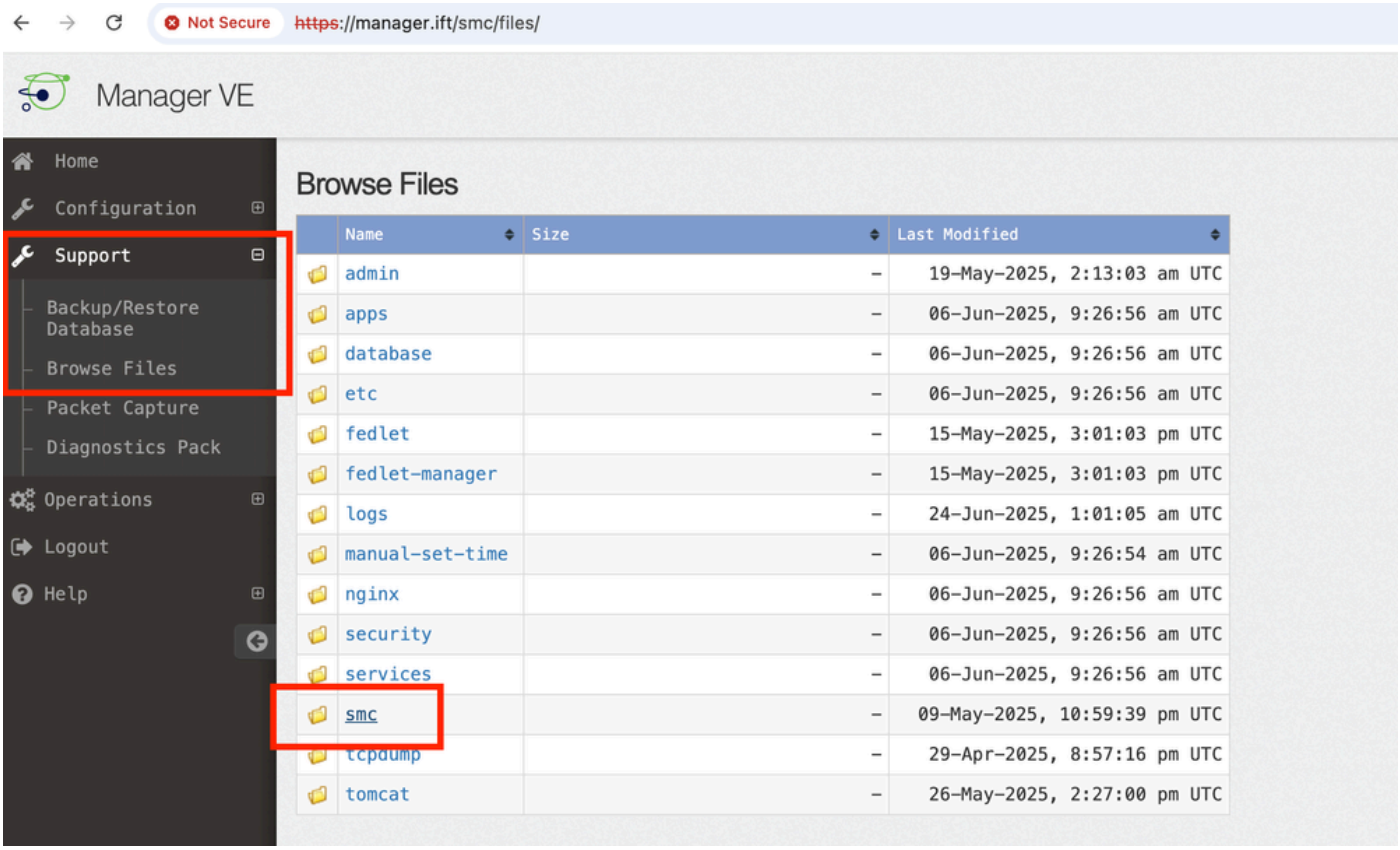
SNA 관리자의 도메인 ID를 어디에서 찾을 수 있습니까?

답변:

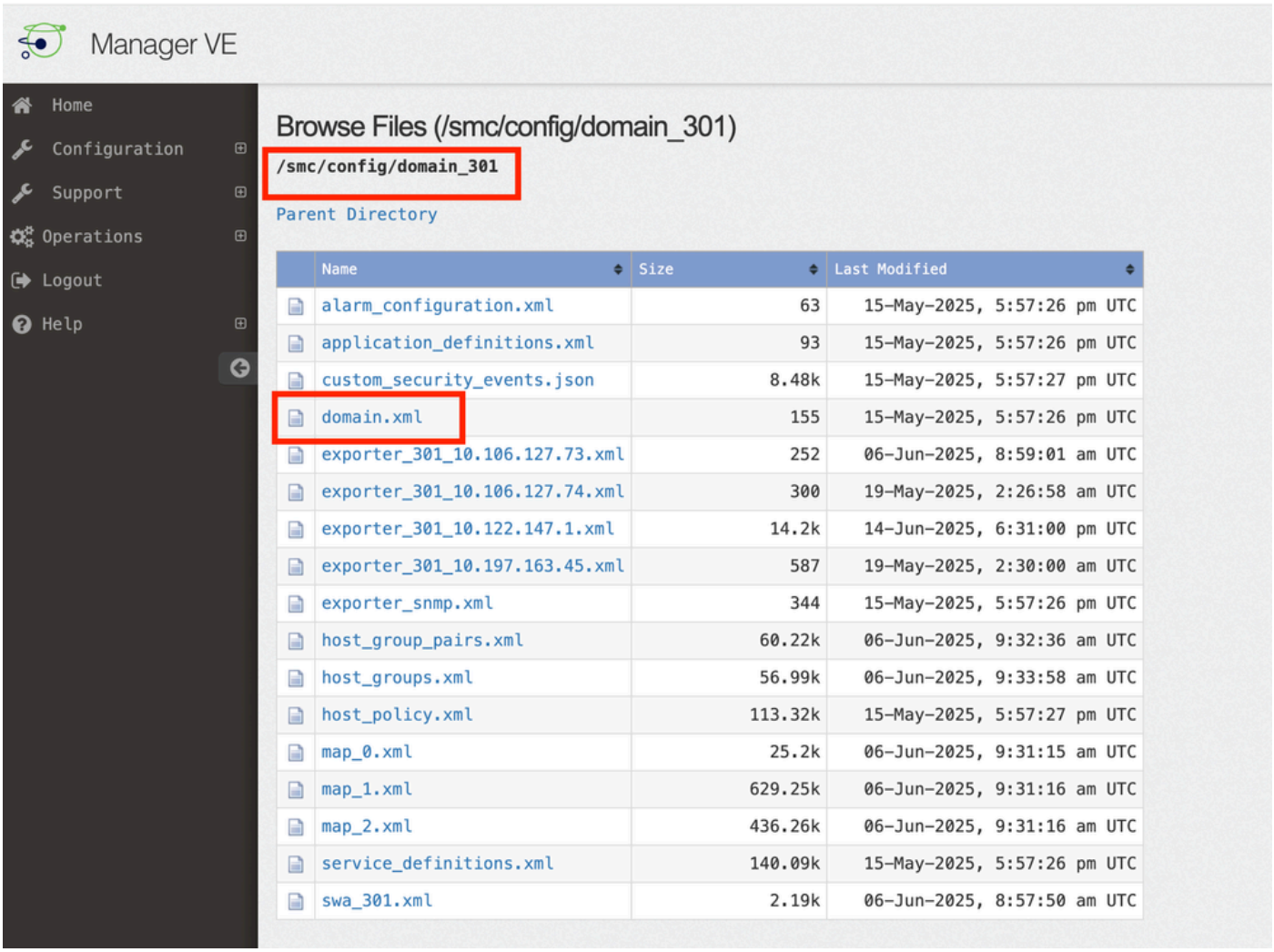
i. SNA 기본 관리자에 로그인하고 어플라이언스 관리 페이지 또는 액세스 관리자 IP 인덱스 URL로

리디렉션합니다.

나. Support 섹션 아래의 smc 폴더를 찾습니다.



iii. config 폴더 아래의 domain_XXX 폴더에서 사용 가능한 domain.xml 파일을 엽니다.


Manager VE
Home
Configuration
Support
Operations
Logout
Help
Browse Files (/smc/config/domain_301)
/smc/config/domain_301
Parent Directory
Name
Size
Last Modified
alarm_configuration.xml 63 15-May-2025, 5:57:26 pm UTC
application_definitions.xml 93 15-May-2025, 5:57:26 pm UTC
custom_security_events.json 8.48k 15-May-2025, 5:57:27 pm UTC
domain.xml 155 15-May-2025, 5:57:26 pm UTC
exporter_301_10.106.127.73.xml 252 06-Jun-2025, 8:59:01 am UTC
exporter_301_10.106.127.74.xml 300 19-May-2025, 2:26:58 am UTC
exporter_301_10.122.147.1.xml 14.2k 14-Jun-2025, 6:31:00 pm UTC
exporter_301_10.197.163.45.xml 587 19-May-2025, 2:30:00 am UTC
exporter_snmp.xml 344 15-May-2025, 5:57:26 pm UTC
host_group_pairs.xml 60.22k 06-Jun-2025, 9:32:36 am UTC
host_groups.xml 56.99k 06-Jun-2025, 9:33:58 am UTC
host_policy.xml 113.32k 15-May-2025, 5:57:27 pm UTC
map_0.xml 25.2k 06-Jun-2025, 9:31:15 am UTC
map_1.xml 629.25k 06-Jun-2025, 9:31:16 am UTC
map_2.xml 436.26k 06-Jun-2025, 9:31:16 am UTC
service_definitions.xml 140.09k 15-May-2025, 5:57:26 pm UTC
swa_301.xml 2.19k 06-Jun-2025, 8:57:50 am UTC

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.