Pxgrid 클라우드를 통한 보안 그룹 태그를 위한 ISE와의 Cisco Secure Access 통합

목차

소개

이 문서에서는 Cisco Secure Access와 Cisco Identity Services Engine 간의 컨텍스트 공유를 활성화하는 방법에 대해 설명합니다

요구 사항

다음 주제에 대해 알고 있으면 유용합니다.

- Cisco Secure Access—제로 트러스트(zero-trust) 네트워크 액세스를 제공하는 클라우드 기반 SSE(Security Service Edge) 솔루션으로, 사용자가 모든 디바이스에서 인터넷 및 프라이빗 애플리케이션에 쉽게 연결할 수 있습니다.
- Cisco ISE(Identity Service Engine) 버전 3.4 패치 5.
- Cisco Security Cloud Control—보안 클라우드 제품 및 ID를 위한 통합 관리 솔루션입니다. 보안 클라우드 제어는 보안 액세스에 포함됩니다.

배경

이러한 통합을 통해 Catalyst SD-WAN 브랜치에서 Cisco Secure Access로 신뢰할 수 있는 터널을 자동으로 생성하여 VPN-ID/이름 및 SGT 컨텍스트를 원활하게 교환할 수 있습니다.

Cisco ISE(Identity Services Engine)는 SGT 컨피그레이션 및 관리를 위한 중앙 기관으로 유지됩니다. ISE에서 수행되는 모든 업데이트는 Cisco Secure Access와 자동으로 동기화됩니다. SGT가 삭제되면 이를 참조하는 기존 규칙은 트래픽 매칭이 예상대로 계속되도록 활성 상태로 유지됩니다.

현재 SGT 매핑에 대해 제한적인 가용성을 제공하고 있습니다. 이는 보안 규칙 내에 SGT 대상 개체를 포함하도록 지원을 확장합니다. 또한 Meraki 및 Cisco Secure Firewall의 SGT를 전달하는 SASE 터널 구축에 대한 지원도 곧 제공될 예정입니다

사용 사례:

SGT 이름 공간 기반 정책:

보안 관리자인 키트는 SSE Private 및 인터넷 바운드 트래픽용 Onprem ISE의 SGT를 사용하여 연속 마이크로 세그멘테이션을 적용하려고 합니다. 정책을 적용하기 위해 SGT를 가져오는 기능.

사용되는 구성 요소

이 문서의 정보는 다음을 기반으로 합니다.

- ISE(Identity Service Engine) 버전 3.4 패치 5
- 보안 액세스
- Cisco 보안 클라우드

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.

컨텍스트 공유 컨피그레이션 개요

- ISE를 Cisco Security Cloud에 연결
- Cisco Secure Access를 ISE에 연결

구성

이 설명서는 전반적인 구성을 다음과 같은 주요 단계로 나눕니다.

1. Cisco ISE를 Cisco Security Cloud에 연결
2. Cisco Secure Access를 Cisco ISE에 연결
3. Cisco Secure Access의 보안 그룹 태그

시작하기 전에

- Cisco ISE 구축에서 Advantage 라이센스를 설치하고 활성화했는지 확인합니다.
- DNA 클라우드 에이전트는 Cisco DNA Cloud에 대한 아웃바운드 HTTPS 연결을 생성합니다. 따라서 네트워크에서 프록시를 사용하여 인터넷에 연결하는 경우 Cisco ISE 프록시 설정을 구성해야 합니다. Cisco ISE에서 프록시 설정을 구성하려면 **Administration** > **System** > **Settings** > **Proxy**
- Cisco ISE에서 Cisco pxGrid Cloud 포털로의 아웃바운드 연결을 위해 포트 443이 열려 있는지 확인합니다. 방화벽 또는 프록시 설정이 구성된 경우 다음 URL이 차단되지 않았는지 확인합니다.

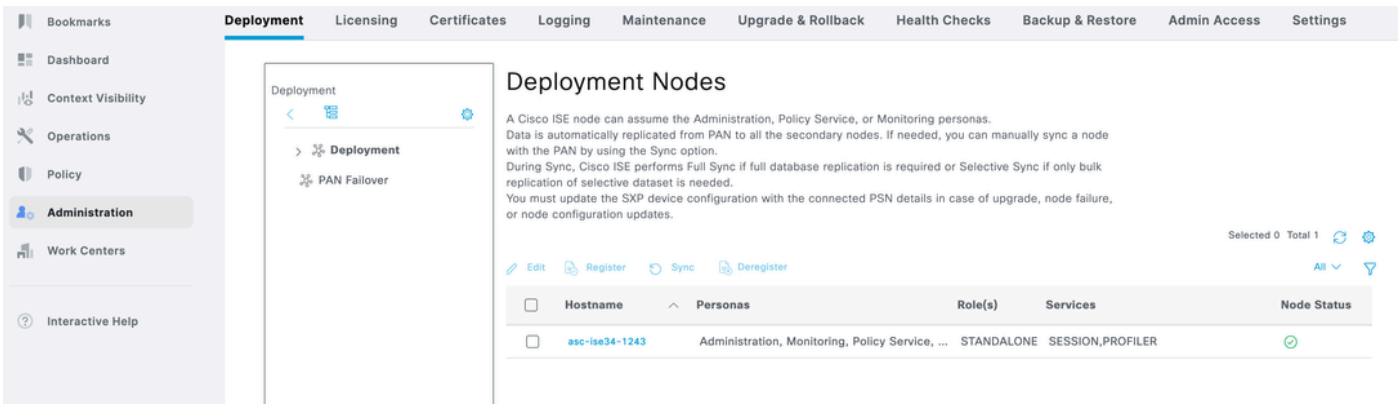
https://dna.cisco.com

https://security.cisco.com/

1단계: ISE에서 Pxgrid 클라우드 활성화

1 ISE GUI로 이동합니다.

2 Administration(관리) - Deployment(구축)를 클릭합니다.

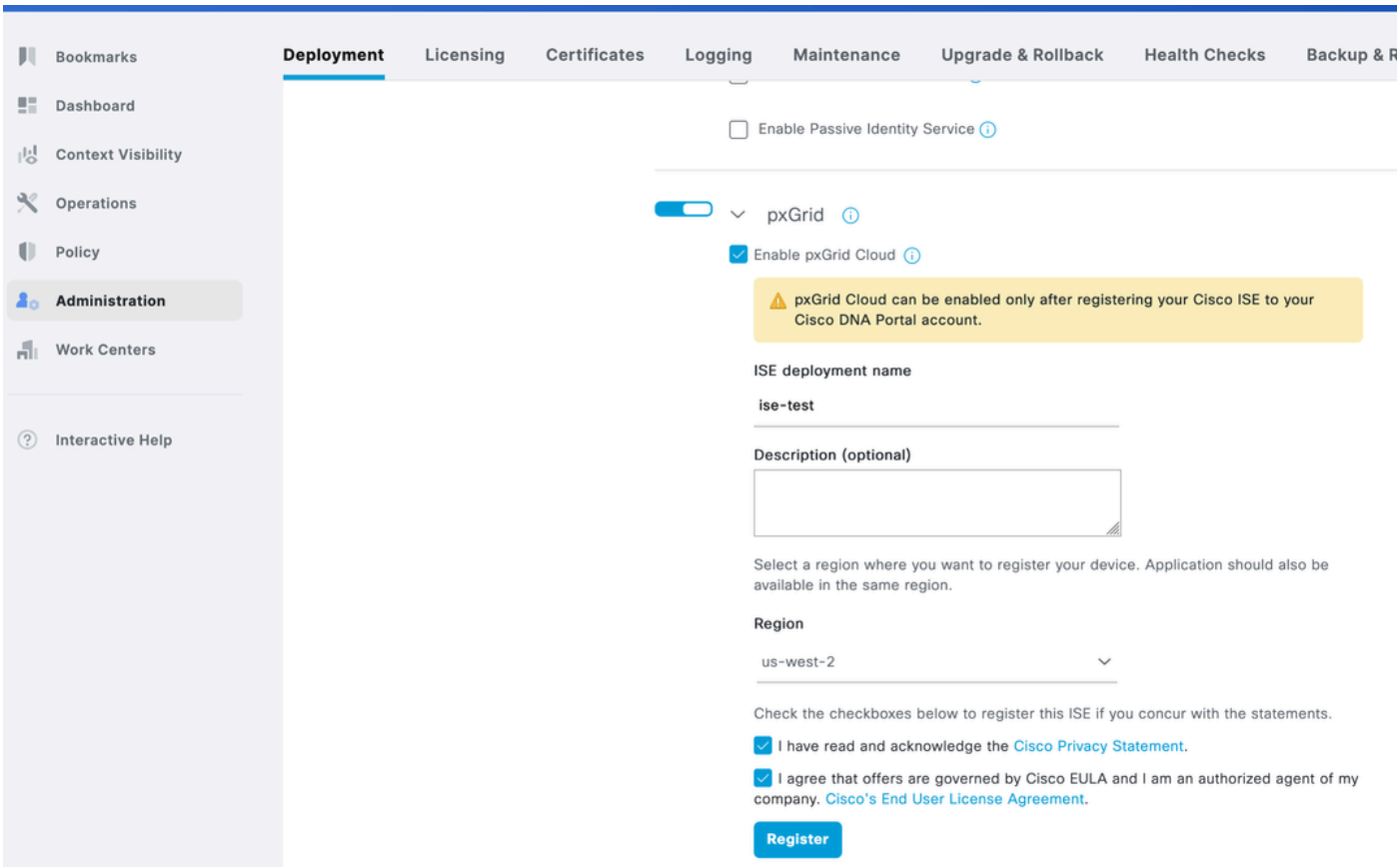


3 Node(노드)를 클릭하고 아래로 스크롤합니다.

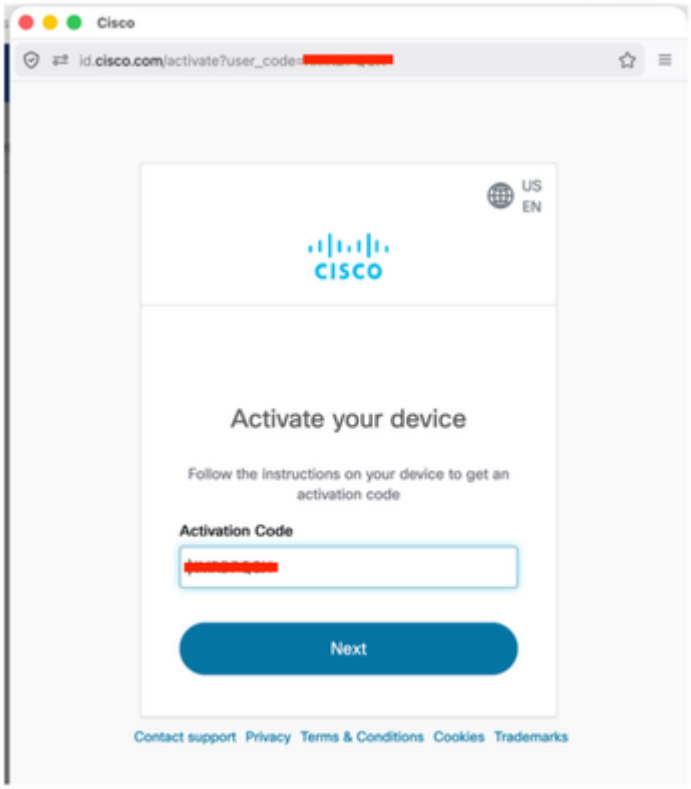
ISE 구축 이름 입력

현재 지원되는 유일한 지역인 미국 서부 2로 지역을 선택합니다.

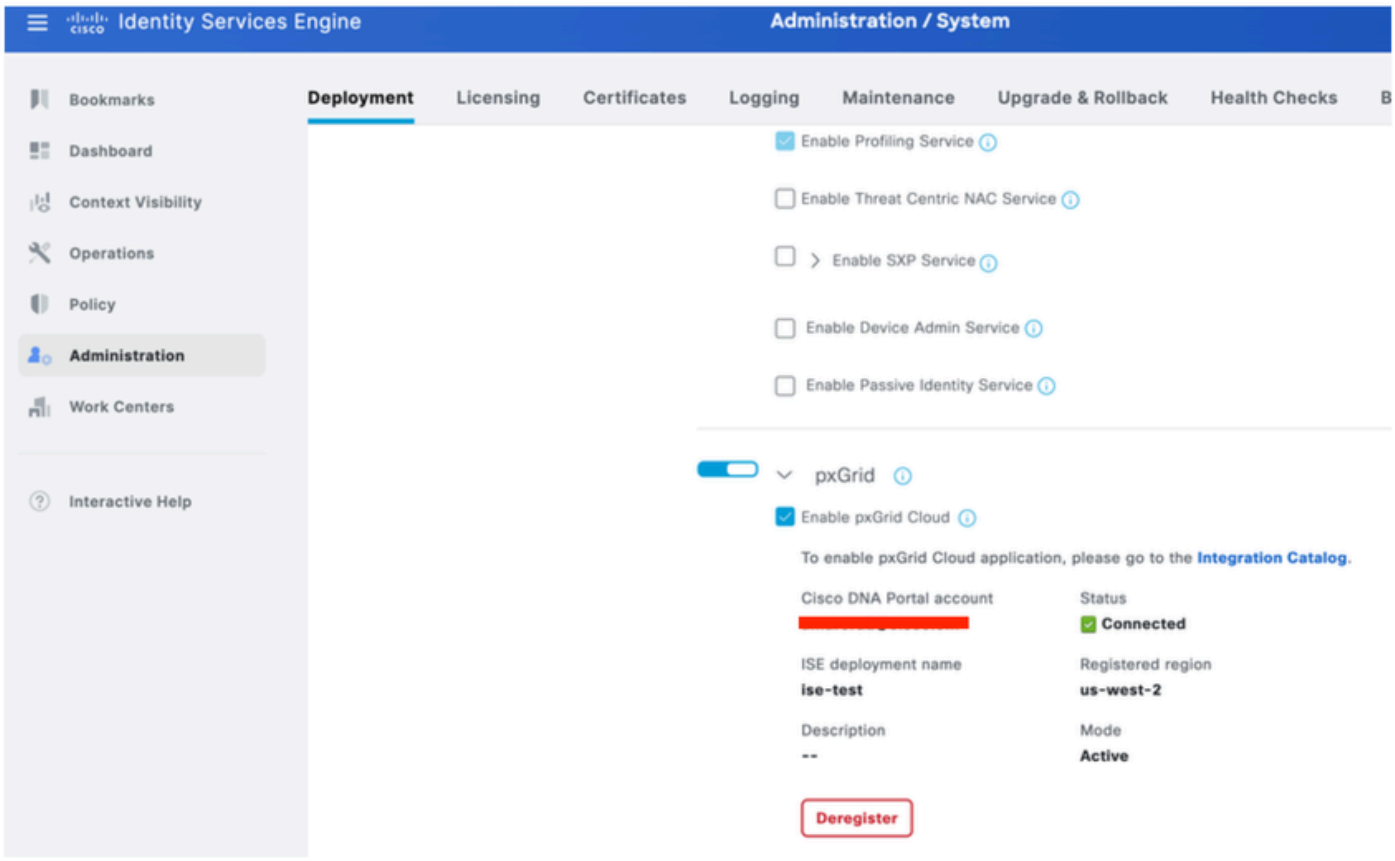
두 확인란을 모두 선택하고 Register(등록)를 클릭합니다.



4 Auto filled Activation Code(자동 활성화 코드)가 포함된 팝업이 표시됩니다.Next(다음)를 클릭합니다.



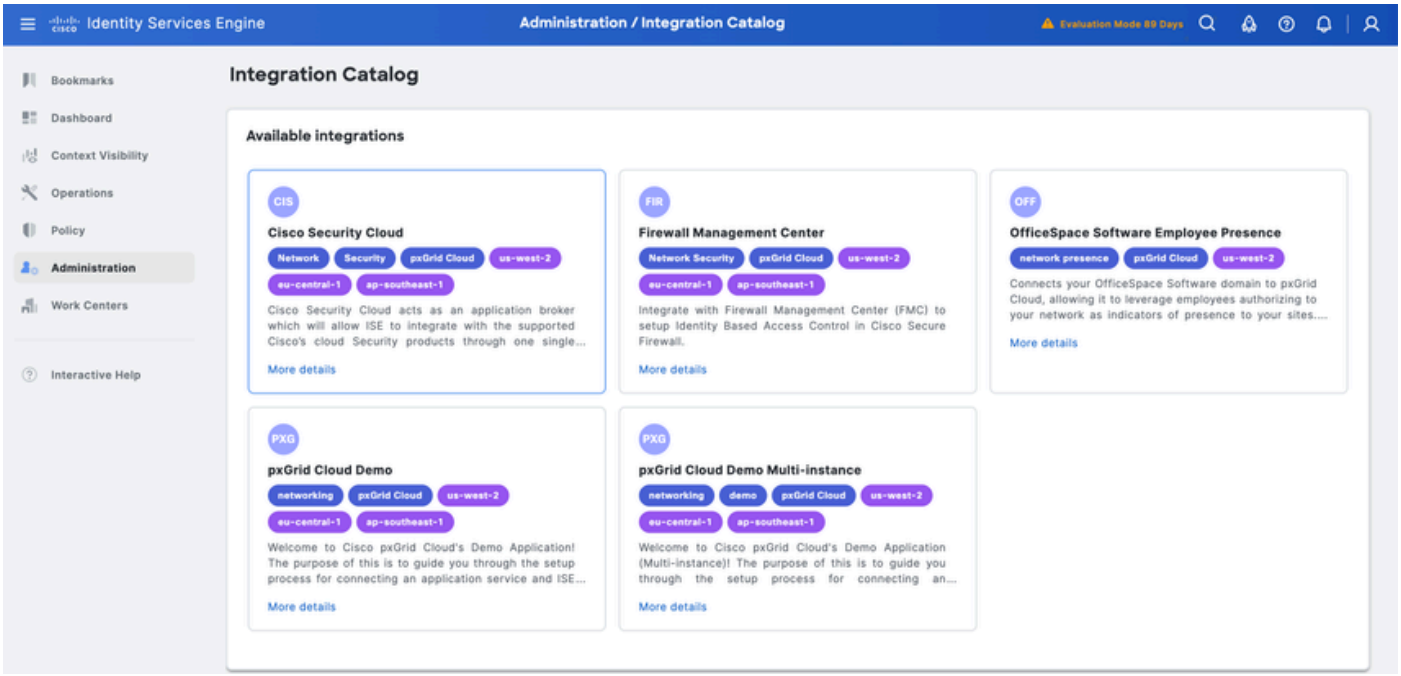
5 ISE는 Pxgrid 클라우드에 연결된 것을 보여줍니다.



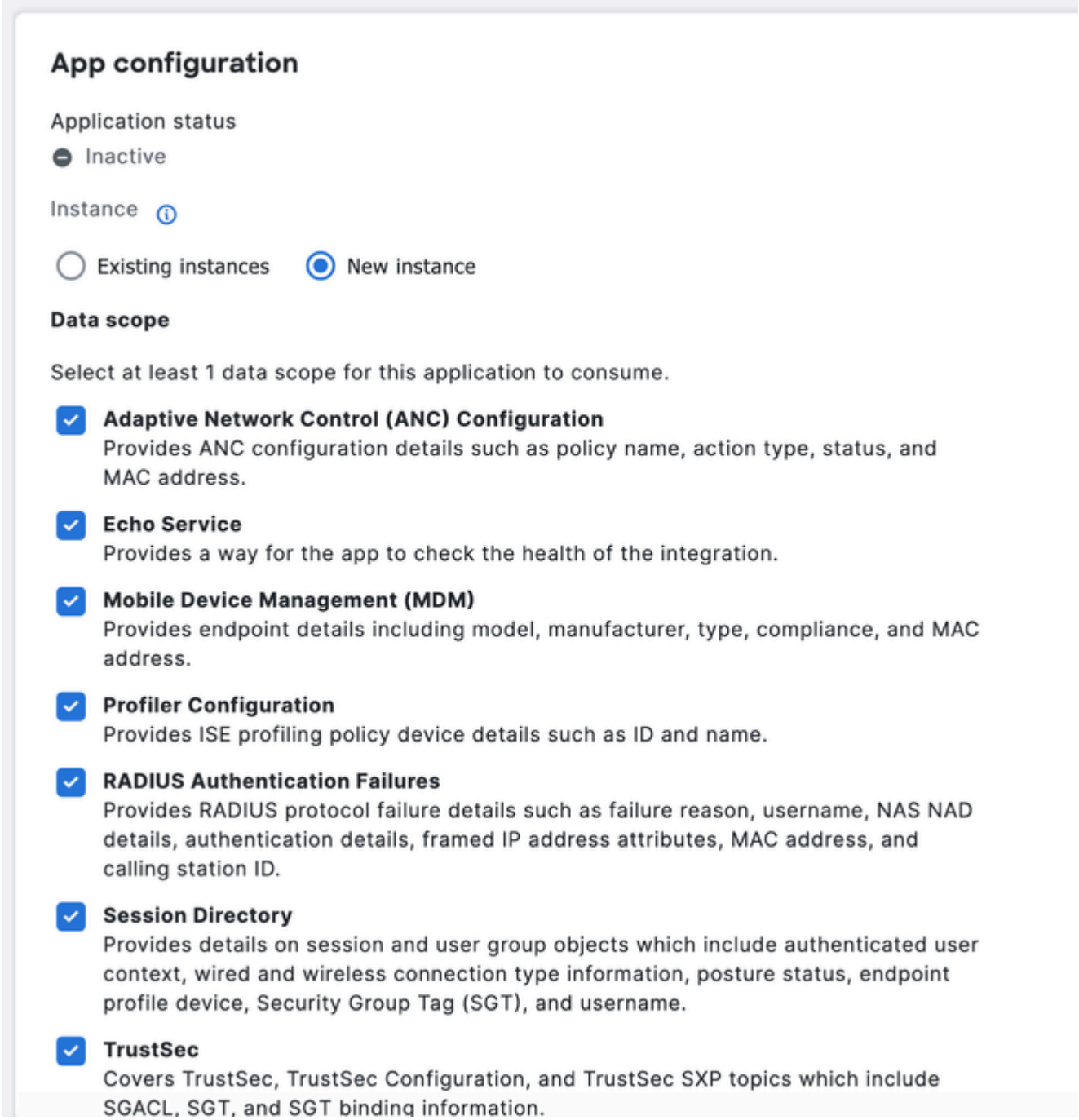
6 5단계에서 Integration Catalog(통합 카탈로그) 링크를 클릭합니다.

Available Integrations(사용 가능한 통합) 아래에서 Cisco Security Cloud를 클릭합니다.

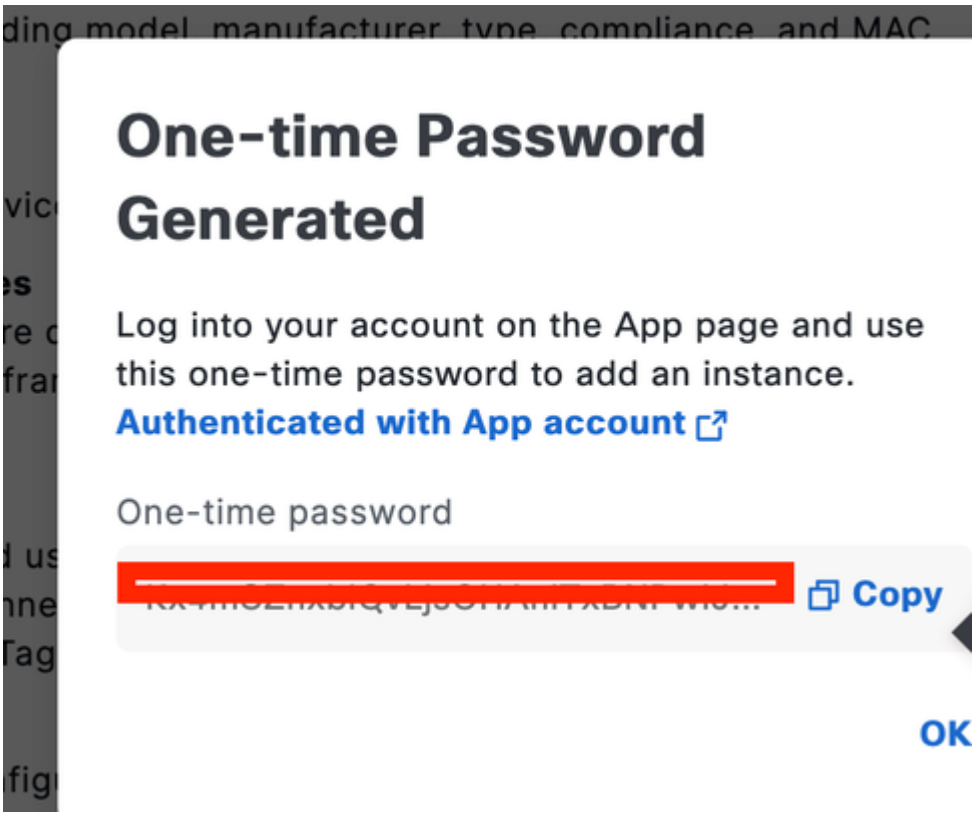
.



7 App Configuration(앱 구성)에서 New Instance(새 인스턴스)를 클릭하고 Activate(활성화)를 클릭합니다.

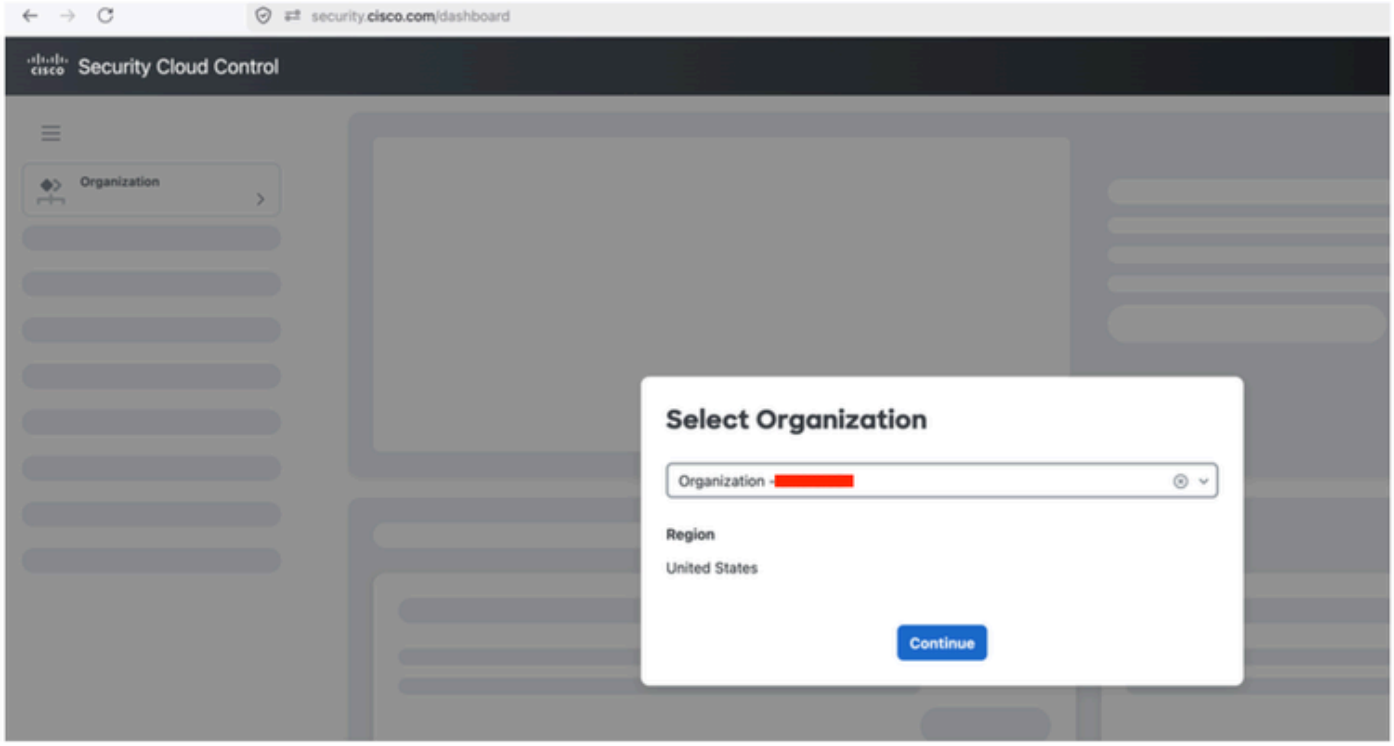


Cisco Secure Access에서 사용할 일회용 비밀번호를 복사합니다.

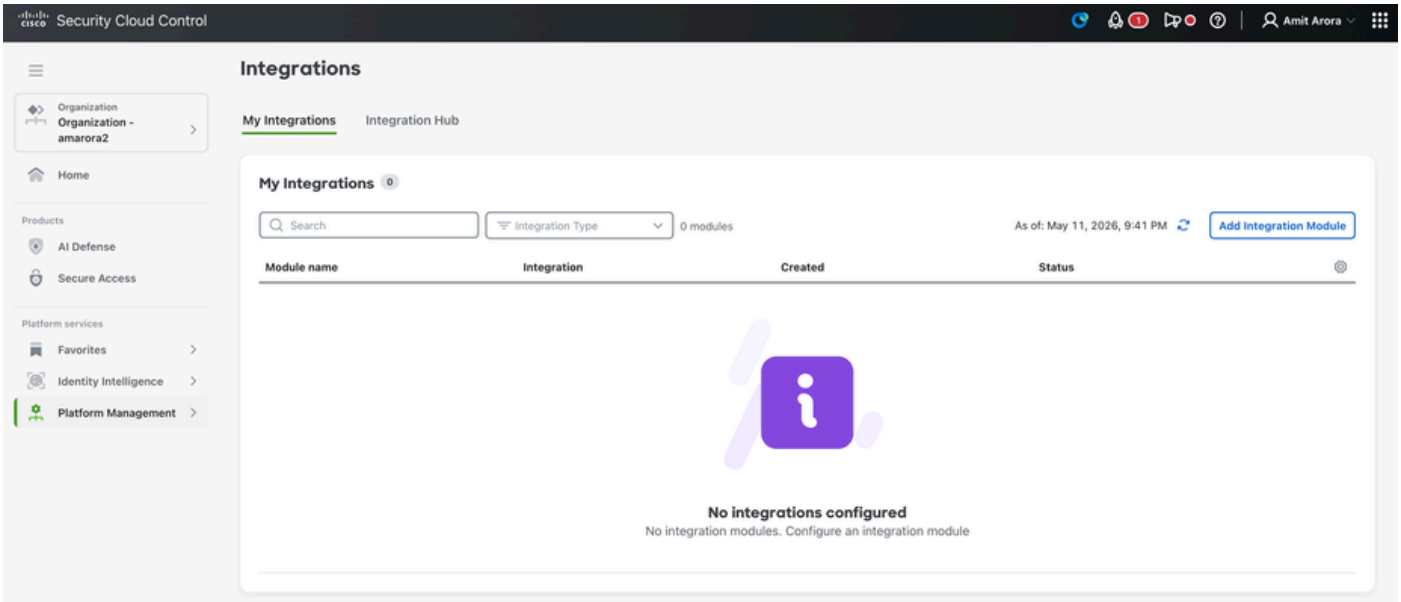


2단계: Cisco Secure Access를 ISE와 통합

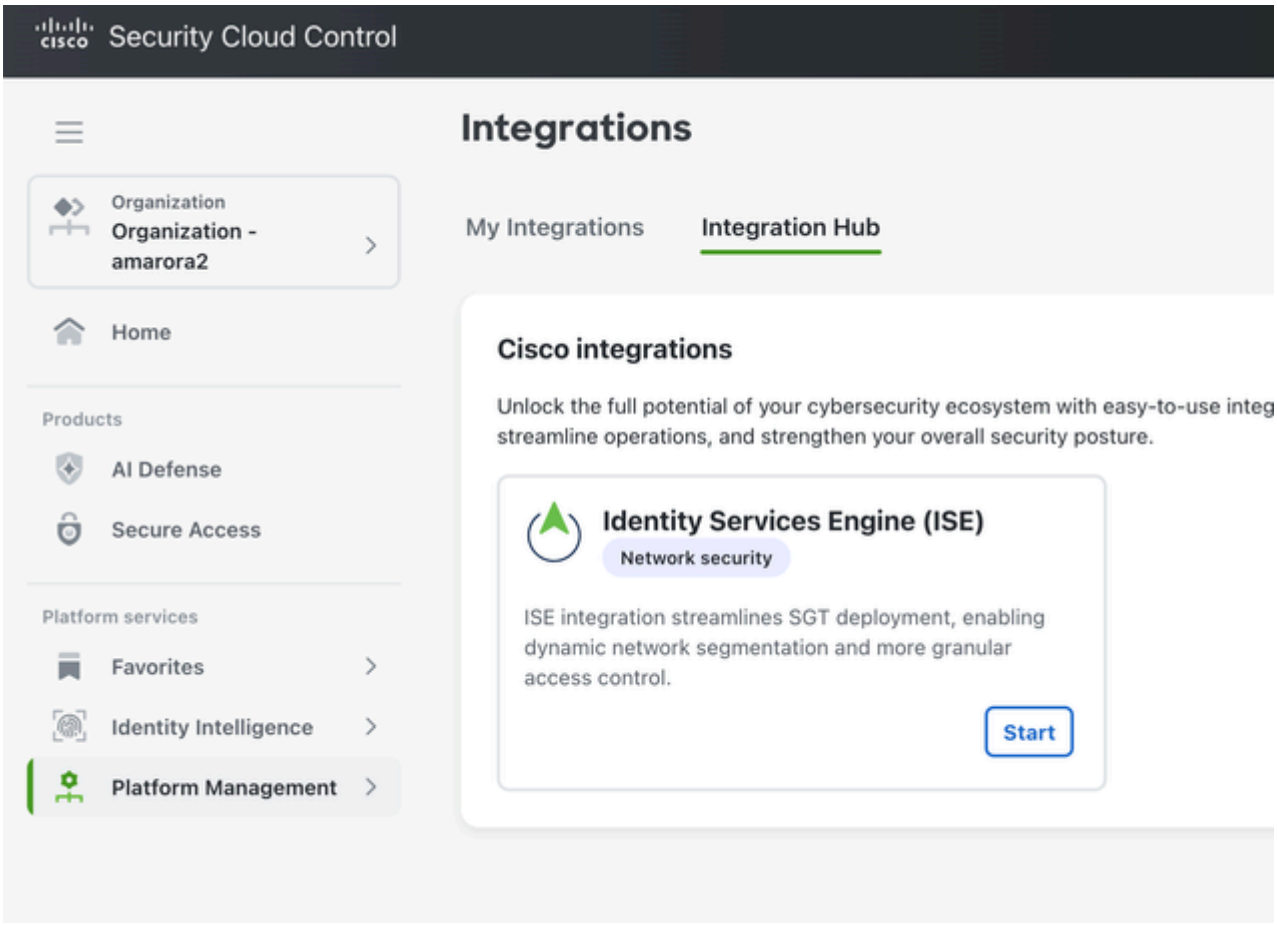
1. security.cisco.com에 로그인합니다.
2. Cisco Secure Access ORG 선택



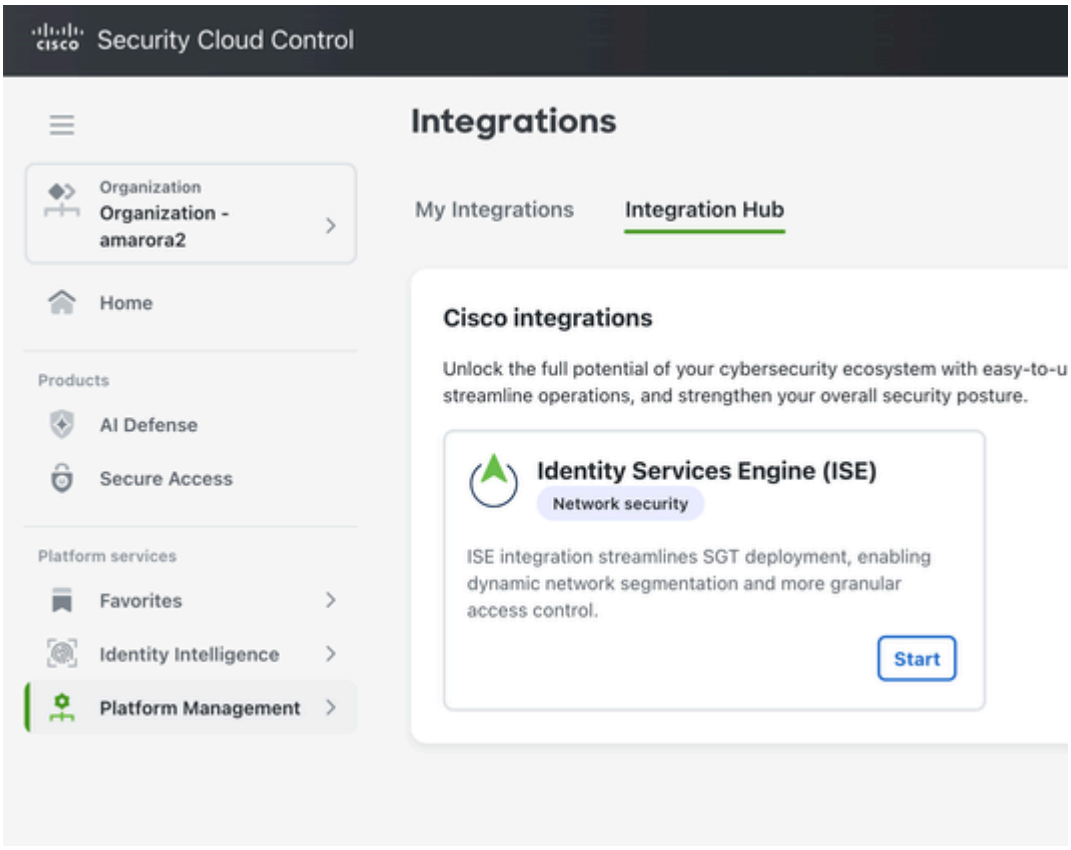
3 Platform Management - Platform Integrations를 클릭합니다.



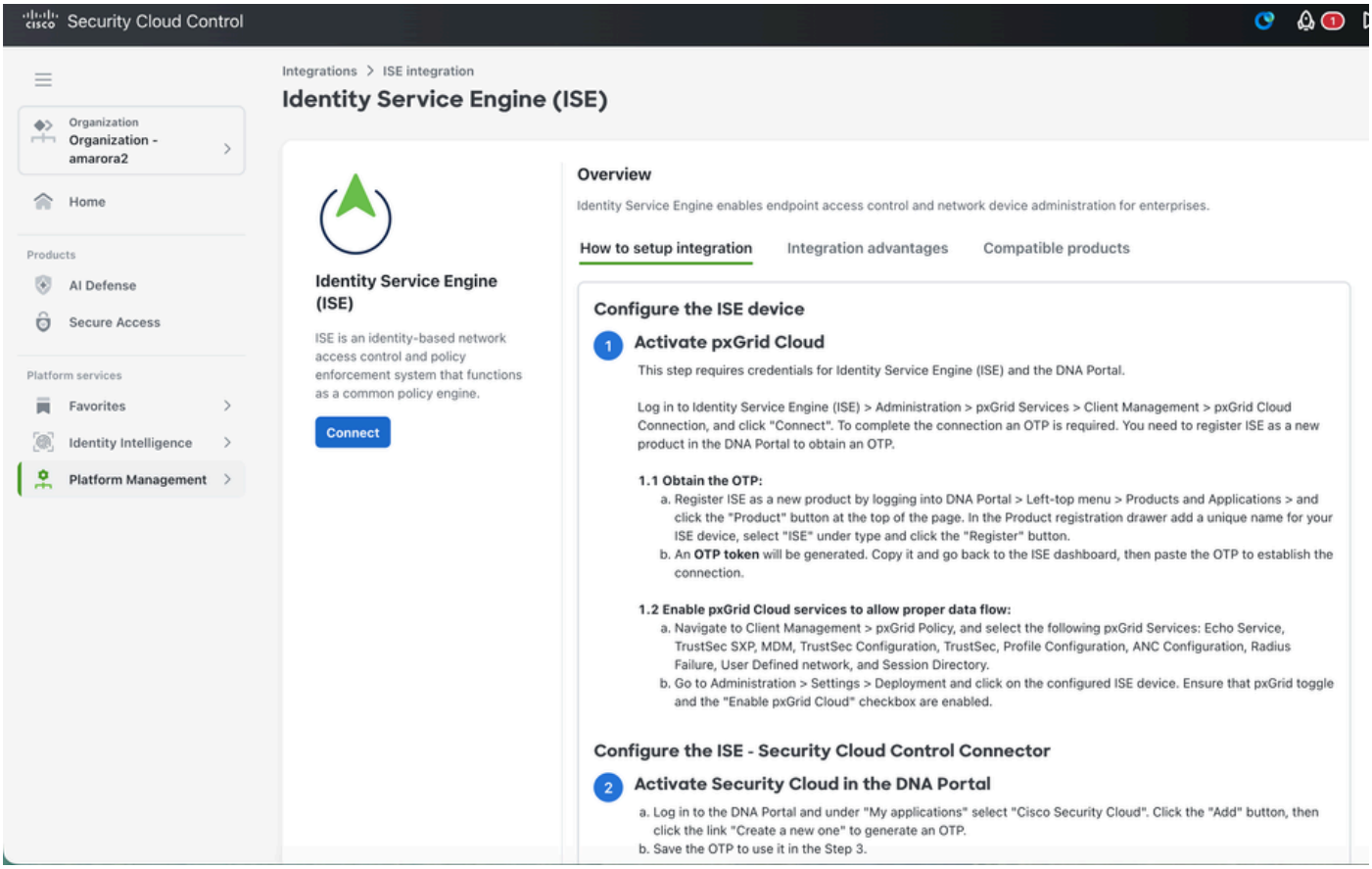
4 Add Integration Module(통합 모듈 추가) 클릭



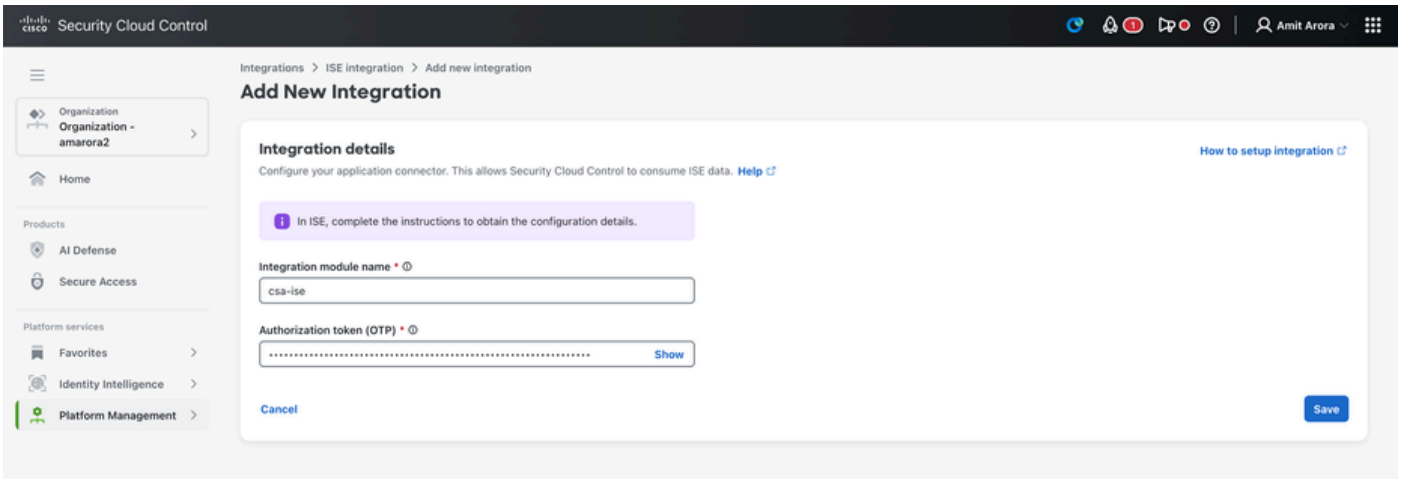
5 Start(시작) 클릭



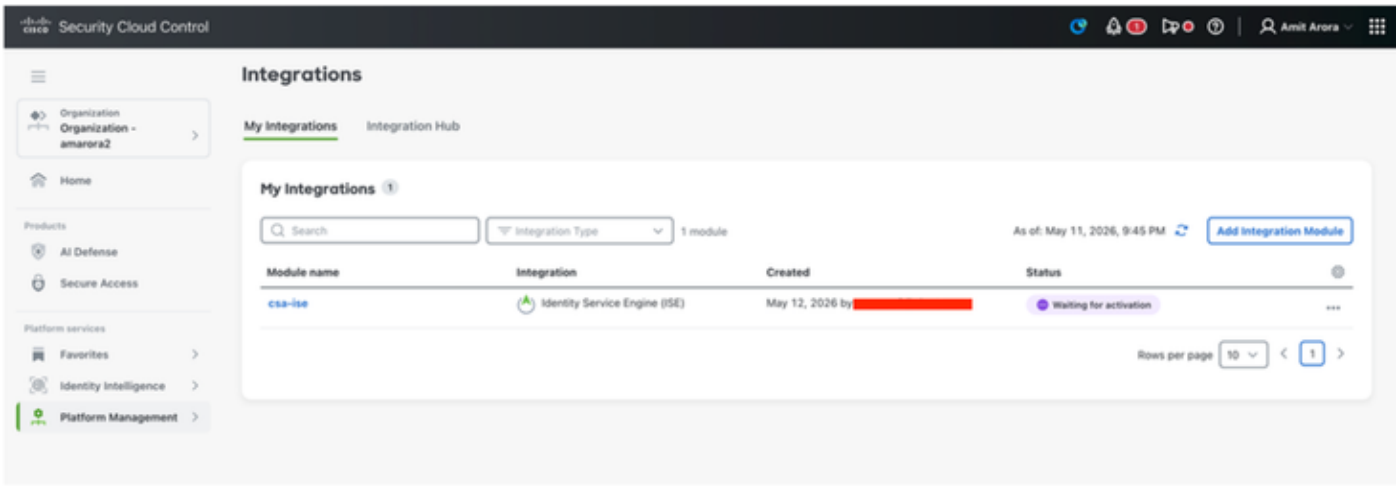
6 Connect(연결) 클릭



7. Cisco ISE에서 통합 모듈 이름과 OTP를 입력하고 Save(저장)를 클릭합니다



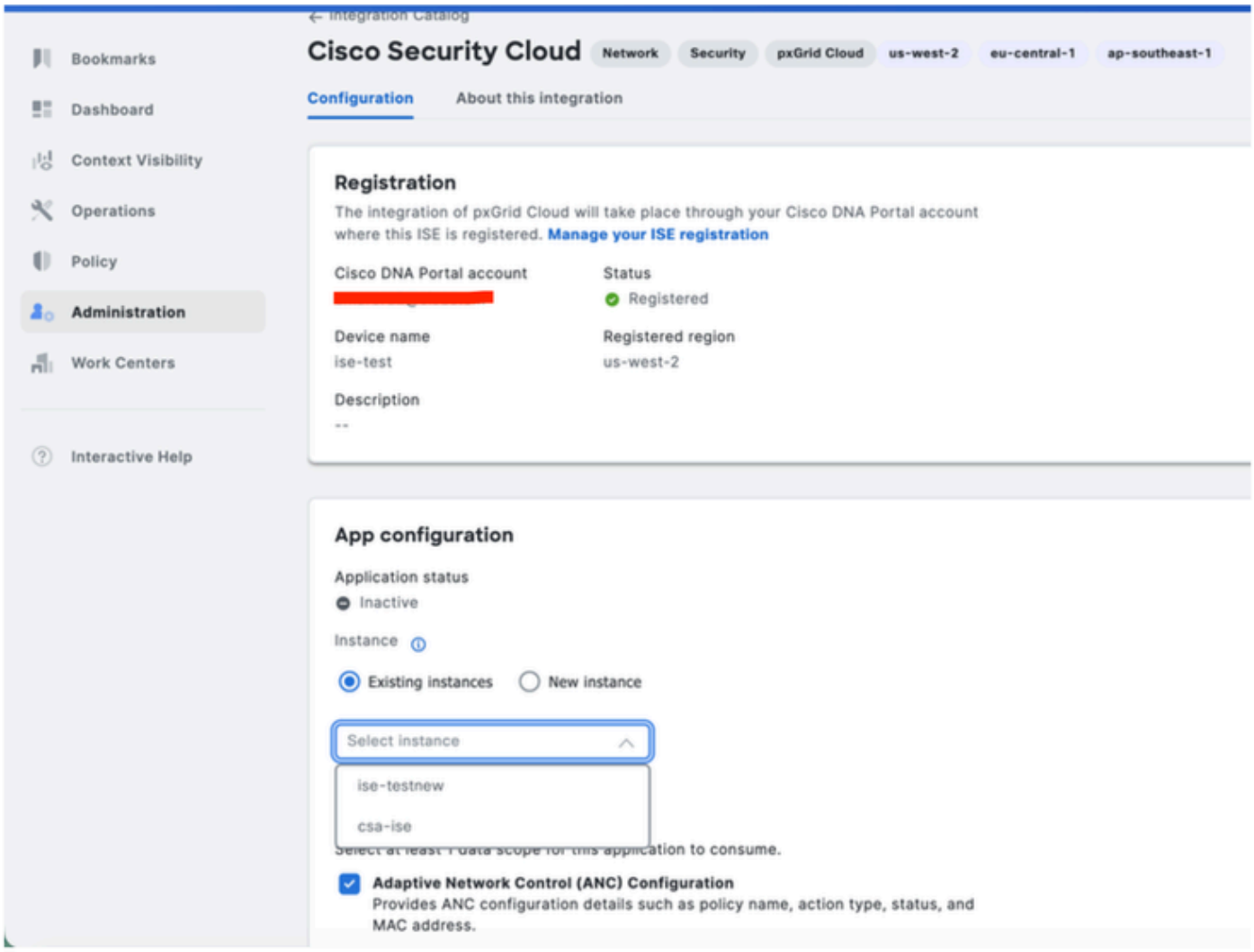
8 Save(저장)를 클릭하면 Waiting for Activation Status(활성화 상태 대기 중)가 표시됩니다.



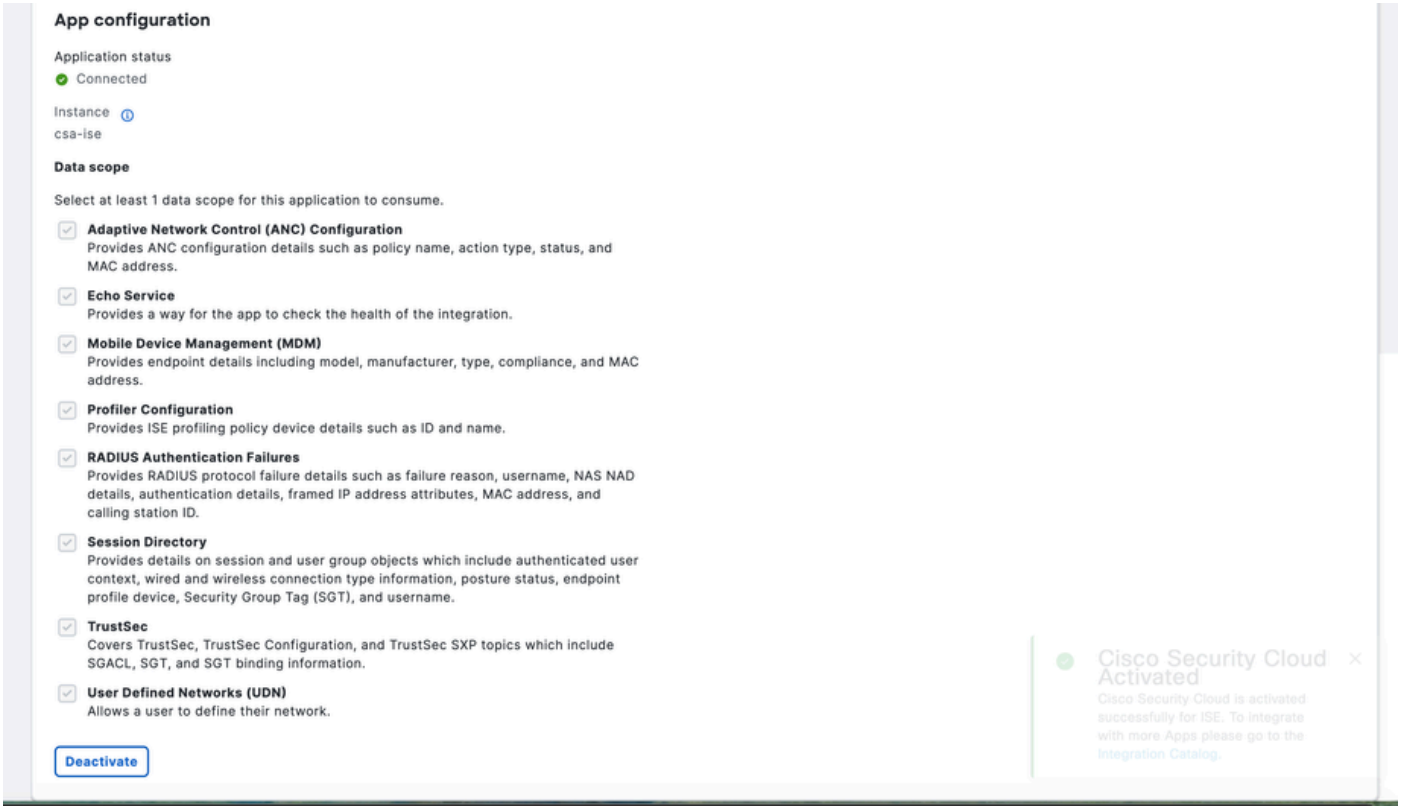
9 ISE에 로그인하고 Administration(관리) - Deployment(구축)로 이동합니다. pxgrid 페르소나가 있는 노드를 클릭하고 Pxgrid Connection(Pxgrid 연결) 아래의 Integration cloud(통합 클라우드)를 클릭합니다.

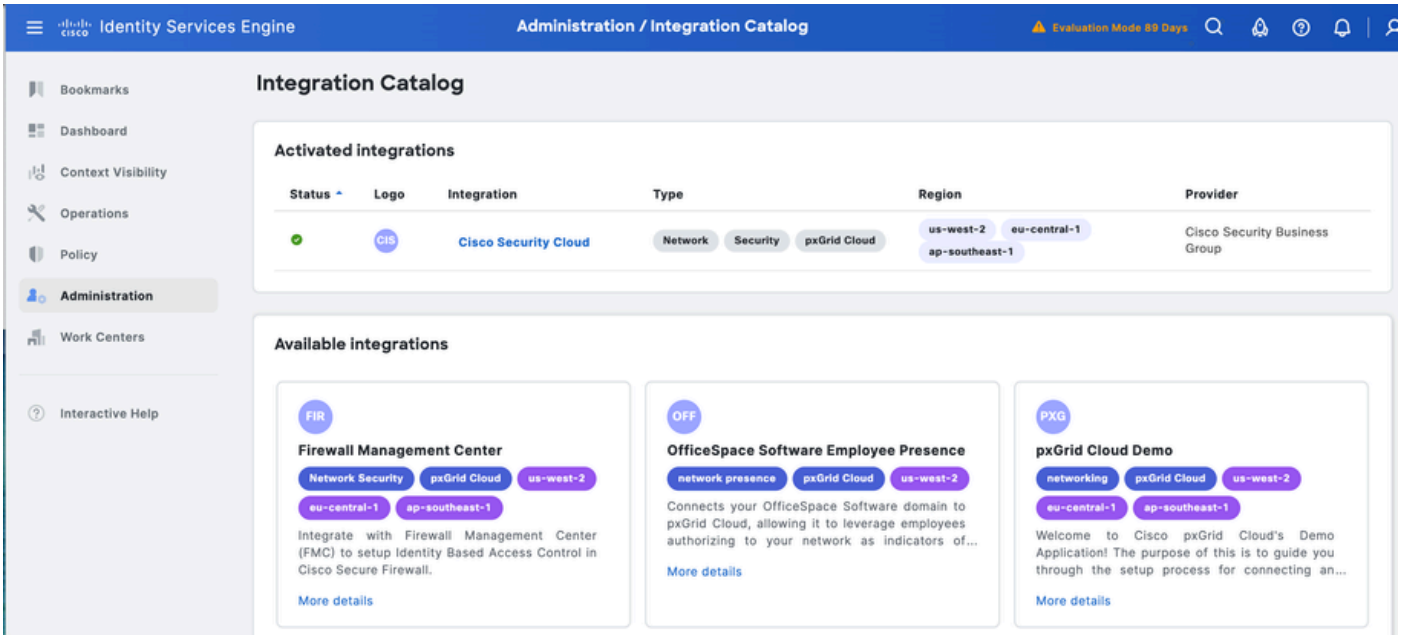
App configuration(앱 컨피그레이션) 아래에서 Security Cloud Control(보안 클라우드 제어)에서 생

성된 ISE 인스턴스를 선택하고 Activate(활성화)를 클릭합니다



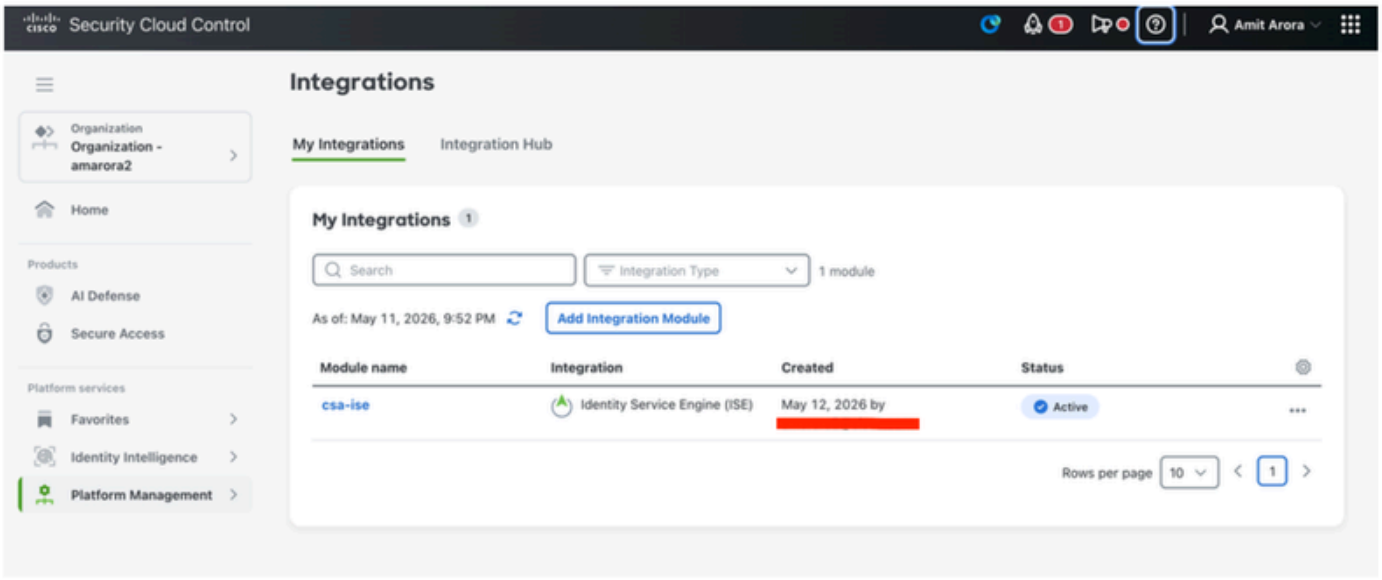
10 Application Status(애플리케이션 상태)가 이제 연결되었습니다.





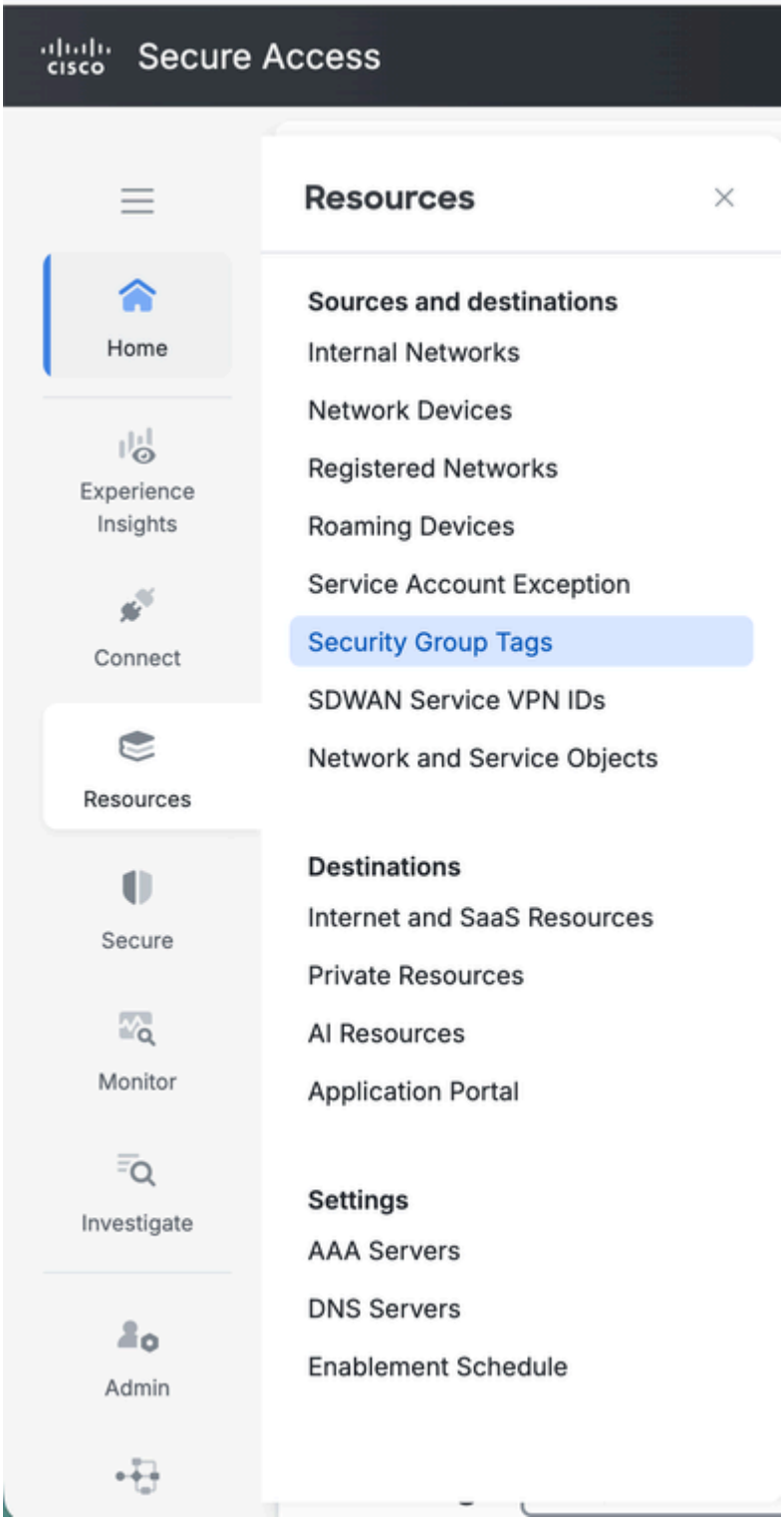
11 보안 클라우드 제어에 로그인 - security.cisco.com

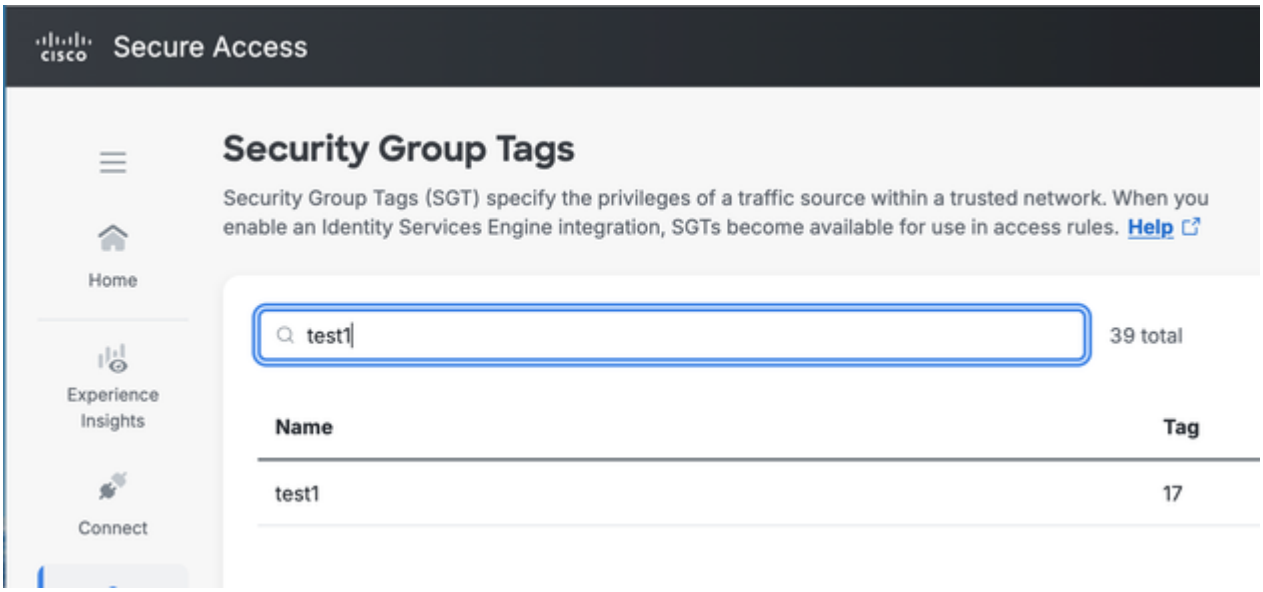
Platform Management - Platform Integrations 아래에서 통합 상태를 Active로 볼 수 있습니다.



보안 그룹 태그 확인:

Cisco Secure Access에 로그인합니다. Resources - Security Group Tags(리소스 - 보안 그룹 태그)로 이동합니다.


Secure Access
Home
Experience Insights
Connect
Resources
Secure
Monitor
Investigate
Admin
Resources
Sources and destinations
Internal Networks
Network Devices
Registered Networks
Roaming Devices
Service Account Exception
Security Group Tags
SDWAN Service VPN IDs
Network and Service Objects
Destinations
Internet and SaaS Resources
Private Resources
AI Resources
Application Portal
Settings
AAA Servers
DNS Servers
Enablement Schedule



Cisco TAC에 필요한 정보

ISE:
Pxgrid 페르소나가 있는 ISE 노드에서 다음 구성 요소가 디버그 레벨로 설정된 ISE 지원 번들을 수집하는 방법:

pxgrid

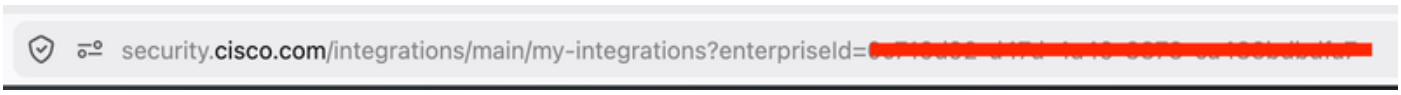
인프라

ERS

디버그 레벨의 hermes 구성 요소입니다.

SCC:

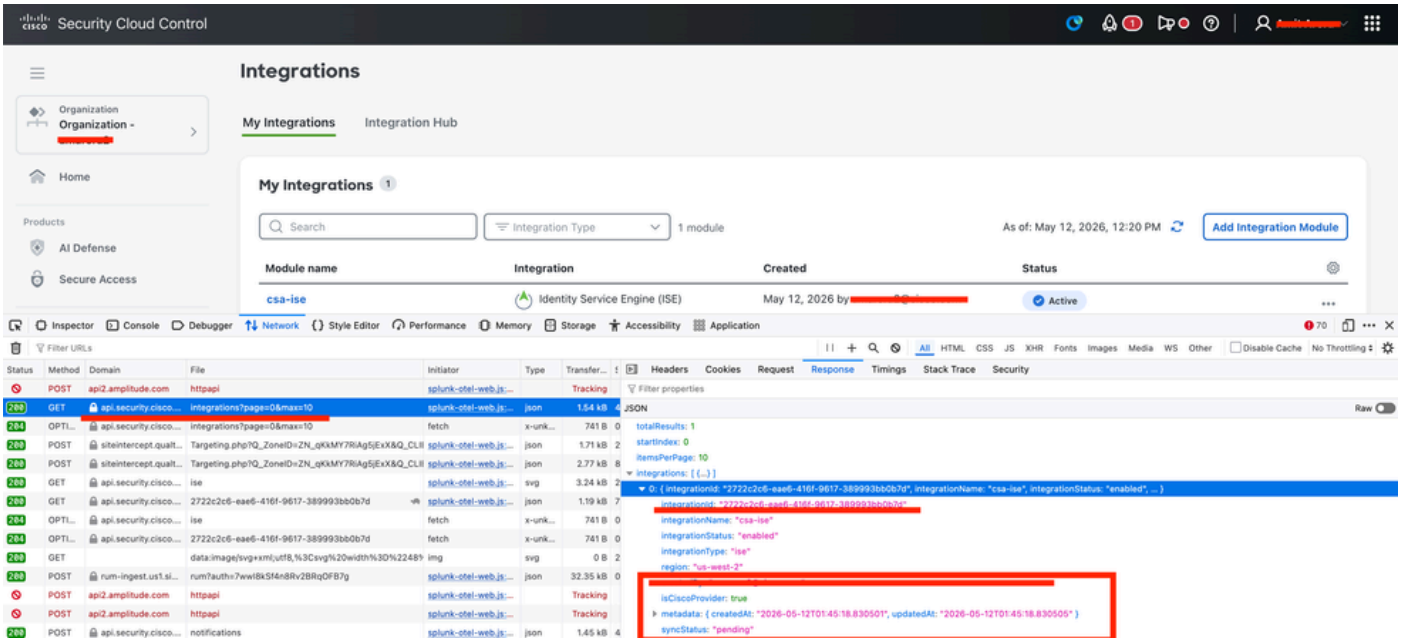
엔터프라이즈 ID: security.cisco.com의 URL에서



통합 ID.
HAR 캡처 시작

Security.cisco.com에 로그인합니다.
Platform Management - Platform Integrations(플랫폼 관리 - 플랫폼 통합)로 이동합니다.

통합 검색—페이지 api 호출 및 응답 탭에서 통합 ID를 찾을 수 있습니다.



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.