오케스트레이션을 통해 ISE와 SecureX 온프레미스 통합

목차

소개

이 문서에서는 오케스트레이션을 통해 Identity Services Engine 및 SecureX를 Cisco Secure GitHub의 워크플로와 통합하는 단계를 설명합니다.

사전 요구 사항

Cisco에서는 다음 항목에 대해 알고 있는 것이 좋습니다.

- Cisco ISE 구성 경험
- ISE API에 대한 지식
- SecureX 오케스트레이션에 대한 지식

요구 사항

네트워크에 Cisco ISE가 구축되어 있고 활성 SecureX 계정이 있어야 합니다. 오케스트레이션 워크플로는 SecureX 브라우저 확장을 통해 트리거됩니다.

이 예에서는 사용할 워크플로를 Cisco Secure GitHub 페이지에서 가져왔으며, 이 절차는 사용자 지정 워크플로에도 적용됩니다.

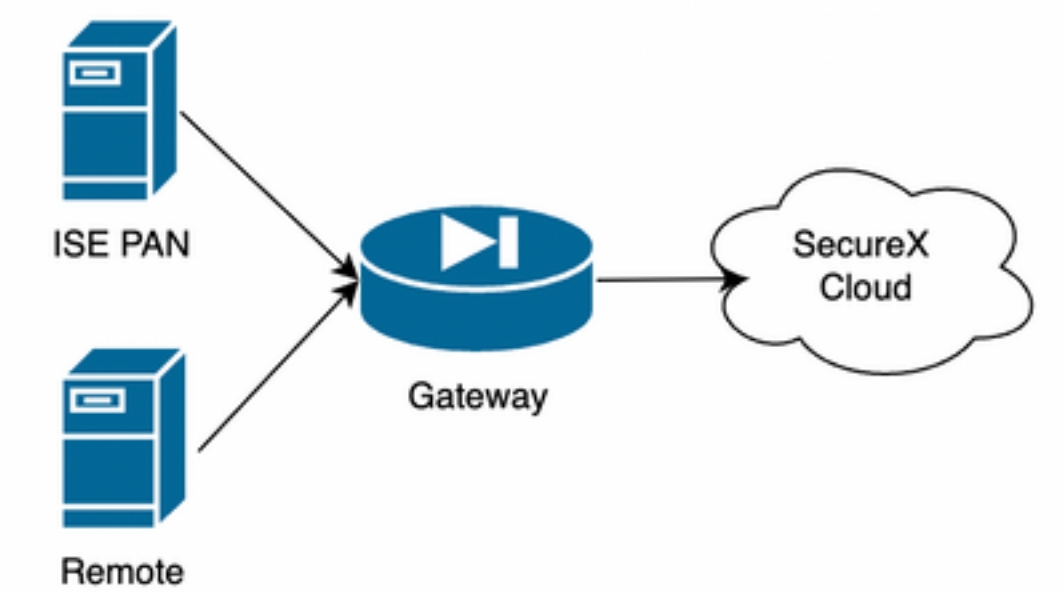
사용되는 구성 요소

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.

- Identity Services Engine ISE 버전 3.1
- SecureX 계정
- SXO Remote 디바이스 버전 1.7

구성

네트워크 다이어그램



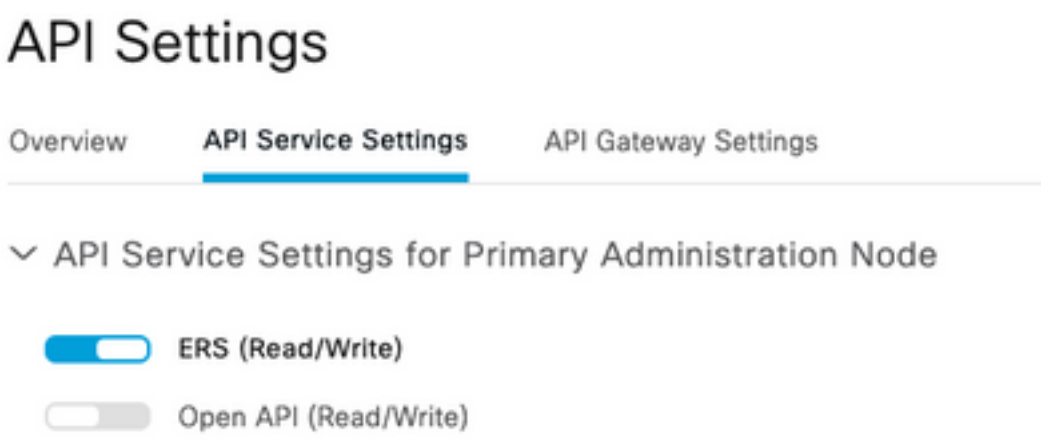
이 예에서 ISE PAN 및 원격 서버는 직접 연결을 위해 동일한 서브넷에 배치됩니다.

ISE는 온프레미스 디바이스이므로 원격 서버가 Secure-X 클라우드에 연결되어 ISE PAN에 정보를 전달합니다

설정

ISE PAN 컨피그레이션

1. **Administration(관리) > System(시스템) > Settings(설정) > API Settings(API 설정) >API Service Settings(API 서비스 설정)로** 이동하여 **ERS(Read/Write)를 활성화합니다**

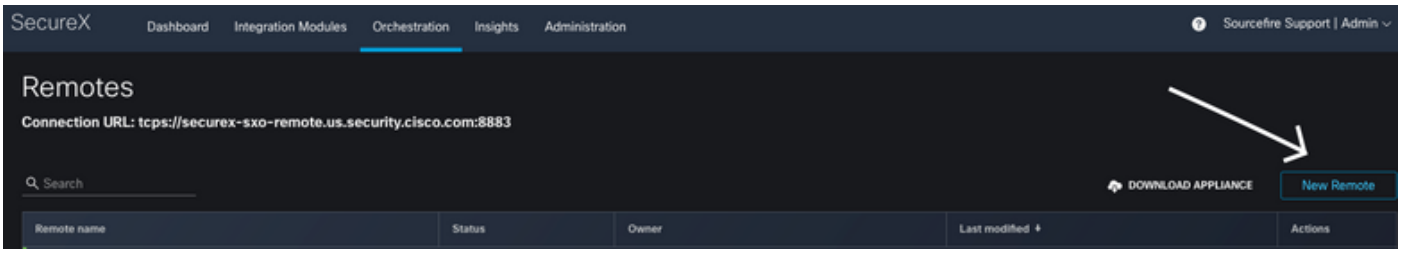


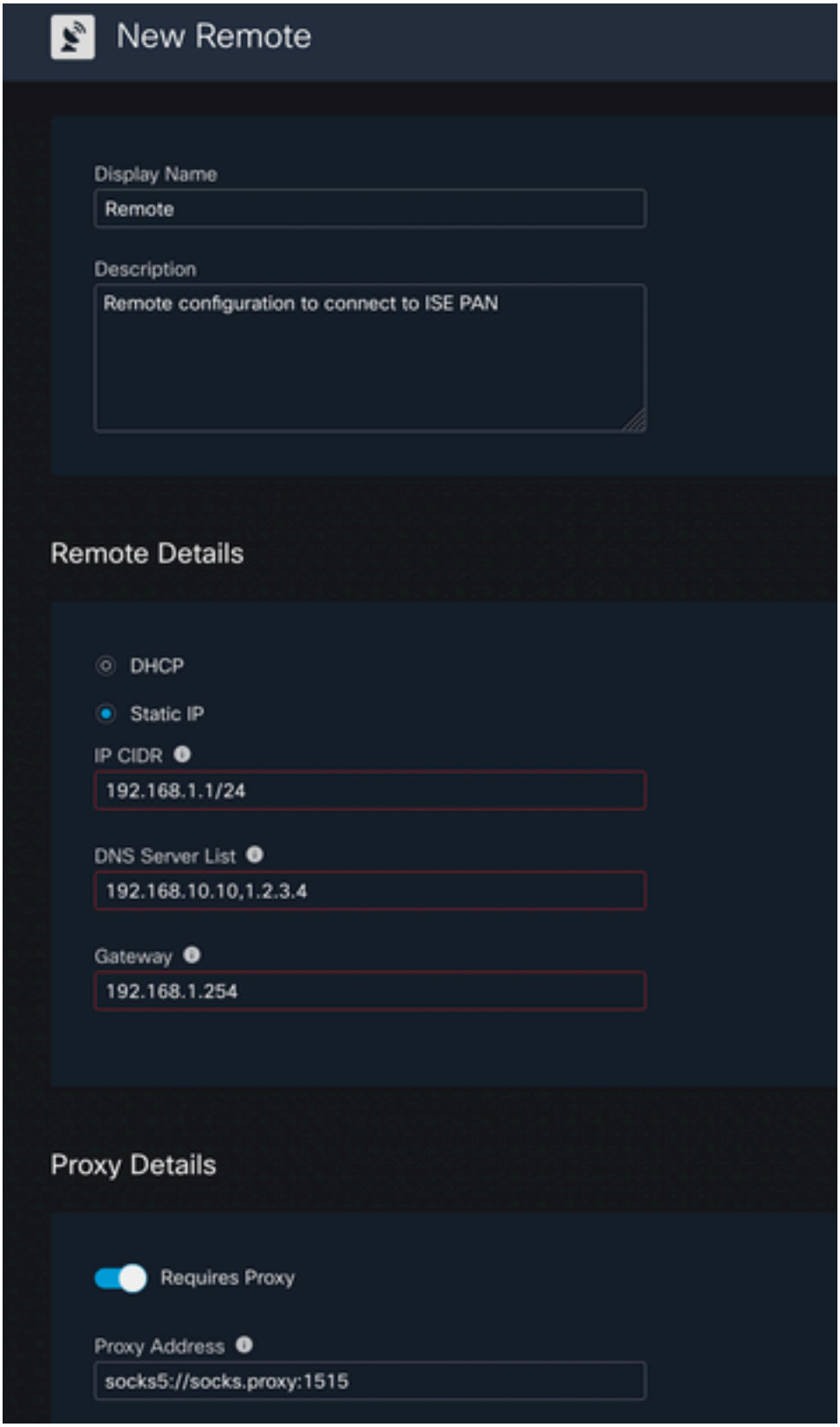
2 . (선택 사항) Secure-X 연결을 위한 새 사용자를 만들고, **Administration(관리) > System(시스템) > Admin Access(관리자 액세스) > Administrator(관리자) > Admin Users(관리자 사용자)로** 이동하여 새 사용자를 만듭니다. 이 새 사용자는 "ERS Admin" 권한이 있어야 합니다. 그렇지 않으면 수퍼 관리자 사용자일 수 있습니다.

원격 서버 구성 및 구축

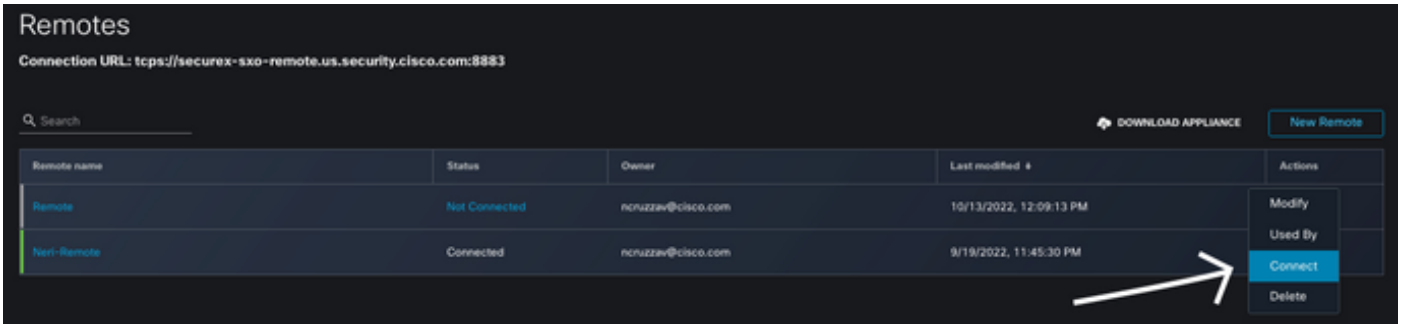
1. 원격 서버를 구성합니다. Secure-X 콘솔에서 **Orchestration(오케스트레이션) > Admin(관리) > Remote Configuration(원격 컨피그레이션)으로 이동하고 New Remote(새 원격) 옵션**을 선택합니다 . IP 주소 정보는 VM을 생성할 때 사용할 것이며 ISE PAN이 구축된 서브넷에 있어야 합니다.

> **참고:** 프록시를 통해 클라우드에 연결하는 경우, 현재 이를 위해 SOCKS5 프록시만 지원됩니다.

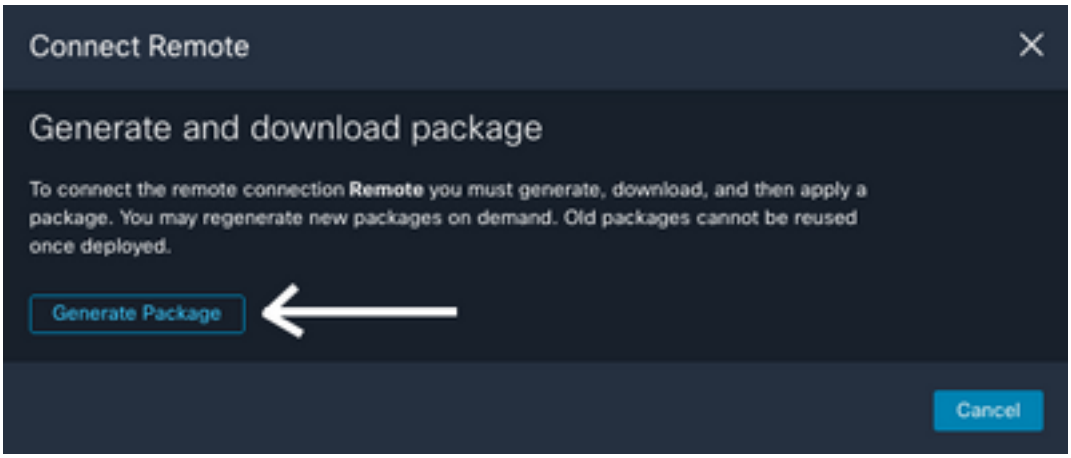




2. VM 구축에 사용할 구성된 설정을 다운로드합니다. 정보가 저장되면 리모콘이 "**연결되지 않음**"으로 표시되고, 작업 아래에서 탐색하고 연결을 **선택합니다**



Generate **Package(패키지 생성)를** 선택하면 이 작업은 VM을 배포할 때 사용하도록 구성된 정보가 포함된 .zip 파일을 다운로드합니다.



3. VM을 다운로드하고 설치합니다. **새 원격** 선택 **어플라이언스 다운로드** 이 작업은 원격 서버 배포에 사용해야 하는 OVA 이미지를 다운로드합니다.

원격 VM 사양은 SecureX Remote Setup Guide를 참조하십시오

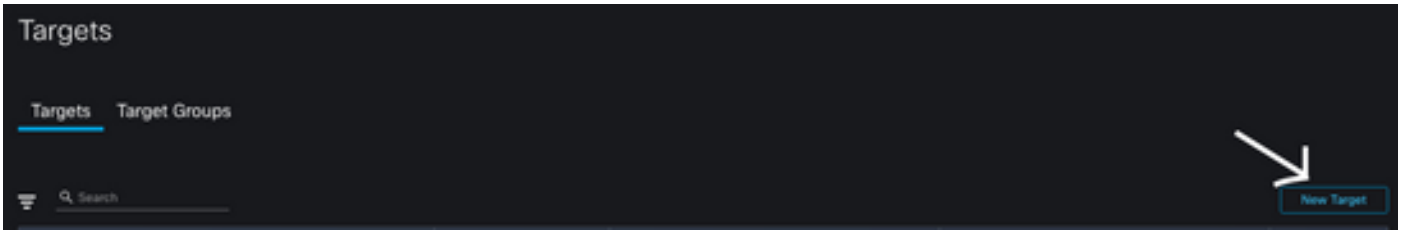
VM이 생성될 때 ZIP 파일 내의 다운로드된 정보를 인코딩된 **사용자 데이터**에서 사용해야 합니다. 이렇게 하면 구성된 원격 정보가 서버가 부팅된 후 서버에 채워집니다.

4. VM이 가동되면 SecureX 계정에 자동으로 연결하여 연결이 가동 중임을 확인합니다. 원격 구성에서 상태가 **"연결됨"**으로 변경되는 것을 확인해야 합니다.

SecureX에서 대상 구성

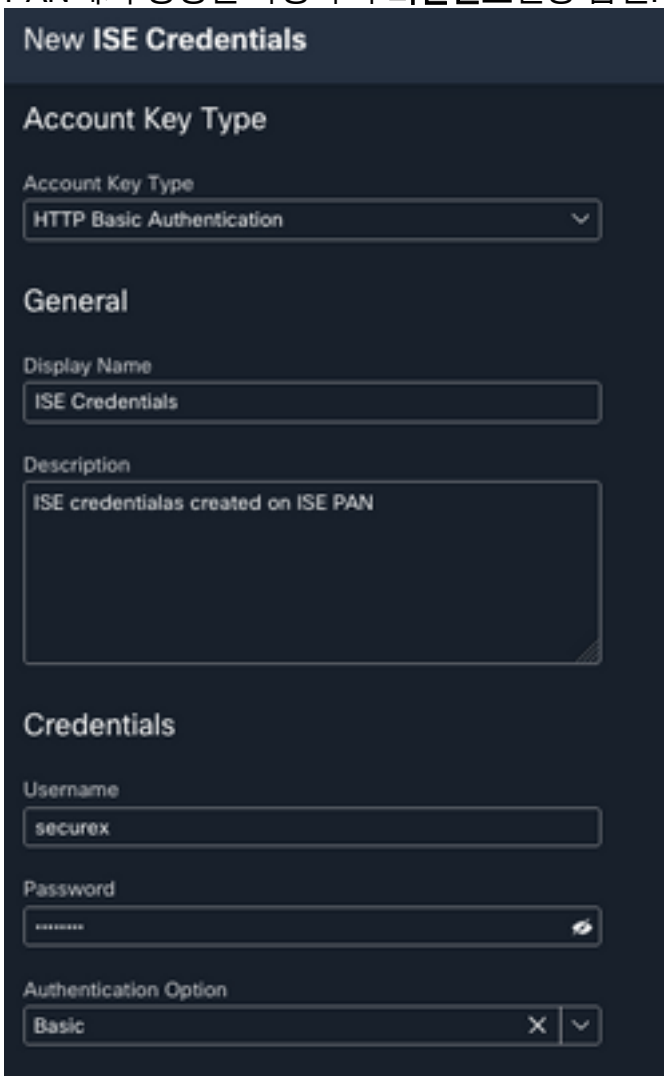
오케스트레이션이 **대상** 구성 시 장치와 함께 작동하는 것이 중요하므로 Secure X는 이 대상을 사용하여 API 호출을 전송하고 오케스트레이션을 통해 장치와 상호 작용합니다

1. Orchestration(오케스트레이션) **> Targets(대상) > New Target(새 대상)으로 이동합니다**

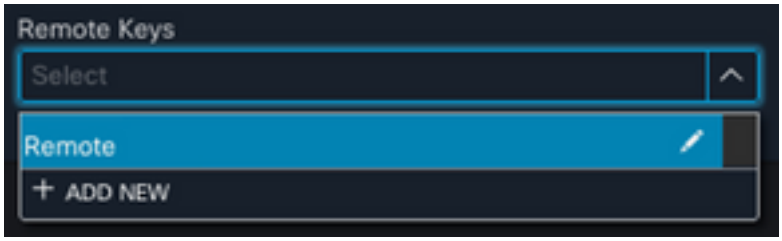


2. 대상 정보에 다음 지침을 입력합니다

- 표시 이름: 대상 식별자
- 설명: 대상의 목적을 식별하는 간단한 설명
- 계정 키: 여기서 API를 통해 ISE에 액세스하려면 사용자/비밀번호를 구성해야 합니다 계정 키 없음: **거짓**기본 계정 키: Add **New(새로 추가)를 선택합니다.** 계정 키 유형: **HTTP 기본 인증**표시 이름: 계정 키 식별자사용자 이름: ISE PAN에서 **ERS 관리자**로 만든 사용자암호: ISE PAN에서 생성된 사용자의 **비밀번호**인증 옵션: **기본**

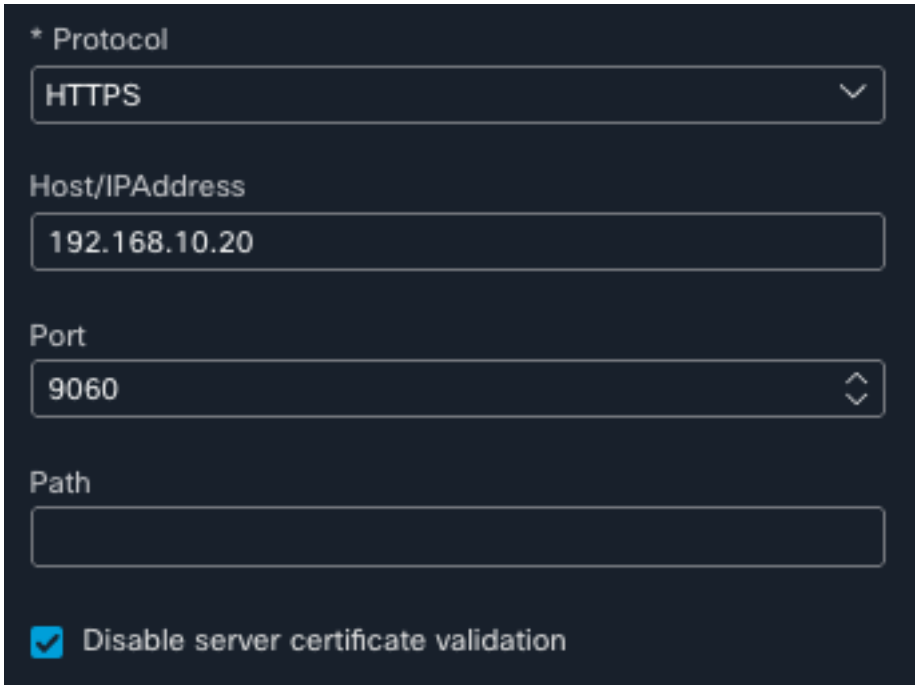


- 원격: 여기서 이전에 구성한 원격 연결을 선택해야 합니다
  원격 키: 드롭다운 메뉴에서 리모컨을 선택합니다.



- HTTP: 여기서 **ISE** PAN에 대한 API 정보를 구성해야 **합니다** 프로토콜: **HTTPS**호스트/IP 주소: **ISE PAN 프라이빗 IP**포트: **9060**경로: 비워 두십시오.서버 인증서 유효성 검사를 비활성화합니

다. **이 확인란을 선택합니다.**



- 프록시: 프록시 컨피그레이션이 원격 컨피그레이션에 포함되었으므로 이 섹션을 비워 둘 수 있습니다
- 제출을 **선택합니다**

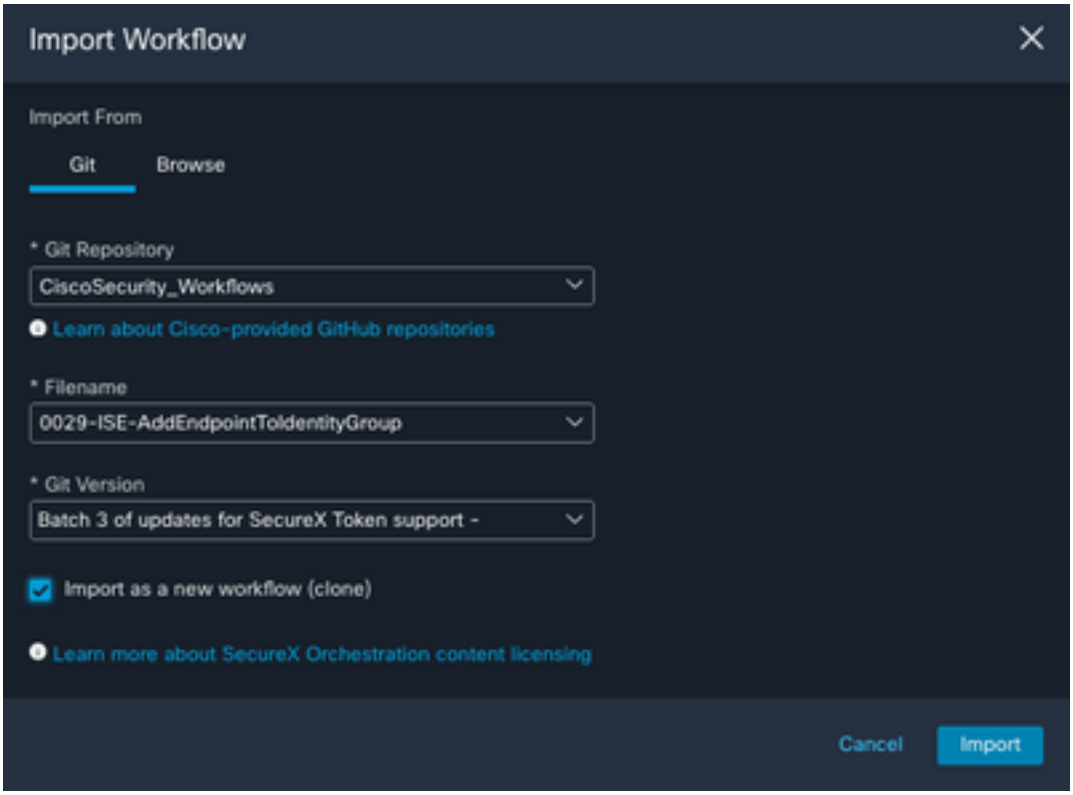
Cisco Secure GitHub에서 워크플로 가져오기

이 예에서 사용할 워크플로는 "Add Endpoint to Identity Group(ID 그룹에 엔드포인트 추가)"이며, Cisco Secure GitHub 페이지에 나열된 워크플로를 사용하거나, 사용자 지정 워크플로를 생성할 수 있습니다.

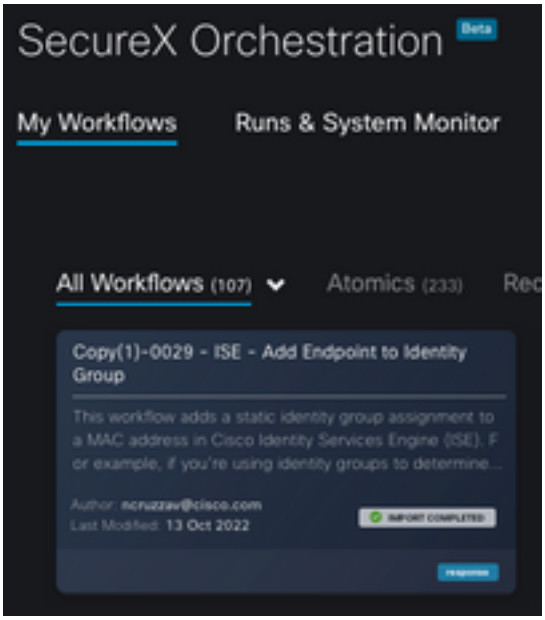
1. Orchestration(오케스트레이션) **> My Workflows(내 워크플로) > Import Workflow(가져오기 워크플로)로 이동합니다.**

2. 워크플로우를 임포트하려면 다음 정보를 입력하고 임포트를 **선택합니다.** 가져올 워크플로를 식별하려면 이름 또는 워크플로 번호로 검색할 수 있습니다

- Git 리포지토리: **CiscoSecurity_**Workflows(워크플로가 있는 위치)
- 파일 이름: **0029-ISE-AddEndpointToIdentityGroup**(사용할 워크플로 수 선택)
- Git 버전: **SecureX 토큰 지원을 위한 업데이트 배치 3**(최신 버전)
- 새 워크플로로 가져오기(복제): **확인**(워크플로를 가져오고 그 복제를 생성합니다.)

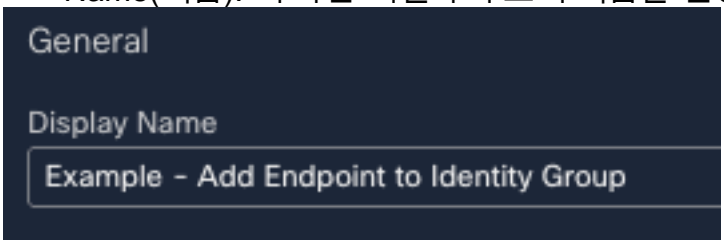


3. 가져오면 새 템플릿이 **내 워크플로 아래**에 나타납니다. 새로 만든 워크플로를 선택하여 매개변수를 편집하여 **ISE**에서 작동하도록 합니다



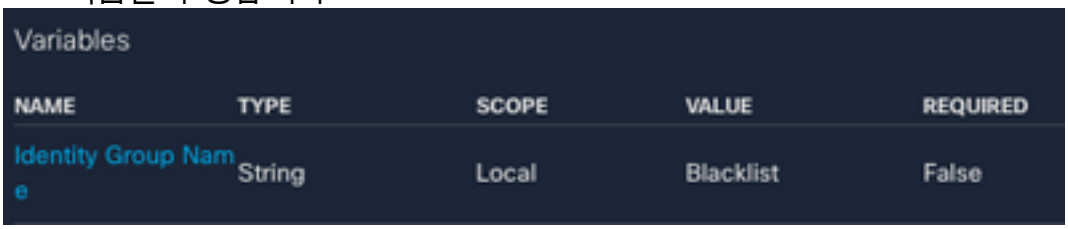
4. 이 워크플로는 빌드 전 워크플로이므로 워크플로의 세 섹션만 수정하면 됩니다.

- Name(이름): 더 나은 식별자의 표시 이름을 변경합니다.

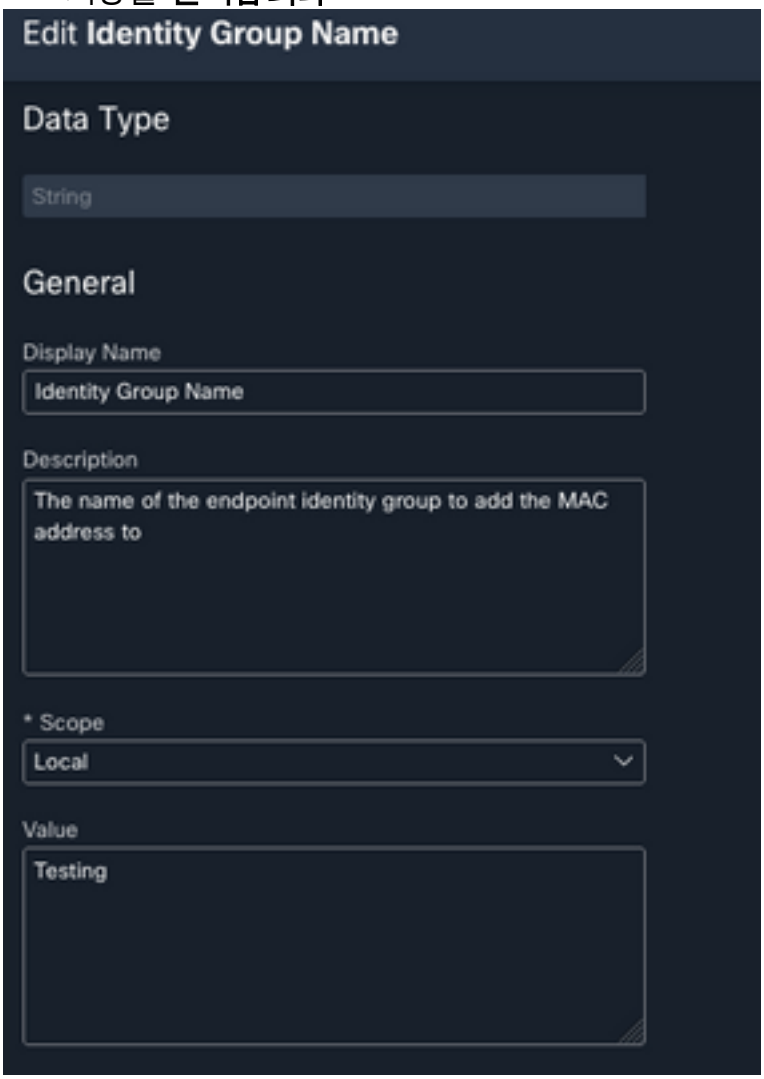


- ID 그룹 변수 Variables(변수)에서 **Identity Group Variable(ID 그룹 변수)**을 기본적으로 **Balcklist(**블랙리스트)로 편집하고 변수를 선택한 다음 오케스트레이션을 통해 수정할 ID 그룹

이름을 구성합니다



- 저장을 **선택합니다**



- 대상: 이전에 **구성한** 대상 구성 대상 유형: **HTTP 엔드포인트**대상: **구성된 대상의 이름**

다음을 확인합니다.

모든 것이 구성되면 워크플로를 테스트할 시간입니다.

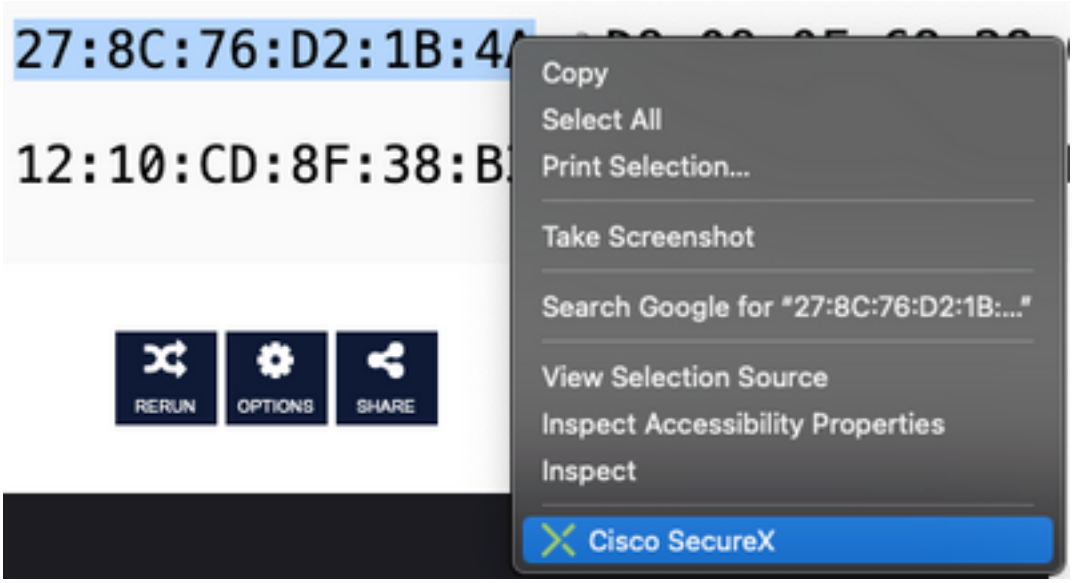
테스트 워크플로에서는 다음 작업을 수행합니다. 웹 페이지에서 MAC 주소를 찾을 경우 ISE 자체 또는 위협 응답과 같은 다른 웹 페이지에 있을 수 있습니다. SecureX 브라우저 확장을 통해 워크플로는 API를 통해 ISE 데이터베이스 내에서 해당 MAC 주소를 찾습니다. MAC가 없는 경우 값을 복사하지 않고 ISE에 액세스하지 않고 엔드포인트 ID 그룹에 관찰 대상이 추가됩니다.

이를 입증하려면 다음 예제를 참조하십시오.

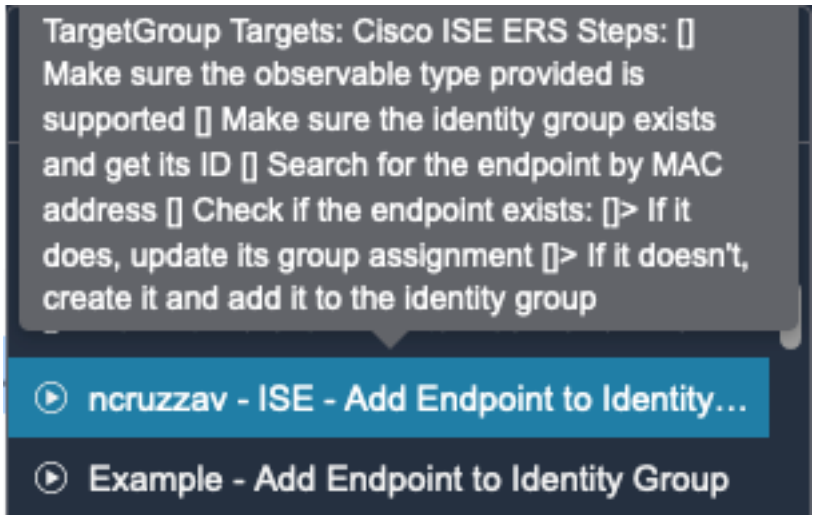
1. 선택한 워크플로는 관찰 가능한 유형 **"MAC 주소"**와 함께 작동합니다

2. 웹 페이지에서 MAC 주소를 찾아 마우스 오른쪽 버튼을 클릭합니다.

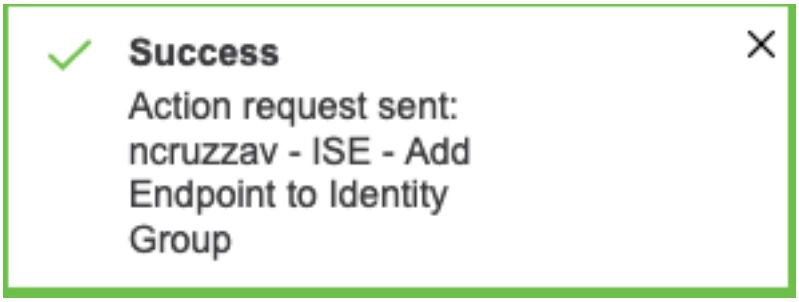
3. SecureX 옵션을 **선택합니다**.



4. 이전에 생성된 **워크플로우**를 선택합니다

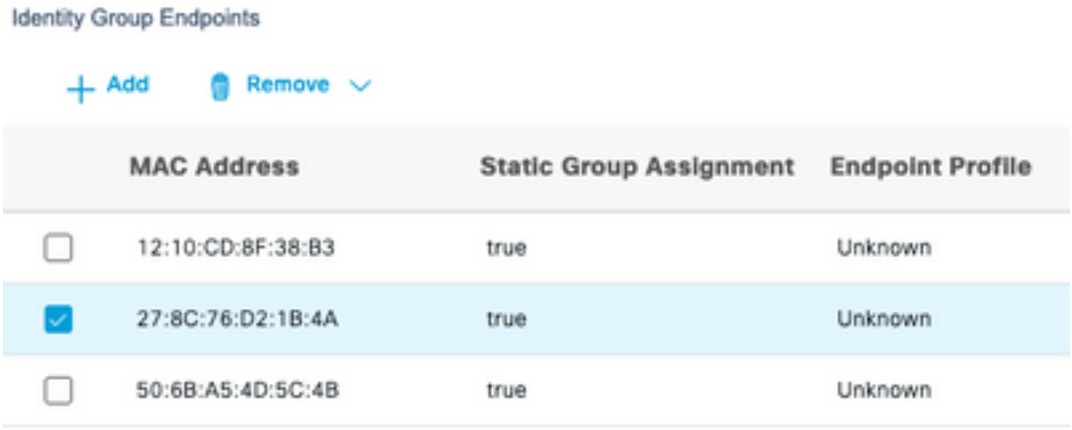


5. 태스크가 성공적으로 실행되었는지 확인합니다



6. ISE PAN에서 **Administration(관리) > Identity Management(ID 관리) > Groups(그룹) > Endpoint Identity Groups(엔드포인트 ID 그룹) > (워크플로에 구성된 그룹)로** 이동합니다

7. 워크플로에 구성된 **엔드포인트 ID** 그룹을 열고 선택한 MAC 주소가 해당 MAC 주소 목록에 추가되었는지 확인합니다



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.