DUO를 사용하여 ISE 3.3 기본 Multi-factor Authentication 구성

목차

소개

이 문서에서는 ISE(Identity Services Engine) 3.3 패치 1을 DUO와 통합하여 다단계 인증을 수행하는 방법에 대해 설명합니다. 버전 3.3 패치 1 ISE에서 DUO 서비스와의 네이티브 통합을 구성할 수 있으므로 인증 프록시가 필요하지 않습니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 기본 지식을 갖춘 것을 권장합니다.

- ISE
- DUO

사용되는 구성 요소

이 문서의 정보는 다음을 기반으로 합니다.

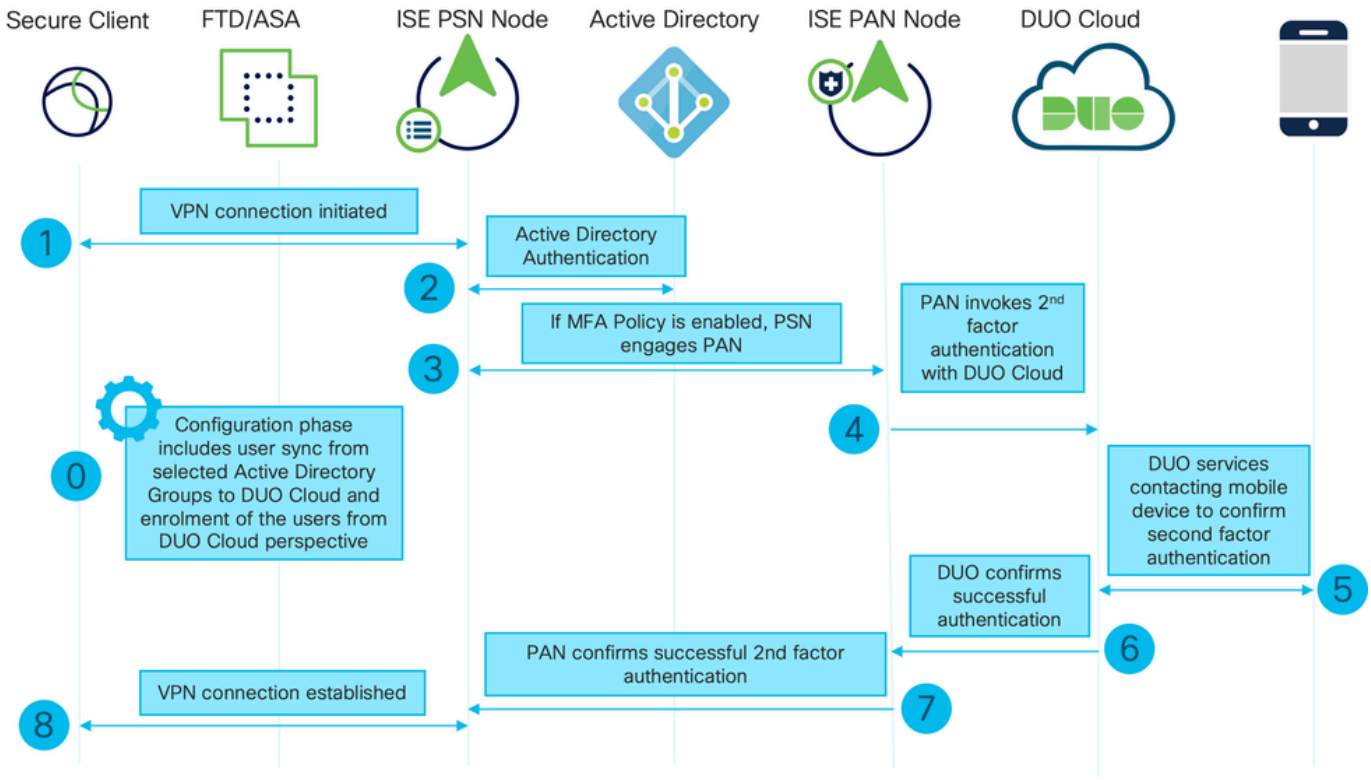
- Cisco ISE 버전 3.3 패치 1

- DUO
- Cisco ASA 버전 9.16(4)
- Cisco Secure Client 버전 5.0.04032

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

순서도



순서도

단계

0. 컨피그레이션 단계에서는 사용자가 동기화되는 Active Directory 그룹을 선택하고 MFA 마법사가 완료되면 동기화가 수행됩니다. 두 단계로 구성되어 있습니다. Active Directory에 대한 조회를 통해 사용자 및 특정 특성 목록을 가져옵니다. Admin API를 사용하여 DUO Cloud를 호출하면 사용자를 해당 위치로 푸시할 수 있습니다. 관리자는 사용자를 등록해야 합니다. 등록에는 사용자가 Duo Push로 원탭 인증을 사용할 수 있도록 하는 Duo Mobile의 사용자를 활성화하는 선택적 단계가 포함될 수 있습니다

1. VPN 연결이 시작되고, 사용자가 사용자 이름 및 비밀번호를 입력하고 OK(확인)를 클릭합니다. 네트워크 디바이스가 RADIUS 액세스 요청을 PSN으로 전송

2. PSN 노드가 Active Directory를 통해 사용자를 인증합니다.

3. 인증이 성공하고 MFA 정책이 구성된 경우 PSN은 PAN을 사용하여 DUO 클라우드에 연결합니다

4. 인증 API를 사용하여 DUO 클라우드를 호출하면 DUO를 사용하여 2단계 인증이 호출됩니다

5. 2단계 인증이 수행됩니다. 사용자가 2단계 인증 프로세스 완료

6. DUO는 2단계 인증 결과로 PAN에 응답합니다.

7. PAN이 2단계 인증 결과로 PSN에 응답합니다.

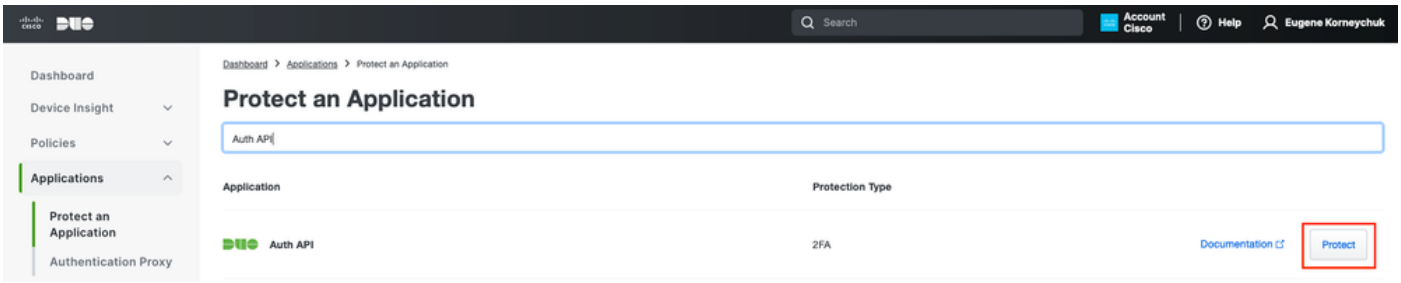
8. 액세스 수락이 네트워크 장치로 전송되면 VPN 연결이 설정됩니다.

설정

보호할 애플리케이션 선택

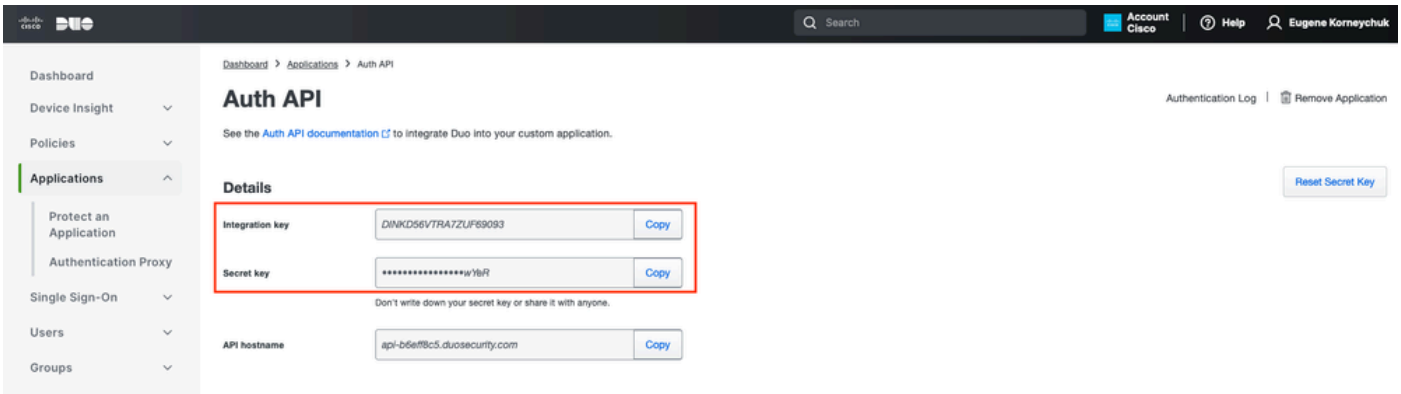
DUO Admin Dashboard(DUO 관리 대시보드) https://admin.duosecurity.com/login으로 이동합니다. 관리자 자격 증명으로 로그인합니다.

Dashboard(대시보드) > Applications(애플리케이션) > Protect an Application(애플리케이션 보호)으로 이동합니다. Auth API(인증 API)를 찾고 Protect(보호)를 선택합니다.



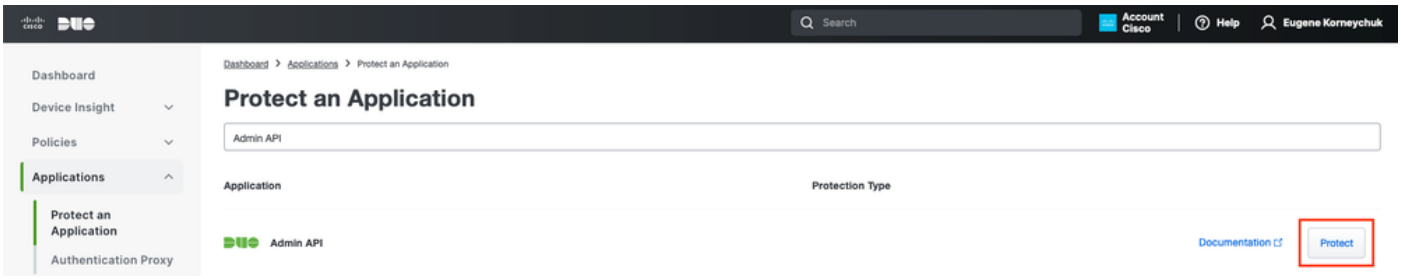
인증 API 1

통합 키 및 비밀 키를 기록해 둡니다.



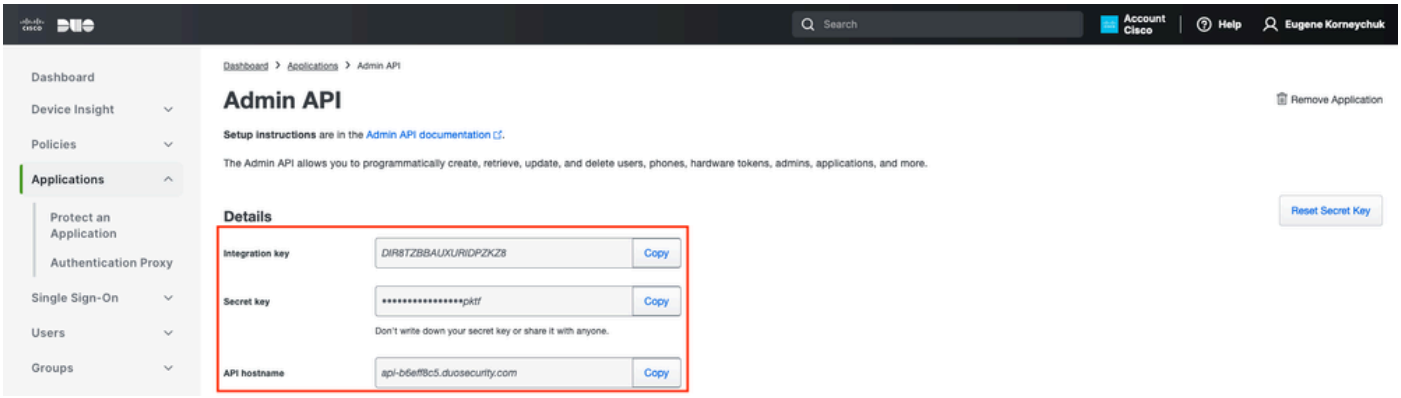
인증 API 2

Dashboard(대시보드) > Applications(애플리케이션) > Protect an Application(애플리케이션 보호)으로 이동합니다. Admin API를 찾고 Protect(보호)를 선택합니다.



인증 API 1

통합 키 및 비밀 키와 API 호스트 이름을 기록해 둡니다.

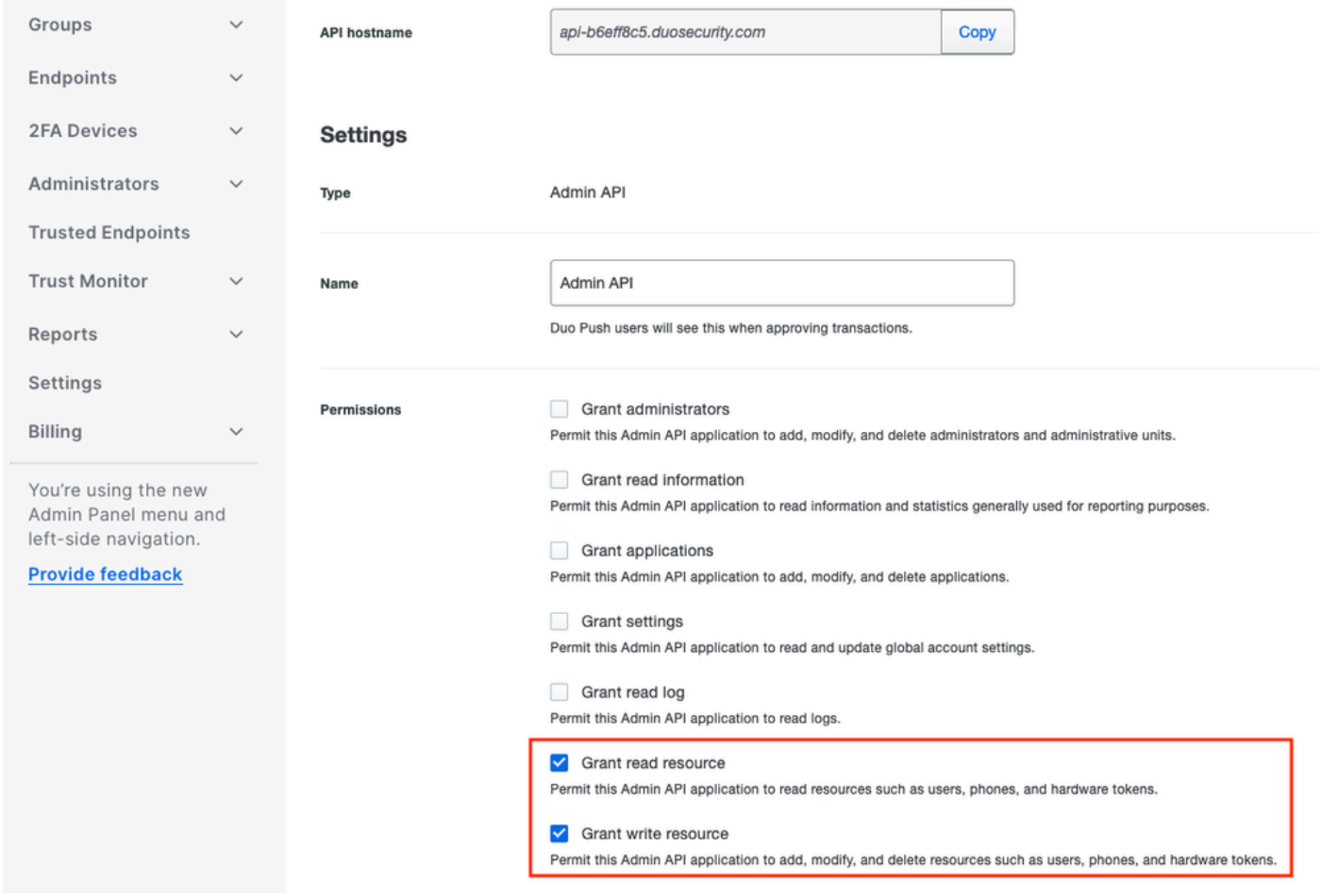


관리 API 2

API 권한 구성

Dashboard(대시보드) > Applications(애플리케이션) > Application(애플리케이션)으로 이동합니다. Admin API를 선택합니다.

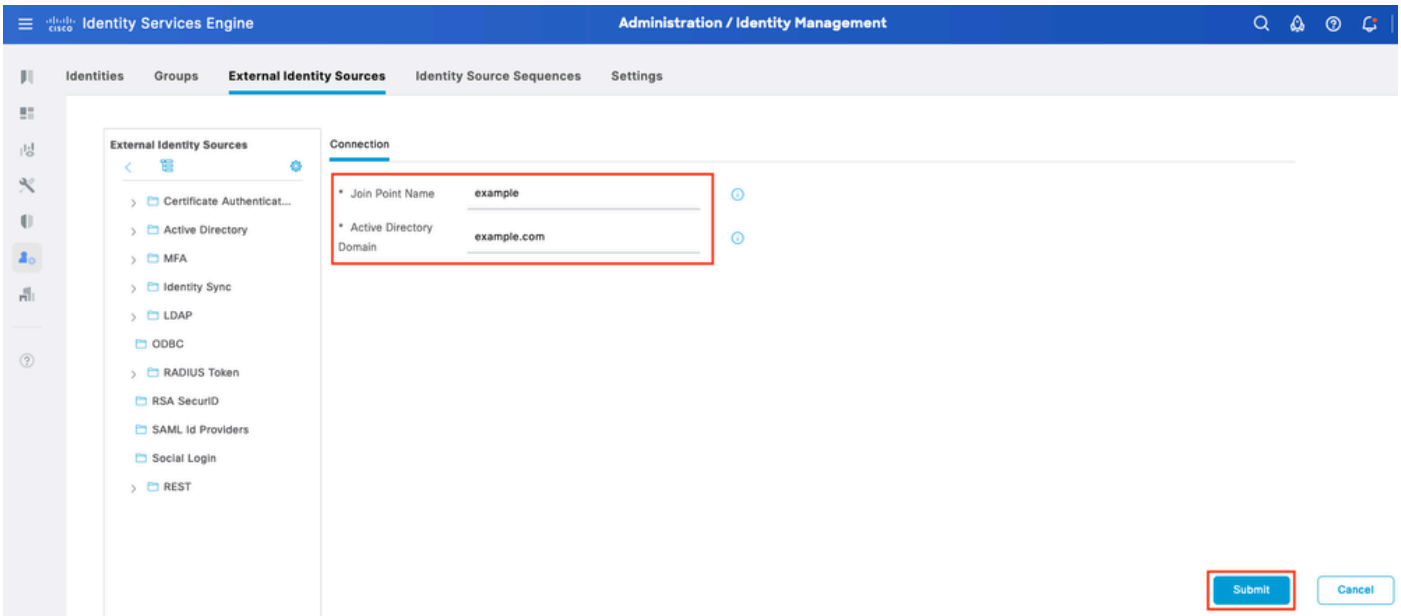
Grant Read Resource(읽기 리소스 허용) 및 Grant Write Resource Permissions(쓰기 리소스 권한 부여)를 선택합니다. Save Changes(변경 사항 저장)를 클릭합니다.



관리 API 3

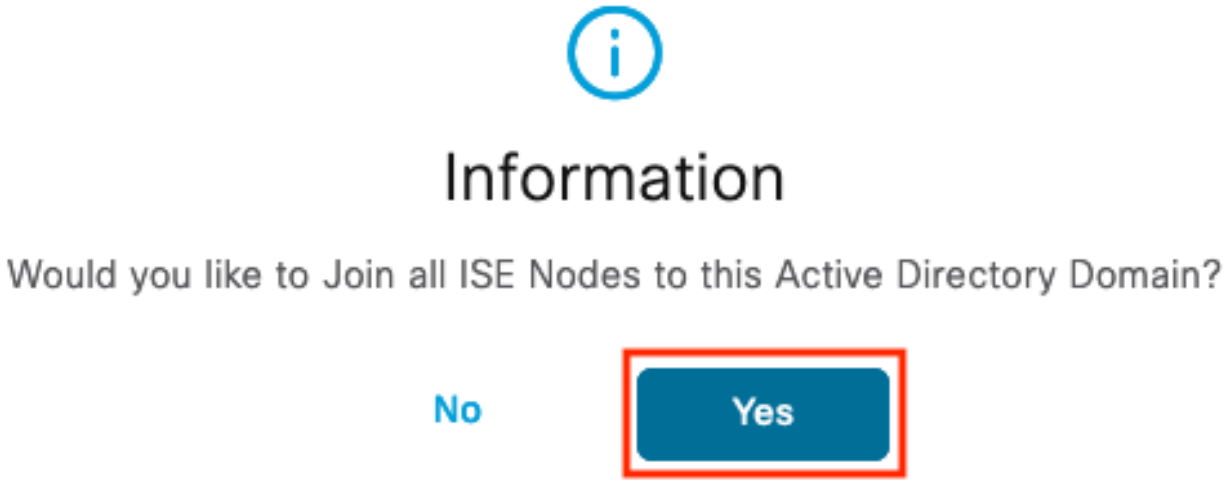
ISE를 Active Directory와 통합

1. Administration(관리) > Identity Management(ID 관리) > External Identity Stores(외부 ID 저장소) > Active Directory > Add(추가)로 이동합니다. 가입 포인트 이름, Active Directory 도메인을 입력하고 Submit(제출)을 클릭합니다.



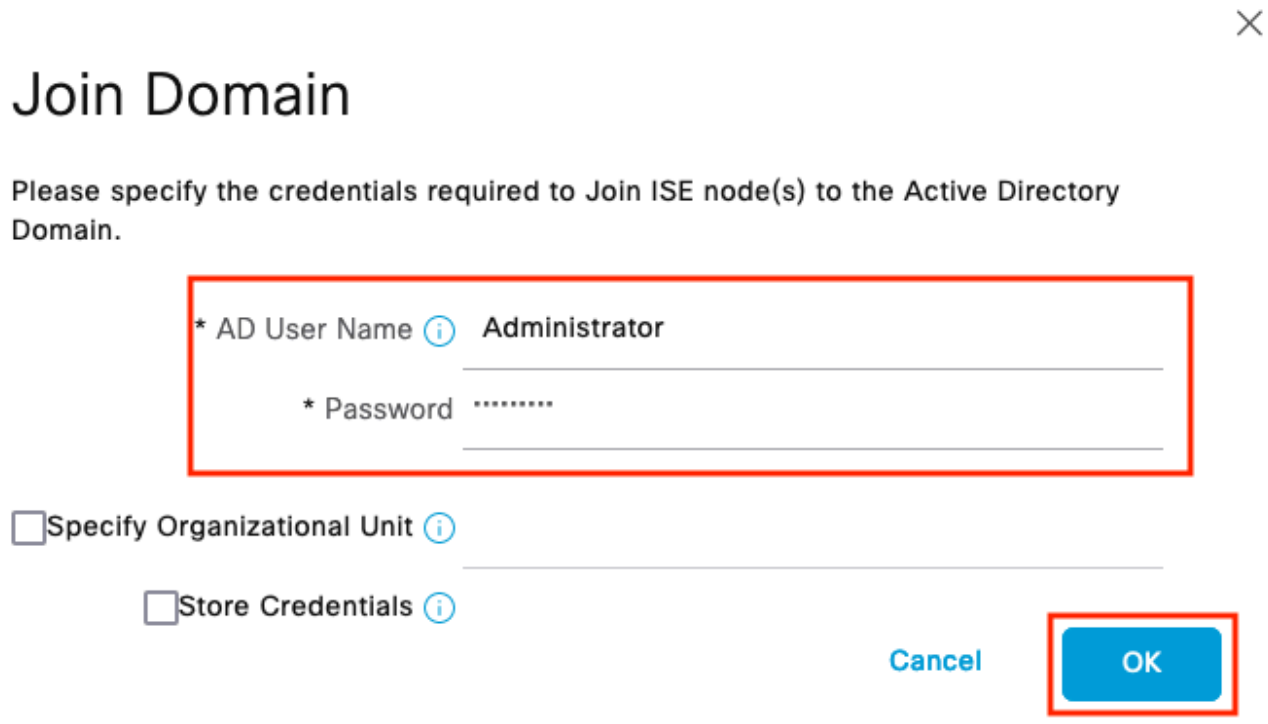
Active Directory 1

2. 모든 ISE 노드를 이 Active Directory 도메인에 가입시키라는 메시지가 표시되면 Yes(예)를 클릭합니다.



Active Directory 2

3. AD 사용자 이름 및 암호를 입력하고 확인을 클릭합니다.



Active Directory 3

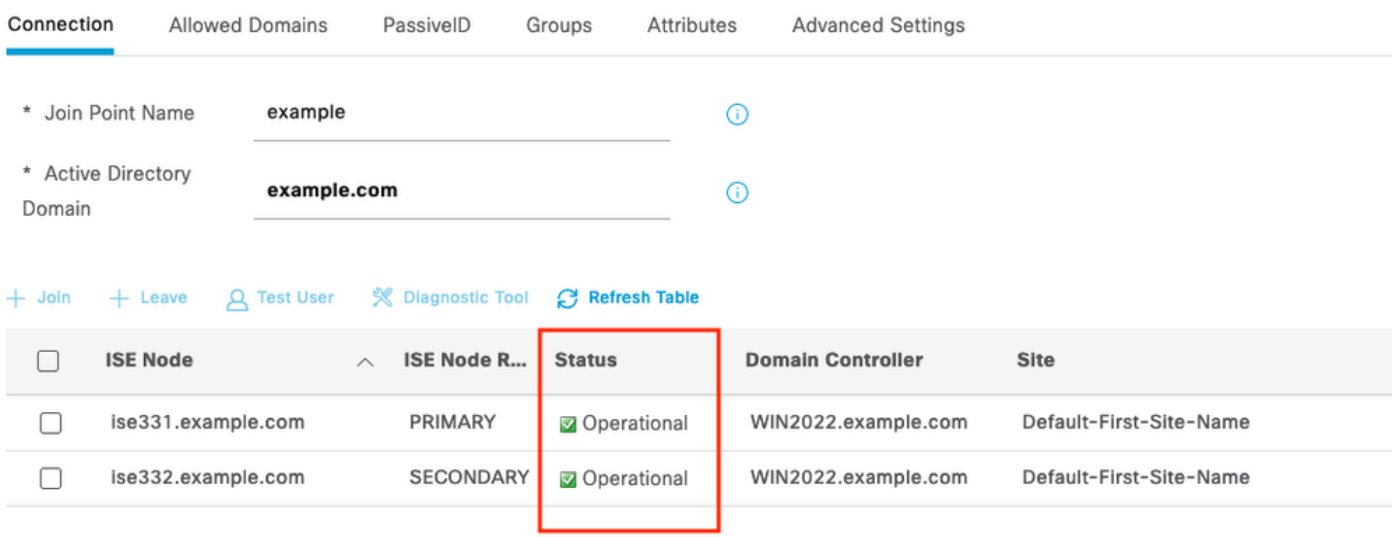
ISE에서 도메인 액세스에 필요한 AD 계정은 다음 중 하나를 가질 수 있습니다.

- 각 도메인의 도메인 사용자 권한에 워크스테이션 추가

- ISE 시스템의 계정이 ISE 시스템을 도메인에 조인하기 전에 생성된 각 컴퓨터 컨테이너에서 컴퓨터 개체 만들기 또는 컴퓨터 개체 삭제 권한

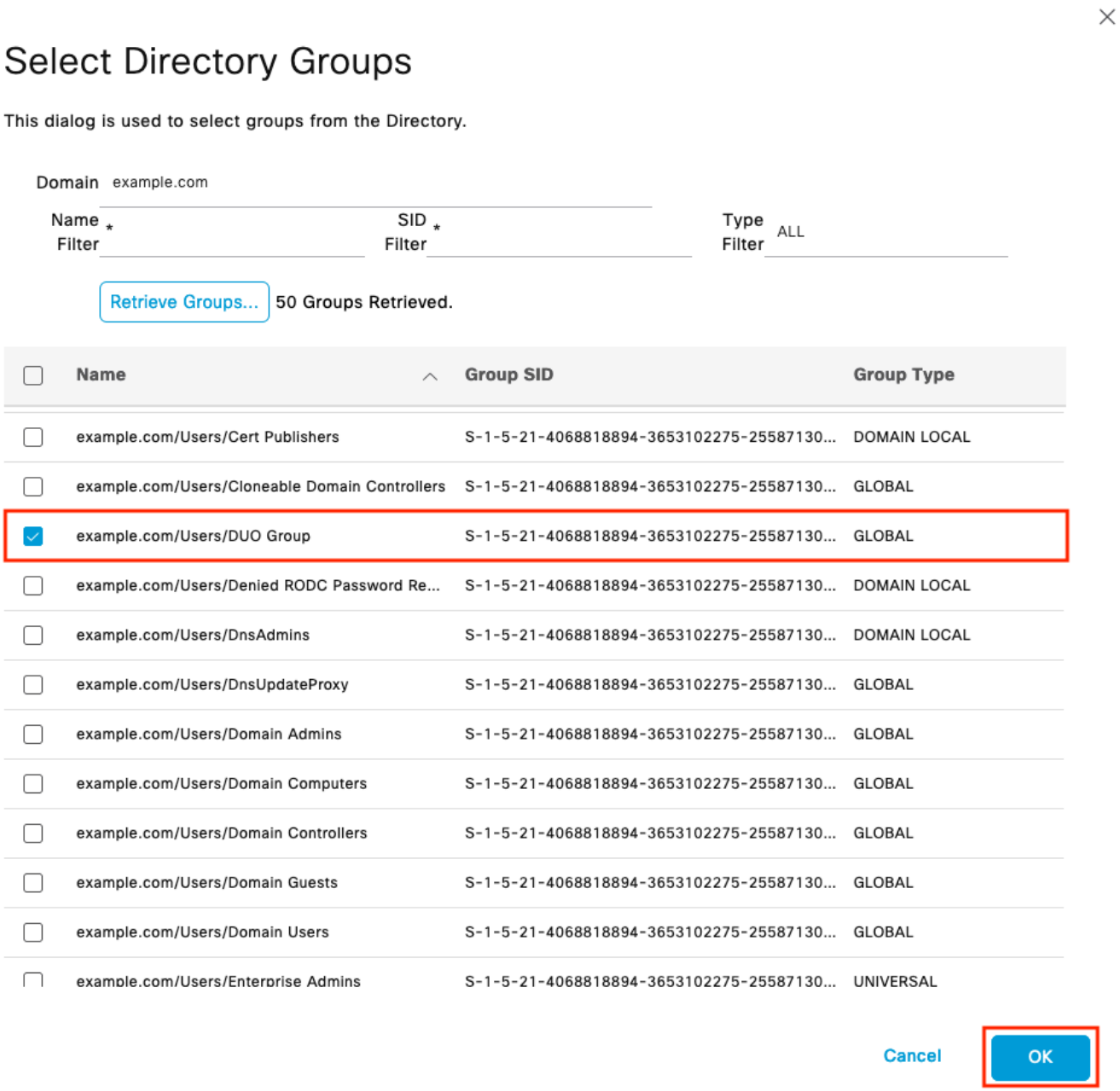
참고: Cisco는 ISE 계정에 대한 잠금 정책을 비활성화하고 해당 계정에 잘못된 비밀번호가 사용되는 경우 관리자에게 알림을 전송하도록 AD 인프라를 구성하는 것을 권장합니다. 잘못된 비밀번호를 입력하면 ISE는 필요한 경우 머신 계정을 생성하거나 수정하지 않으므로 모든 인증을 거부할 수 있습니다.

4. AD 작동 상태



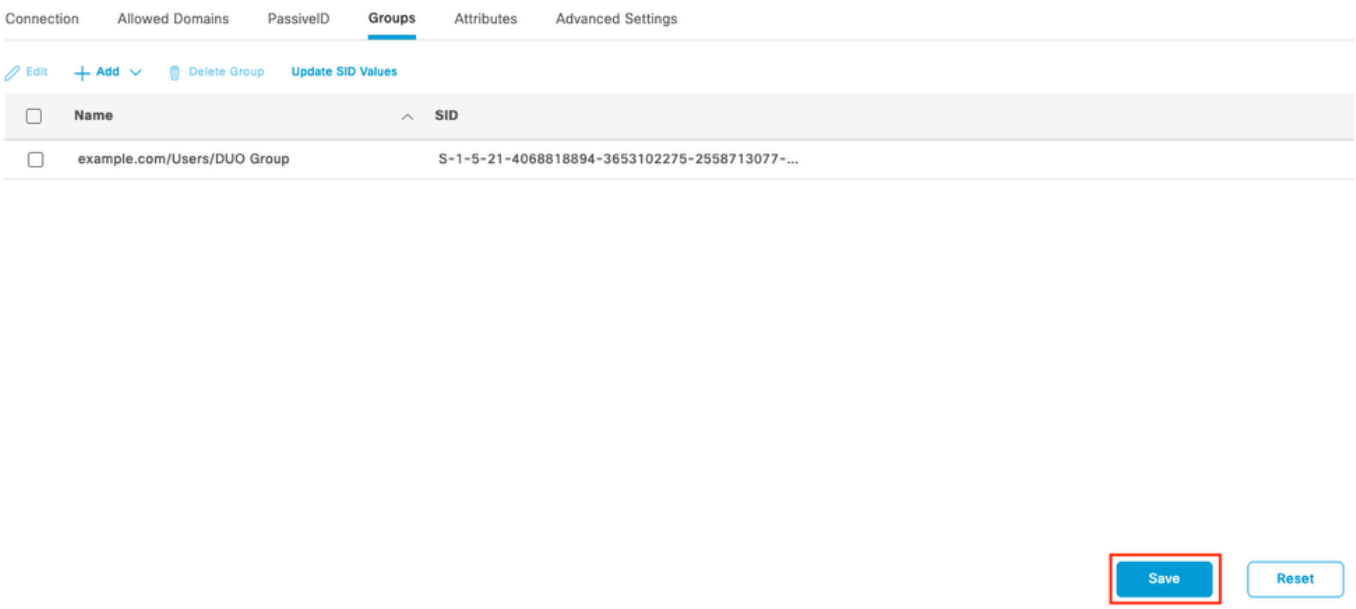
Active Directory 4

5. 그룹 > 추가 > 디렉토리에서 그룹 선택 > 그룹 검색으로 이동합니다. 이 이미지에 표시된 대로 선택한 AD 그룹(사용자 동기화 및 권한 부여 정책에 사용됨)에 대한 확인란을 선택합니다.



Active Directory 5

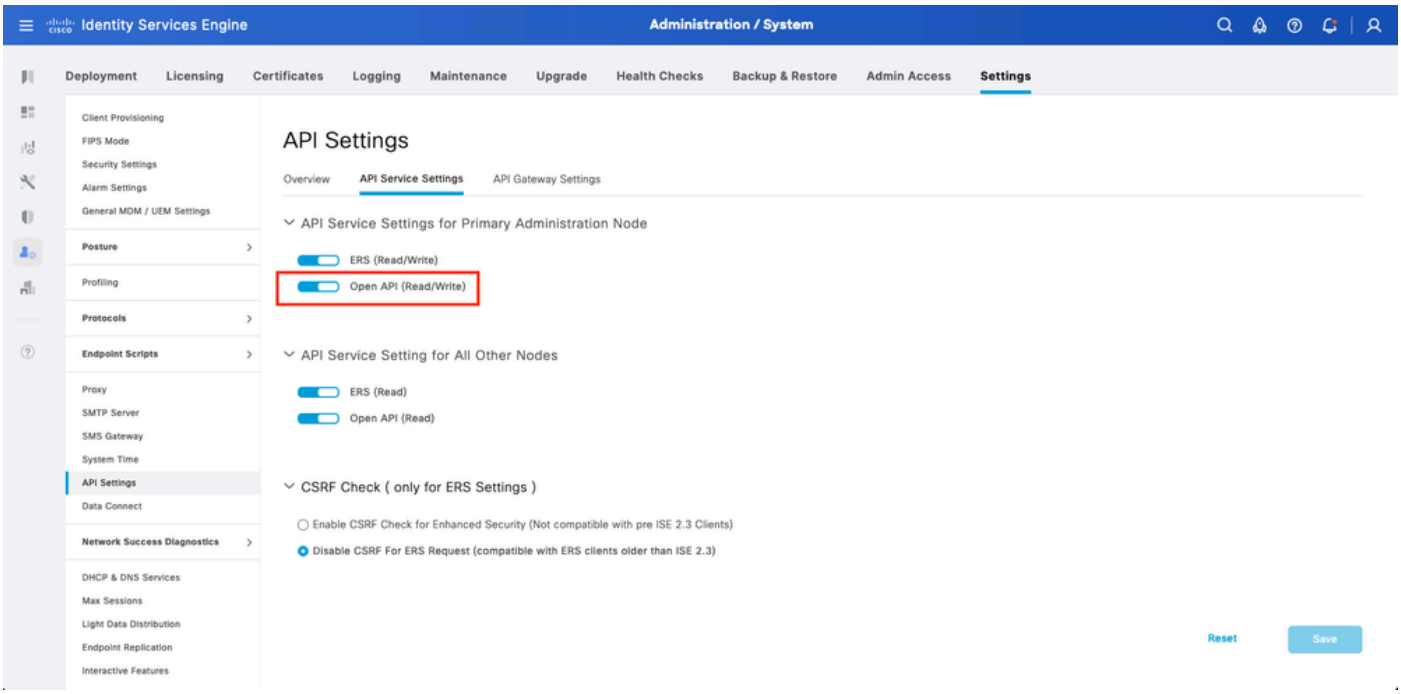
6. 검색된 AD 그룹을 저장하려면 저장을 클릭합니다.



Active Directory 6

Open API 활성화

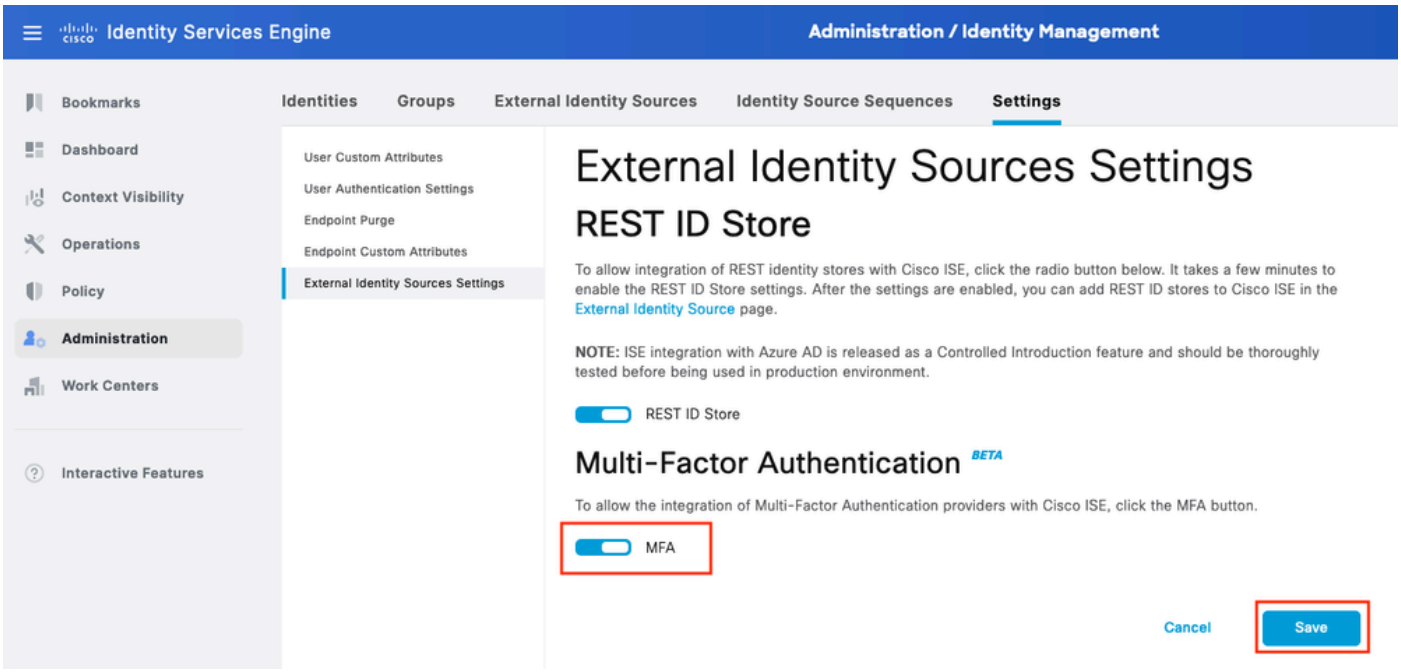
Administration(관리) > System(시스템) > Settings(설정) > API Settings(API 설정) > API Service Settings(API 서비스 설정)로 이동합니다. Open API를 활성화하고 Save를 클릭합니다.



개방형 API

MFA ID 소스 사용

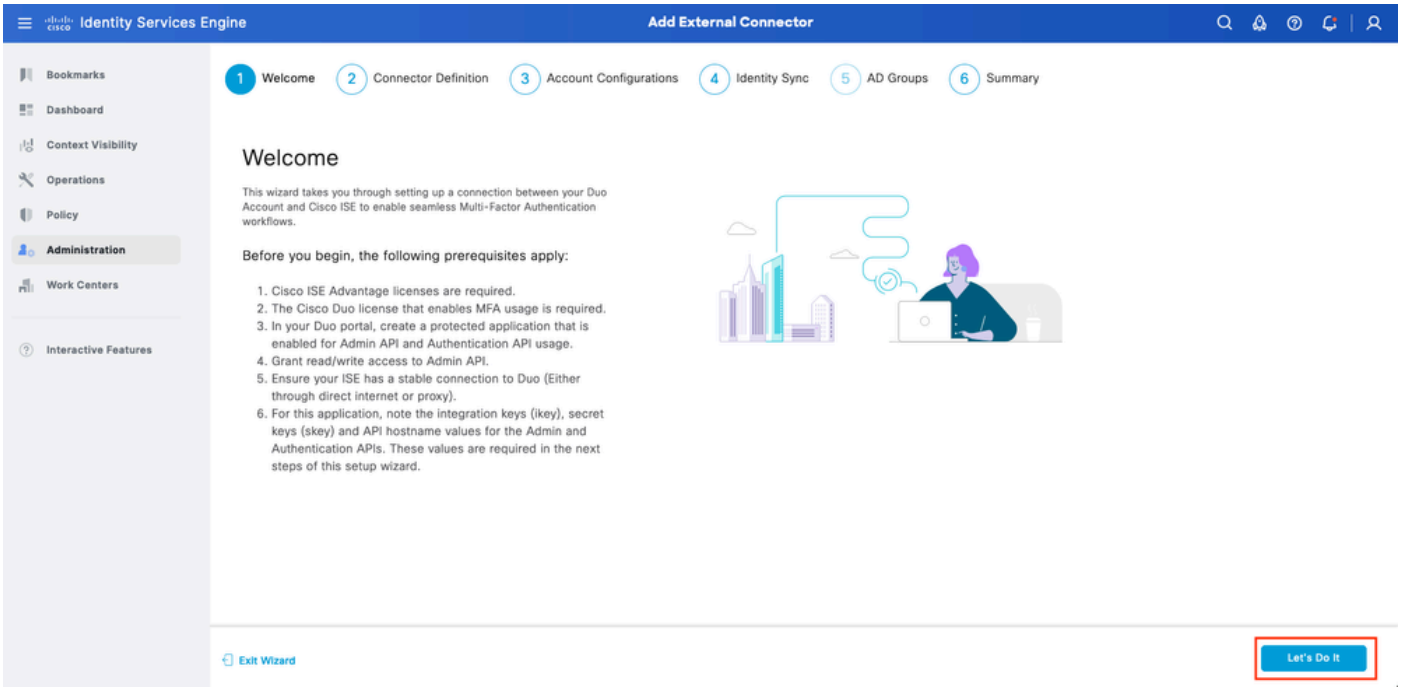
Administration(관리) > Identity Management(ID 관리) > Settings(설정) > External Identity Sources Settings(외부 ID 소스 설정)로 이동합니다. MFA를 활성화하고 Save(저장)를 클릭합니다.



ISE MFA 1

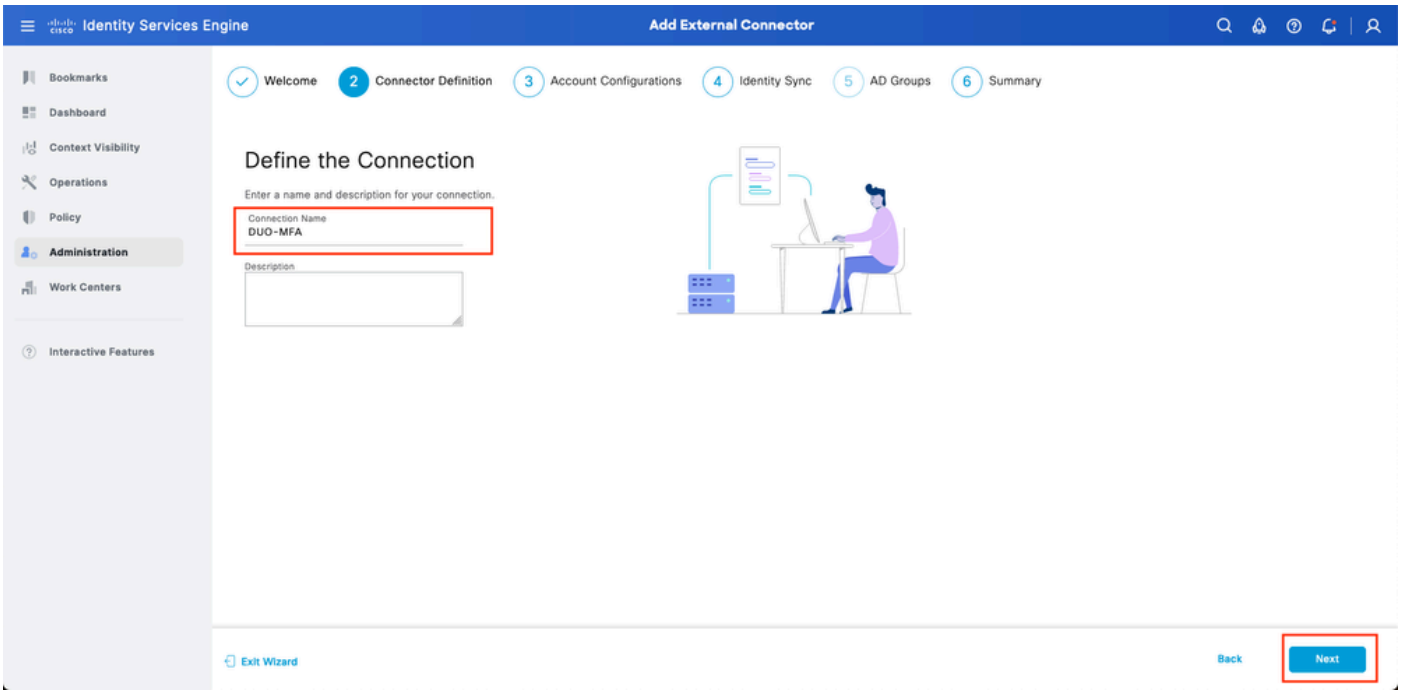
MFA 외부 ID 소스 구성

Administration(관리) > Identity Management(ID 관리) > External Identity Sources(외부 ID 소스)로 이동합니다. Add를 클릭합니다. Welcome(시작) 화면에서 Let's Do It(시작하겠습니다)을 클릭합니다.



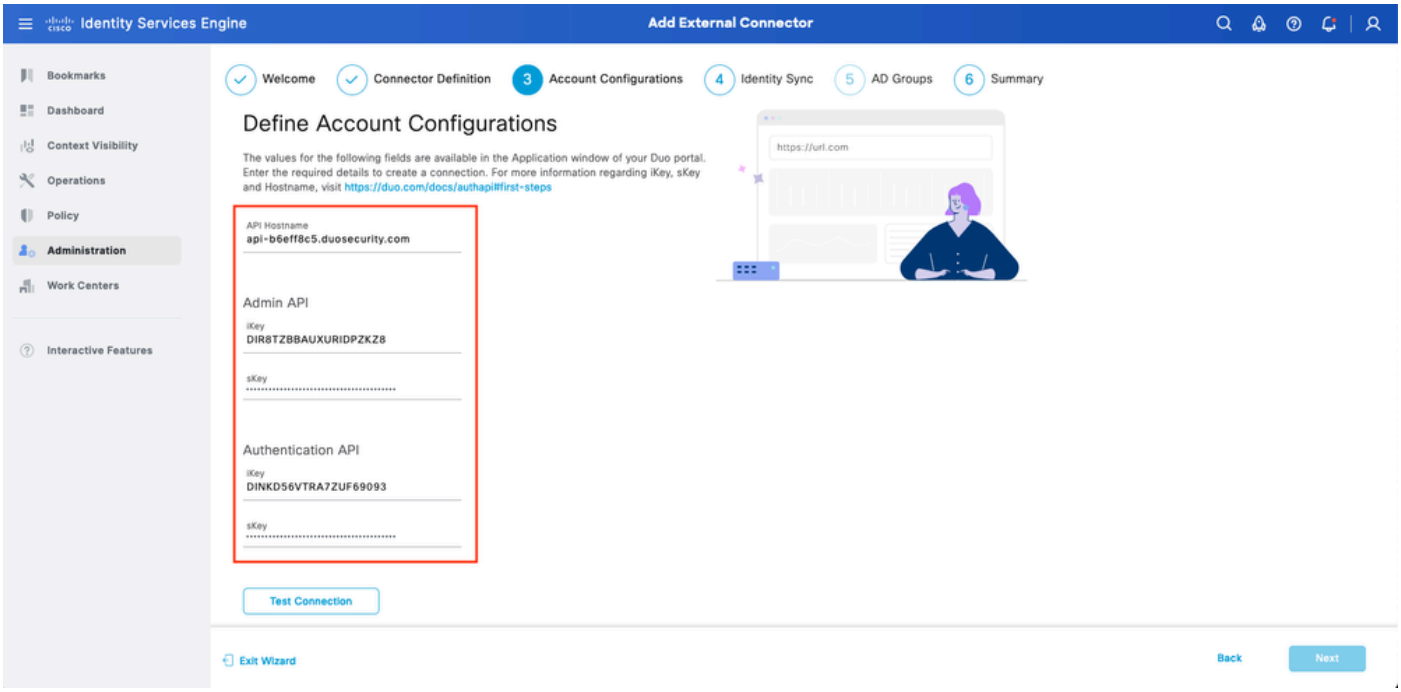
ISE DUO 마법사 1

다음 화면에서 Connection Name(연결 이름)을 구성하고 Next(다음)를 클릭합니다.



ISE DUO 마법사 2

보호할 애플리케이션 선택 단계에서 API 호스트 이름, 관리 API 통합 및 비밀 키, 인증 API 통합 및 비밀 키의 값을 구성합니다(S).



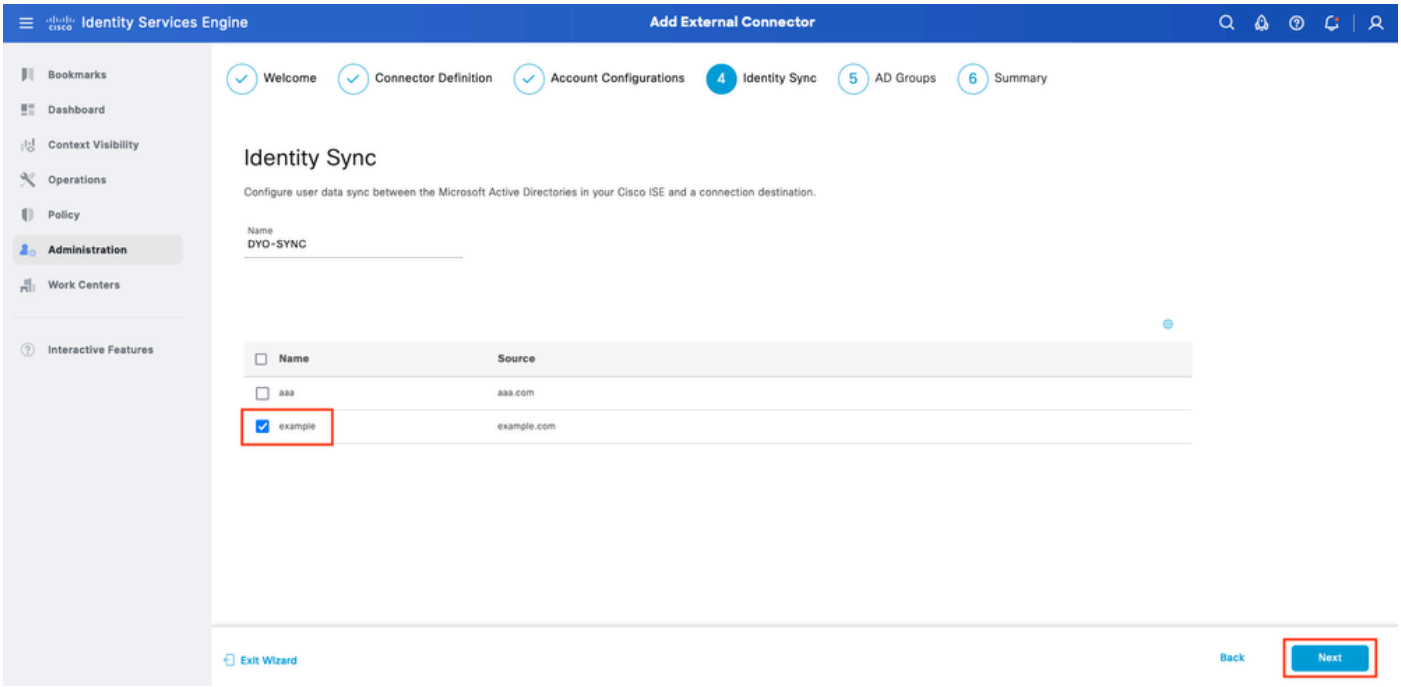
ISE DUO 마법사 3

Test Connection(연결 테스트)을 클릭합니다. Test Connection(연결 테스트)이 성공하면 Next(다음)를 클릭할 수 있습니다.

ISE DUO 마법사 4

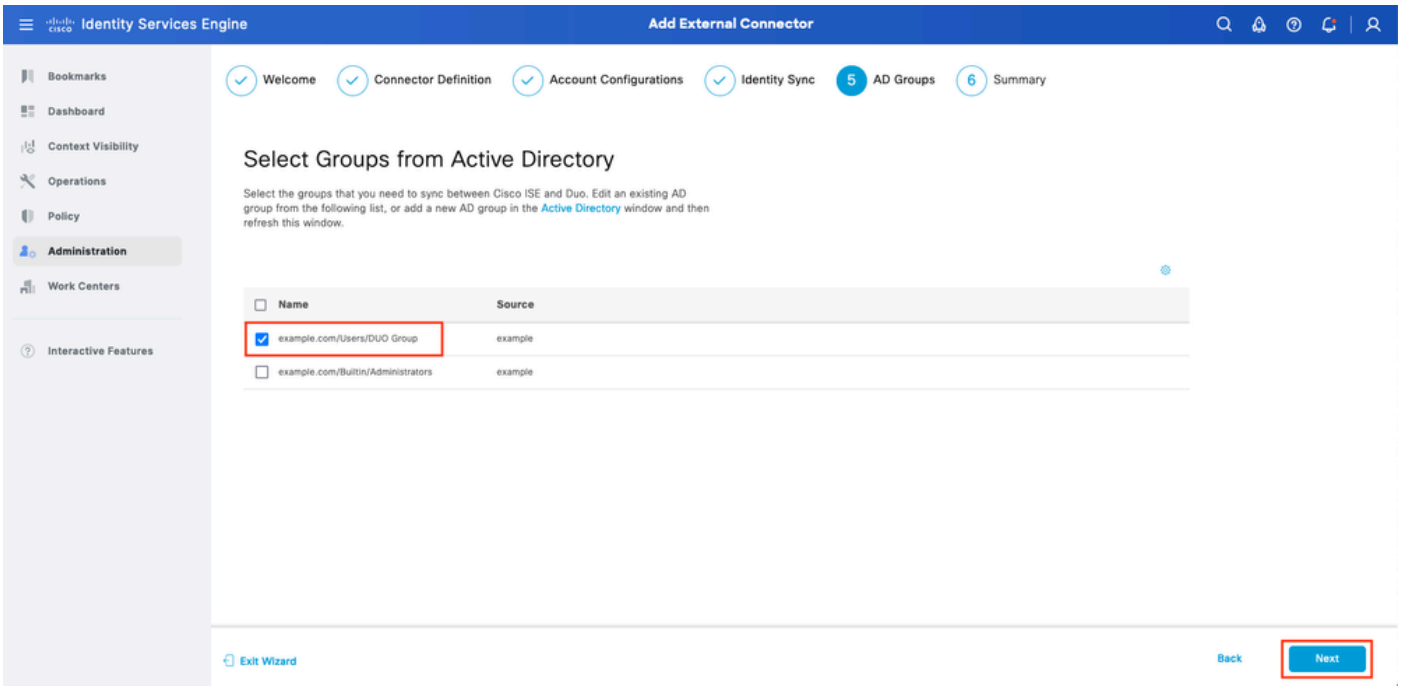
ID 동기화를 구성합니다. 이 프로세스는 이전에 제공된 API 자격 증명을 사용하여 선택한 Active Directory 그룹의 사용자를 DUO 계정으로 동기화합니다. Active Directory Join Point를 선택합니다. Next(다음)를 클릭합니다.

참고: Active Directory 컨피그레이션이 문서 범위에 속하지 않습니다. ISE를 Active Directory와 통합하려면 이 문서를 따르십시오.



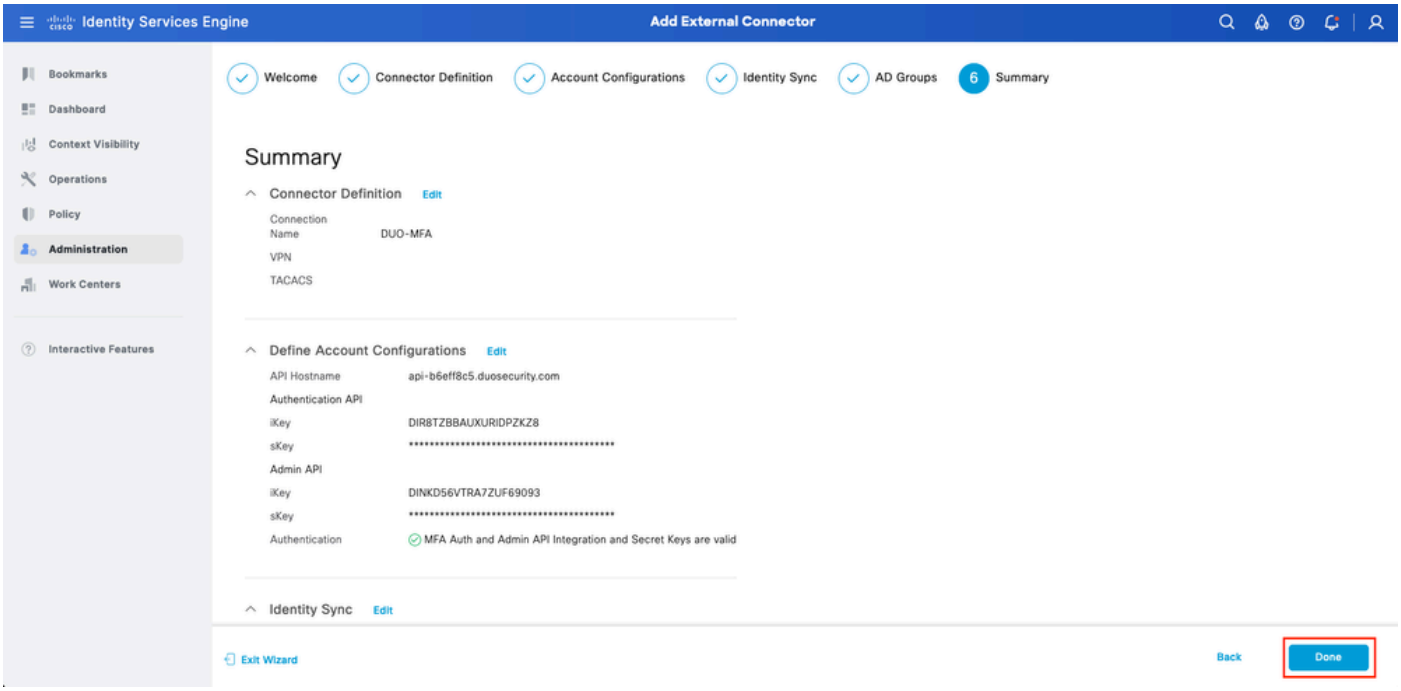
ISE DUO 마법사 5

사용자를 DUO와 동기화하려는 Active Directory 그룹을 선택합니다. Next(다음)를 클릭합니다.



ISE DUO 마법사 6

설정이 올바른지 확인하고 Done(완료)을 클릭합니다.



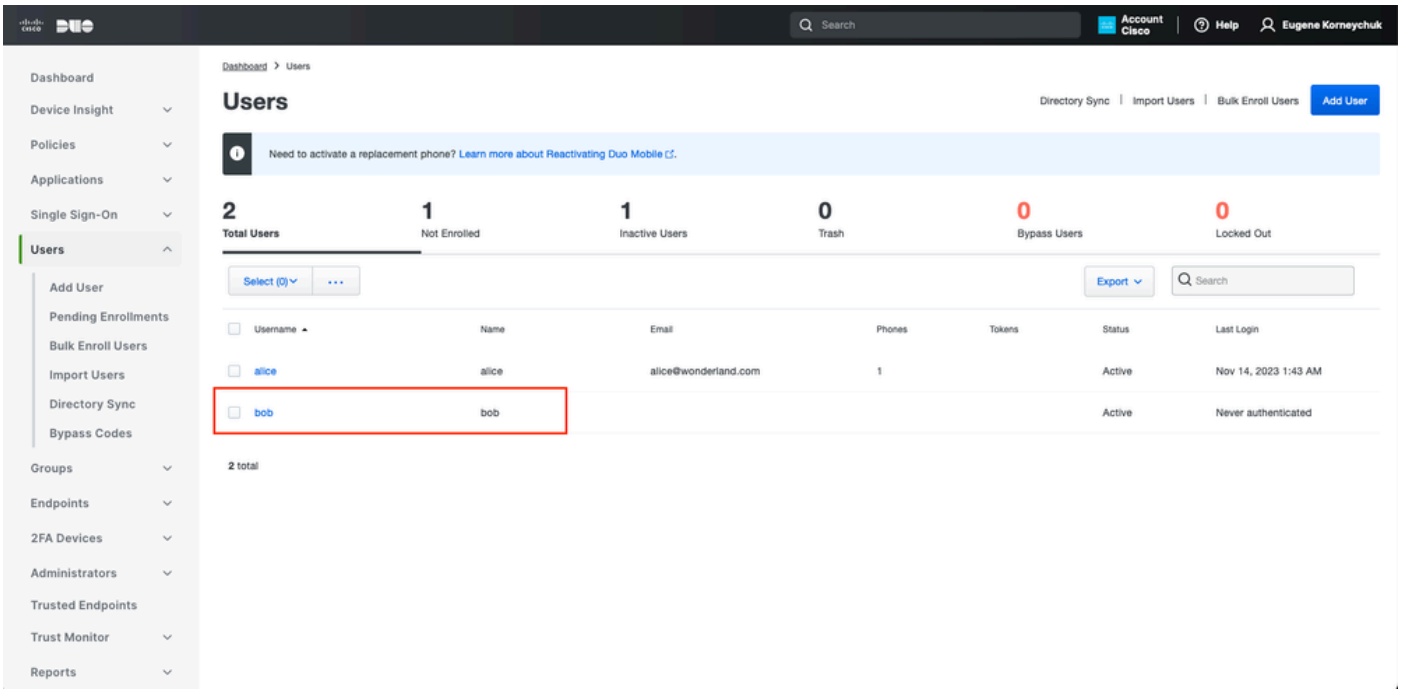
ISE DUO 마법사 7

DUO에 사용자 등록

> 참고: DUO User Enrollment(DUO 사용자 등록)는 이 문서의 범위에 속하지 않습니다. 사용자 등록에 대한 자세한 내용은 이 문서를 참조하십시오. 이 문서에서는 수동 사용자 등록을 사용합니다.

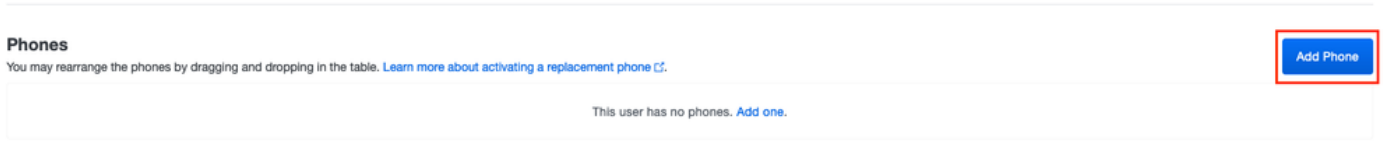
DUO 관리 대시보드를 엽니다. Dashboard(대시보드) > Users(사용자)로 이동합니다. ISE에서 동기

화된 사용자를 클릭합니다.



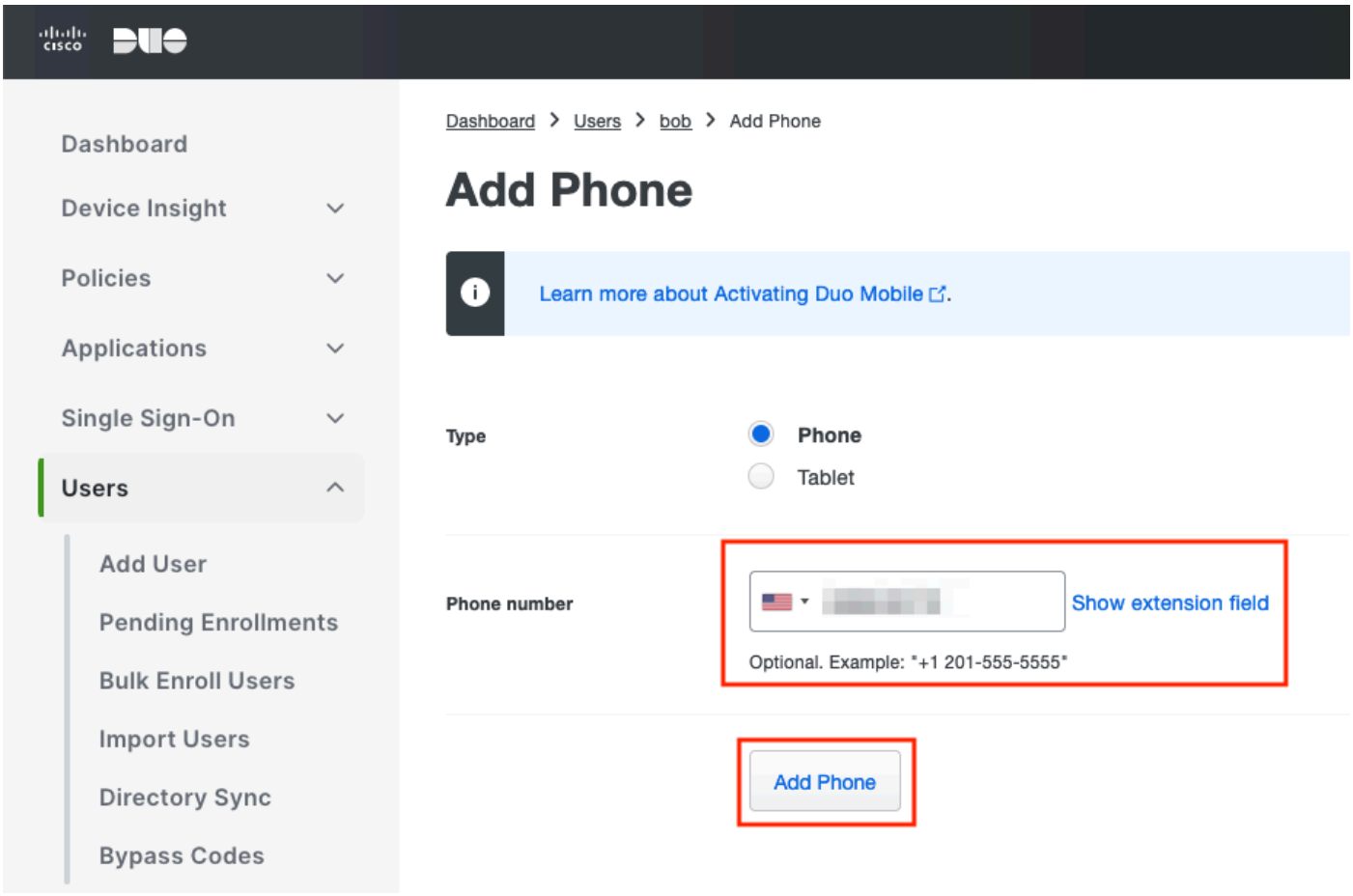
DUO 등록 1

아래로 스크롤하여 전화기로 이동합니다. Add Phone(전화기 추가)을 클릭합니다.



DUO 등록 2

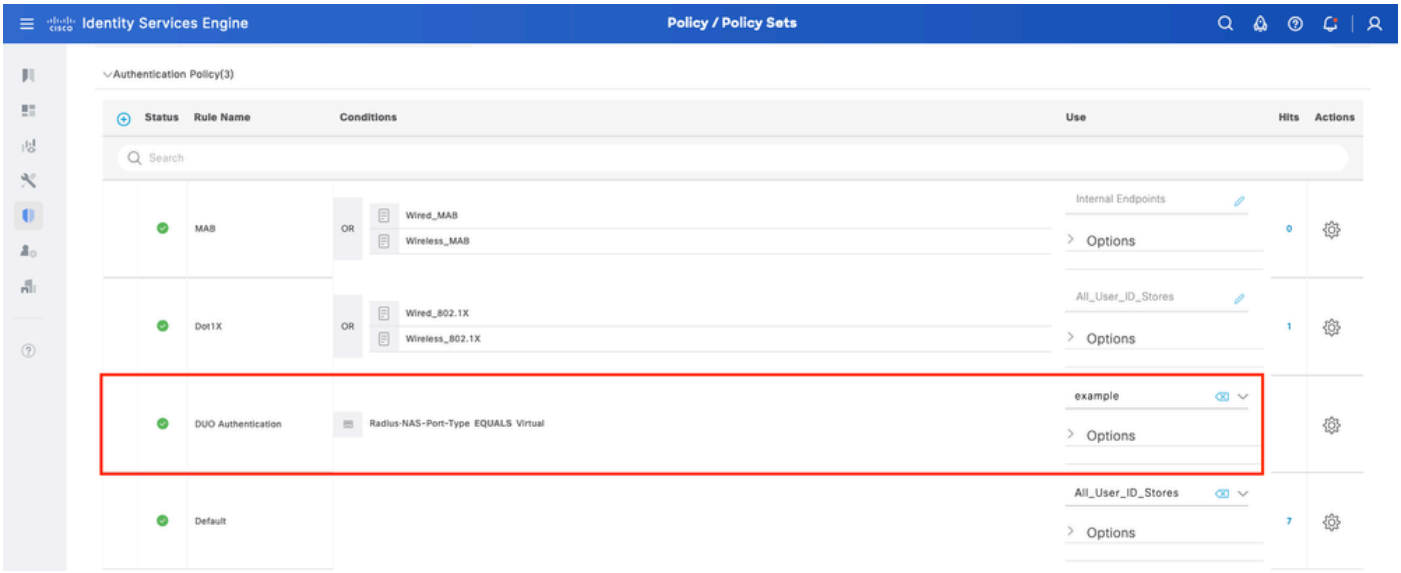
전화 번호를 입력하고 Add Phone(전화 추가)을 클릭합니다.



정책 집합 구성

1. 인증 정책 구성

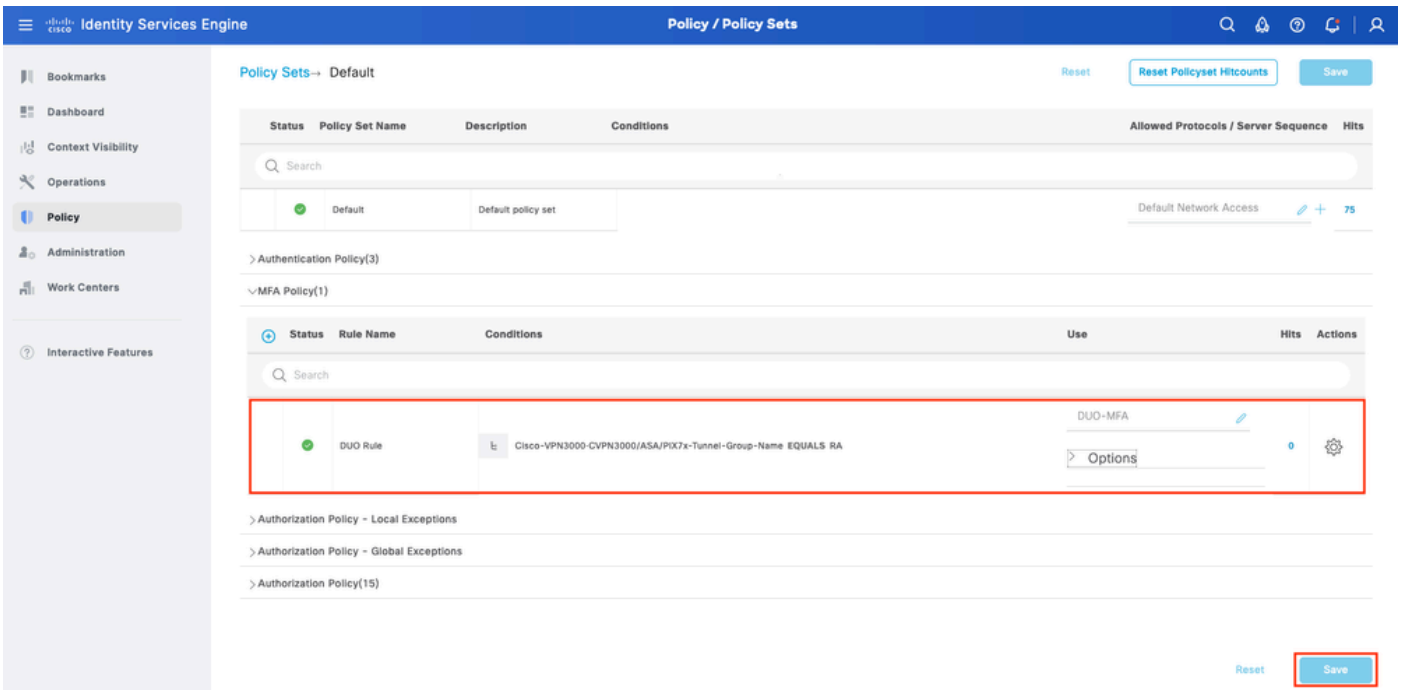
Policy(정책) > Policy Set(정책 집합)로 이동합니다. MFA를 활성화하려는 정책 집합을 선택합니다. 기본 인증 ID 저장소를 Active Directory로 사용하여 인증 정책을 구성합니다.



정책 설정 1

2. MFA 정책 구성

ISE에서 MFA가 활성화되면 ISE 정책 세트의 새 섹션을 사용할 수 있습니다. MFA Policy(MFA 정책)를 확장하고 +를 클릭하여 MFA 정책을 추가합니다. 선택한 MFA 조건을 구성합니다. 앞서 사용 섹션에서 구성한 DUO-MFA를 선택합니다. Save(저장)를 클릭합니다.

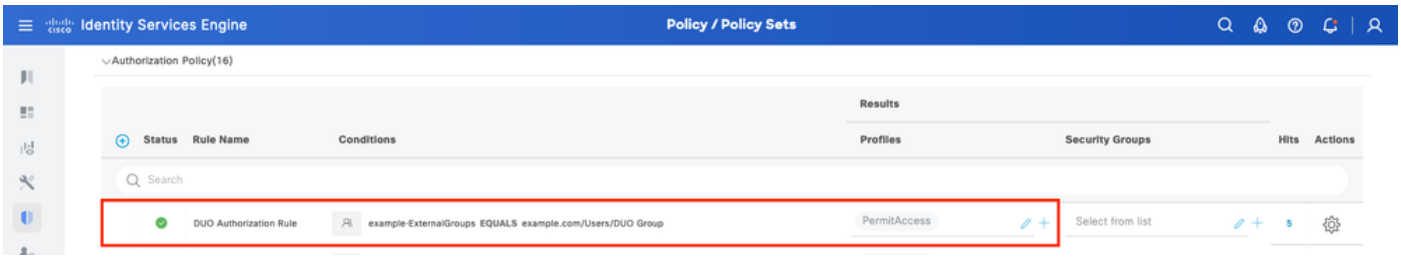


ISE 정책

참고: 위에서 구성한 정책은 Tunnel-Group Named RA를 사용합니다. RA 터널 그룹에 연결된 사용자는 MFA를 수행해야 합니다. ASA/FTD 구성은 이 문서의 범위에 포함되지 않습니다. ASA/FTD를 구성하려면 이 문서를 사용하십시오

3. 권한 부여 정책 구성

Active Directory 그룹 조건 및 선택한 권한으로 권한 부여 정책을 구성합니다.



정책 설정 3

제한 사항

이 문서를 작성하는 시점:

1. DUO 푸시 및 전화만 2단계 인증 방법으로 지원됩니다.

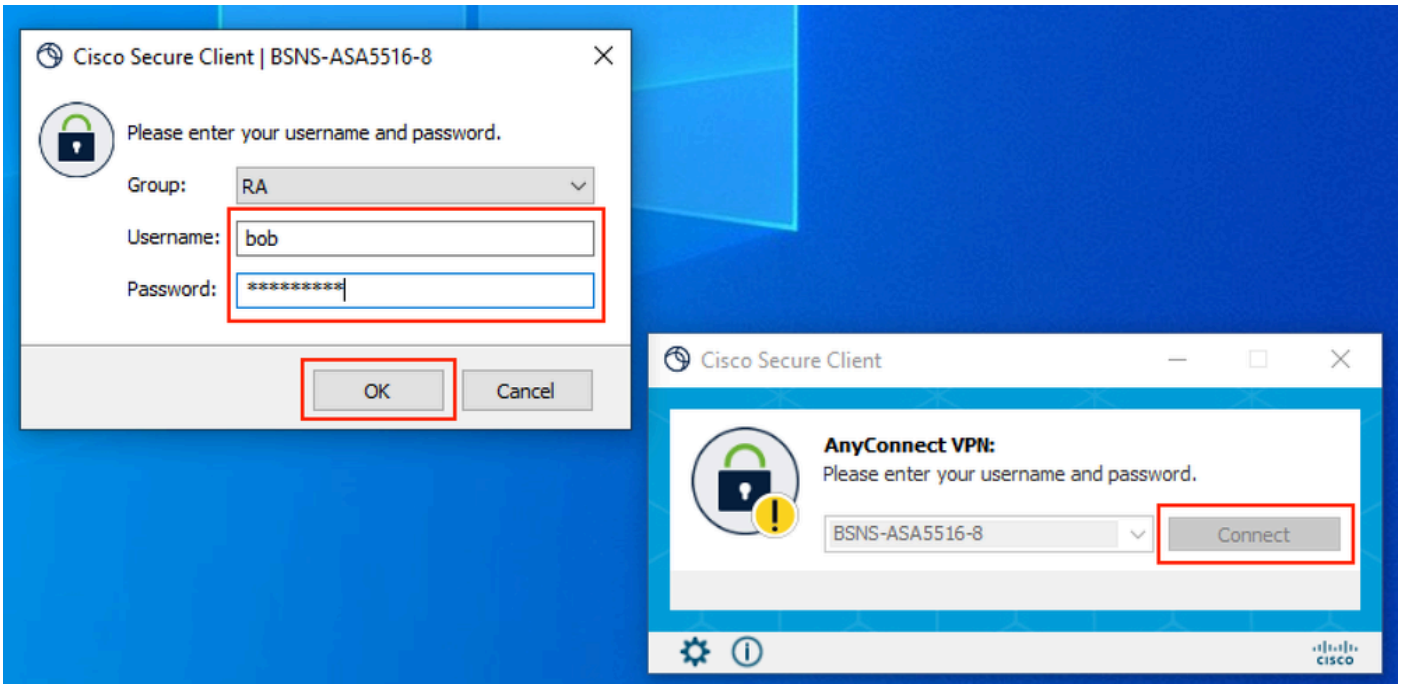
2. 그룹이 DUO 클라우드에 푸시되지 않으며 사용자 동기화만 지원됩니다.

3. 다음 다단계 인증 활용 사례만 지원됩니다.

- VPN 사용자 인증
- TACACS+ 관리자 액세스 인증

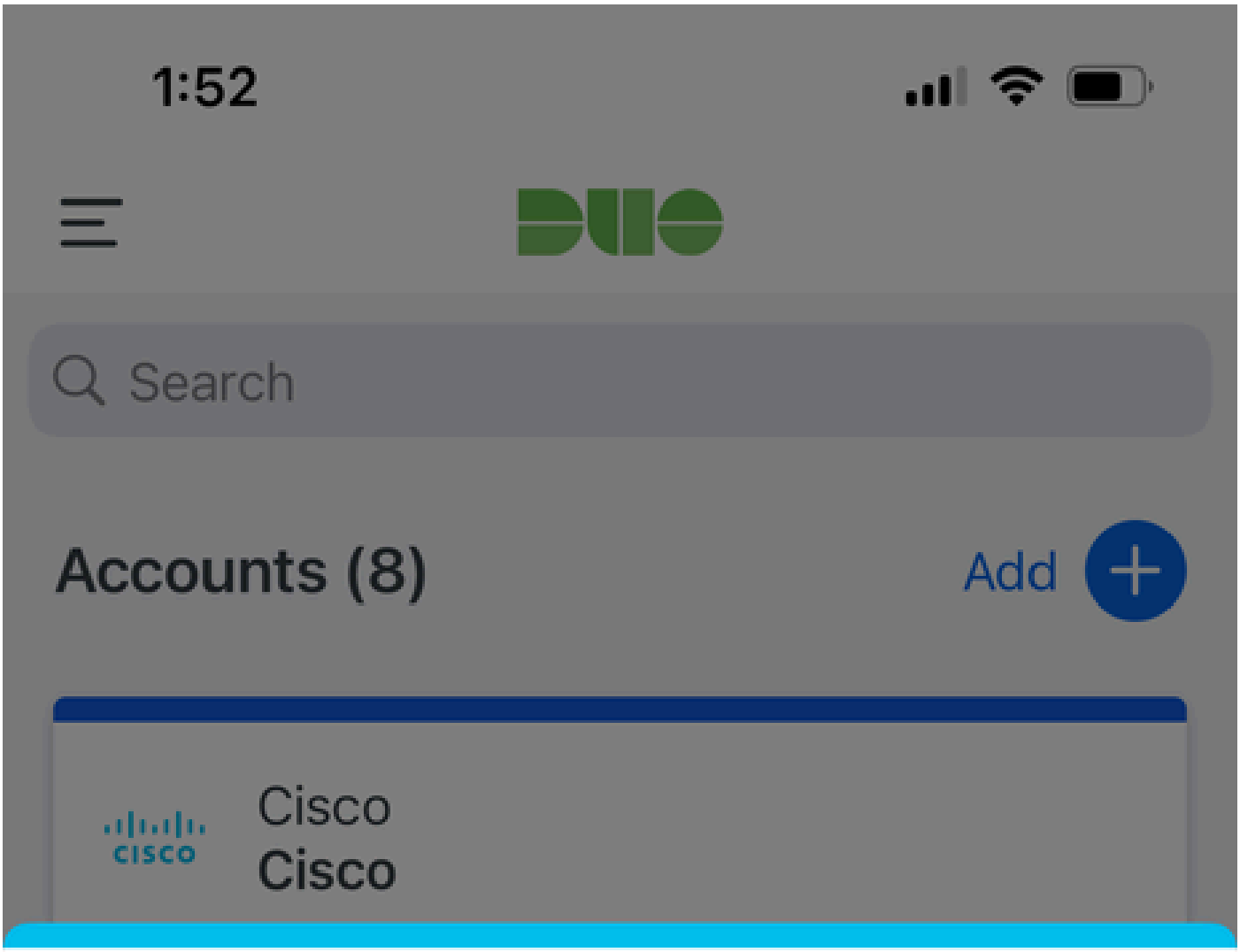
다음을 확인합니다.

Cisco Secure Client를 열고 Connect(연결)를 클릭합니다. 사용자 이름과 비밀번호를 입력하고 OK를 클릭합니다.



VPN 클라이언트

사용자 모바일 장치는 DUO 푸시 알림을 받아야 합니다. 승인. VPN 연결이 설정되었습니다.



Are you logging in to **Auth API**?

Cisco

1:52 PM

bob

MFA 관련 로그	정책 엔진	ise-psc.log	DuoMfaAuthApiUtils -::::- Duo Client Manager에 요청을 제출했습니다. DuoMfaAuthApiUtils —> Duo 응답
정책 관련 로그	포트-JNI	prrt-management.log	RadiusMfaPolicyRequestProcessor TacacsMfaPolicyRequestProcessor
인증 관련 로그	런타임 AAA	prrt-server.log	MfaAuthenticator::onAuthenticateEvent MfaAuthenticator::sendAuthenticateEvent MfaAuthenticator::onResponseEvaluatePolicyEvent
DUO 인증, ID 동기화 관련 로그		duo-sync-service.log	

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.