OKTA를 통한 액세스 보안을 위해 사용자 및 그룹 프로비저닝

목차

소개

이 문서에서는 OKTA에서 Cisco Secure Access로 사용자 그룹을 프로비저닝하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco 보안 액세스
- 옥타

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

- Cisco Secure Access 대시보드

- 옥타

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.

배경 정보

Cisco Secure Access는 OKTA에서 사용자 및 그룹의 프로비저닝을 지원합니다.

이러한 프로비저닝을 통해 보안 액세스는 다음 권한을 부여받은 사용자 디렉토리를 유지 관리할 수 있습니다.

- ZTA(Zero Trust Access)에 등록
- VPNaaS에 연결합니다.
- Umbrella Roaming 사용자에게 ID 기반 정책을 적용합니다.

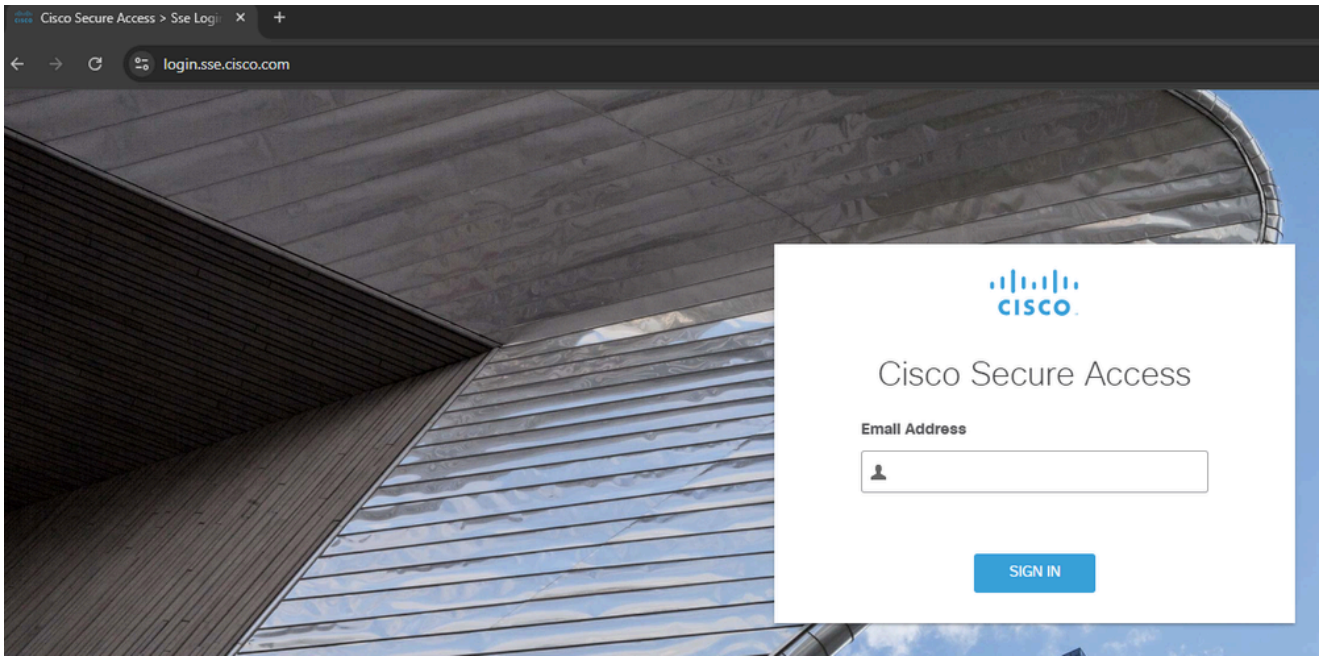
참고: 이 문서에서는 특히 OKTA의 사용자 및 그룹 프로비저닝에 초점을 맞춥니다. ZTA 등록, VPNaaS 인증 또는 특정 Umbrella Roaming 설정을 위한 Entra ID 또는 기타 IdP(Identity Providers)의 컨피그레이션은 이 가이드의 범위를 벗어납니다.

구성

Cisco Secure Access 구성

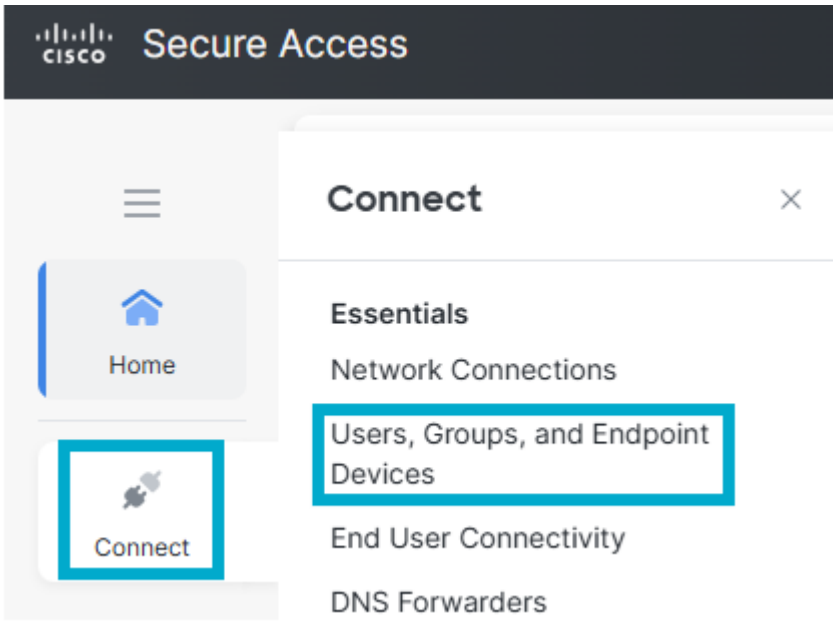
프로비저닝 프로세스를 시작하려면 먼저 Cisco Secure Access 대시보드 내에서 디렉토리 통합을 구성해야 합니다. 이 단계에서는 OKTA와의 보안 연결을 설정하는 데 필요한 자격 증명 및 컨피그레이션 매개변수를 생성합니다.

1. Cisco Secure Access Dashboard에 로그인합니다.



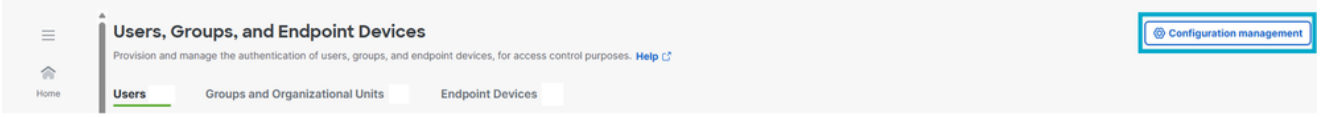
CSA에 로그인

2. Connect(연결) > Users, Groups and Endpoint Devices(사용자, 그룹 및 엔드포인트 디바이스)로 이동합니다.



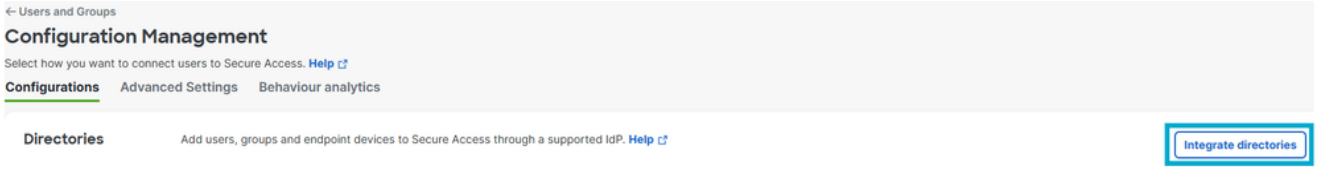
사용자 및 그룹

3. Configuration management(컨피그레이션 관리)를 클릭합니다.



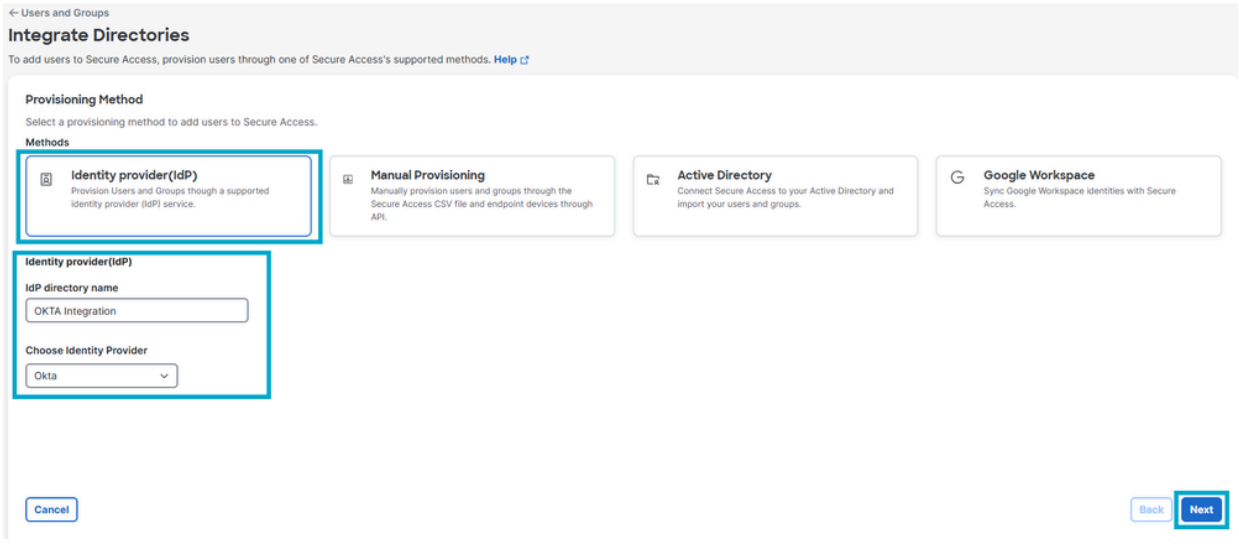
컨피그레이션 관리

4. 디렉토리 통합을 클릭합니다.



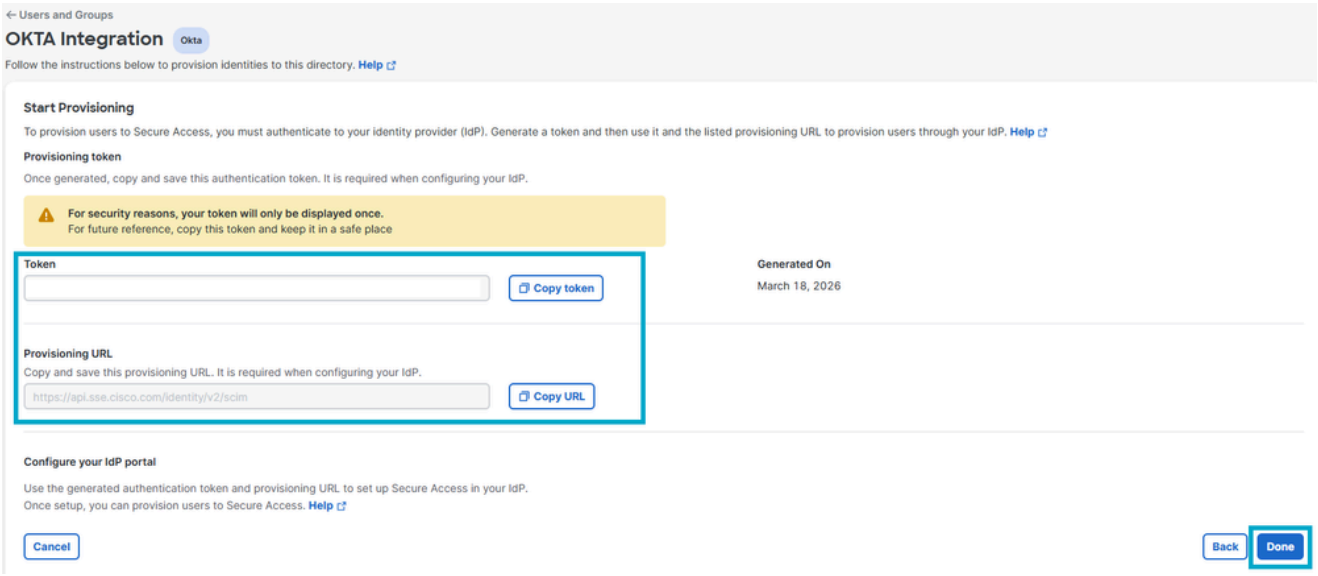
디렉터리 통합

5. Provision Method(프로비저닝 방법)에서 Identity Provider(ID 제공자)를 클릭합니다.
    - IdP 디렉터리 이름: OKTA 통합.
    - ID 공급자 선택: 좋아.
    - Next(다음)를 클릭합니다.



Directory Configuration

6. 토큰 생성을 누릅니다. 생성된 토큰과 프로비전 URL을 저장한 다음 완료를 누릅니다.

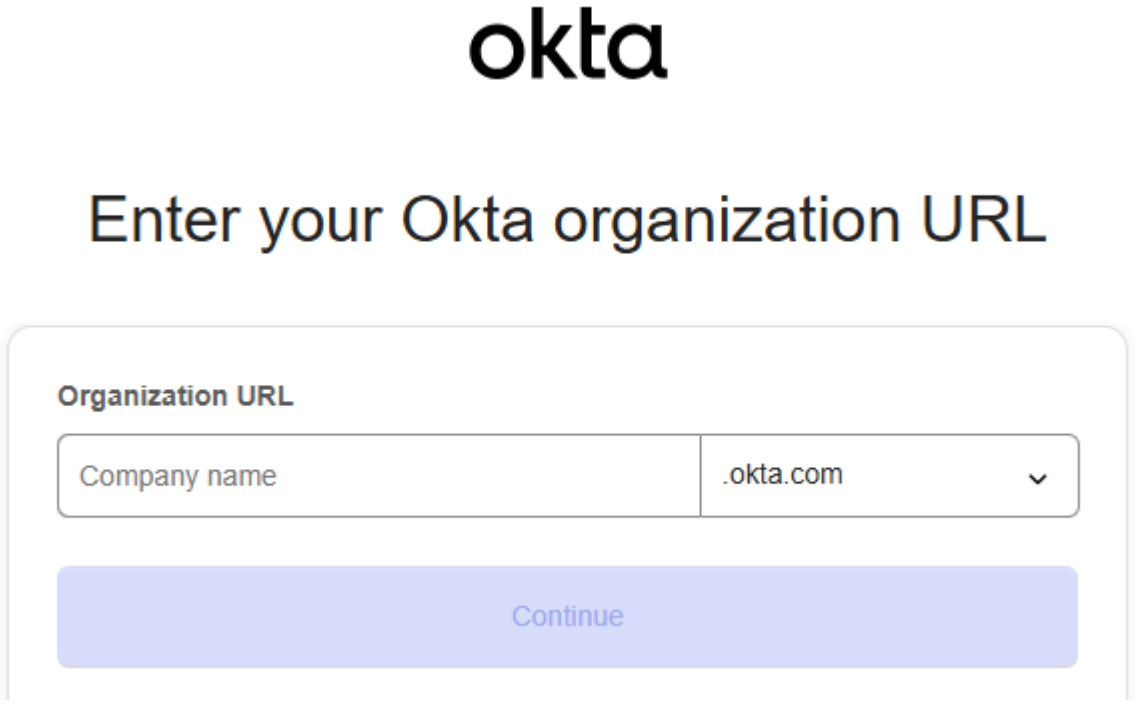


토큰 생성

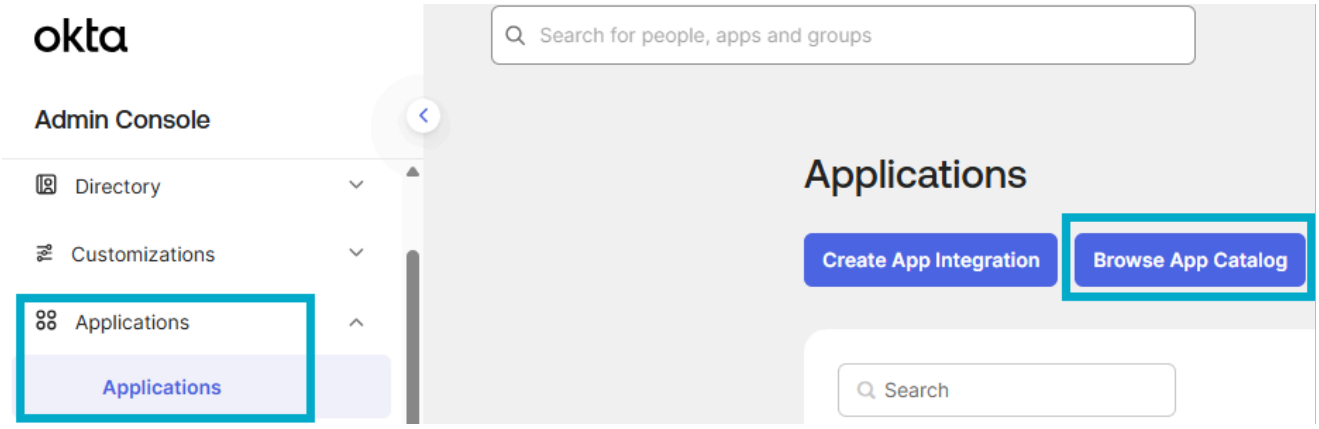
OKTA에서 프로비저닝 구성

Cisco Secure Access 대시보드에서 자격 증명을 생성한 후에는 OKTA 테넌트 내에서 프로비저닝 설정을 구성하여 사용자 및 그룹의 동기화를 활성화해야 합니다.

1. OKTA에 로그인합니다.

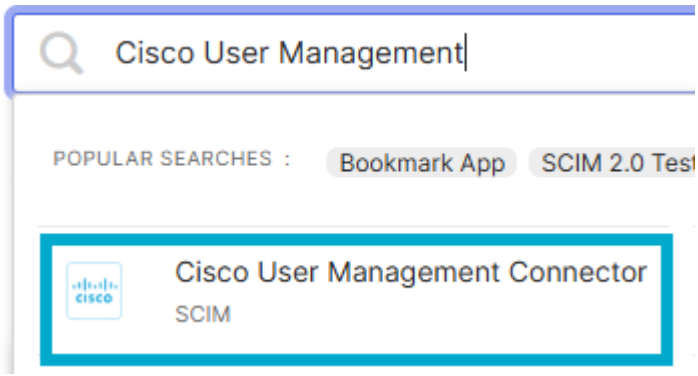


2. Applications(애플리케이션) > Browser App Catalog(브라우저 앱 카탈로그)로 이동합니다.



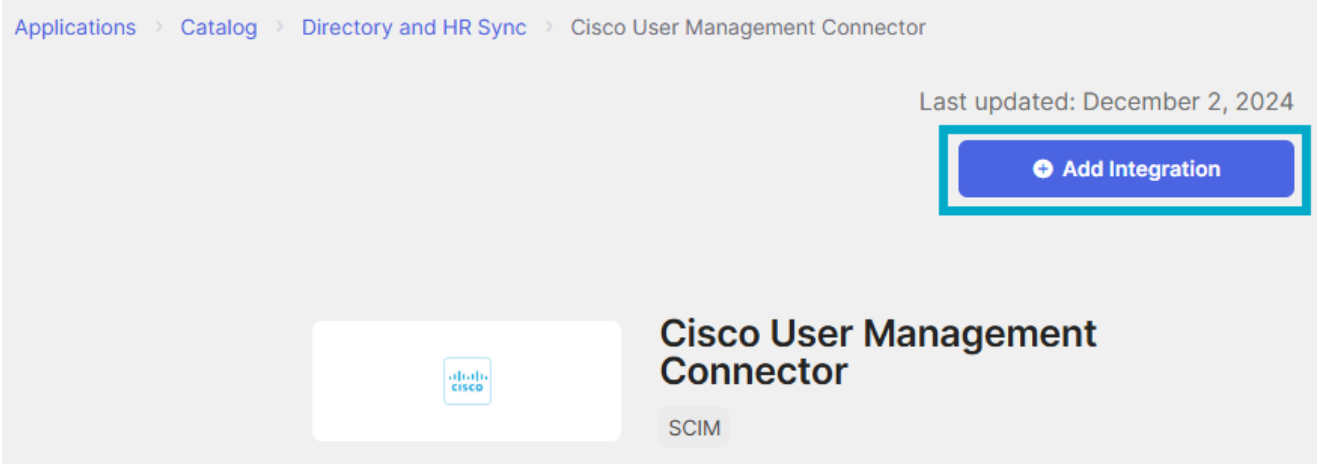
앱 카탈로그 찾아보기

3. Cisco User Management Connector 앱을 선택합니다.



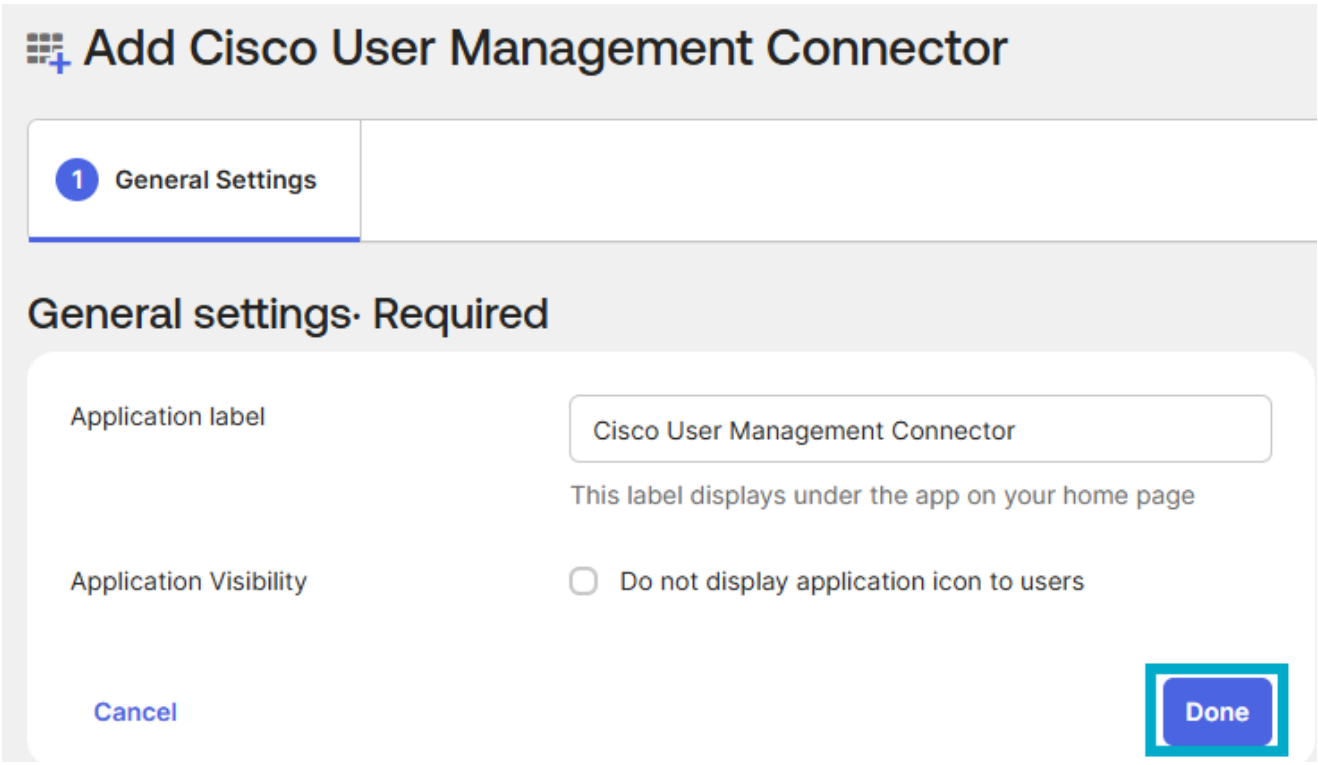
Cisco 앱

4. Add Integration(통합 추가)을 클릭합니다.



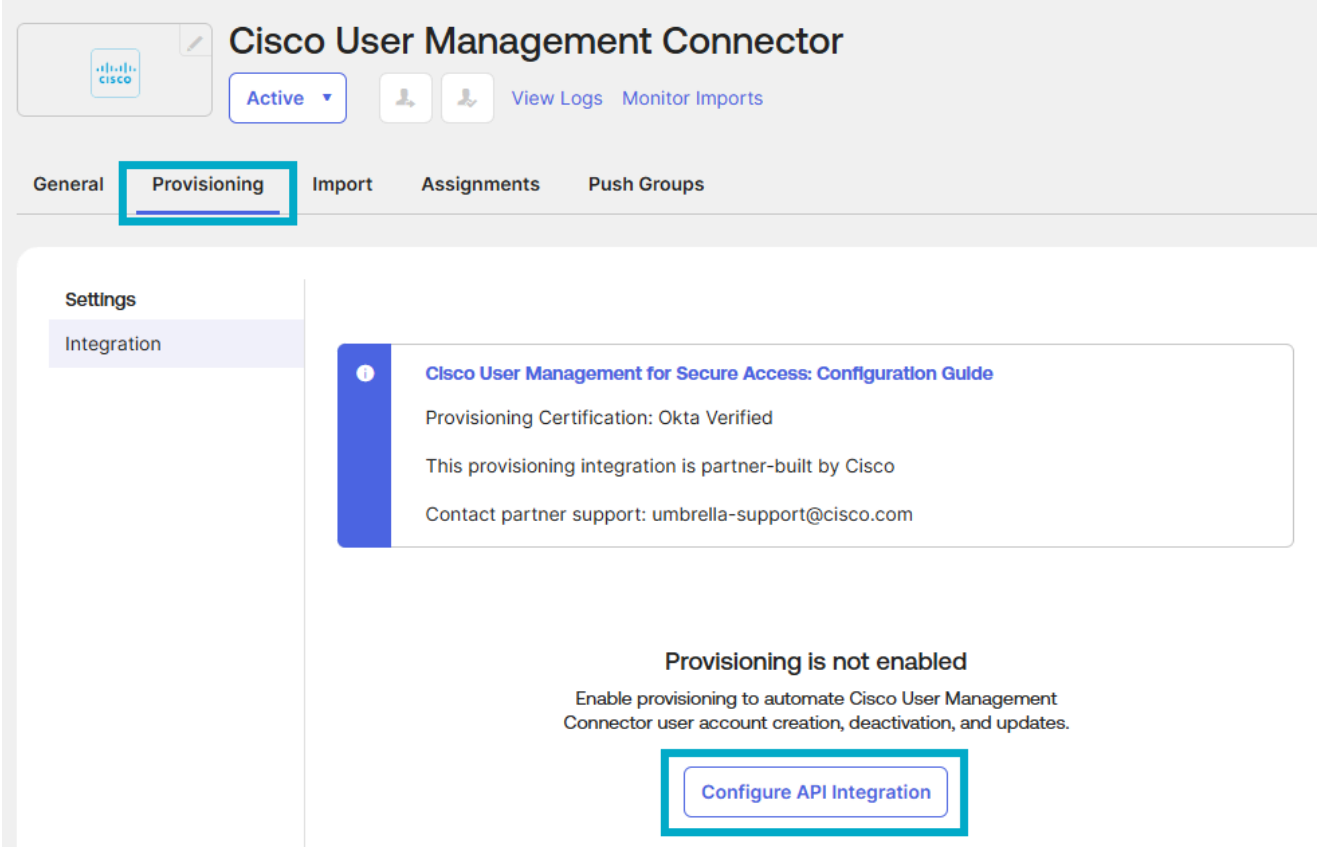
통합 추가

5. 완료를 클릭합니다.



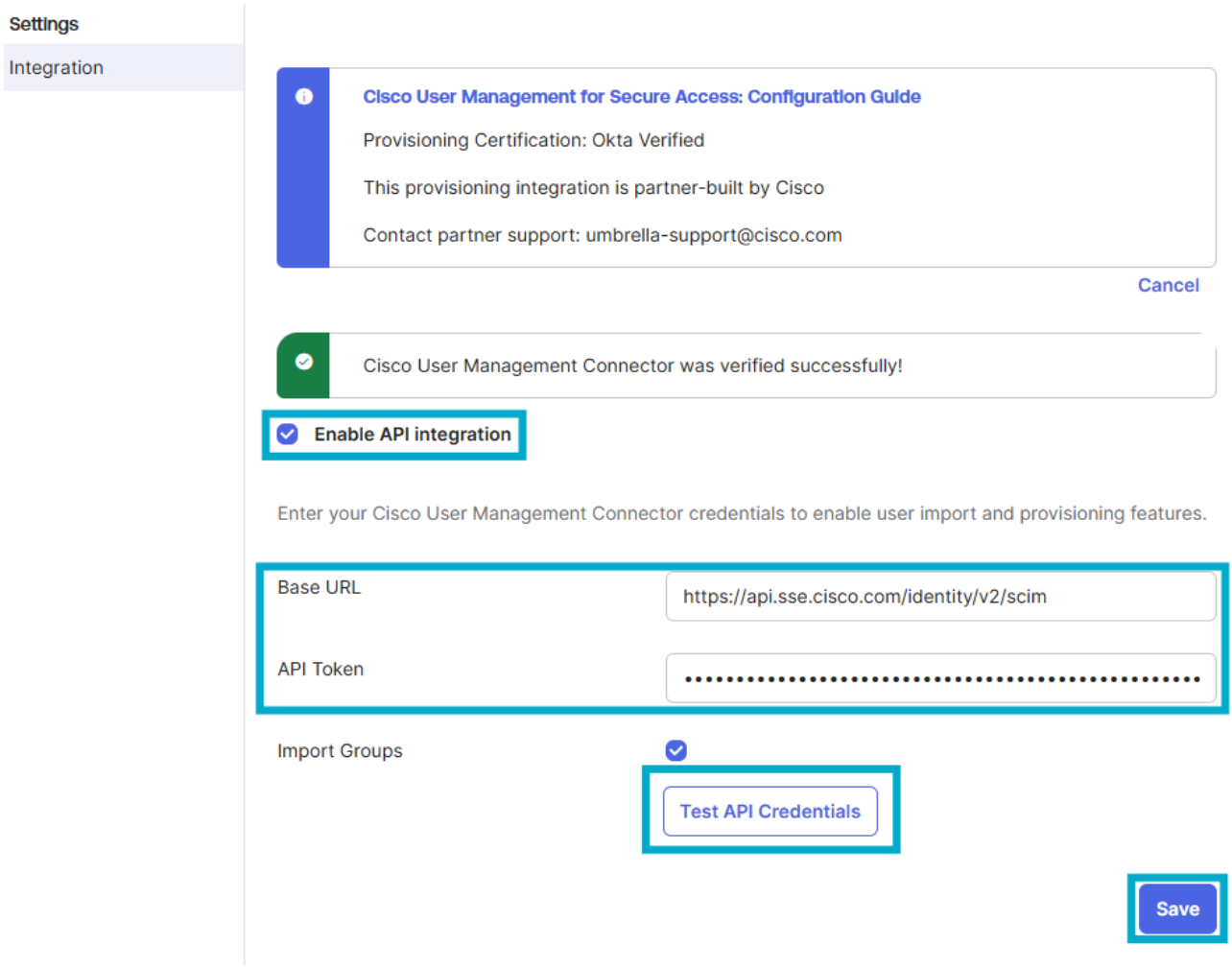
앱 추가

6. Provisioning(프로비저닝) > Configure API Integration(API 통합 구성)을 클릭합니다.



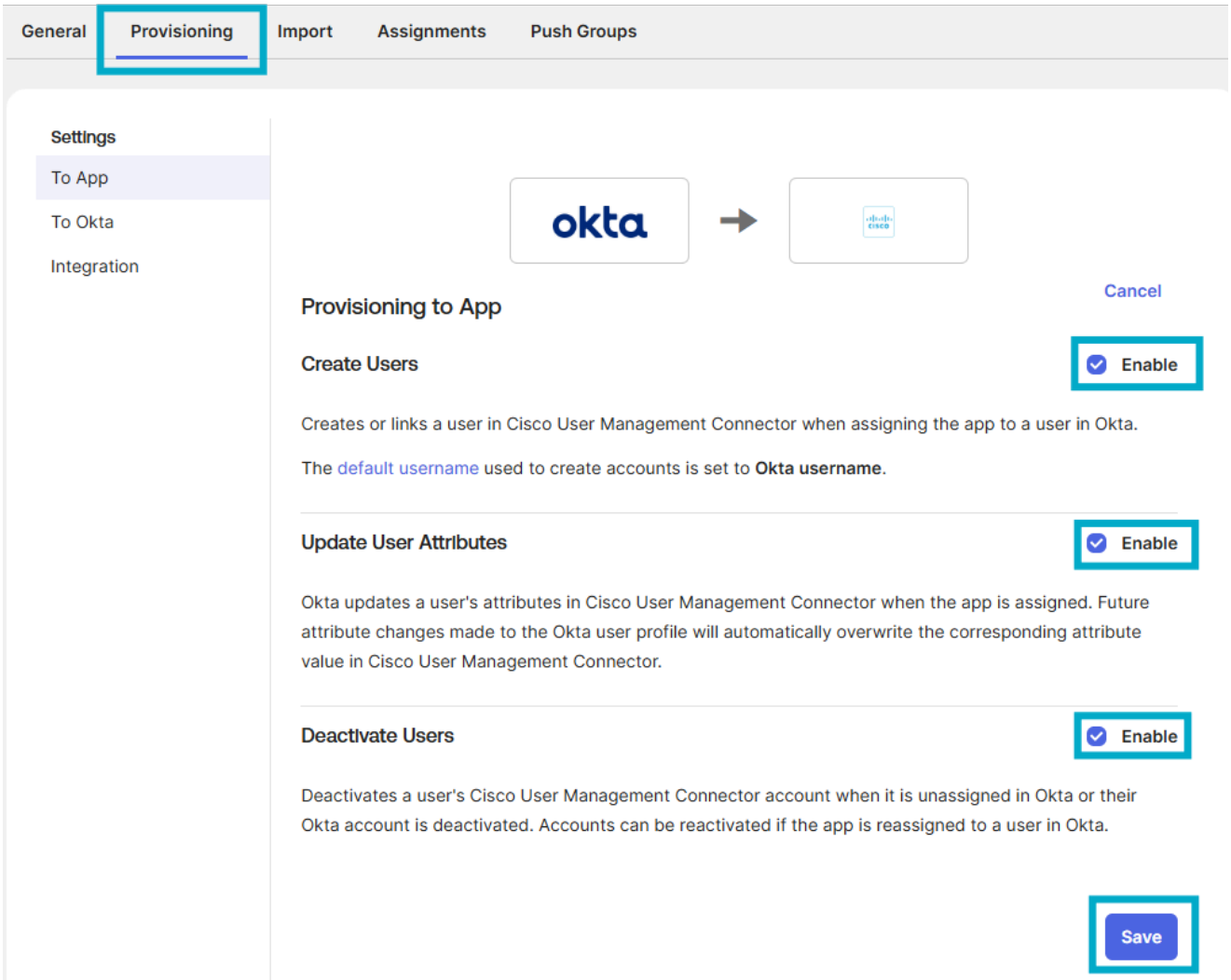
API 통합 구성

7. Enable API Integration(API 통합 활성화)을 클릭하고 Secure Access Configuration(보안 액세스 컨피그레이션)의 #6단계에서 저장된 Based URL and API Tokensaved(기반 URL 및 API 토큰)를 입력합니다. Test API Credentials(API 자격 증명 테스트)를 클릭한 다음 Save(저장)를 클릭합니다.



API 테스트

8. Provisioning(프로비저닝) > To App(애플리케이션으로)으로 이동합니다. Create Users(사용자 생성), Update User Attributes(사용자 특성 업데이트) 및 Deactivate Users(사용자 비활성화) 옵션을 활성화하고 Save(저장)를 클릭합니다.

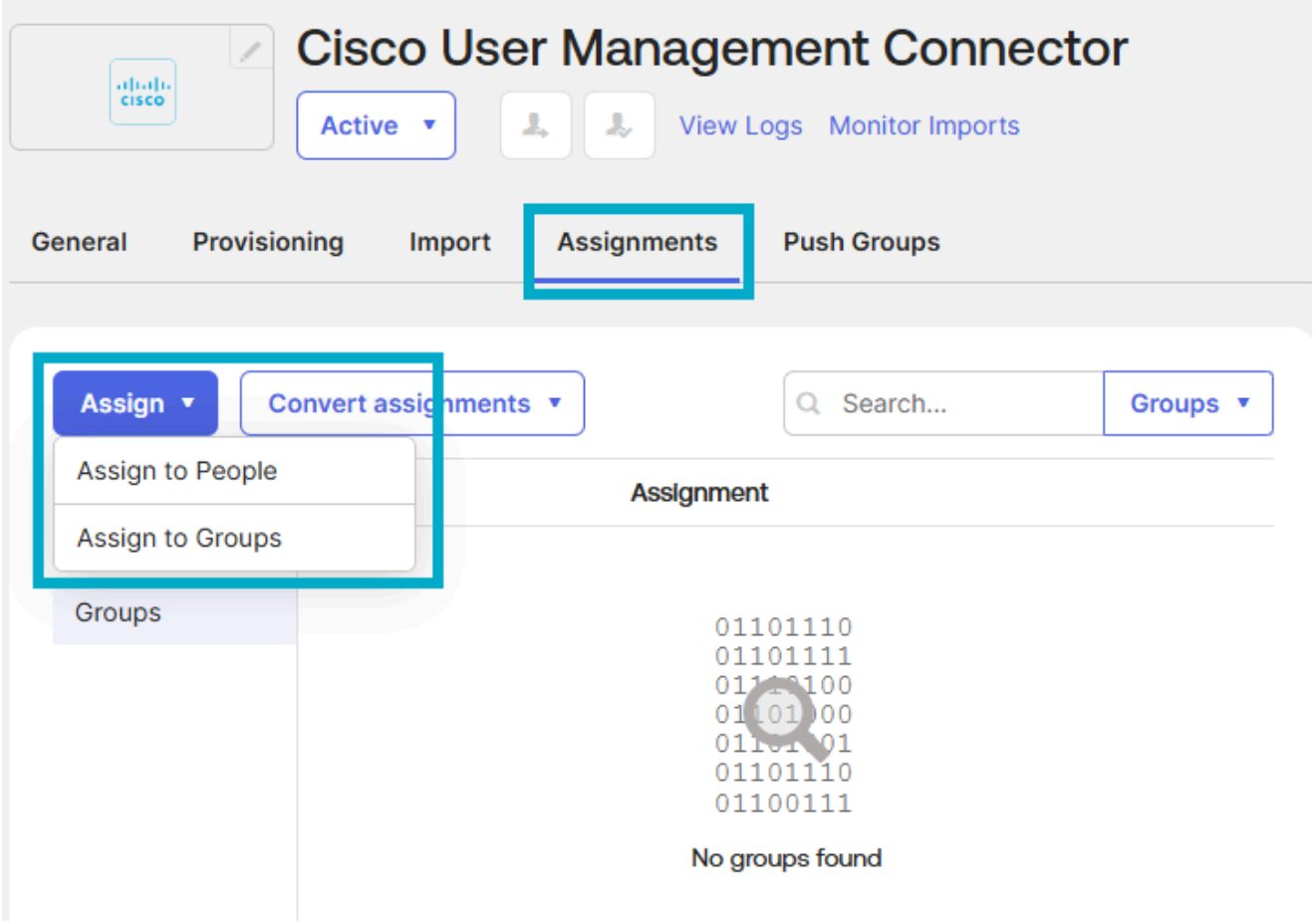


앱에 프로비전

참고: Secure Access로 동기화하기 위해 이러한 특성을 선택했는지 확인합니다. Secure Access에는 사용자에 대한 표시 이름 및 사용자 이름 특성만 나열되며, 지정된 이름 및 제품군 이름 특성은 나열되지 않습니다. 사용자 이름, 지정된 이름, 제품군, 이름, 표시 이름, 이메일

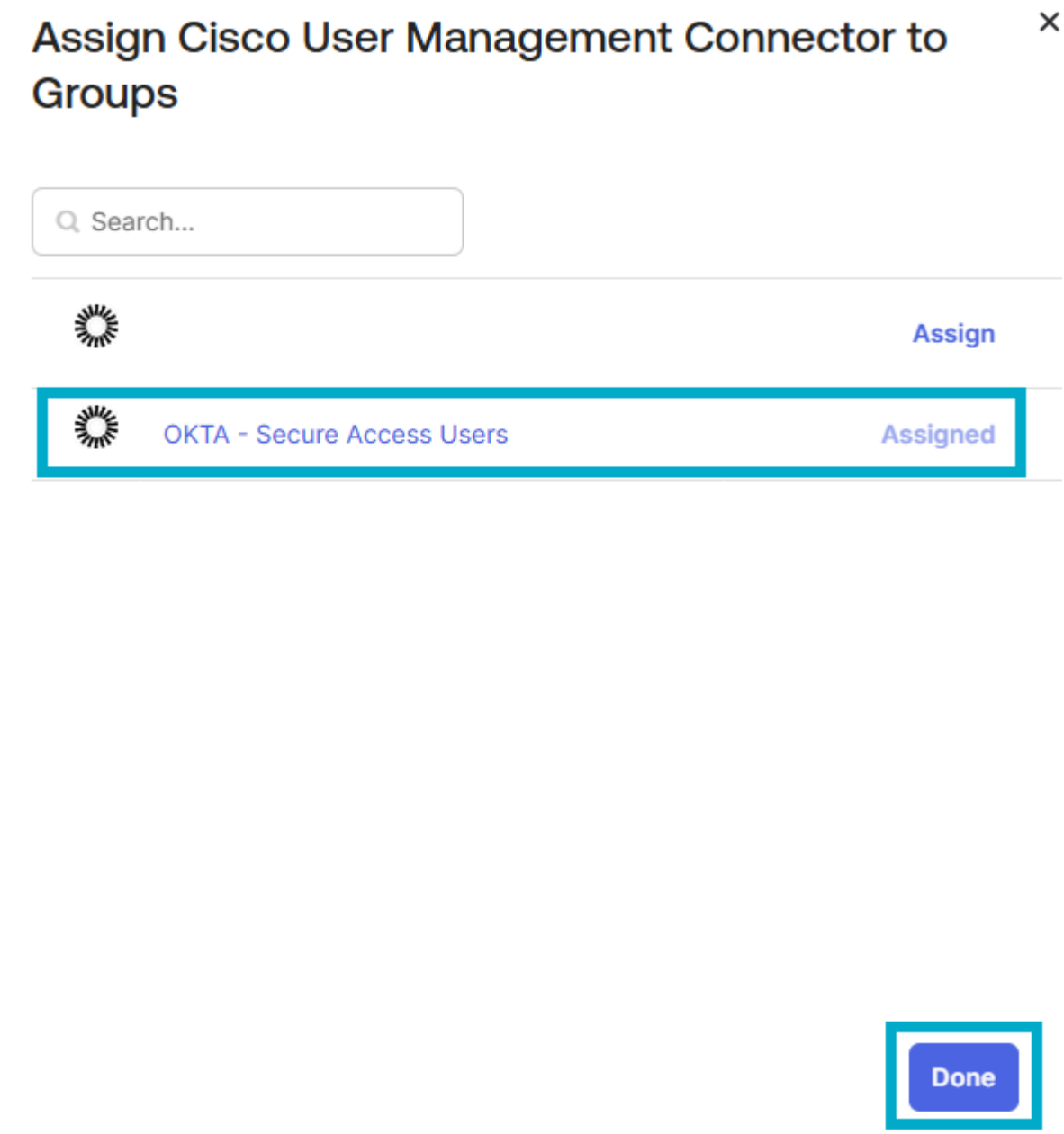
(선택 사항) objectGUID 특성을 추가하고 사용자 프로필 매핑을 만듭니다. 사용자에 대한 objectGUID 특성을 가져와야 하는 경우 새 특성을 추가하고 프로필 매핑에서 특성을 매핑합니다.

9. 사람/그룹을 추가하려면 발령 > 발령 > 인력에 지정/그룹에 지정을 누릅니다.



할당

10. Secure Access에 프로비저닝할 그룹/사용자를 선택하고 Assign(할당)을 클릭한 다음 Done(완료)을 클릭합니다.

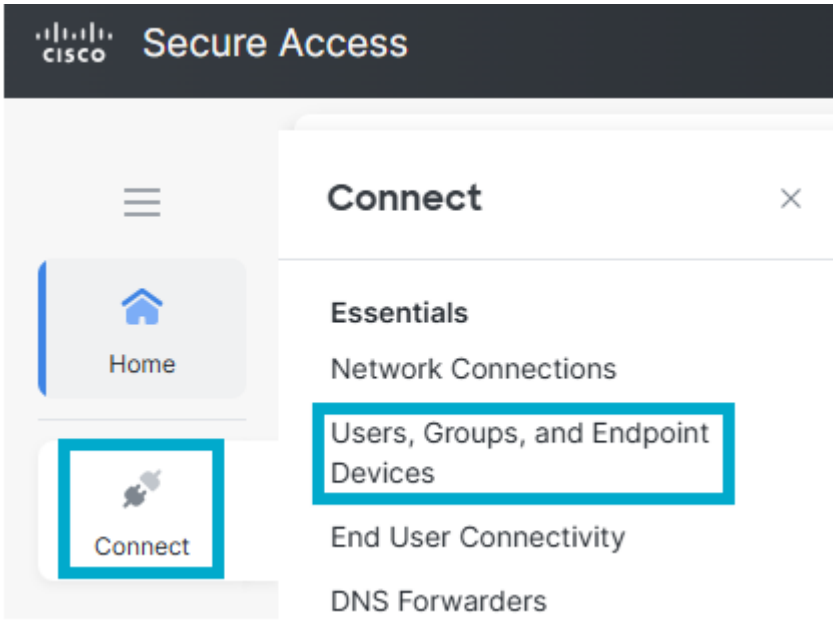


그룹 할당

다음을 확인합니다.

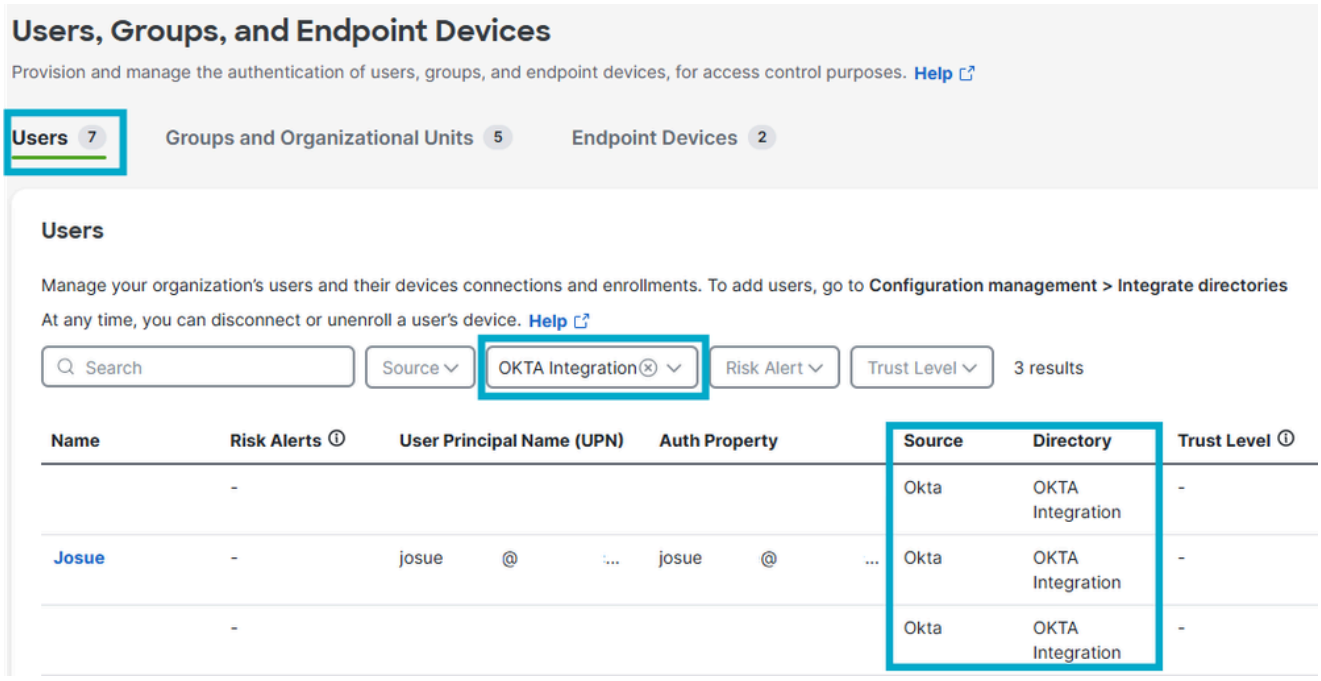
Cisco Secure Access의 Verity

- Connect(연결) > Users, Groups and Endpoint Devices(사용자, 그룹 및 엔드포인트 디바이스)로 이동합니다.



CSA의 사용자 및 그룹

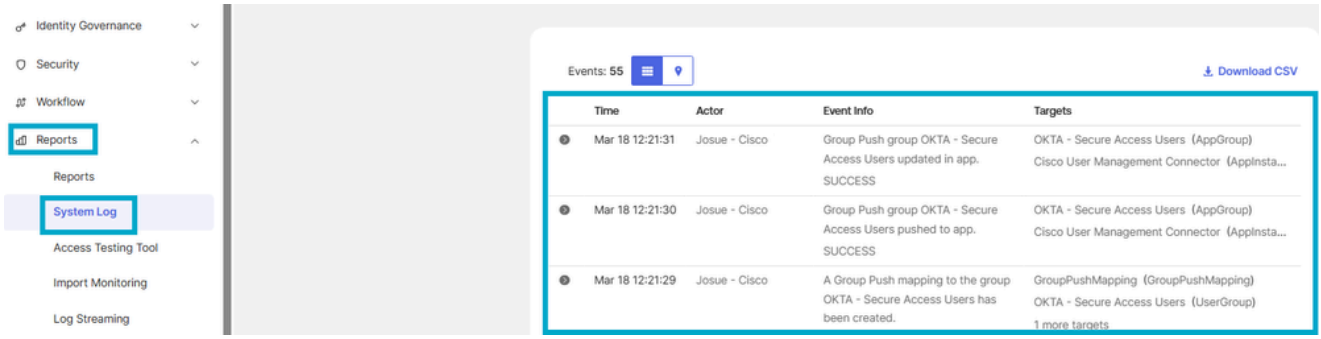
- Users를 클릭합니다.



CSA의 사용자 확인

오크타의 베리티

- Reports(보고서) > System Log(시스템 로그)로 이동합니다.



OKTA 로그

관련 정보

[ID 제공자 구성]

[Okta에서 사용자 및 그룹 프로비저닝]

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.