SD-WAN에서 OKTA SSO(Single Sign-On) 구성

목차

소개

이 문서에서는 SD-WAN(Software-Defined Wide Area Network)에서 OKTA SSO(Single Sing-On)를 통합하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- SD-WAN 일반 개요
- SAML(Security Assertion Markup Language)
- IdP(ID 공급자)
- 인증서

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco vManage 릴리스 18.3.X 이상

- Cisco vManage 버전 20.6.3
- Cisco vBond 버전 20.6.3
- Cisco vSmart 버전 20.6.3

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

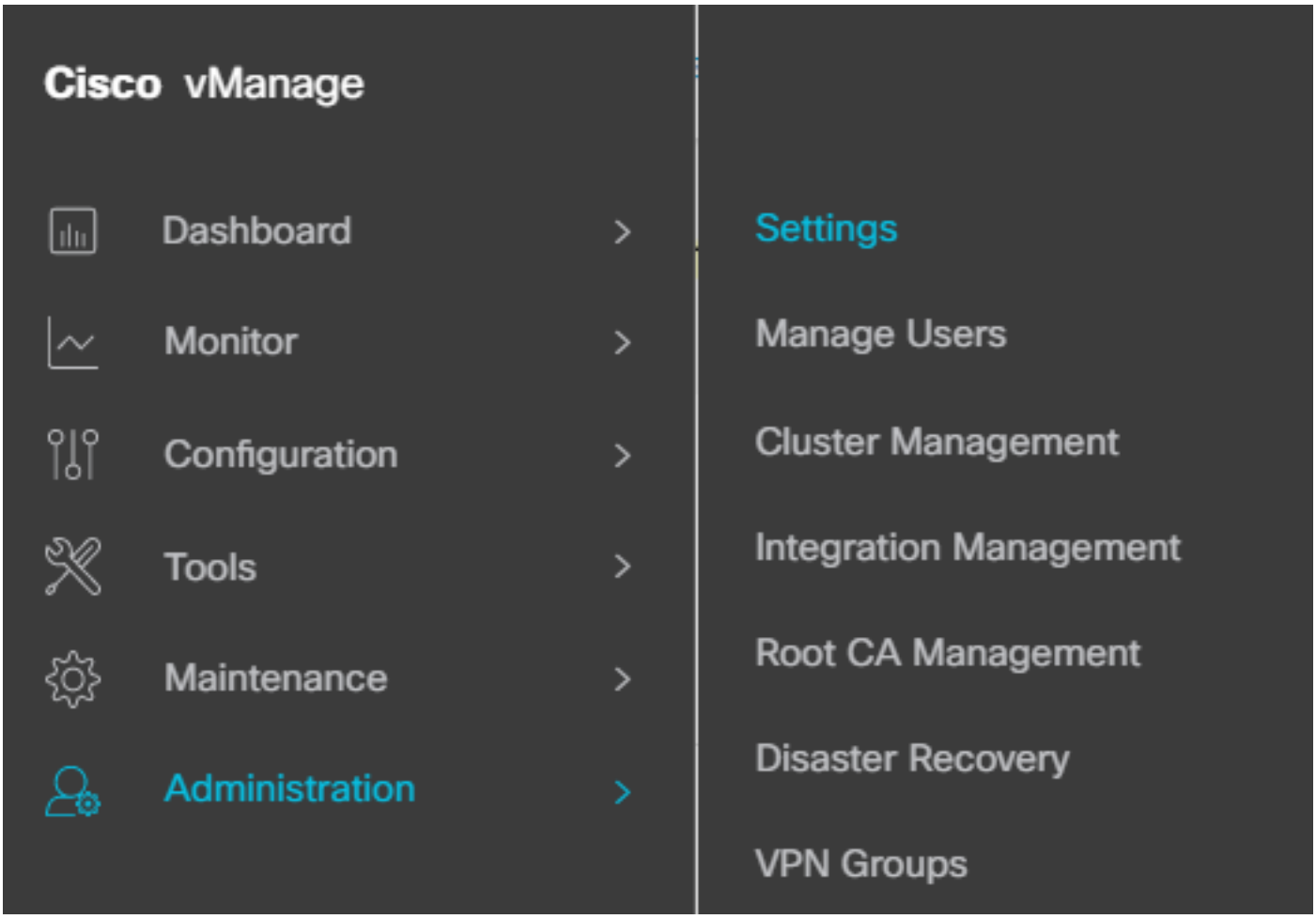
SAML(Security Assertion Markup Language)은 당사자 간에, 특히 ID 제공자와 서비스 제공자 간에 인증 및 권한 부여 데이터를 교환하기 위한 개방형 표준입니다. SAML의 이름에서 알 수 있듯이, SAML은 보안 어설션(통신 사업자가 액세스 제어 결정을 내리는 데 사용하는 명령문)을 위한 XML 기반 마크업 언어입니다.

IdP(Identity Provider)는 다른 웹 사이트에 액세스하기 위해 SSO(Single Sign-On)를 사용할 수 있는 신뢰할 수 있는 공급자입니다. SSO는 비밀번호 피로도를 줄이고 사용성을 개선합니다. 잠재적 공격 표면을 줄이고 더 우수한 보안을 제공합니다.

구성

vManage 컨피그레이션

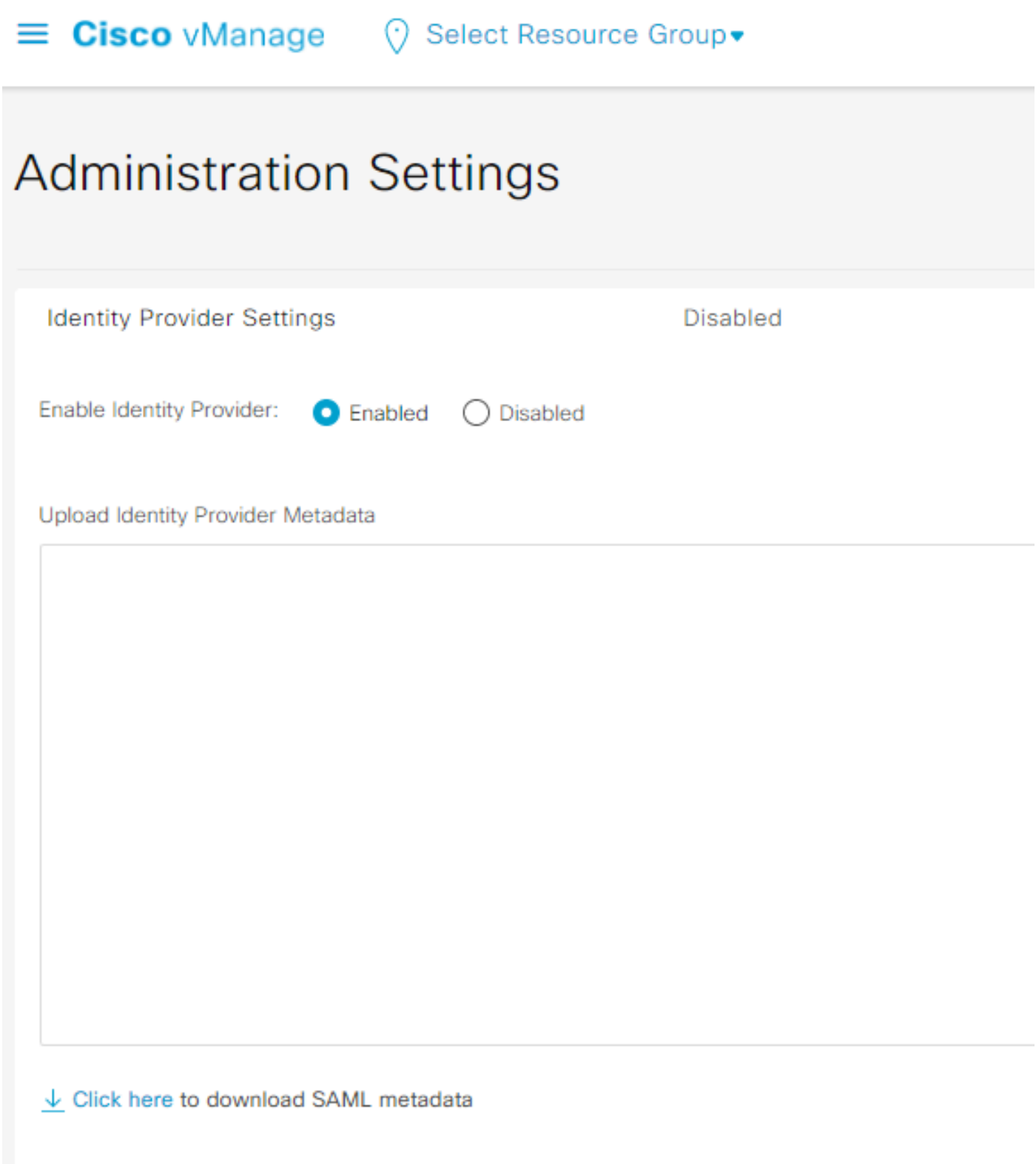
1. Cisco vManage에서 Administration(관리) > Settings(설정) > Identify Provider Settings(사업자 설정 식별) > Edit(편집)로 이동합니다.



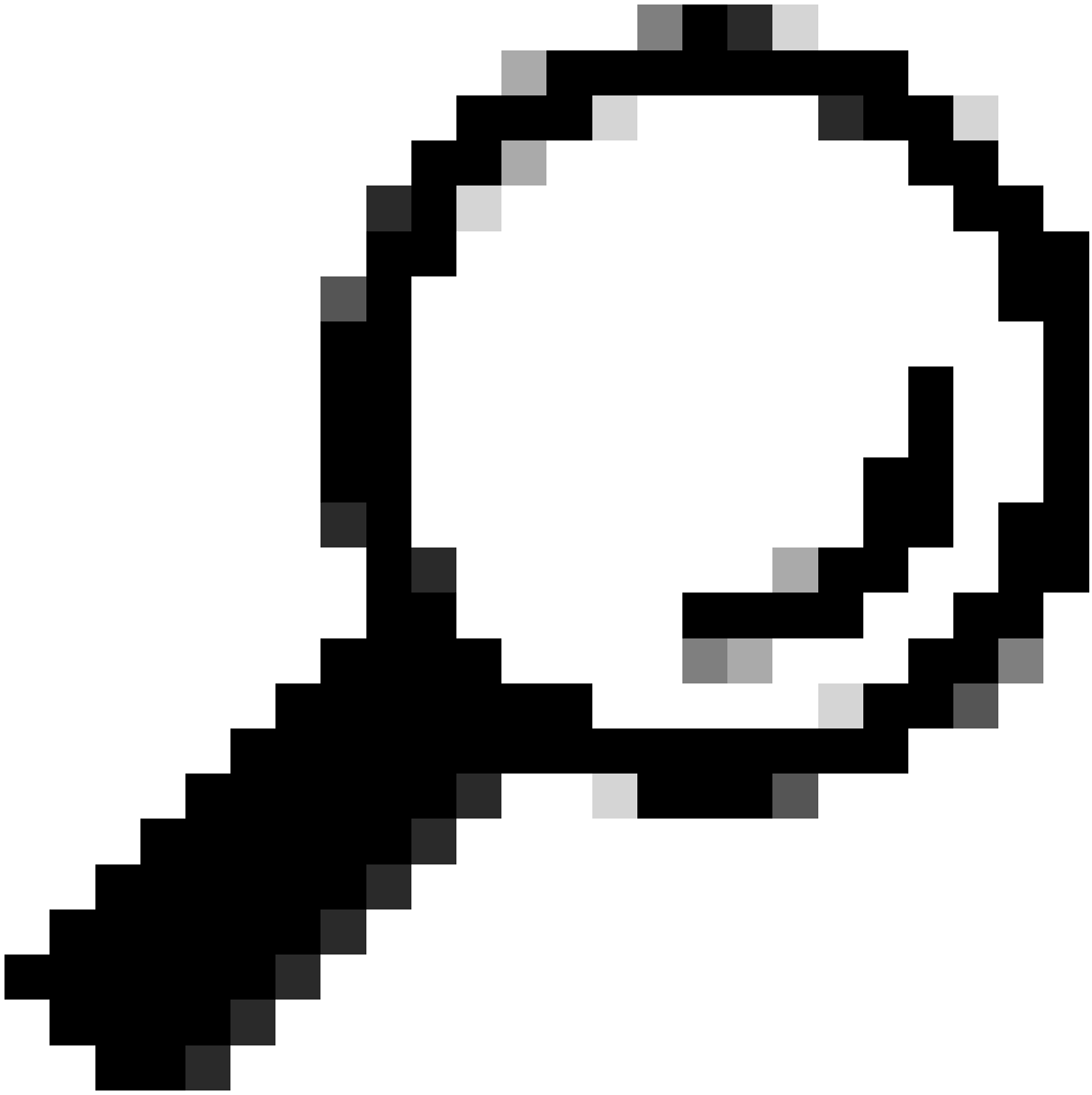
Configuration(구성) > Settings(설정)

2. 사용을 클릭합니다.

3. SAML 메타데이터를 다운로드하고 파일에 내용을 저장하려면 클릭합니다. 이것은 OKTA 측에 필요합니다.


Cisco vManage
Select Resource Group
Administration Settings
Identity Provider Settings
Disabled
Enable Identity Provider:
Enabled
Disabled
Upload Identity Provider Metadata
Click here to download SAML metadata

SAML 다운로드



팁: Cisco vManage로 OKTA를 구성하려면 메타데이터에서 이러한 정보가 필요합니다.

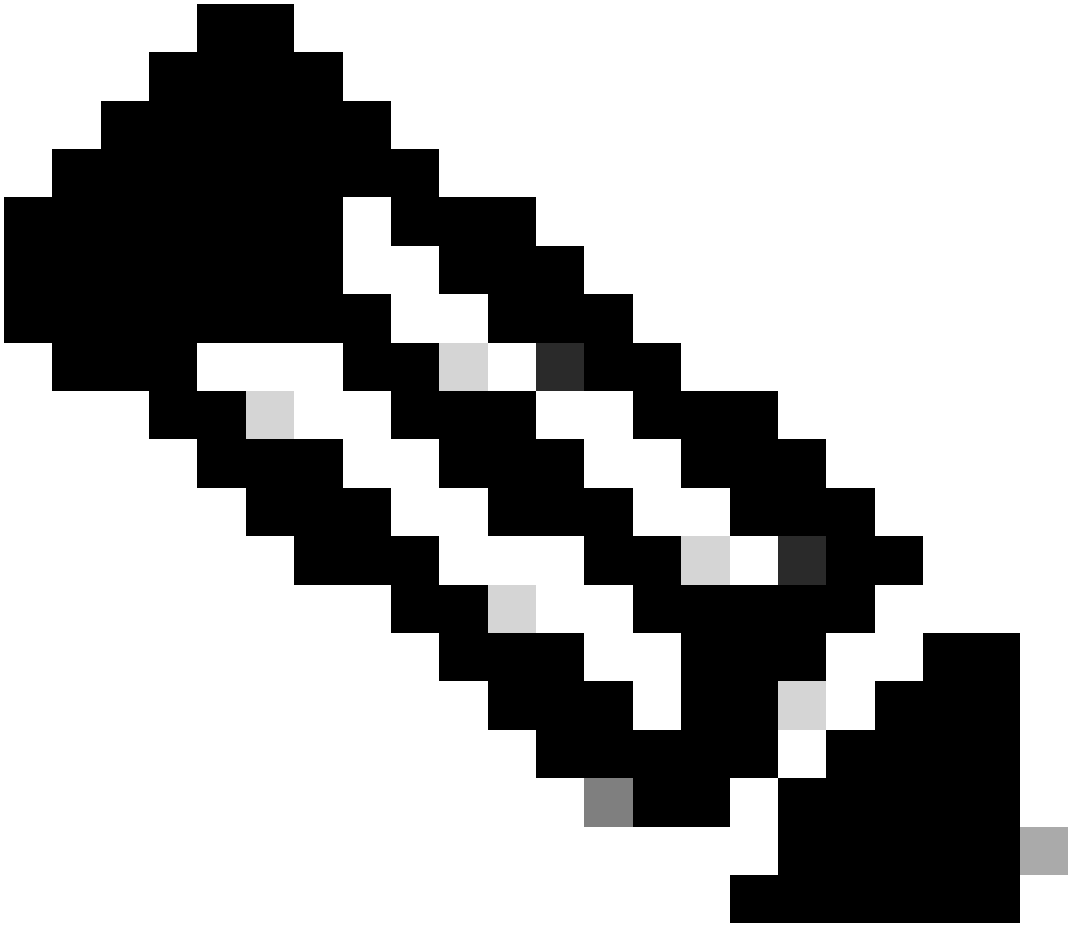
a. 엔티티 ID

b. 서명 인증서

c. 암호화 인증서

d. 로그아웃 URL

e. URL 로그인



참고: 인증서는 x.509 형식이어야 하며 .CRT 확장자로 저장해야 합니다.

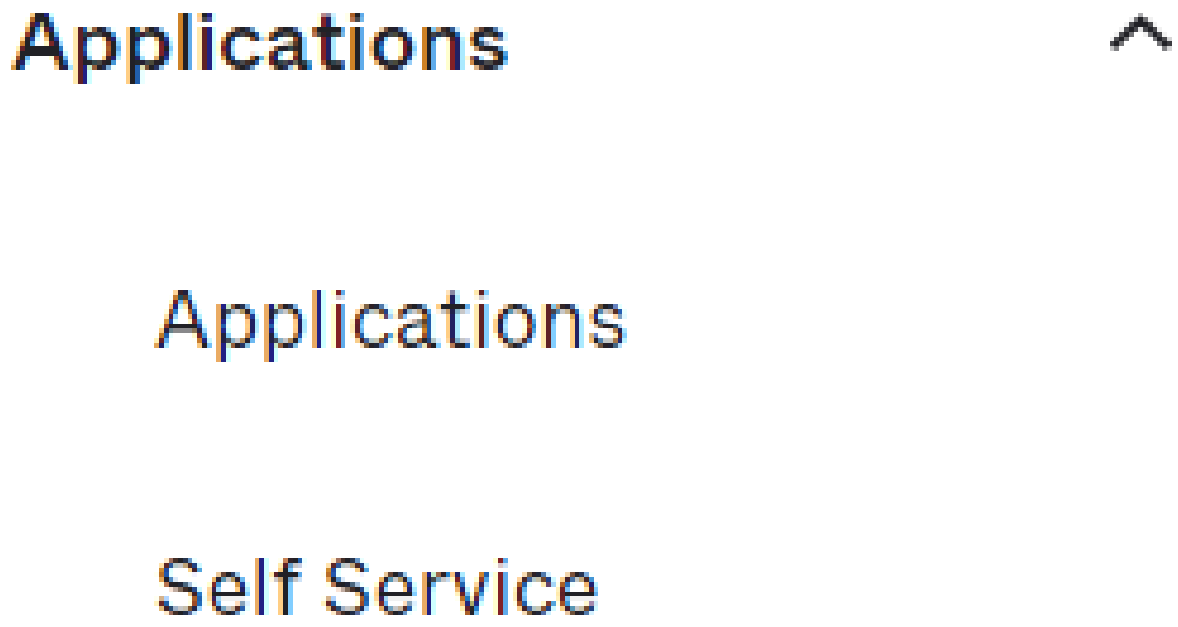
```
-----BEGIN CERTIFICATE-----
MIIDfTCCAmWgAwIBAgIhAM8T9QVLqX/lp1oK/q2XNUbJcGhRmGvqdXxGTUkrKUBhMA0GCSqGSIb3
DQEBCwUAMHIxDDAKBgNVBAYTA1VTQTELMAkGA1UECBMCQ0ExETAPBgNVBAcTCFNhbiBKb3NlMRQw
EgYDVQQKEwtDSVNDT1JUUExBQjEUMBIGA1UECxMLQ01lTQ09SVFBMQUIxFjAUBgNVBAMTDURlZmF1
bHRUZW5hbnQwHhcNMjAwNTI4MTQxMzQzWhcNMjUwNTI4MTQxMzQzWjByMQwwCgYDVQQGEwNVU0Ex
CzAJBgNVBAgTAkNBMREwDwYDVQQHEwhTYW4gSm9zZTEUMBIGA1UEChMLQ01lTQ09SVFBMQUIxFDAS
BgNVBAsTC0NJU0NPUlRQTEFCMRYwFAYDVQQDEw1EZWZhdWx0VGVuYW50MIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAg9HOIwjWHD3pbkCB3wRUsn01PTsNAhCqRKOf5aY4QDWbu7U3+6gF
TzZgrB9189rLSkkb7cEzRcE7ZbZ1a3zICVw76ZN8jj2BZMYpuTLS9LSGRq2FClYMAg6JU4Yc9prg
T6IcmJKHPfuFM3izXKVsrzfn8tDZ7UDHGIUNPs2kjntamU4ZB7BRTE1zJXp+Zh3CvnfLE9g3aXK9
SM9qRFDjAaC8GhWphOYyK3RisQZ/bIZJ2vWkVo91p+6/kQy7/oxFKznK/2oAXaAe26P8HYw+XC0b
mkCwb3e9a1vCGrCmPJwJPjn9j09dX426/LbjdmDAo6HudjTEoQMZduD3Z9GU5QIDAQABMA0GCSqG
SIb3DQEBCwUAA4IBAQBbO/FdHT365rzOHpgHo8YWbxbYdhjAMrHUBbuXLq6MEaHvm4GoTYsgJzc9
Scy/Iwoa6kRjBXHJPPthtBwzYYXvK6CJxh8J/r1ednlmai0z9growg/sSEgbXPpuQw6qT9hM8s2i
FHlFcHPoqiaZFldNF4iupuzFPTcD8kmzEC3mGlcxfm2TaVjLFDu7McRAmLZTV+yPY+WZXjuoMI8P
hXapKdUt0B6RxzuCBRac2ZB22g7HWDQuDZUzf966Q2k5Us1QxtNlpXLU5X+i+YDW01lT2AP6+UUi
vrN1A6vFVPP3QtAd7ao7VziMeEvxfYTuK690b+ej4MNtWIKdHneU+/YC
-----END CERTIFICATE-----
```

X.509 인증서

OKTA 컨피그레이션

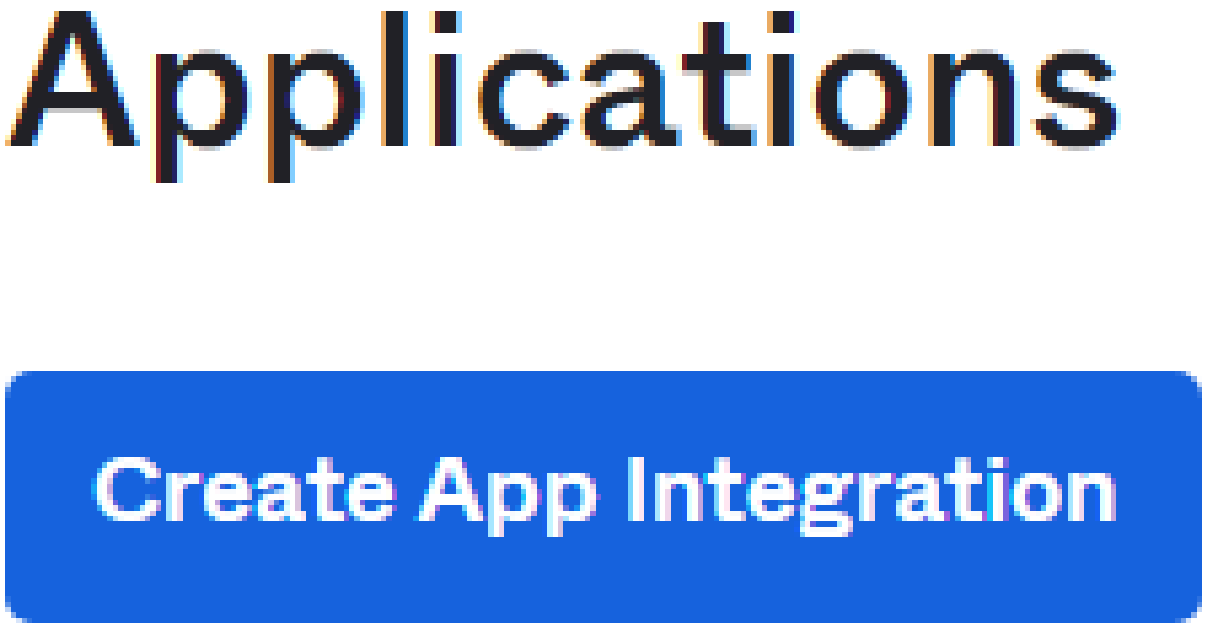
1. OKTA 계정에 로그인합니다.

2. 애플리케이션 > 애플리케이션으로 이동합니다.



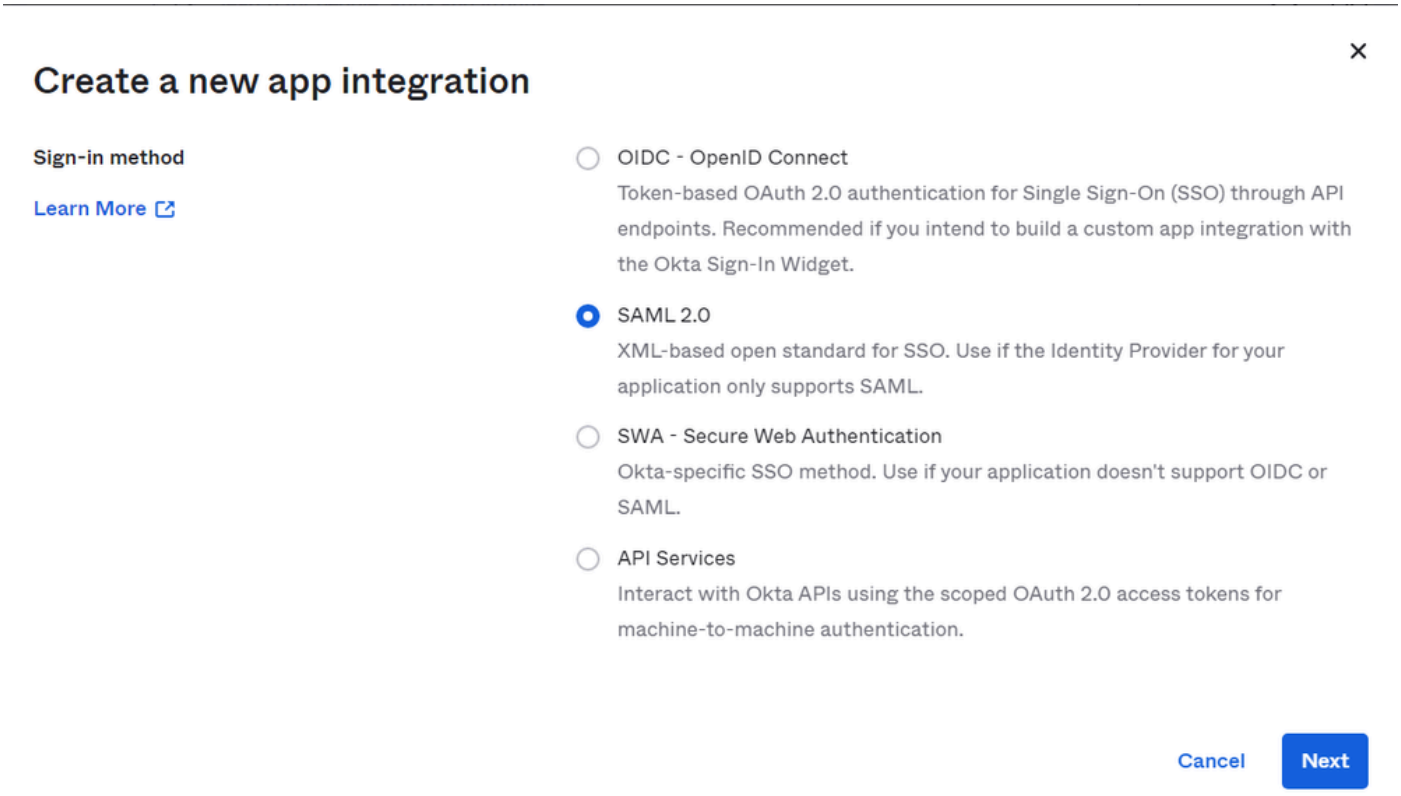
Applications(애플리케이션) > Applications(애플리케이션)

3. 클릭 앱 통합을 만듭니다.



응용 프로그램 만들기

4. SAML 2.0과 다음 을 클릭합니다.



SAML2.0 구성

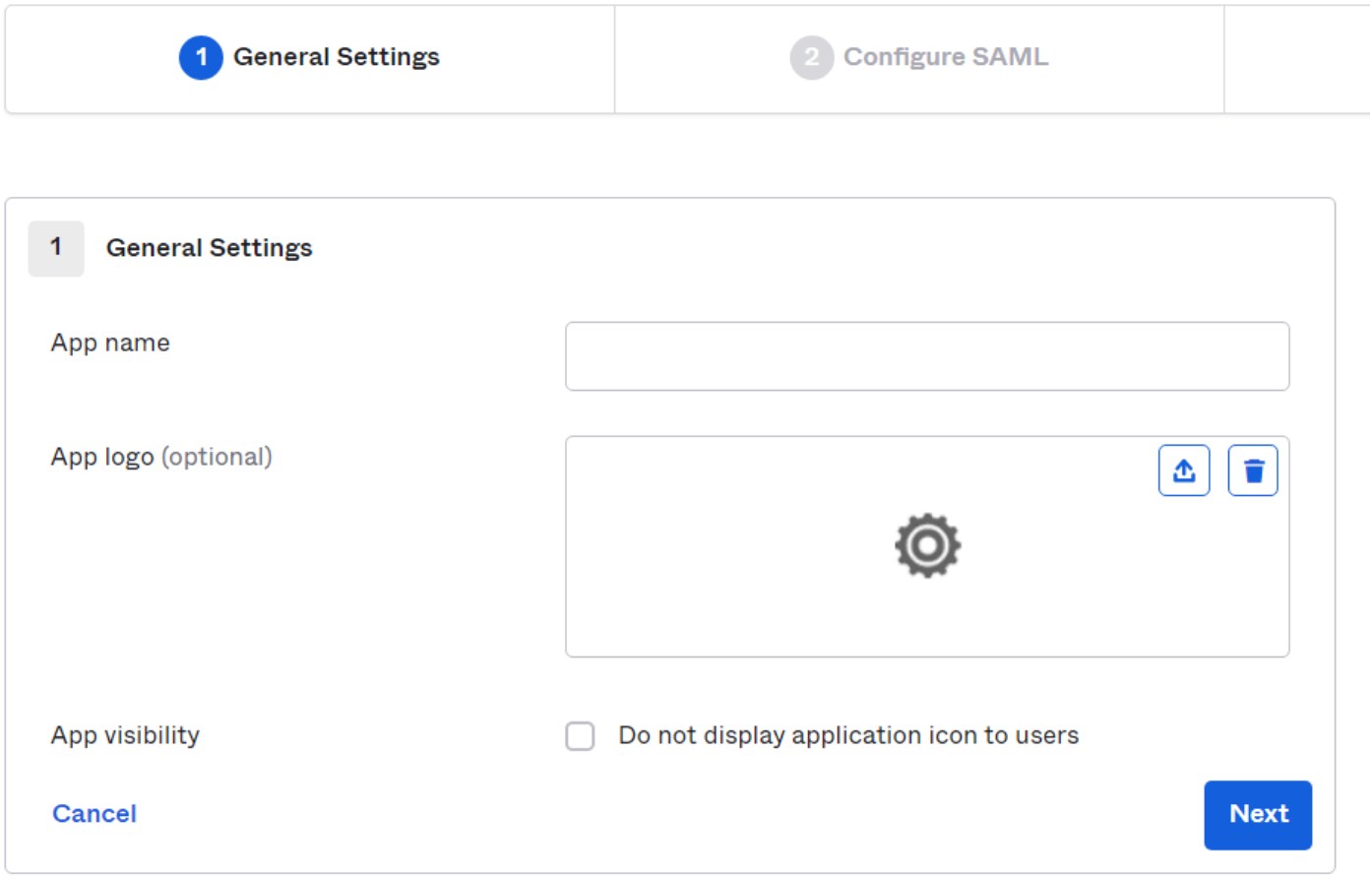
일반 설정

1. 지원명을 입력합니다.

2. 애플리케이션에 대한 로고를 추가합니다(선택 사항).

3. 앱 가시성(선택 사항)

4. 다음을 클릭합니다.



SAML 일반 설정

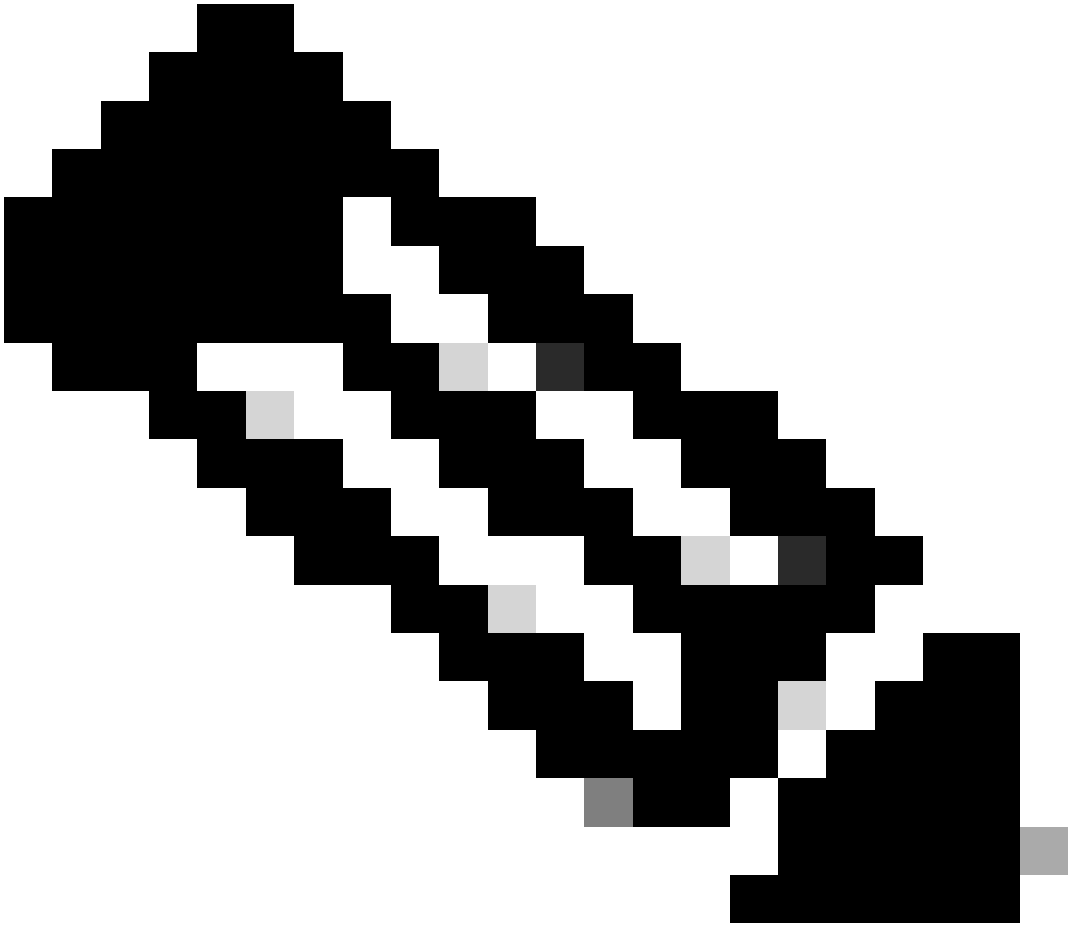
SAML 구성

이 표에서는 이 섹션에서 구성해야 하는 매개변수에 대해 설명합니다.

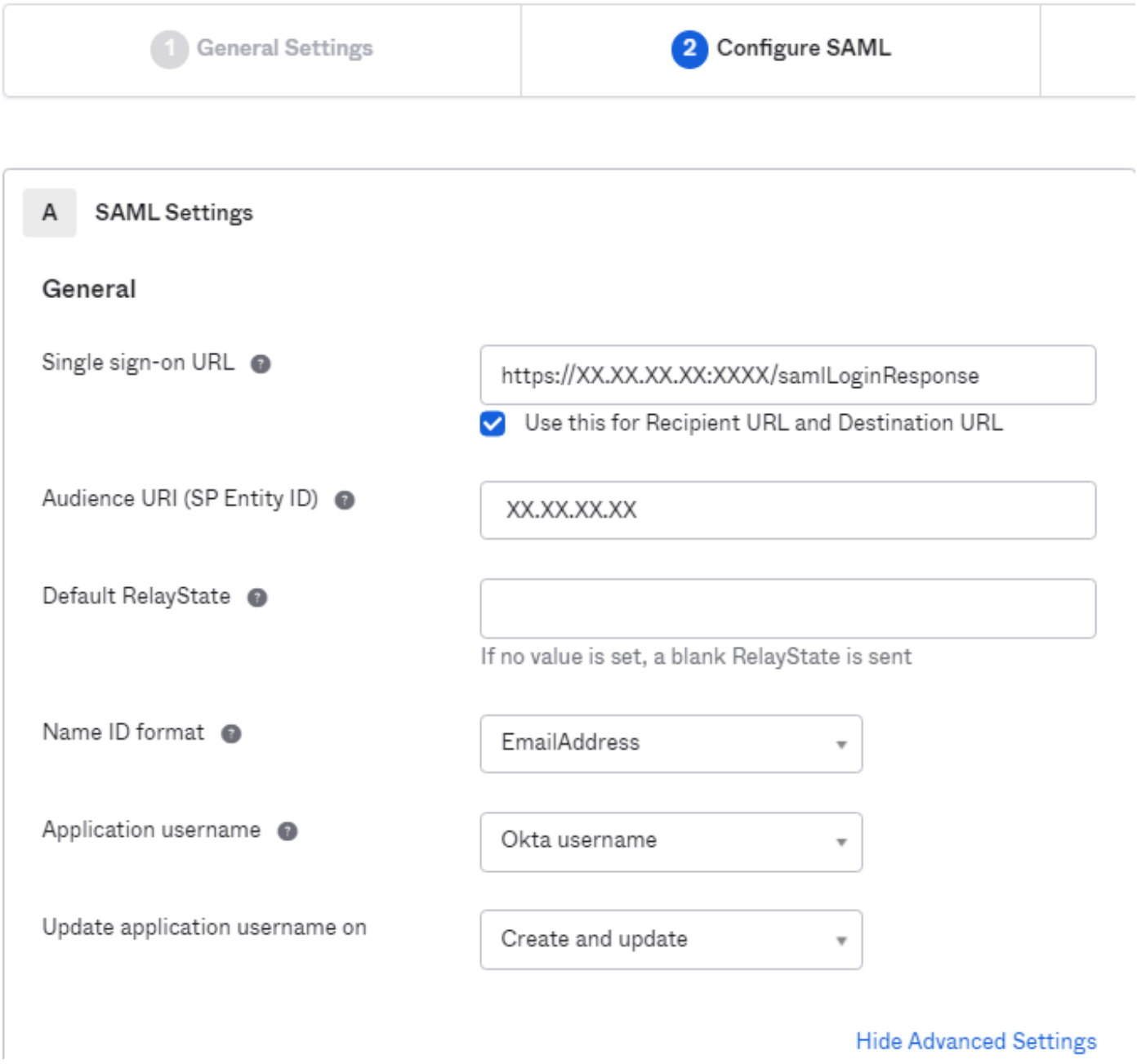
구성 요소	가치	설정
단일 로그인 URL	https://XX.XX.XX.XX:XXXX/samlLoginResponse	메타데이터에서 가져옵니다.
대상 그룹 URI(SP 엔티티 ID)	XX.XX.XX.XX	Cisco vManage의 IP 주소 또는 DNS

구성 요소	가치	설정
기본 릴레이 상태		비어 있음
이름 ID 형식		기본 설정에 따라
애플리케이션 사용자 이름		기본 설정에 따라
애플리케이션 사용자 이름 업데이트	생성 및 업데이트	생성 및 업데이트
응답	서명됨	서명됨
어설션 서명	서명됨	서명됨
서명 알고리즘	RSA-SHA256	RSA-SHA256
다이제스트 알고리즘	SHA256	SHA256
어설션 암호화	암호화	암호화
암호화 알고리즘	AES256-CBC	AES256-CBC
키 전송 알고리즘	RSA-OAEP	RSA-OAEP
암호화 인증서		메타데이터의 암호화 인증서는 x.509 형식이어야 합니다.
단일 로그아웃 사용		확인해 보세요.
단일 로그아웃 URL	https://XX.XX.XX.XX:XXXX/samlLogoutResponse	메타데이터에서 가져옵니다.

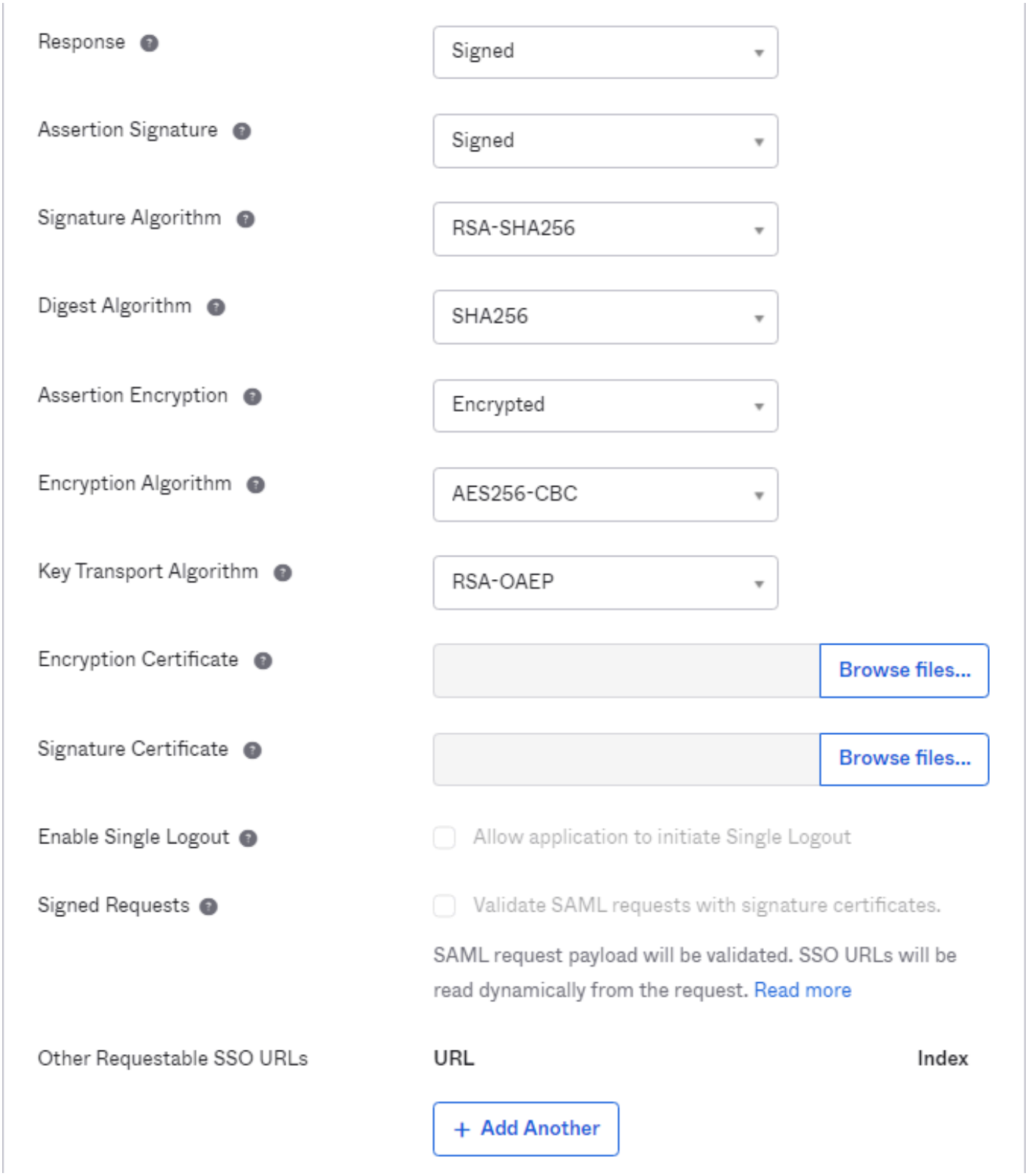
구성 요소	가치	설정
SP 발급자	XX.XX.XX.XX	vManage용 IP 주소 또는 DNS
서명 인증서		메타데이터의 암호화 인증서는 x.509 형식이어야 합니다.
어설션 인라인 후크	없음(비활성화)	없음(비활성화)
인증 컨텍스트 클래스	X.509 인증서	
Honor Force 인증	예	예
SAML 발급자 ID 문자열	SAML 발급자 ID 문자열	문자열 텍스트 입력
Attributes 문(선택 사항)	이름 ► 사용자 이름 이름 형식(선택 사항) ► 지정되지 않음 user.login► 값	이름 ► 사용자 이름 이름 형식(선택 사항) ► 지정되지 않음 user.login► 값
그룹 속성 문(선택 사항)	그룹 ► 이름 형식(선택 사항) ► 지정되지 않음 필터 ►regex ►.*	그룹 ► 이름 형식(선택 사항) ►지정되지 않음 필터 ►regex ►.*



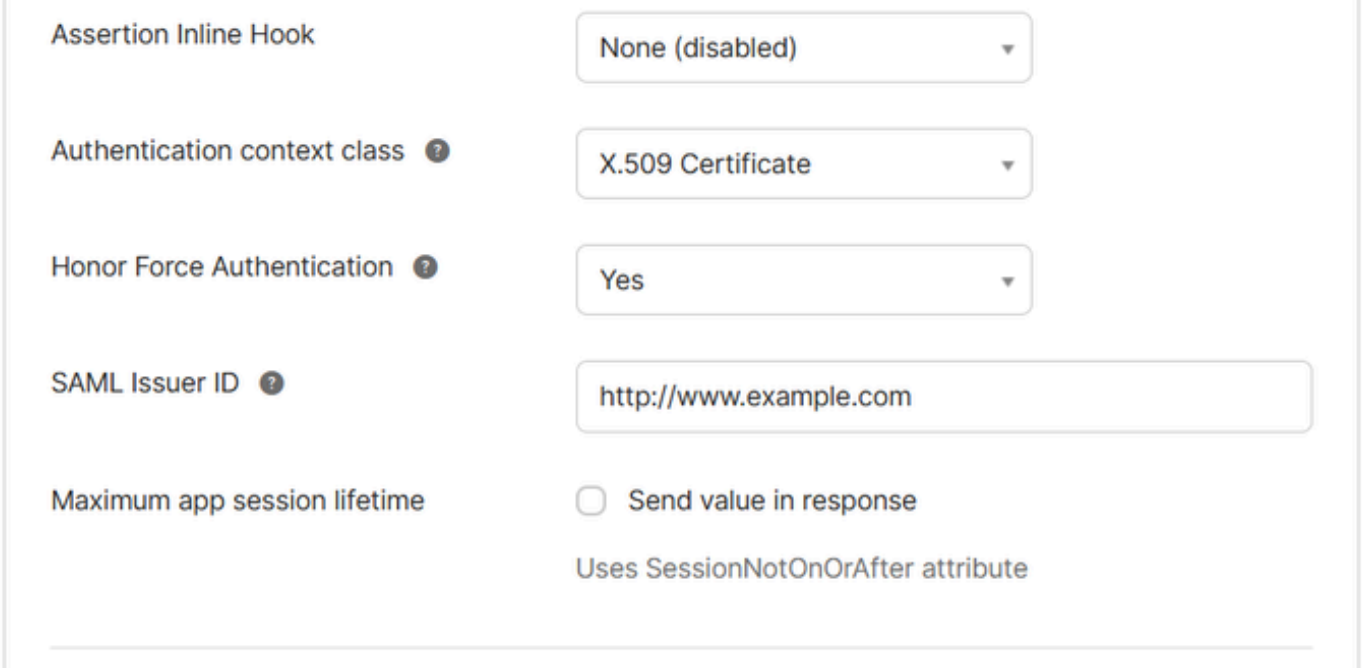
참고: CONFIGURE SAML 테이블에 표시된 대로 Username 및 Groups를 사용해야 합니다.

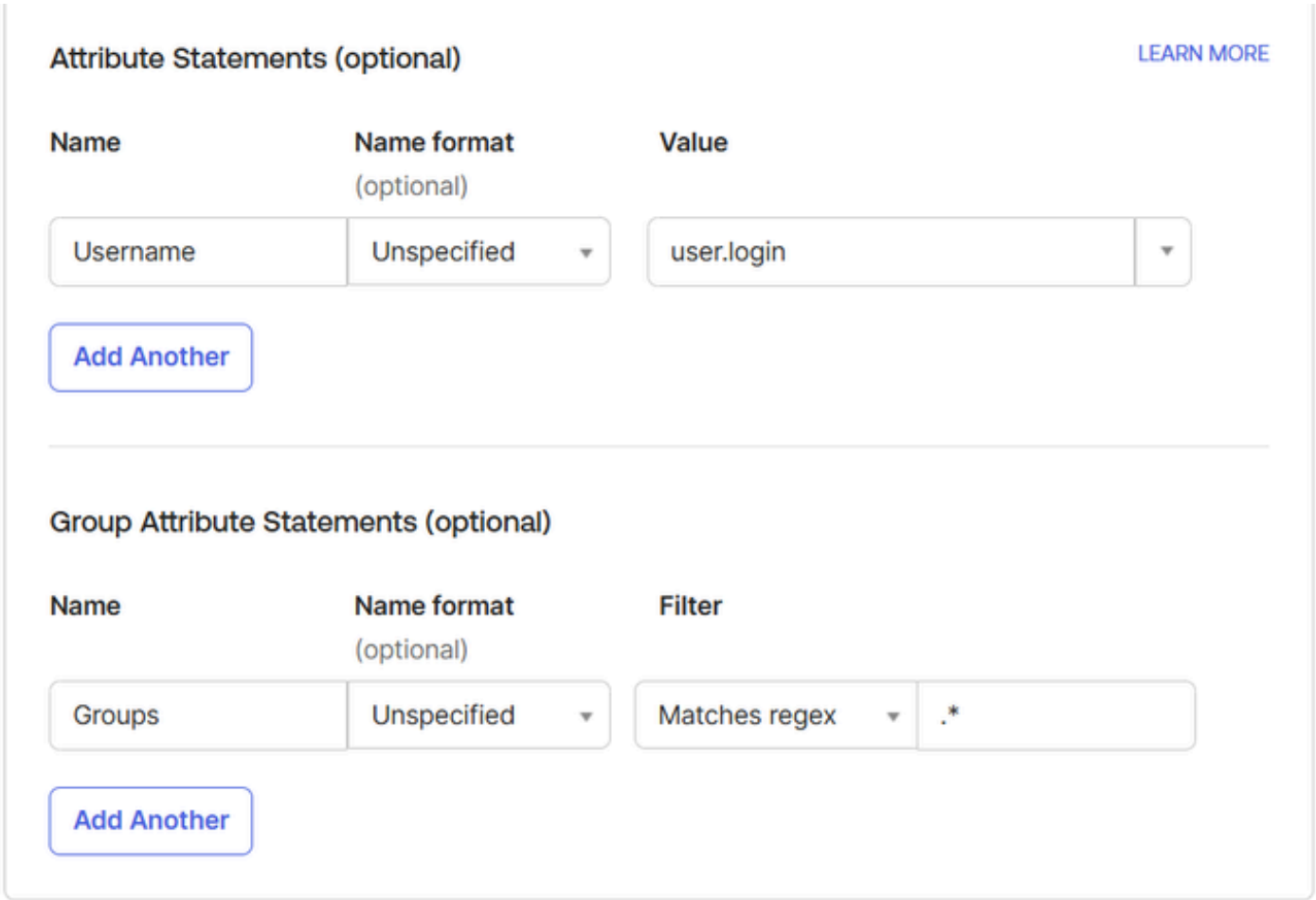


SAML Part 1 구성



SAML Part 2 구성



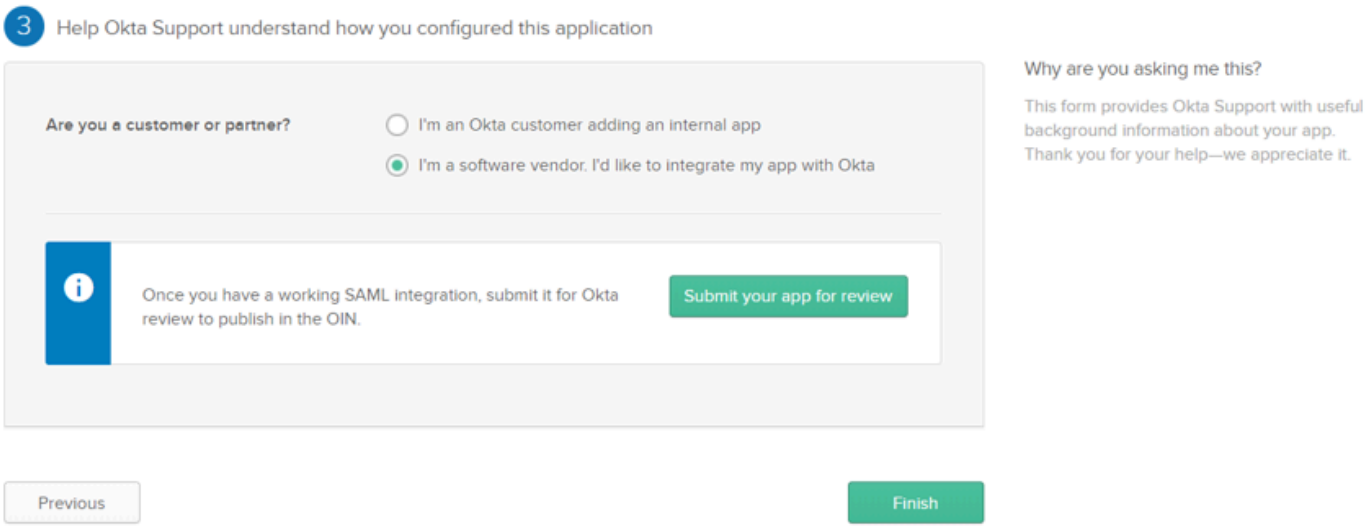


- Next(다음)를 클릭합니다.

피드백

1. 옵션 중 하나를 환경설정으로 선택합니다.

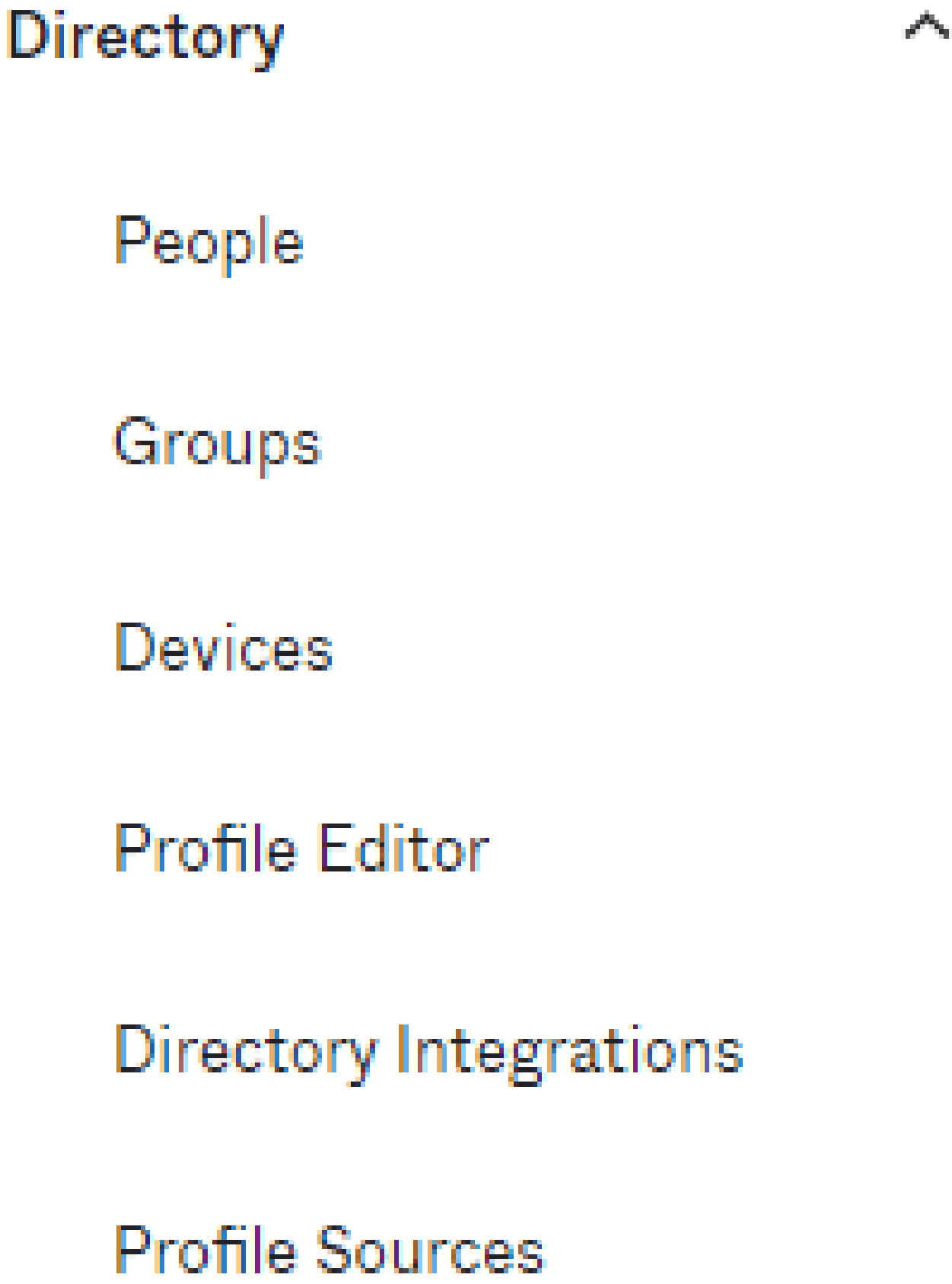
2. 완료를 클릭합니다.



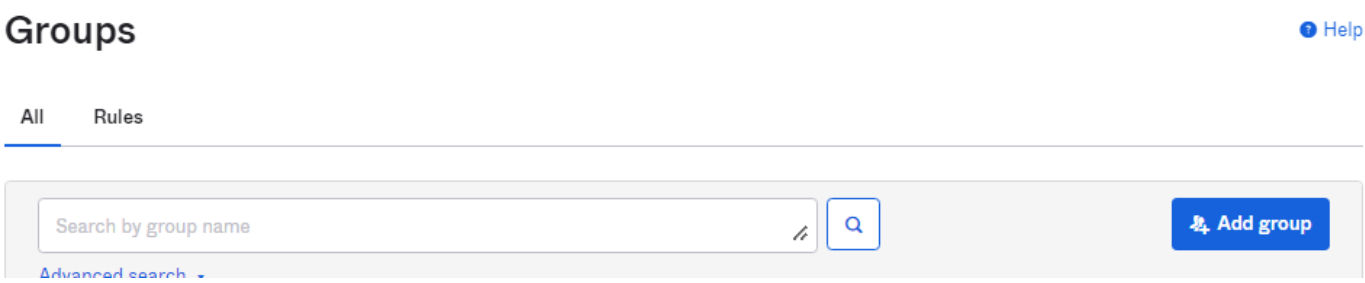
SMAL 피드백

OKTA에서 그룹 구성

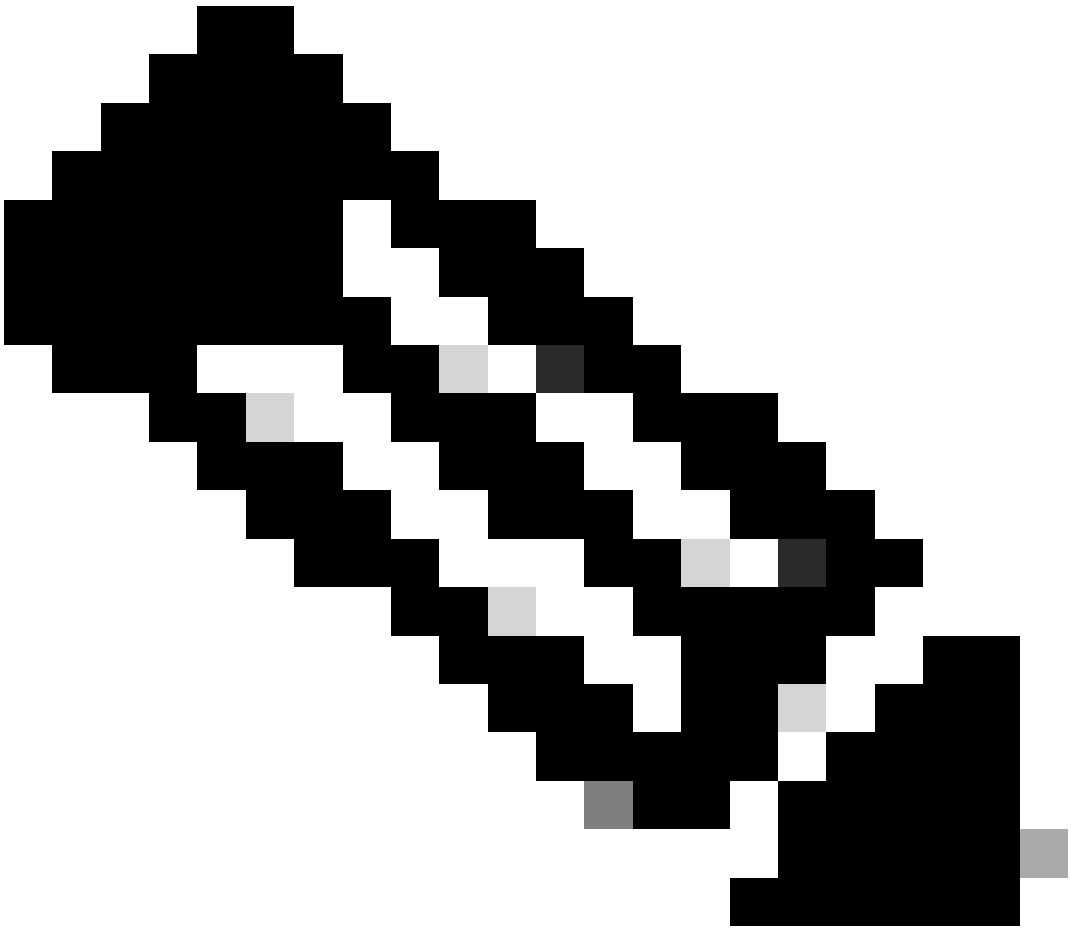
1. 디렉토리 > 그룹으로 이동합니다.


Directory
People
Groups
Devices
Profile Editor
Directory Integrations
Profile Sources

2. 그룹 추가를 클릭하고 새 그룹을 만듭니다.



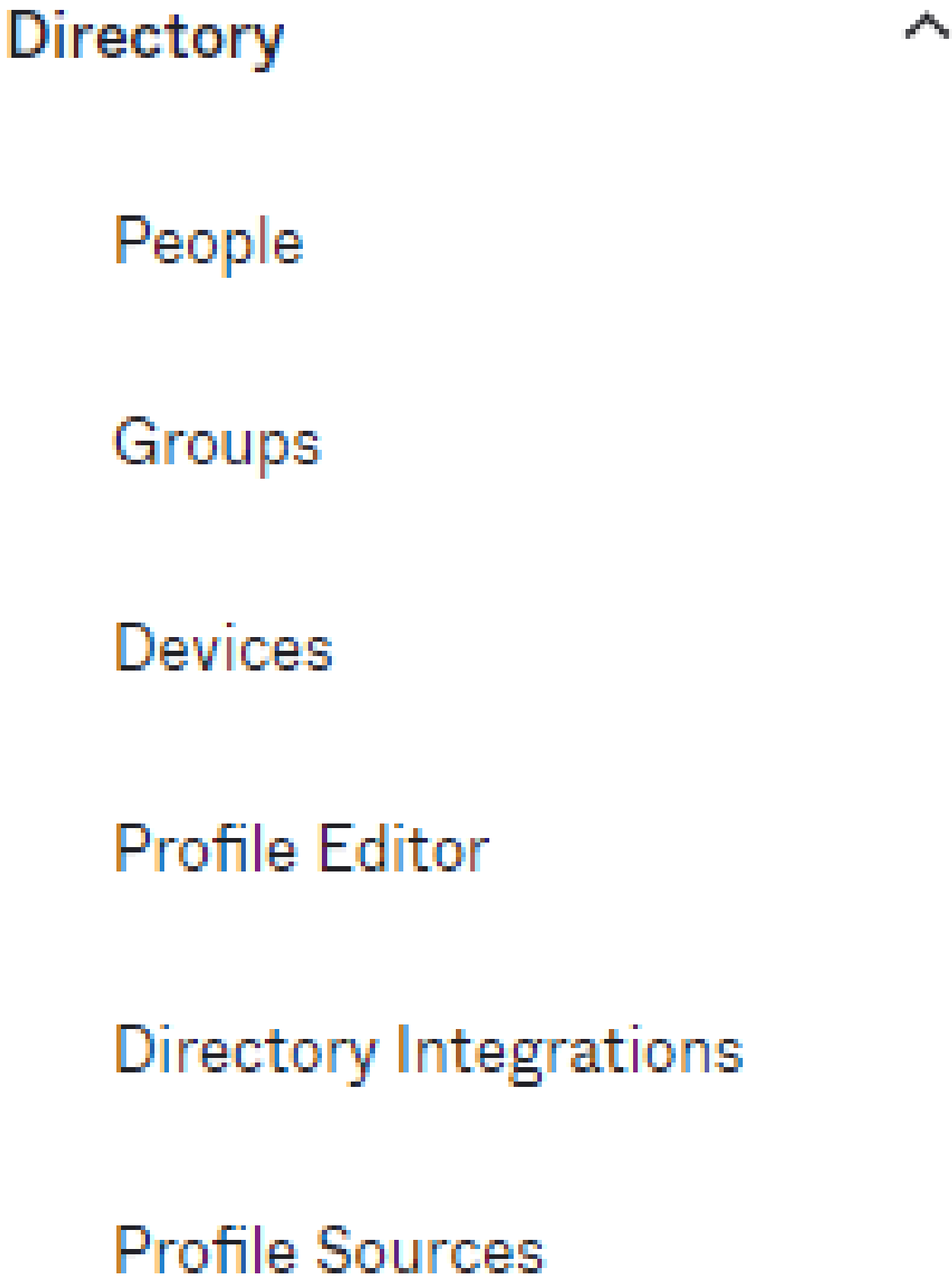
그룹 추가



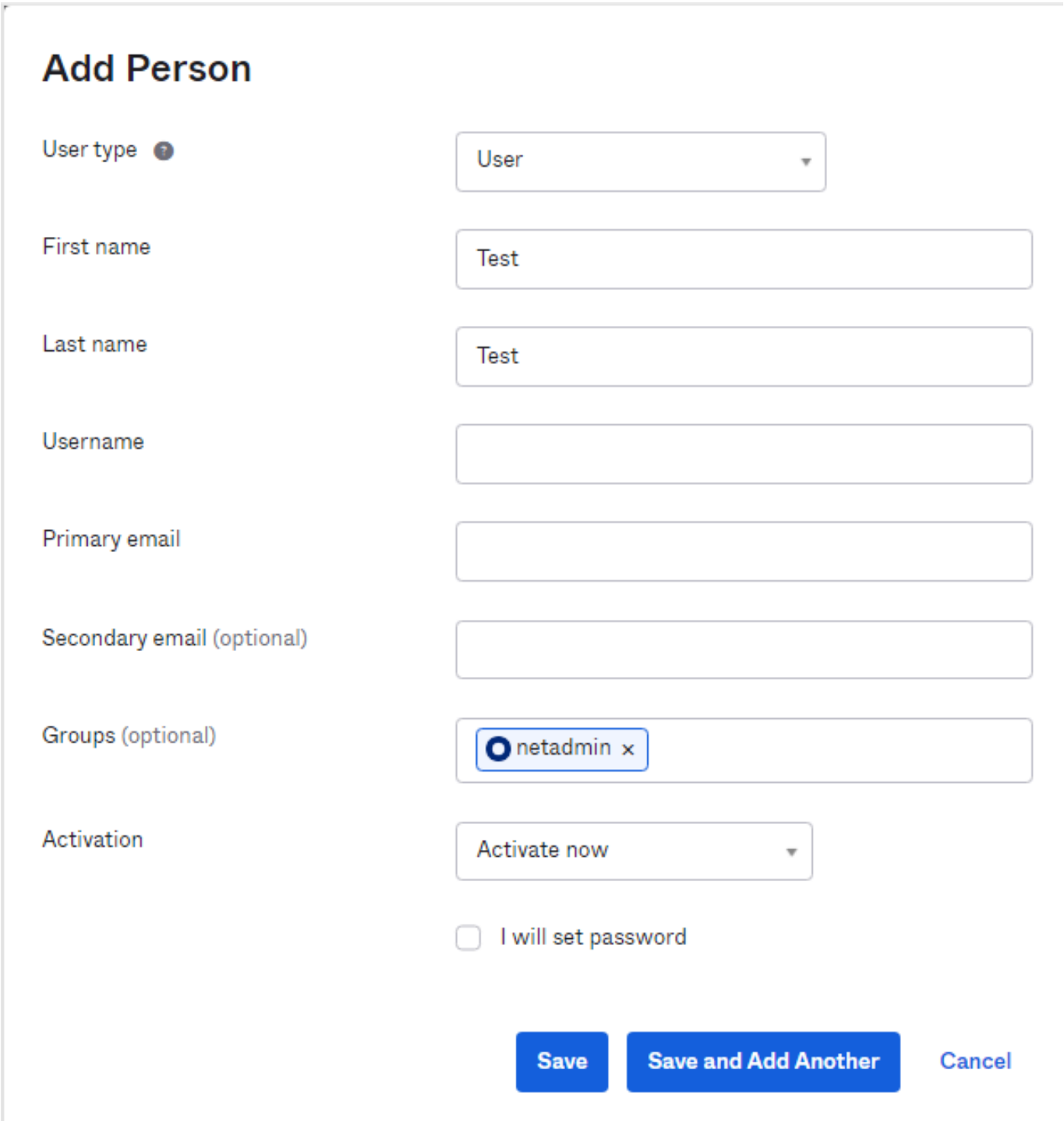
참고: 그룹은 Cisco vManage 그룹과 일치해야 하며 소문자여야 합니다.

OKTA에서 사용자 구성

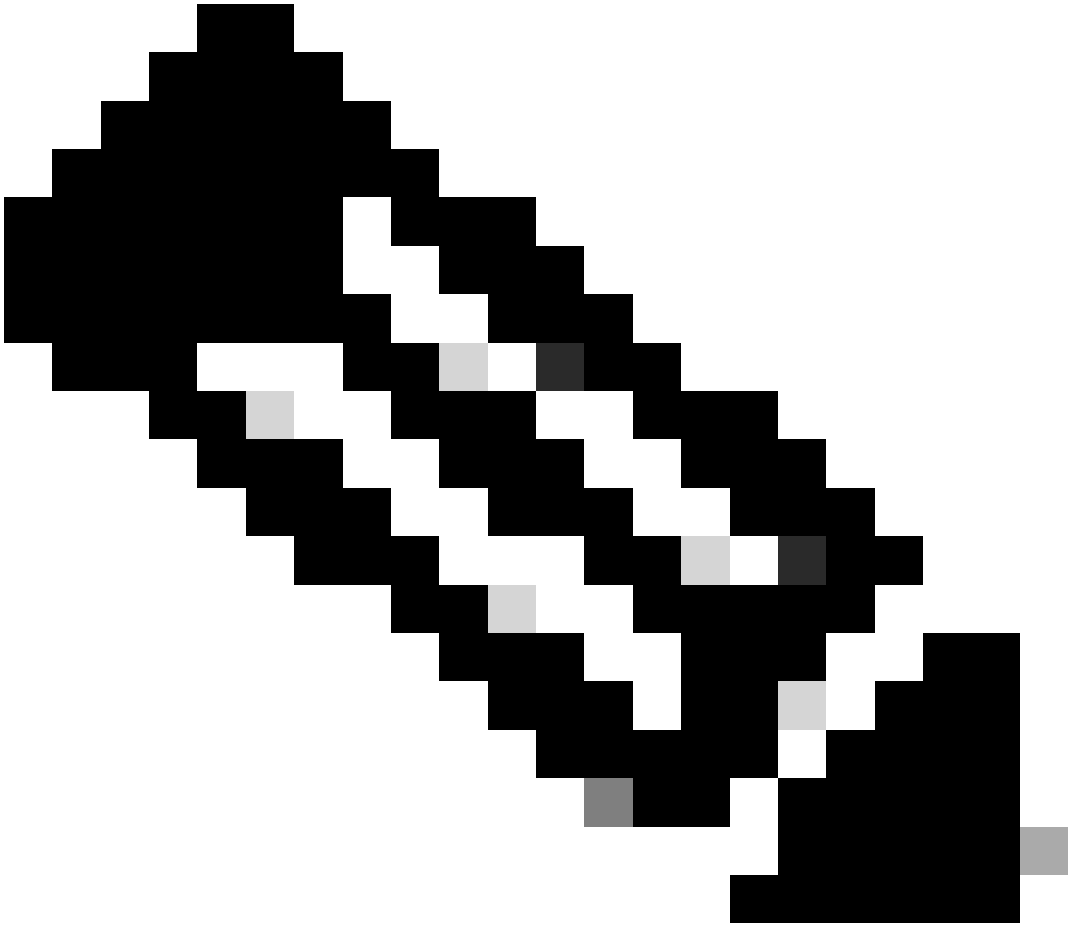
1. 디렉토리 > 인력으로 이동합니다.


Directory
People
Groups
Devices
Profile Editor
Directory Integrations
Profile Sources

2. 개인 추가를 클릭하고 새 사용자를 생성한 다음 그룹에 지정하고 저장합니다.



사용자 추가

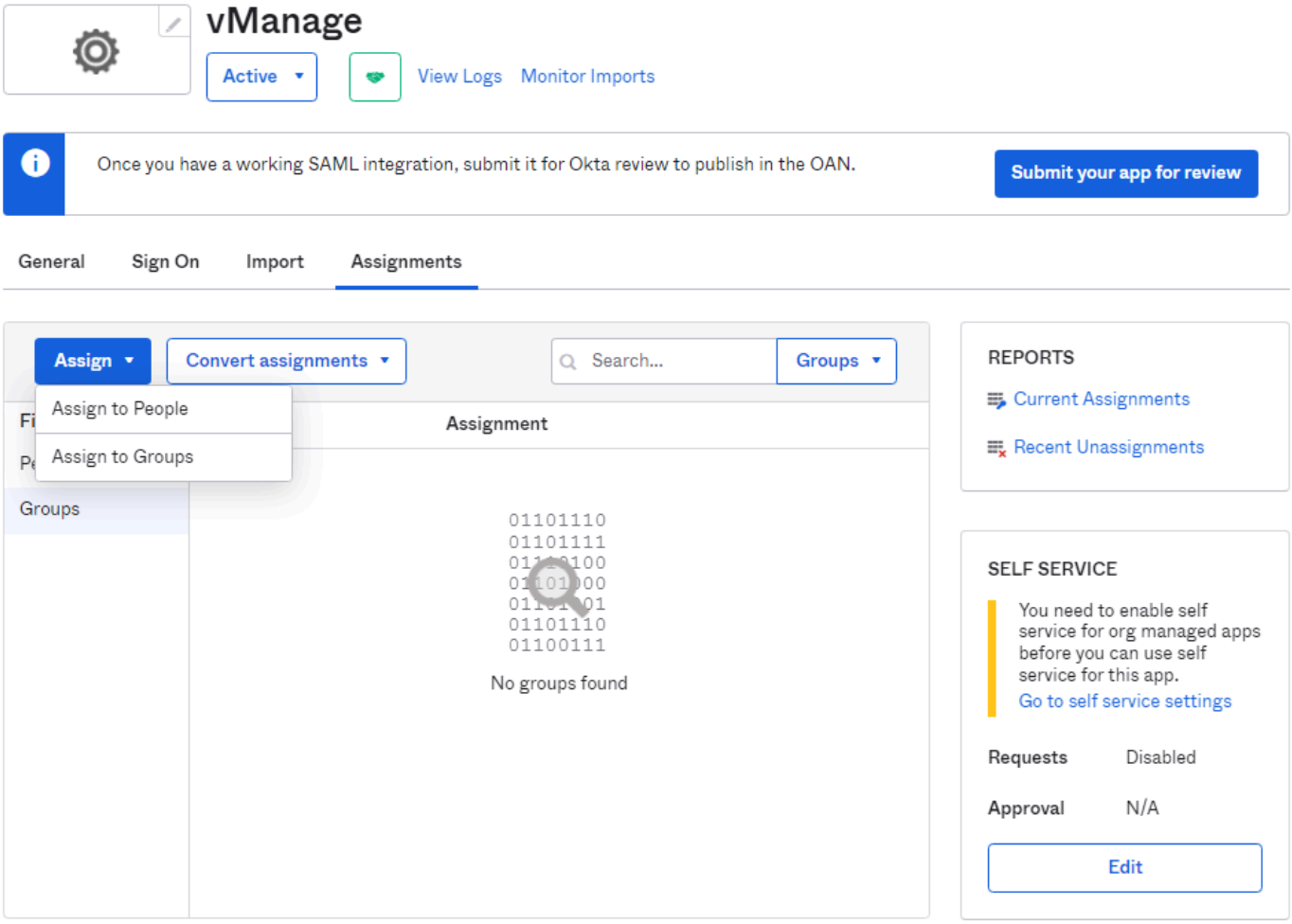


참고: OKTA 사용자 대신 Active Directory를 사용할 수 있습니다.

응용 프로그램에서 그룹 및 사용자 할당

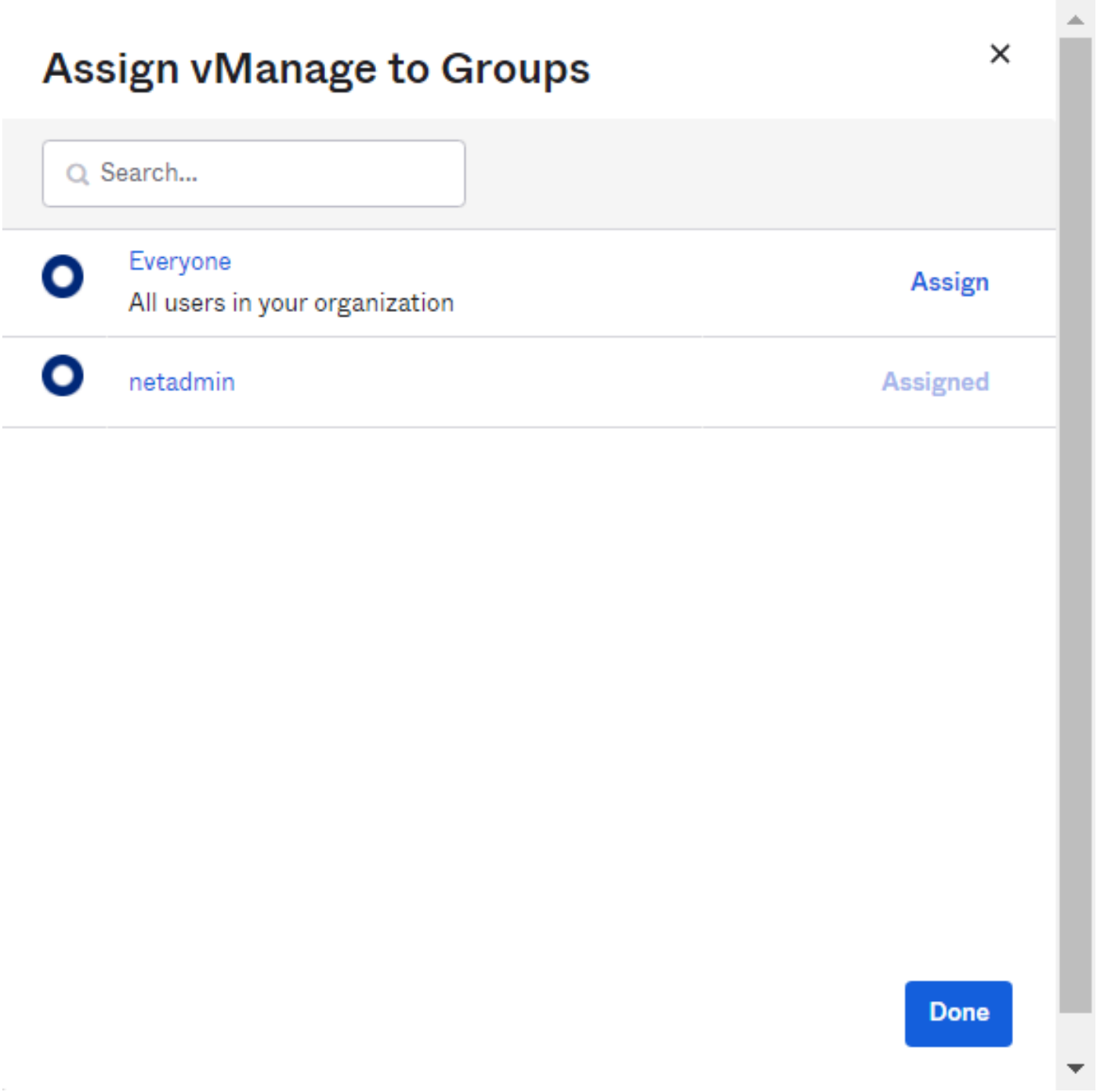
1. 애플리케이션 > 애플리케이션> 신규 애플리케이션을 선택합니다.

2. 지정 > 그룹에 지정을 클릭합니다.



Application(애플리케이션) > Groups(그룹)

3. 그룹을 식별하고 지정 > 완료를 클릭합니다.

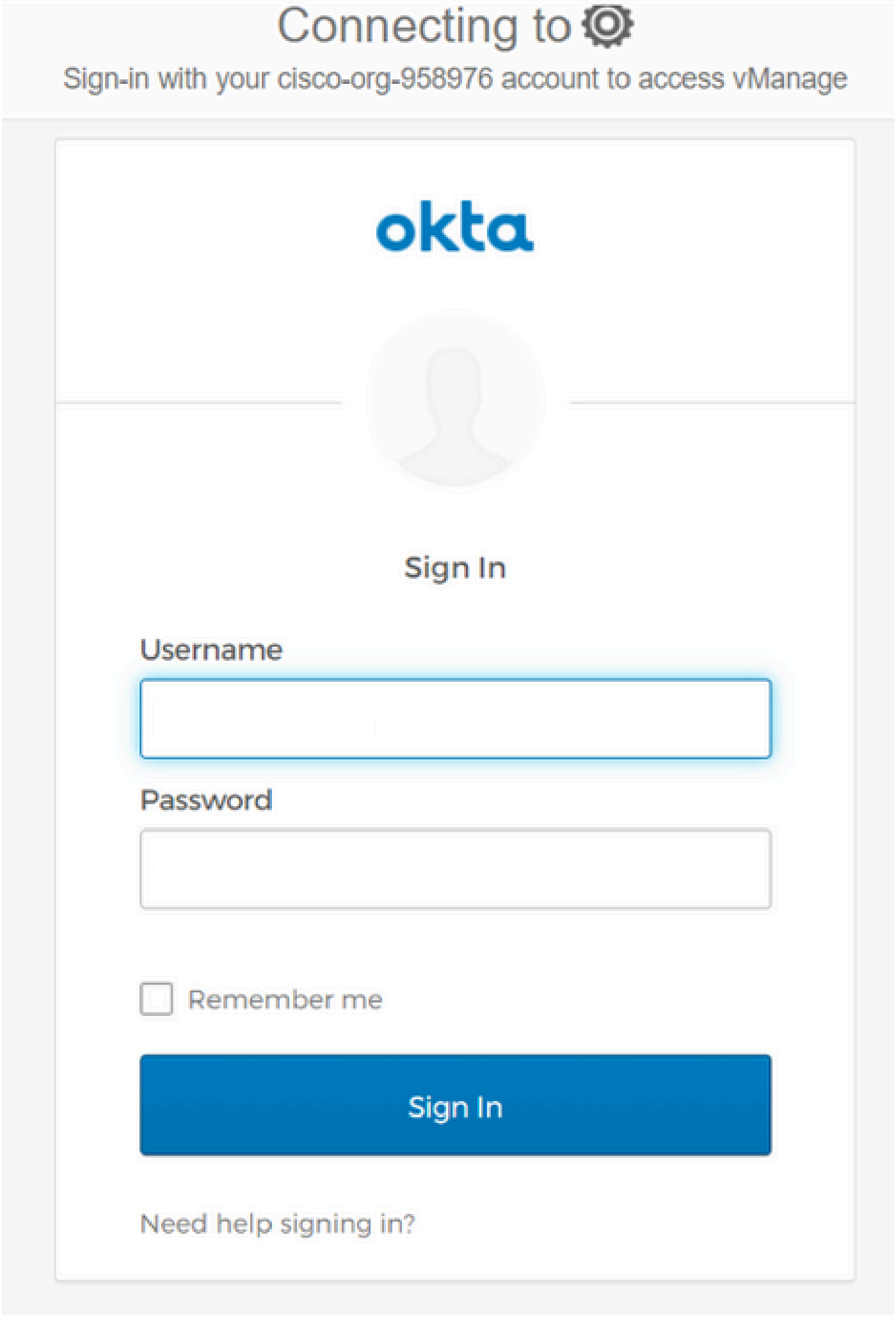


그룹 및 사용자 할당

4. 이제 그룹 및 사용자를 애플리케이션에 할당해야 합니다.

다음을 확인합니다.

컨피그레이션이 완료되면 OKTA를 통해 Cisco vManage에 액세스할 수 있습니다.



SSO 로그인 Vmanage

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.