# Configure OKTA Single Sign-On (SSO) on SD-WAN

## Contents



## Introduction

This document describes how to integrate OKTA Single Sing-On (SSO) on a Software-Defined Wide Area Network (SD-WAN).

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- SD-WAN general overview
- Security Assertion Markup Language (SAML)
- Identity Provider (IdP)
- Certificates

### Components Used

The information in this document is based on these software and hardware versions:

- Cisco vManage Release 18.3.X or later
- Cisco vManage Version 20.6.3

- Cisco vBond Version 20.6.3
- Cisco vSmart Version 20.6.3

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

### Background

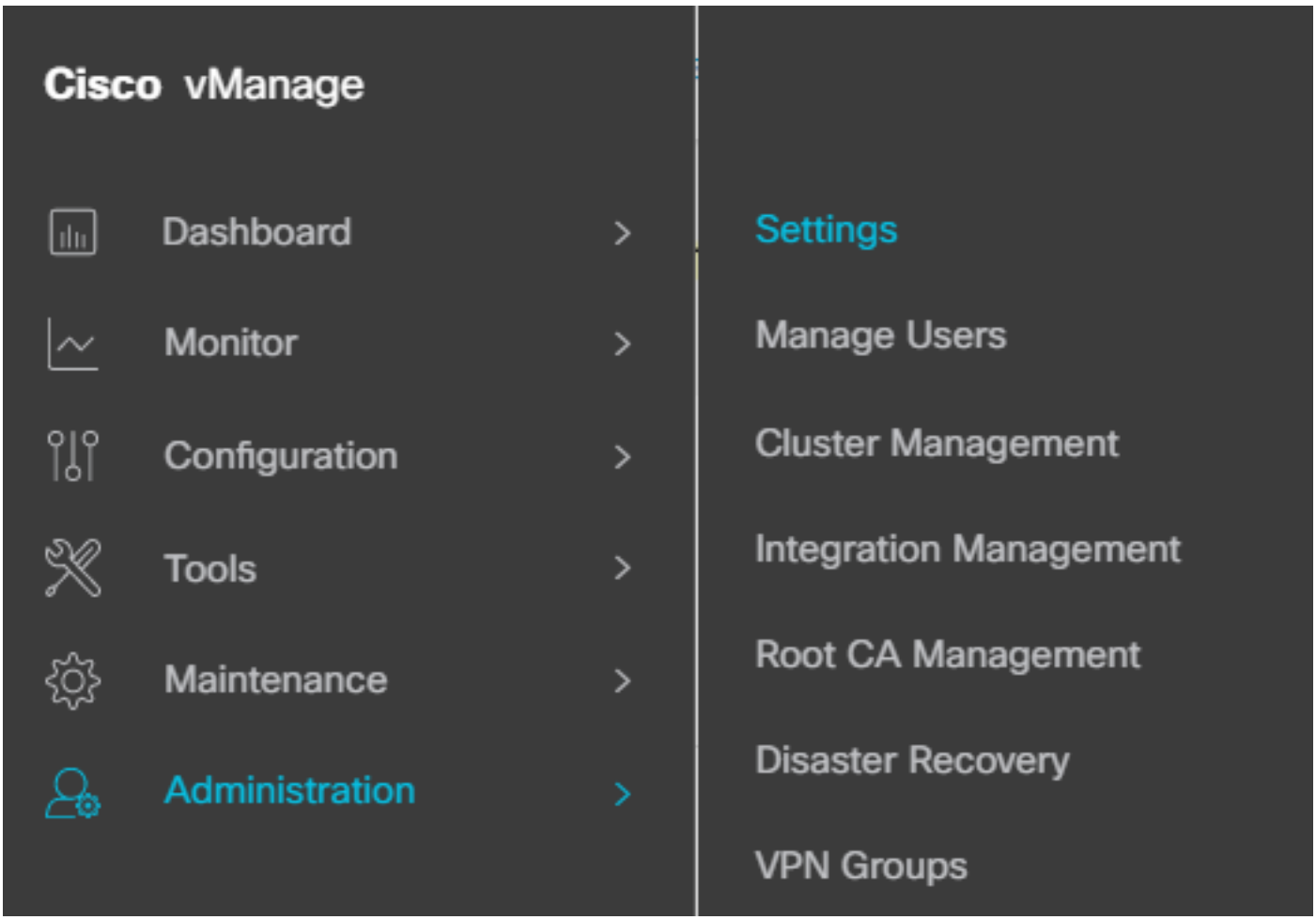
Security Assertion Markup Language (SAML) is an open standard for exchange authentication and authorization data between parties, in particular, between an identity provider and a service provider. As its name implies, SAML is an XML-based markup language for security assertions (statements that service providers use to make access-control decisions).

An Identity Provider (IdP) is a trusted provider that lets you use single sign-on (SSO) in order to access other websites. SSO reduces password fatigue and enhances usability. It decreases the potential attack surface and provides better security.

## Configure

### vManage Configuration

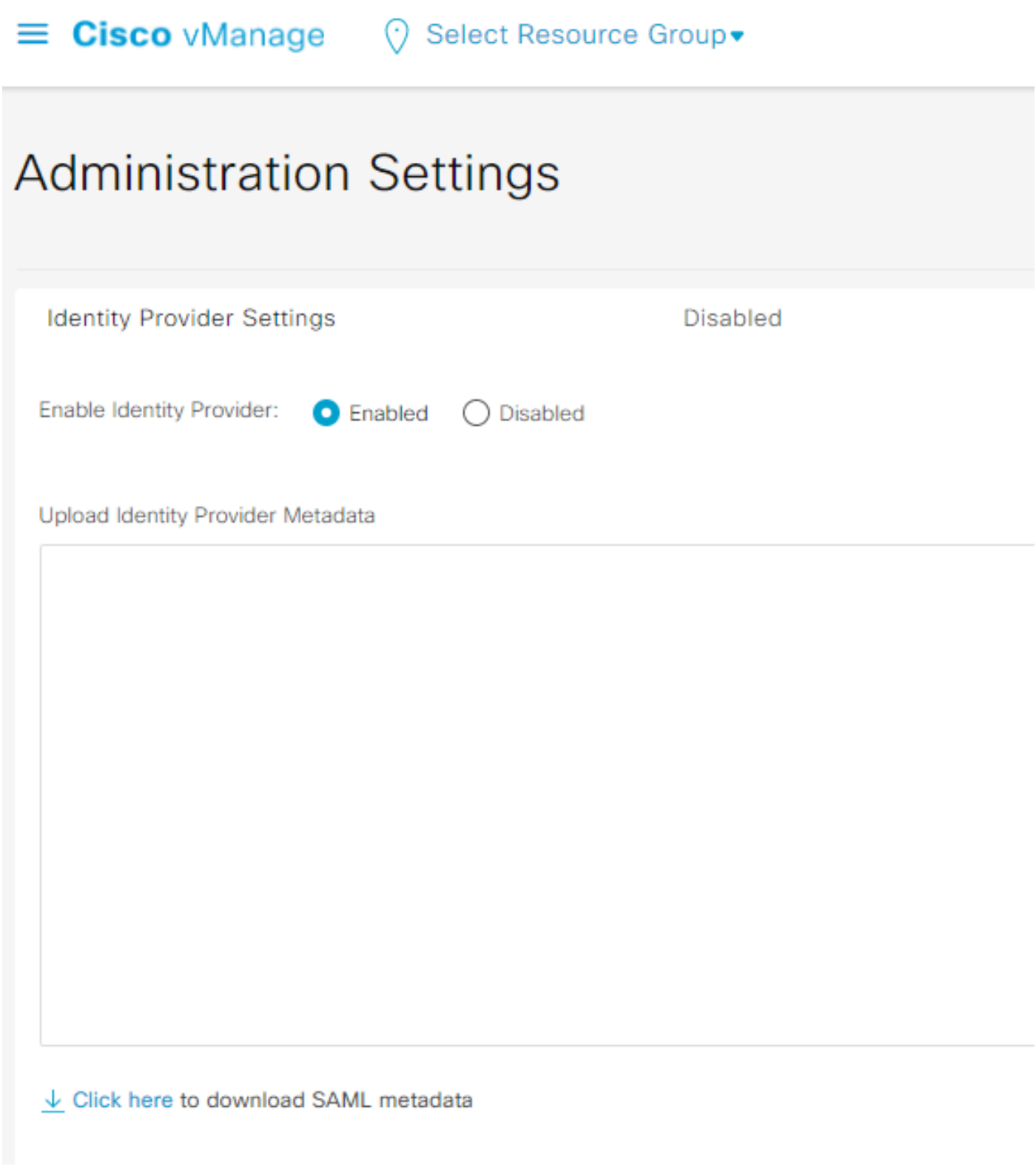
1. In Cisco vManage, navigate to **Administration** > **Settings** > **Identify Provider Settings** > **Edit**.



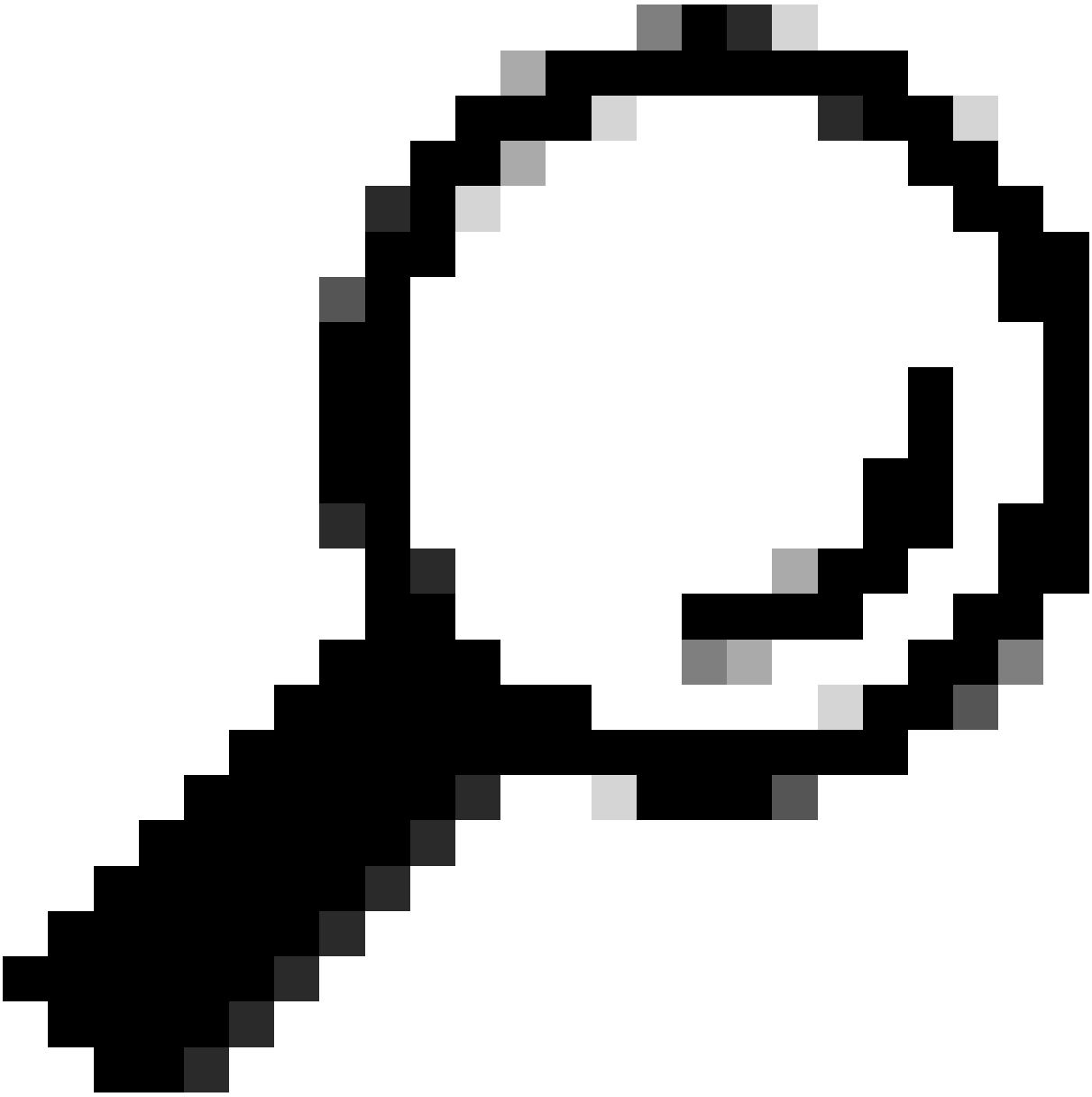

*Configuration > Settings*

2. Click **Enabled**.

3. Click to **download the SAML metadata** and save the content in a file. This is needed on the OKTA side.




*Download SAML*



**Tip**: You need these information from **METADATA** to configure OKTA with Cisco vManage.

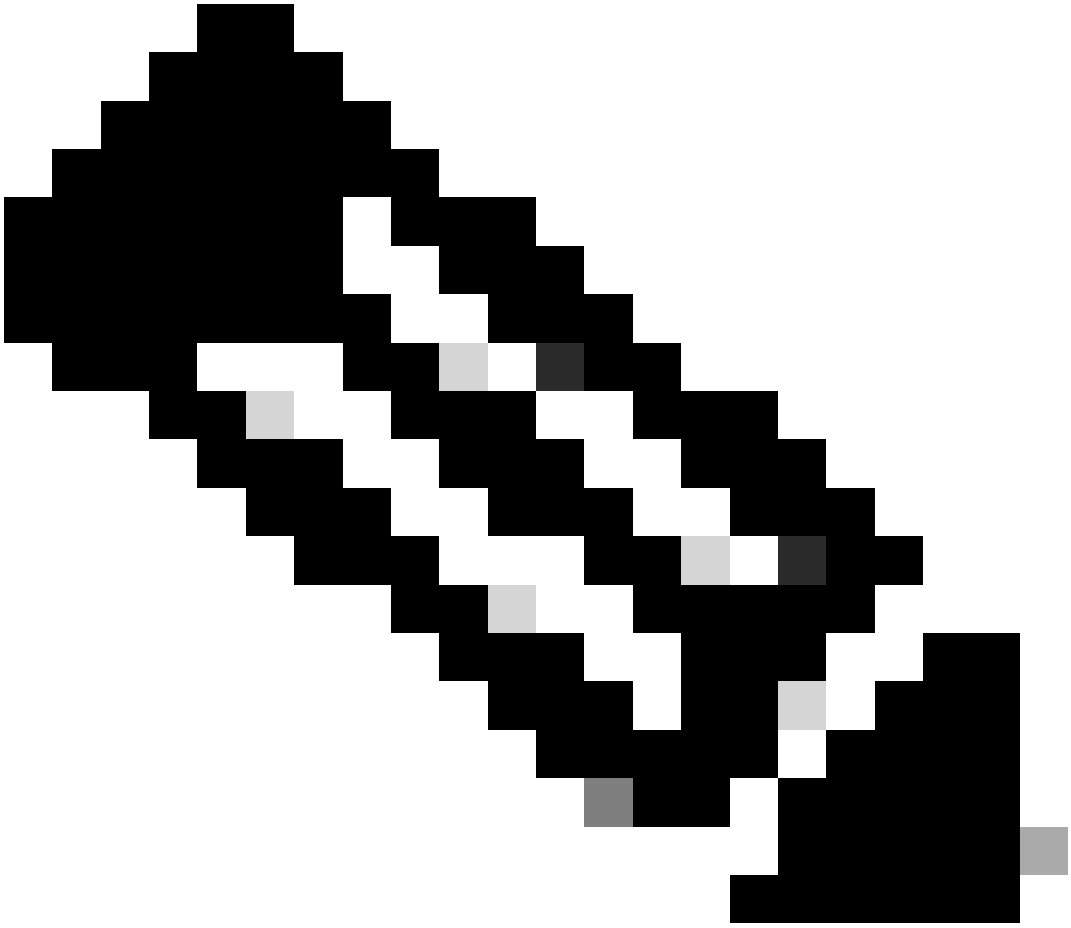
**a. Entity ID**

**b. Sign certificate**

**c. Encryption certificate**

**d. Log out URL**

**e. Log in UR**



**Note**: Certificates must be in **x.509** format and save them with **.CRT** extension.

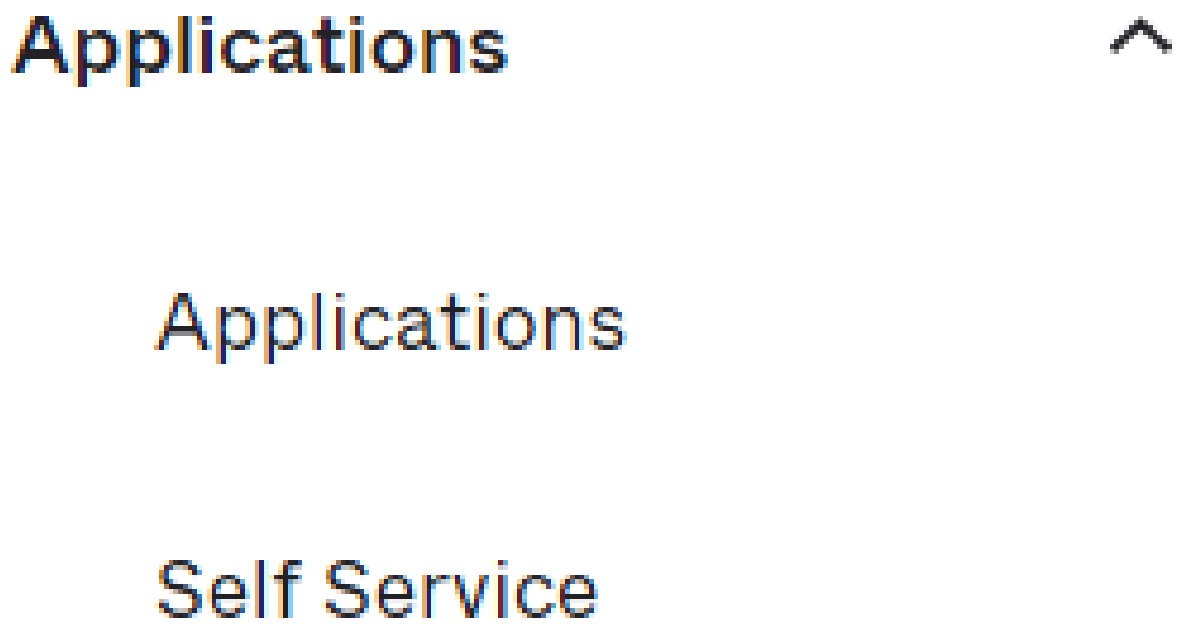
```
-----BEGIN CERTIFICATE-----
MIIDfTCCAmWgAwIBAgIhAM8T9QVLqX/lp1oK/q2XNUbJcGhRmGvqdXxGTUkrKUBhMA0GCSqGSIb3
DQEBCwUAMHIxDDAKBgNVBAYTA1VTQTELMAkGA1UECBMCQ0ExETAPBgNVBAcTCFNhbiBKb3NlMRQw
EgYDVQQKEwtDSVNDT1JUUExBQjEUMBIGA1UECxMLQ01lTQ09SVFBMQUIxFjAUBgNVBAMTDURlZmF1
bHRUZW5hbnQwHhcNMjAwNTI4MTQxMzQzWhcNMjUwNTI4MTQxMzQzWjByMQwwCgYDVQQGEwNVU0Ex
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 Certificate*

## OKTA Configuration

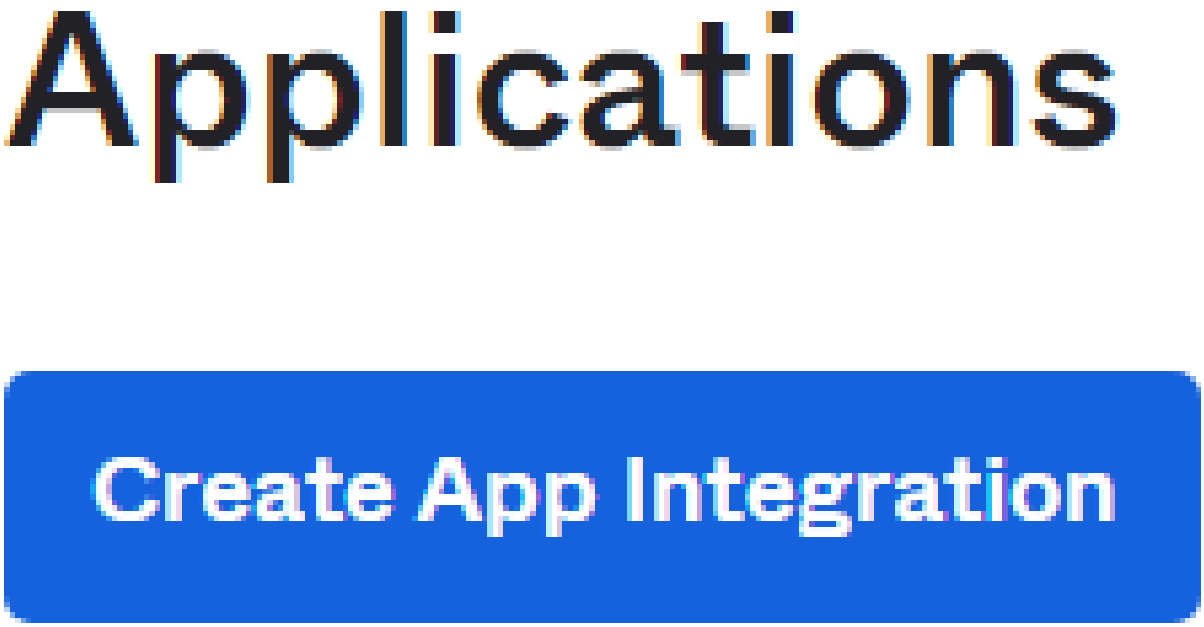
1. Log in OKTA account.

2. Navigate to **Applications** > **Applications.**



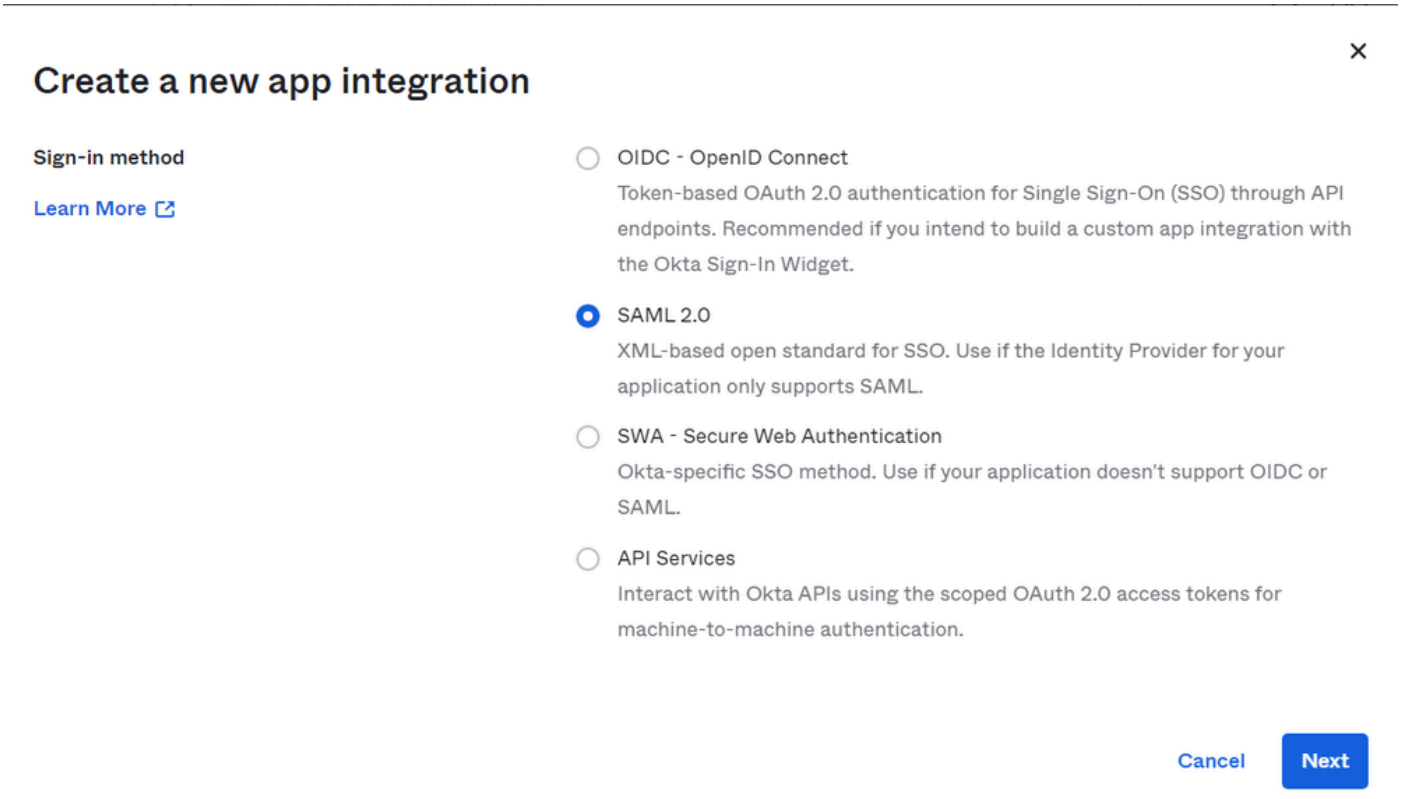

*Applications > Apllications*

3. Click **Create App Integration.**




*Create Application*

4. Click **SAML 2.0** and **next**.




*Configure SAML2.0*

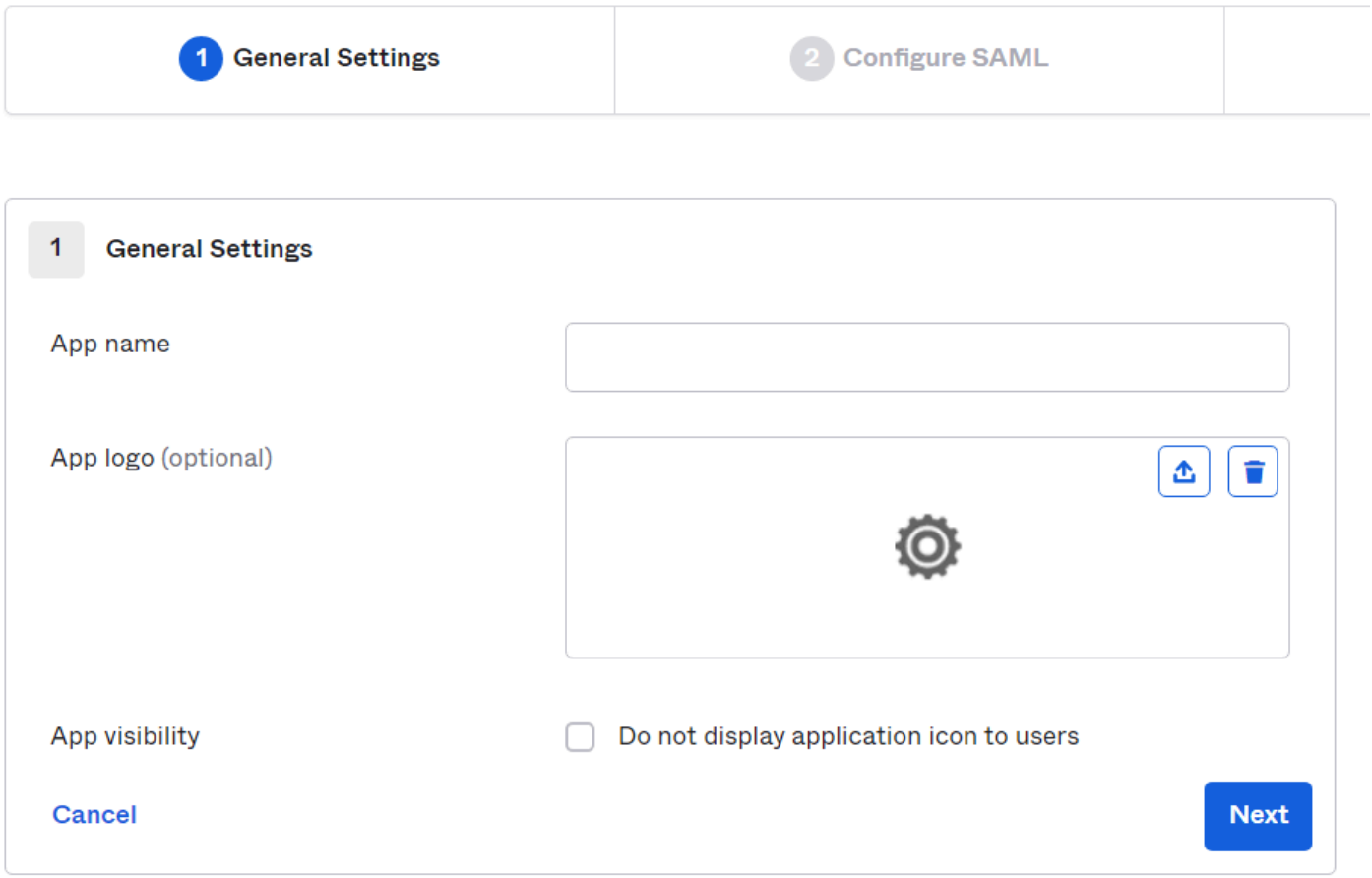
## General Settings

1. Enter a name of application.

2. Add logo for application (optional).

3. App visibility (optional).

4. Click **NEXT**.




*SAML General Settings*

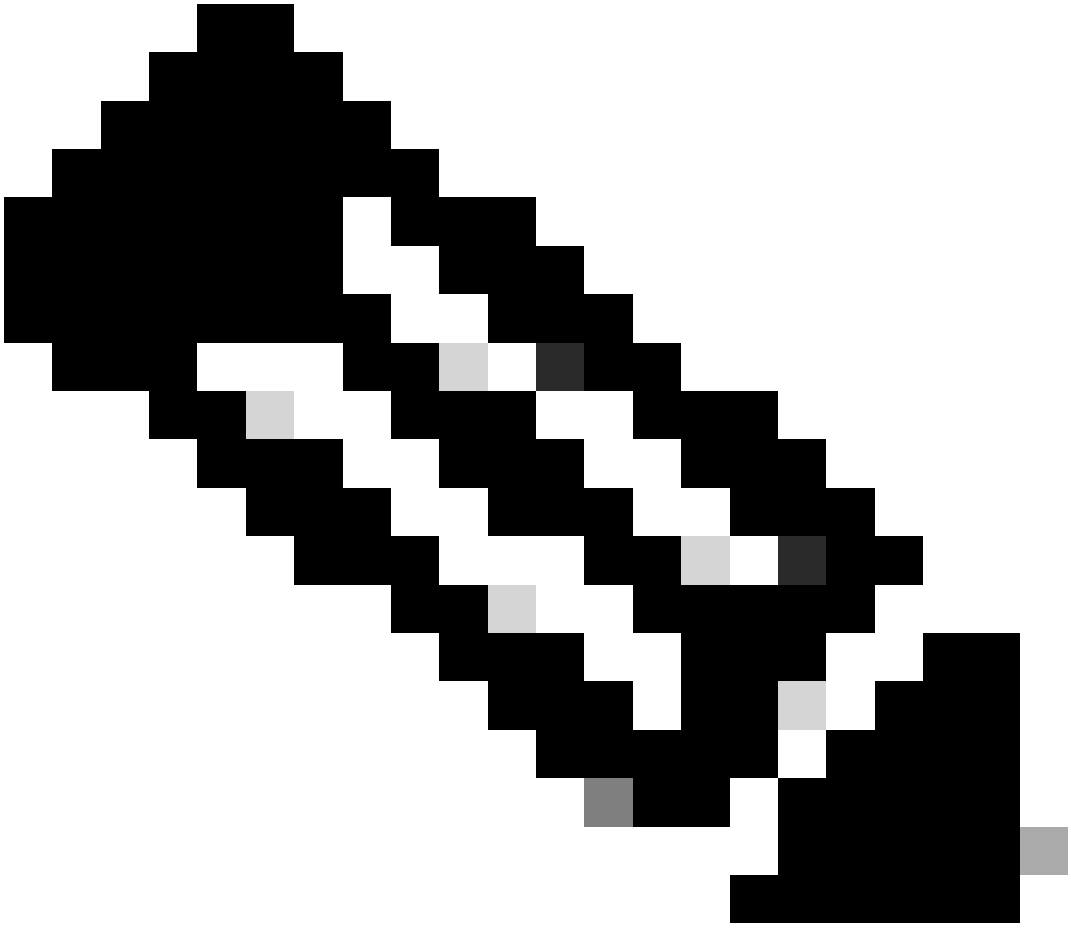
## Configure SAML

This table describe the parameters must need configure on this section.

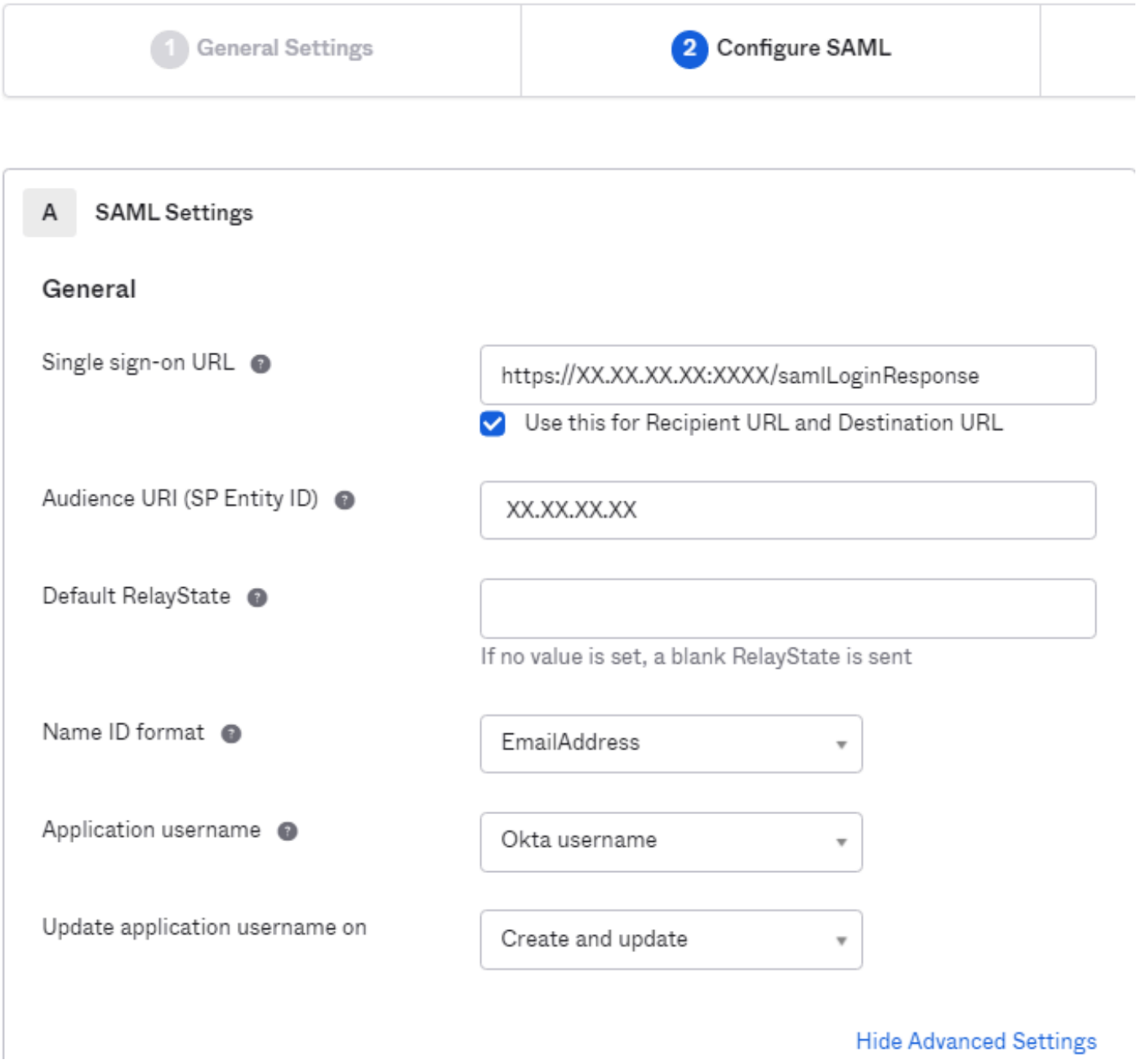
| Component | Value | Configuration |
|---|---|---|
| Single sign on URL | https://XX.XX.XX.XX:XXXX/samlLoginResponse | Get it from the metadata. |
| Audience URI (SP Entity ID) | XX.XX.XX.XX | Ip address or DNS for Cisco vManage |
| Default RelayState | | EMPTY |

| Component | Value | Configuration |
|---|---|---|
| Name ID format | | As per your preference |
| Application username | | As per your preference |
| Update application username on | Create and update | Create and update |
| Response | Signed | Signed |
| Assertion Signature | Signed | Signed |
| Signature Algorithm | RSA-SHA256 | RSA-SHA256 |
| Digest Algorithm | SHA256 | SHA256 |
| Assertion Encryption | Encrypted | Encrypted |
| Encryption Algorithm | AES256-CBC | AES256-CBC |
| Key Transport Algorithm | RSA-OAEP | RSA-OAEP |
| Encryption Certificate | | Encryption certificate from metadata, must be on format **x.509**. |
| Enable Single Logout | | muct be checked. |
| Single Logout URL | https://XX.XX.XX.XX:XXXX/samlLogoutResponse | Get from the metadata. |
| SP Issuer | XX.XX.XX.XX | Ip address or DNS for vManage |
| Signature | | Encryption certificate from the |

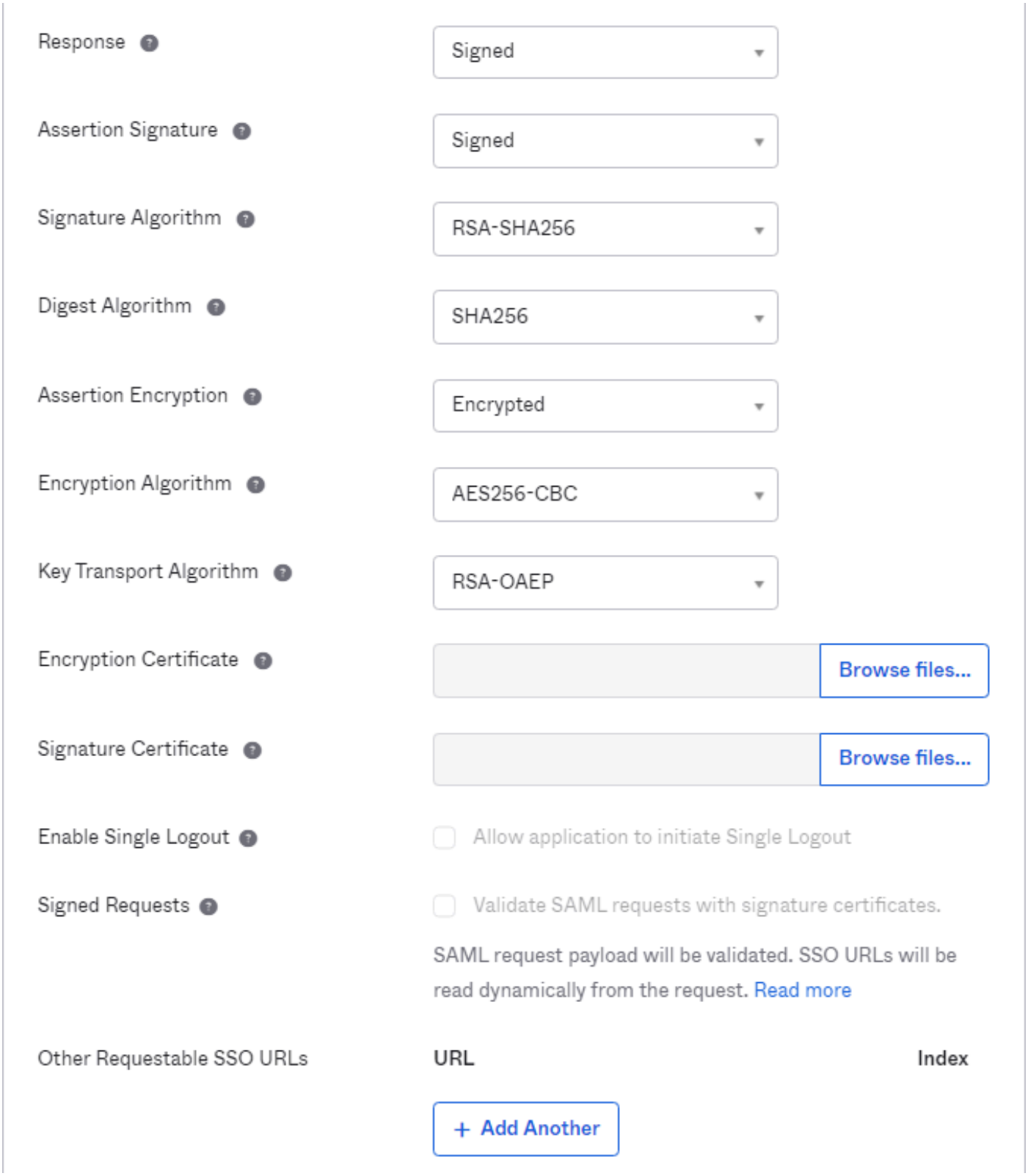
| **Component** | **Value** | **Configuration** |
|---|---|---|
| Certificate | | metadata, must be on format **x.509**. |
| Assertion Inline Hook | None(disable) | None(disable) |
| Authentication context class | **X.509** Certificate | |
| Honor Force Authentication | Yes | Yes |
| SAML issuer ID string | SAML issuer ID string | Type an string text |
| Attributes Statements (optional) | Name ► Username<br>Name format (optional) ► Unspecified<br>Value ► **user.login** | Name ► Username<br>Name format (optional) ► Unspecified<br>Value ► **user.login** |
| Group Attribute Statements (optional) | Name ► Groups<br>Name format (optional) ► Unspecified<br>Filter ► Matches regex ► .* | Name ► Groups<br>Name format (optional) ► Unspecified<br>Filter ► Matches regex ► .* |



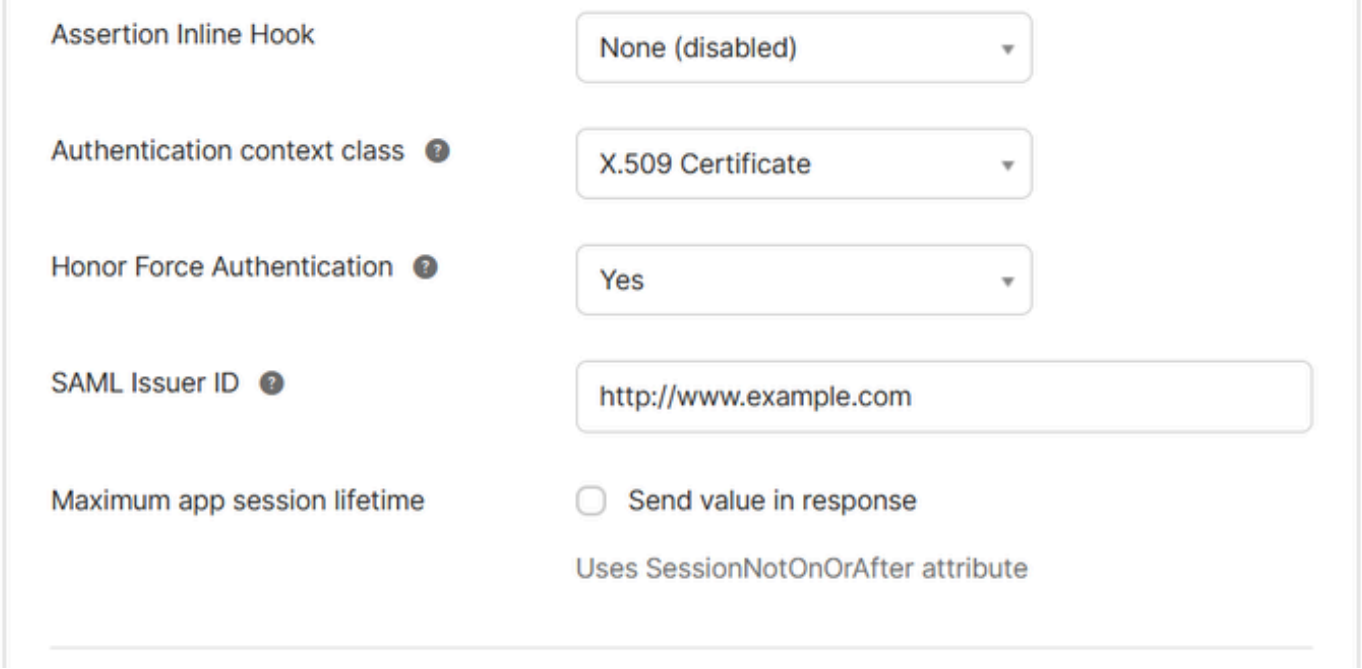
**Note**: Must use **Username** and **Groups**, exactly as shown in **CONFIGURE SAML** table.

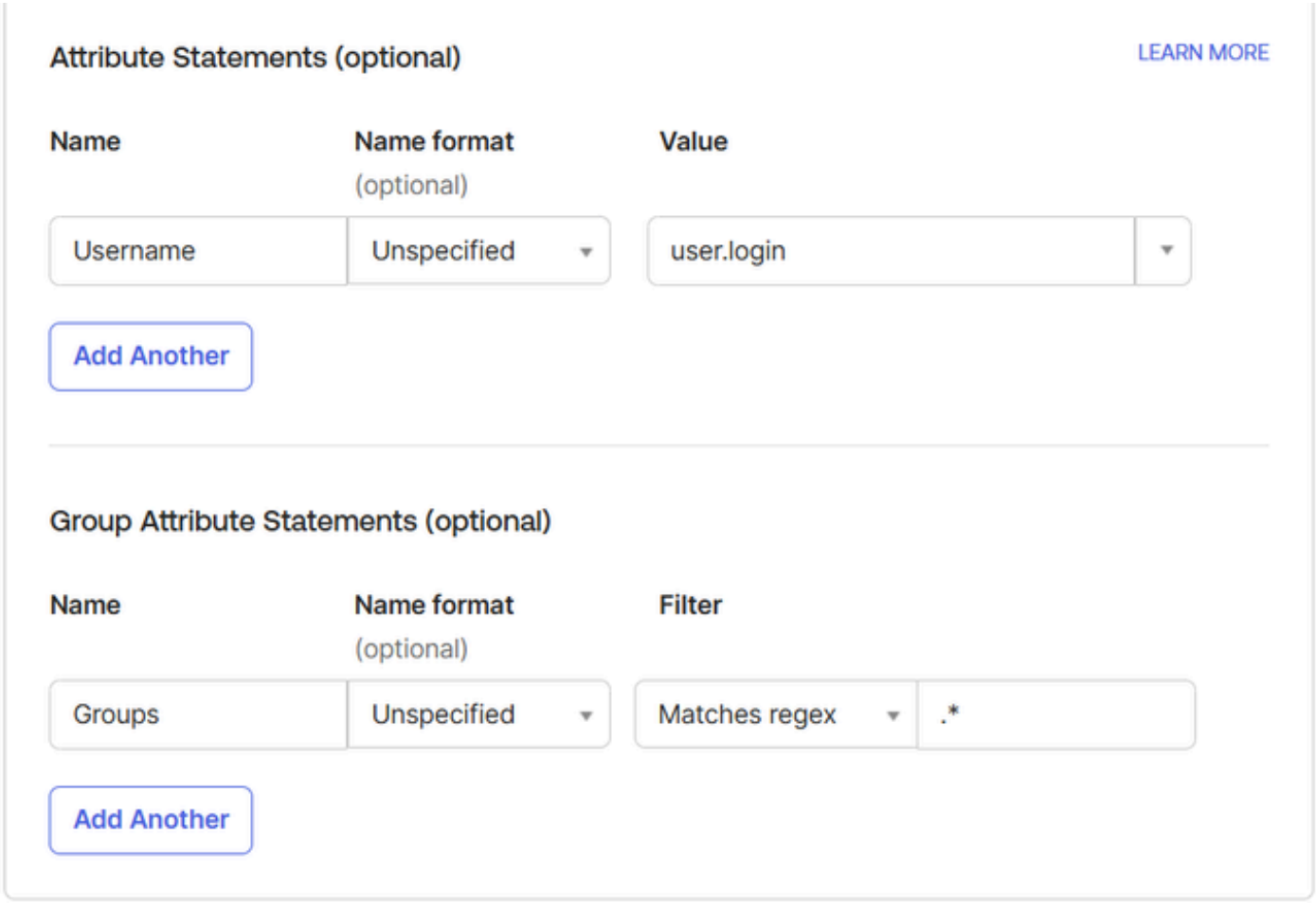



*Configure SAML Part 1*




*Configure SAML Part 2*



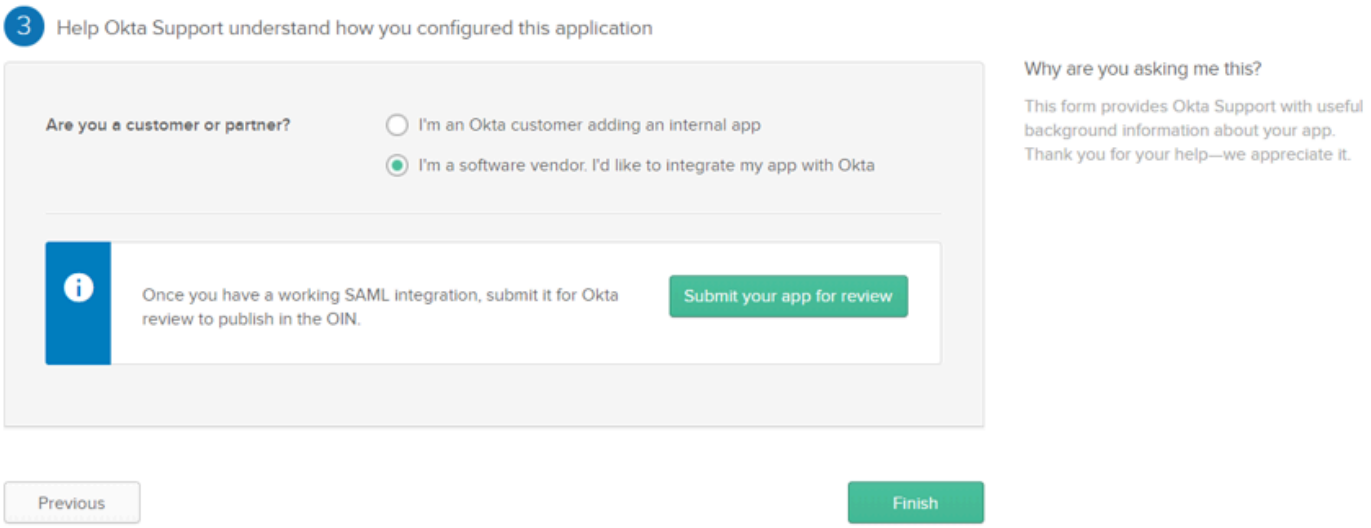




- Click **Next**.

## Feedback

1. Select one of the option as your preference.

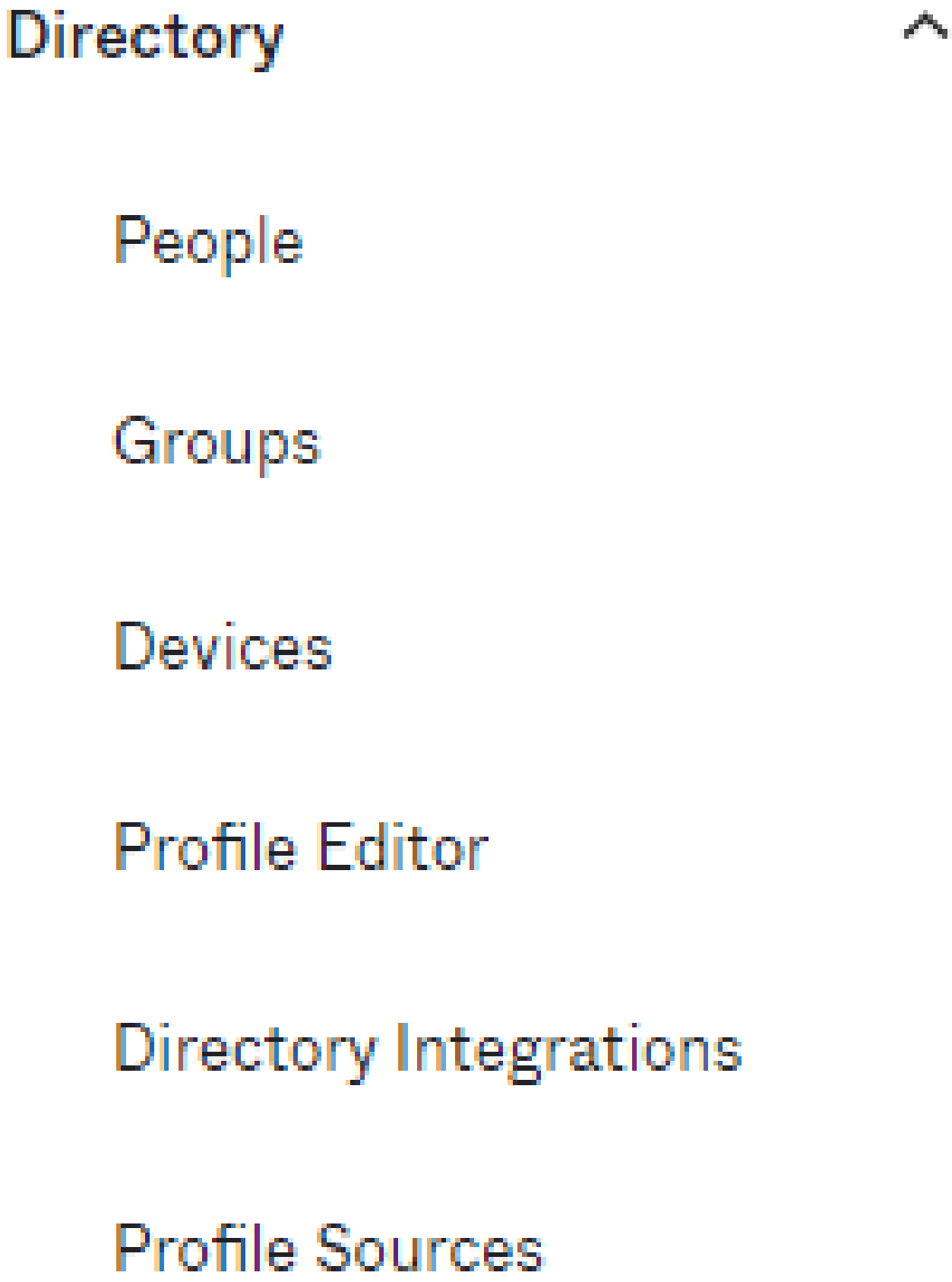
2. Click **Finish**.




*SMAL Feedback*

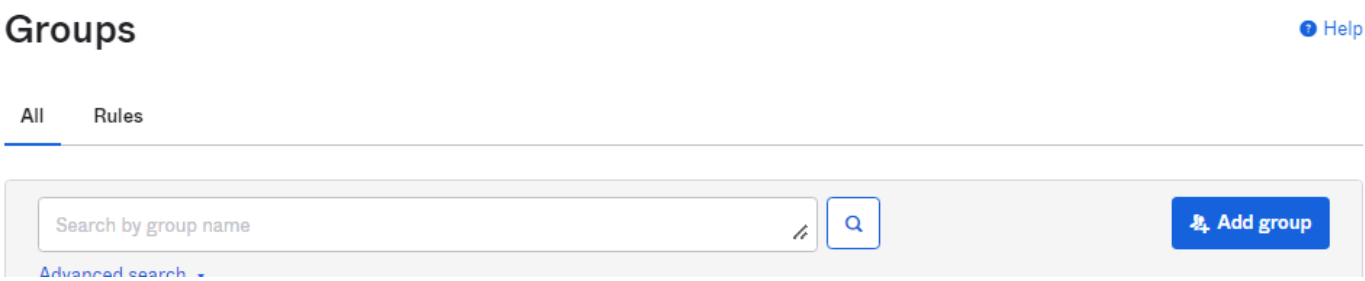
## Configure Groups in OKTA

**1.** Navigate to **Directory** > **Groups.**


Directory
People
Groups
Devices
Profile Editor
Directory Integrations
Profile Sources

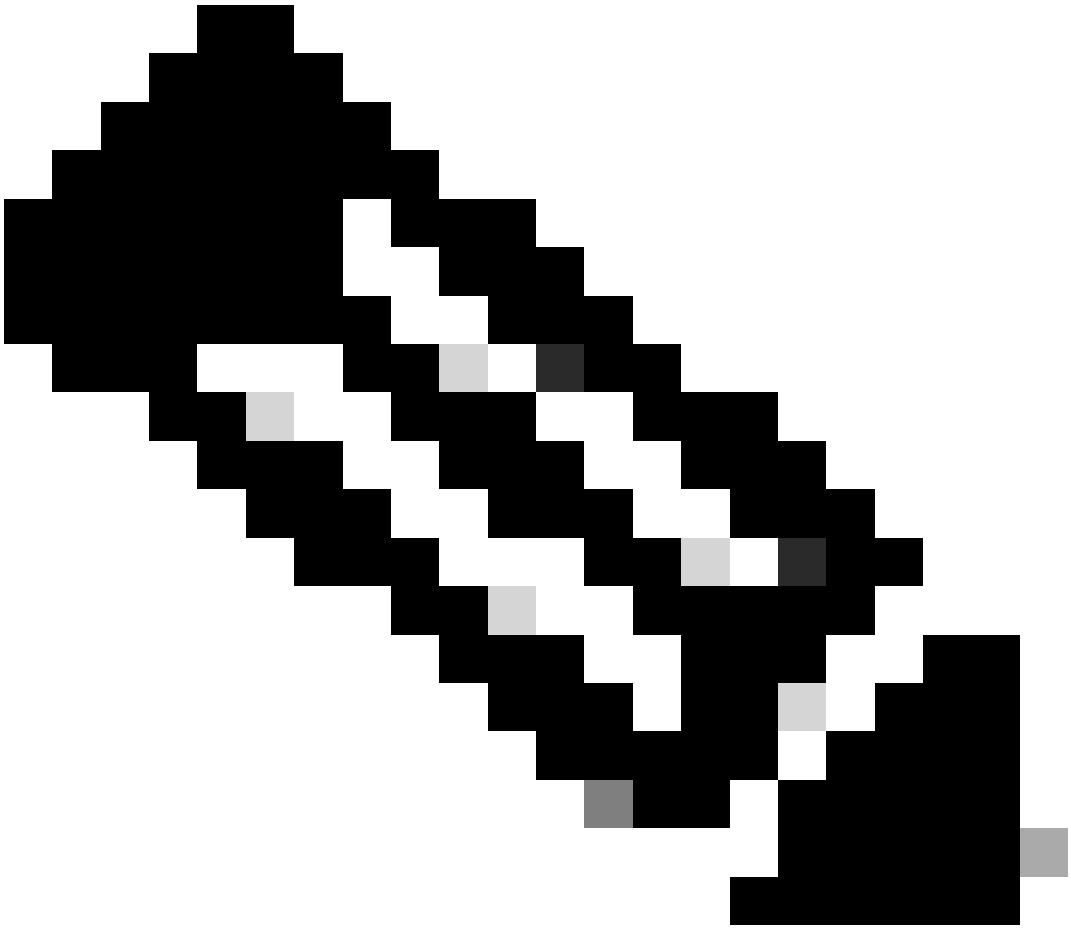
*OKTA Groups*

2. Click **Add group** and creat new group.




*Add Group*

---

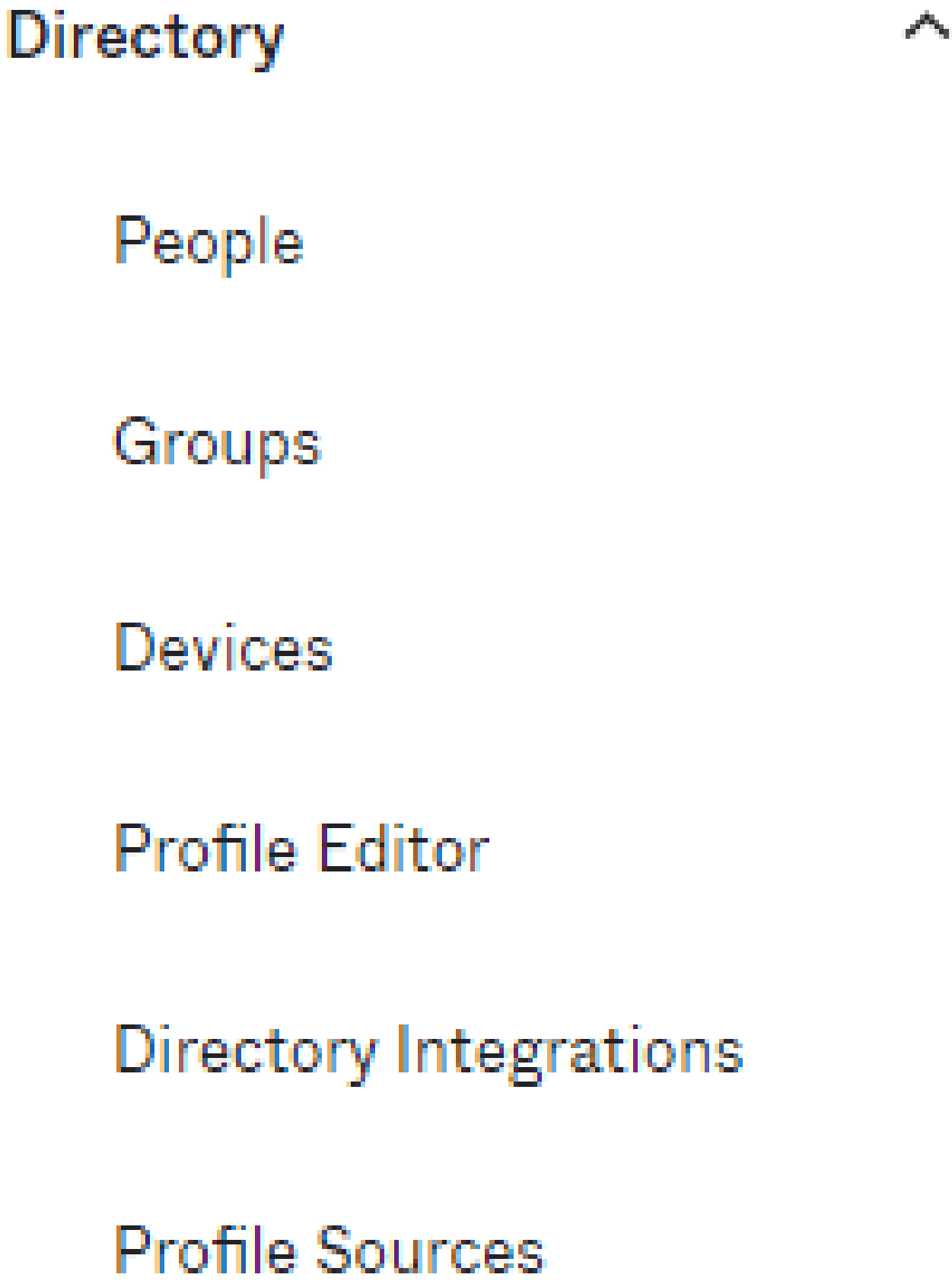


**Note**: Groups must match with the Cisco vManage groups and they need to be in lower case.

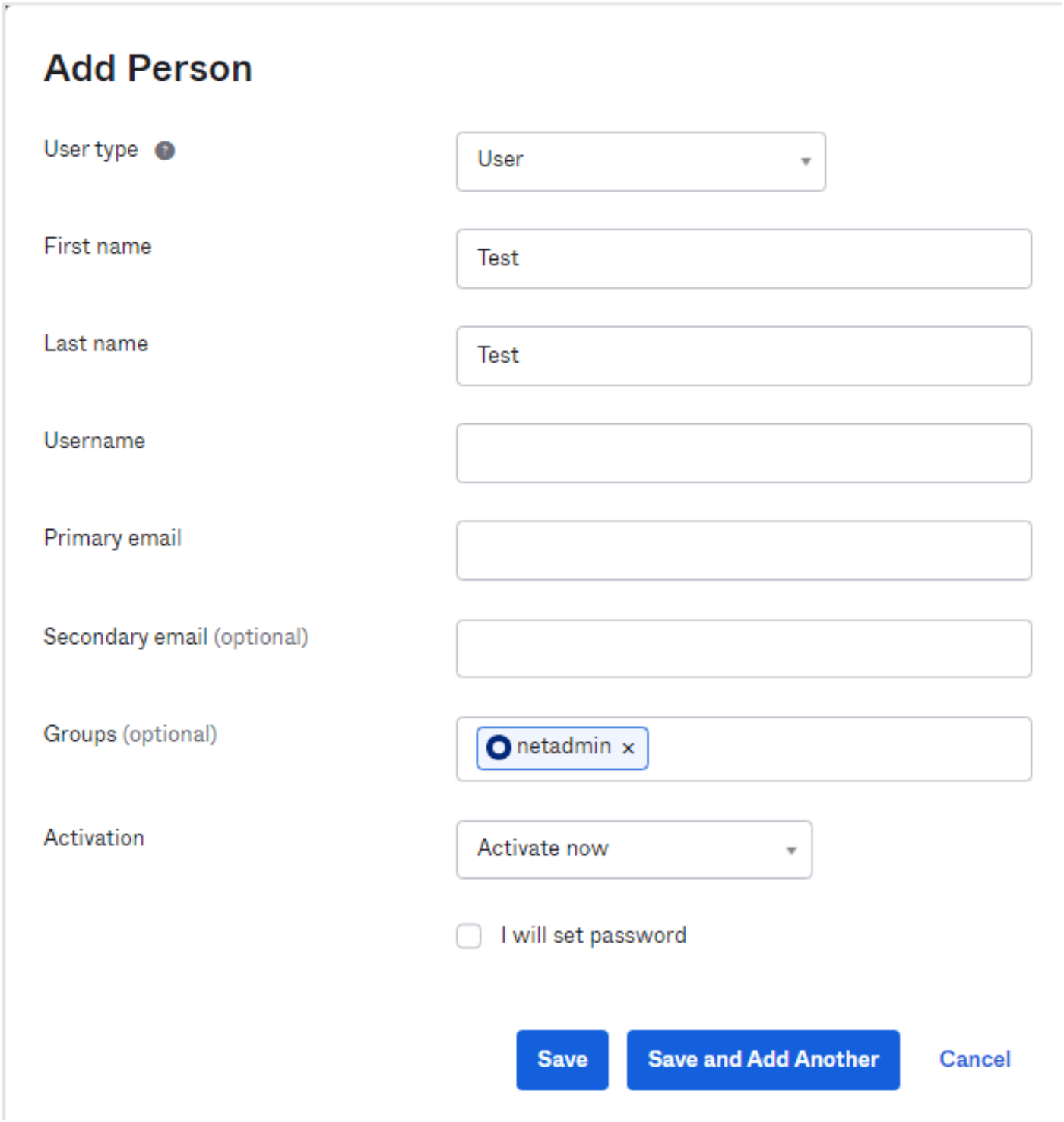
---

## Configure Users in OKTA

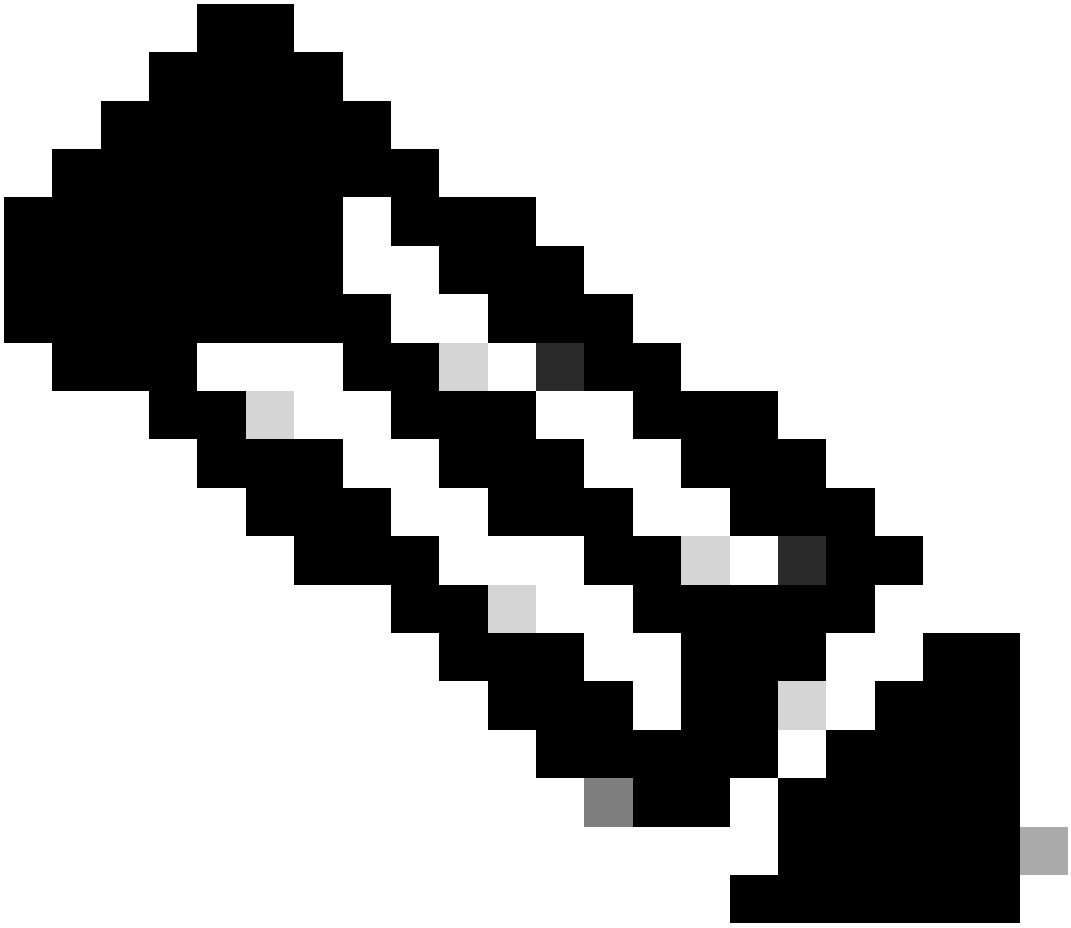
1. Navigate to **Directory** > **People.**


Directory
People
Groups
Devices
Profile Editor
Directory Integrations
Profile Sources

2. Click **Add person,** create a new user, assigne it to the group and save it.




*Add User*

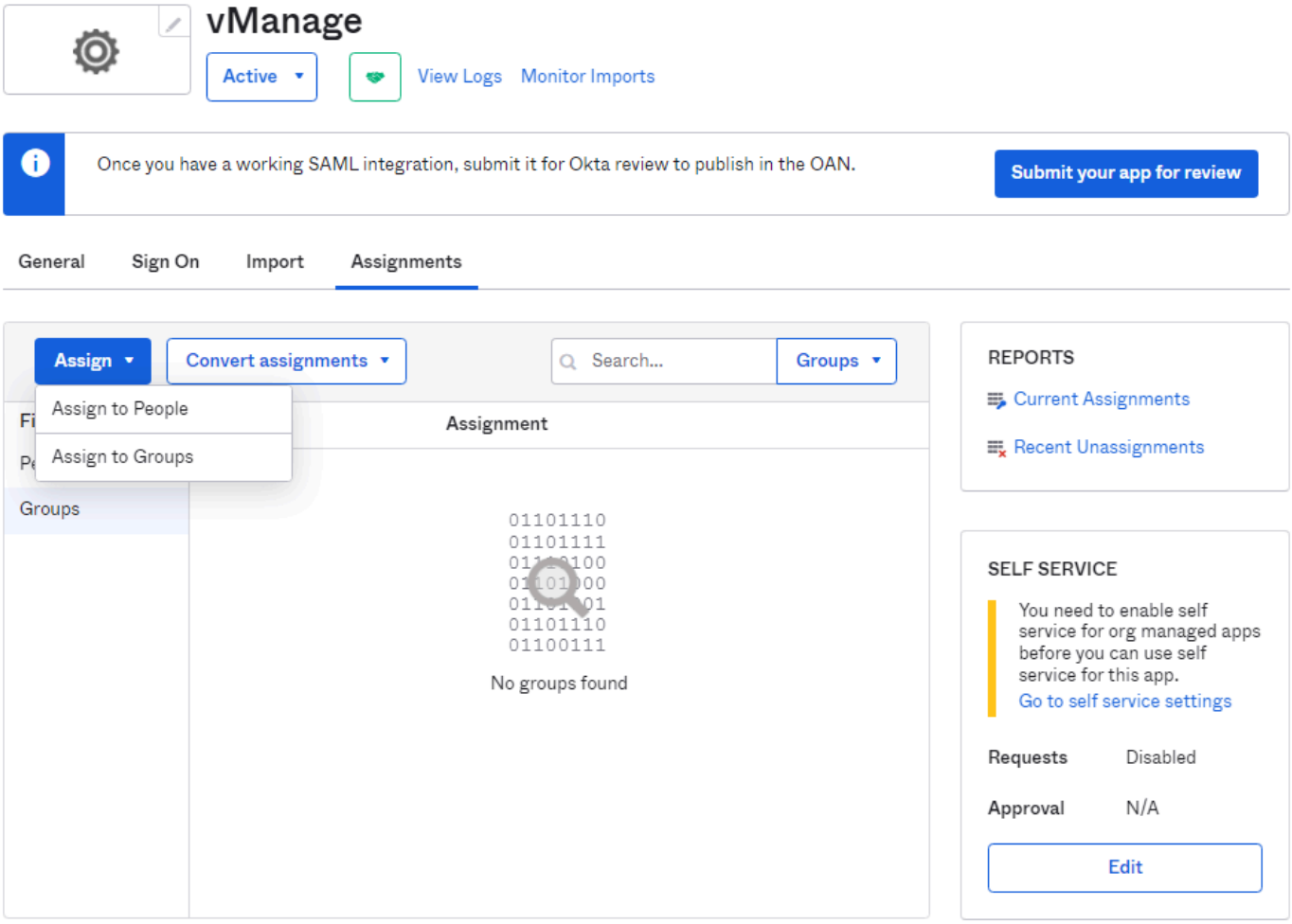


**Note**: Active Directory can be use instead of OKTA users.

## Assign Groups and Users in Application

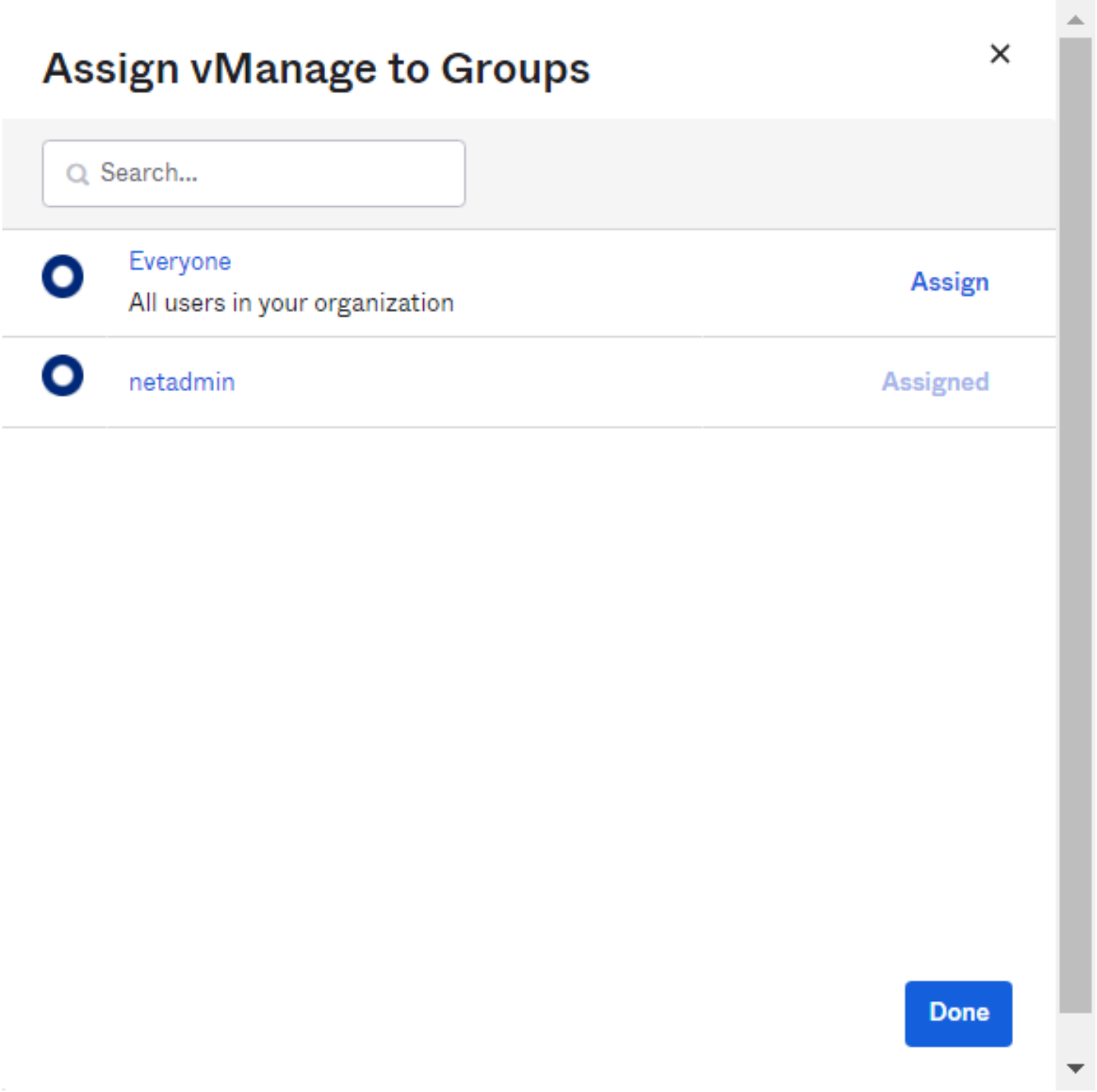
1. Navigate to **Applications** > **Applications** > Select the new application.

2. Click **Assign** > **Assign to Groups**.




*Application > Groups*

3. Identify the group and click **Assign** > **Done.**

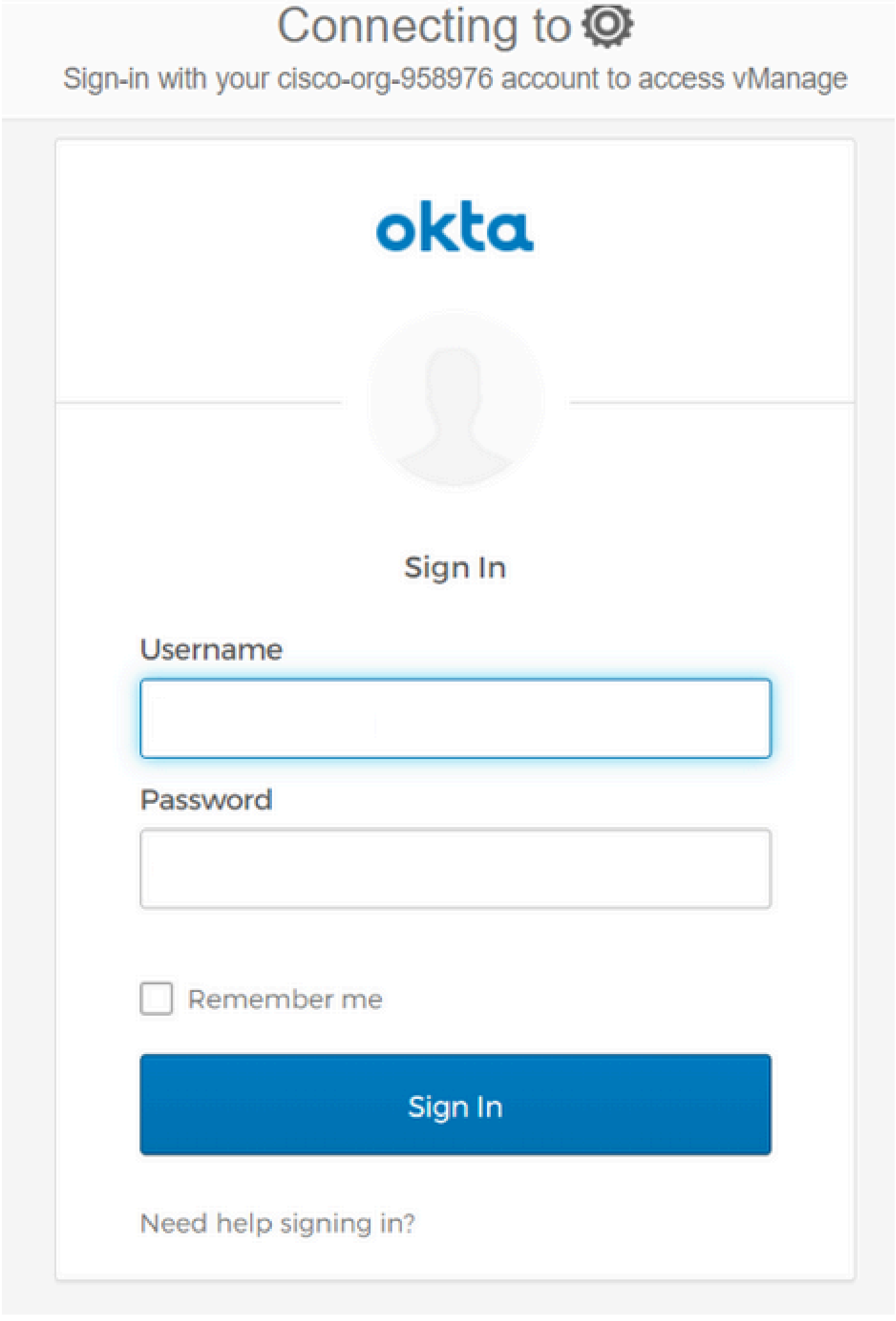



*Assign Group and User*

4. Group and Users now must be assigned to application.

## Verify

Once the configuration be completed, you can get access to Cisco vManage through OKTA.




*SSO Login Vmanage*