SD-WANでのOKTAシングルサインオン(SSO)の設定

内容

はじめに

このドキュメントでは、ソフトウェア定義型ワイドエリアネットワーク(SD-WAN)でOKTAシングルサインオン(SSO)を統合する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- SD-WANの概要
- Security Assertion Markup Language(SAML)
- アイデンティティプロバイダー(IdP)
- 証明書

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco vManageリリース18.3.X以降
- Cisco vManageバージョン20.6.3
- Cisco vBondバージョン20.6.3
- Cisco vSmartバージョン20.6.3

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景

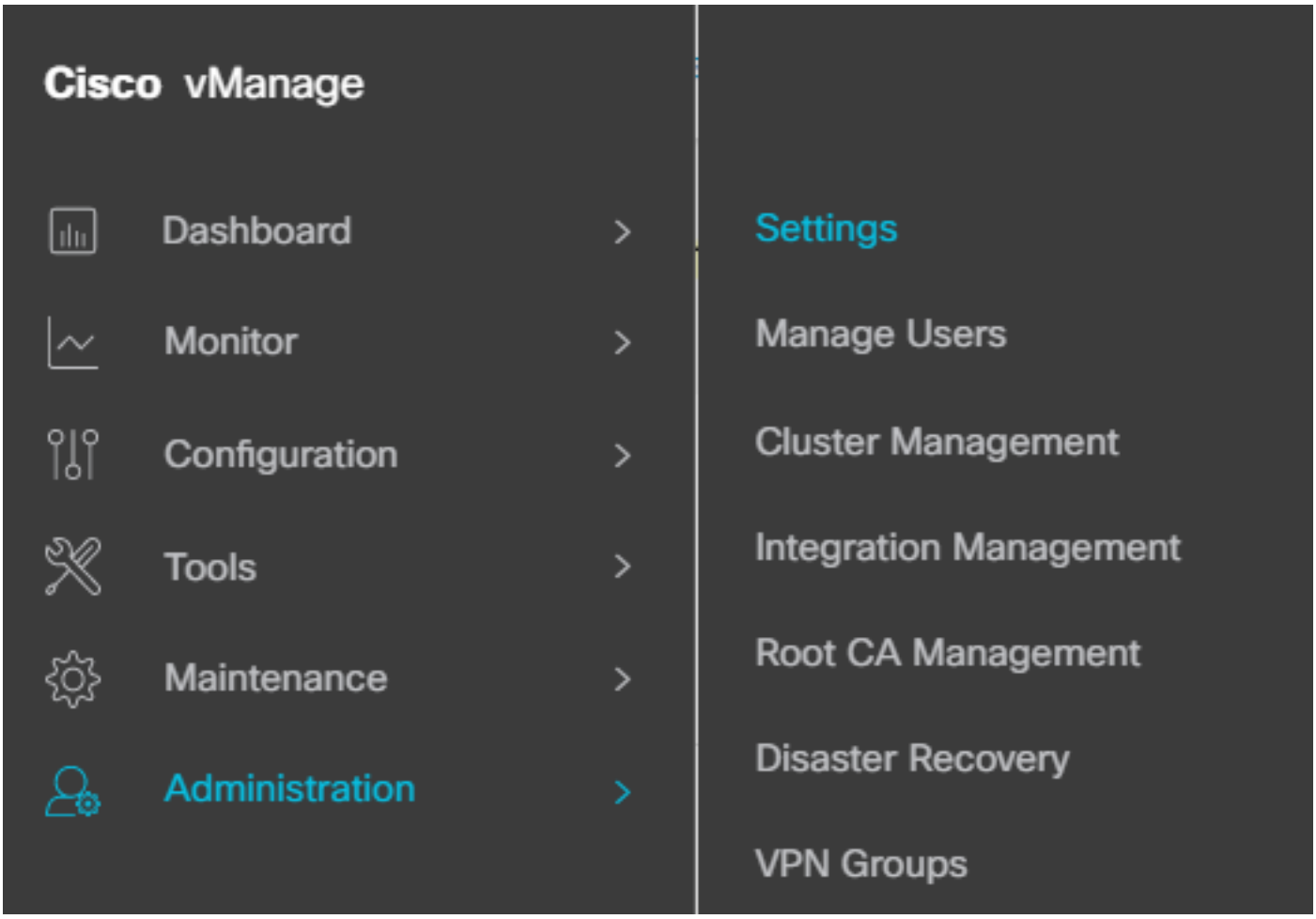
Security Assertion Markup Language(SAML)は、パーティ間、特にアイデンティティプロバイダーとサービスプロバイダーの間で認証および許可データを交換するためのオープンスタンダードです。その名前が示すように、SAMLはセキュリティアサーション（サービスプロバイダーがアクセス制御の決定に使用するステートメント）用のXMLベースのマークアップ言語です。

アイデンティティプロバイダー(IdP)は、シングルサインオン(SSO)を使用して他のWebサイトにアクセスできる信頼されたプロバイダーです。SSOは、パスワードの疲労を軽減し、使いやすさを向上させます。潜在的な攻撃対象領域が減少し、セキュリティが向上します。

設定

vManageの設定

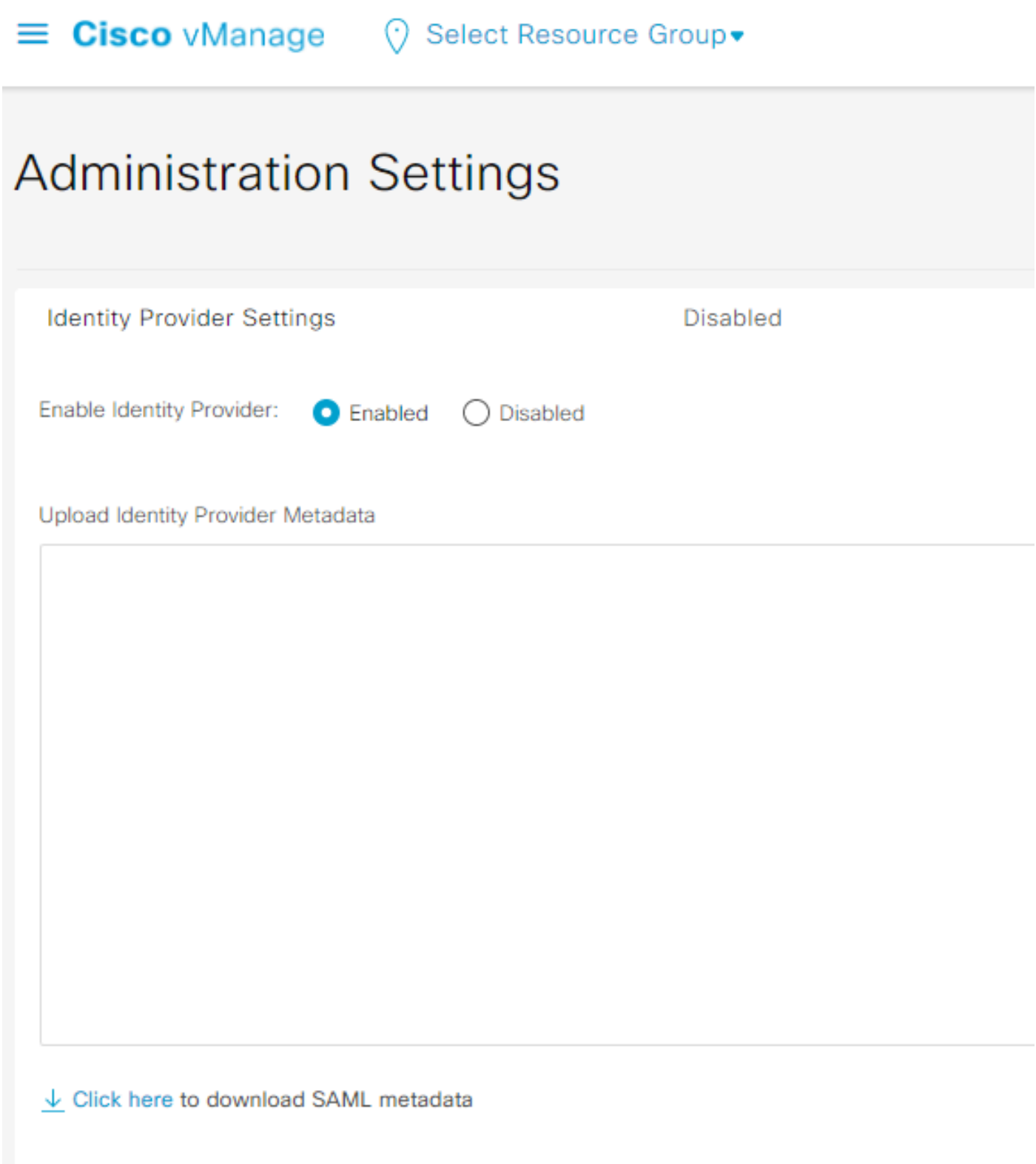
1. Cisco vManageで、Administration > Settings > Identify Provider Settings > Editの順に移動します。



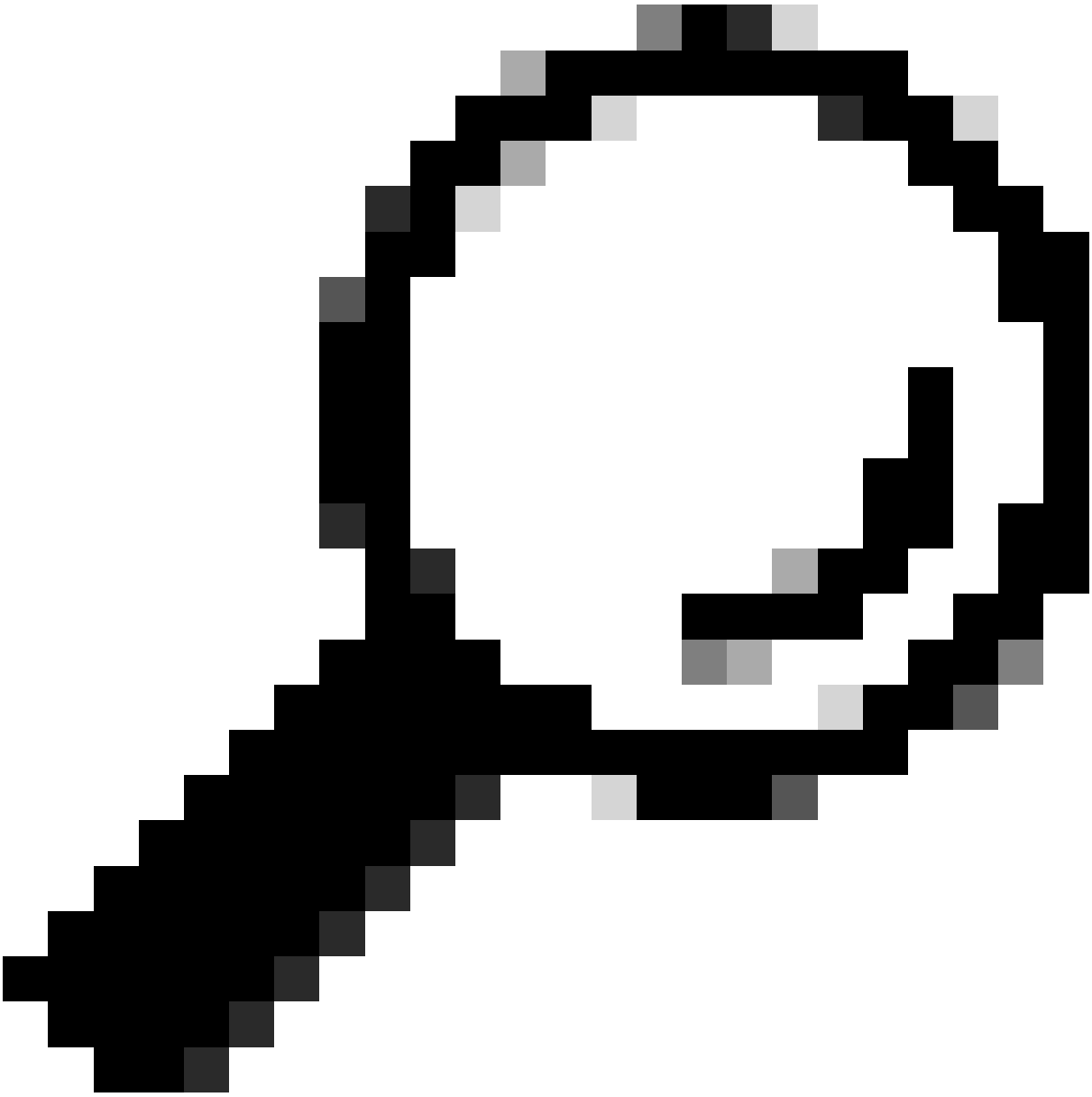
設定>設定

2. Enabledをクリックします。

3. SAMLメタデータをダウンロードしてファイルに保存する場合にクリックします。これはOKTA側で必要です。



SAMLのダウンロード



ヒント:Cisco vManageでOKTAを設定するには、METADATAの次の情報が必要です。

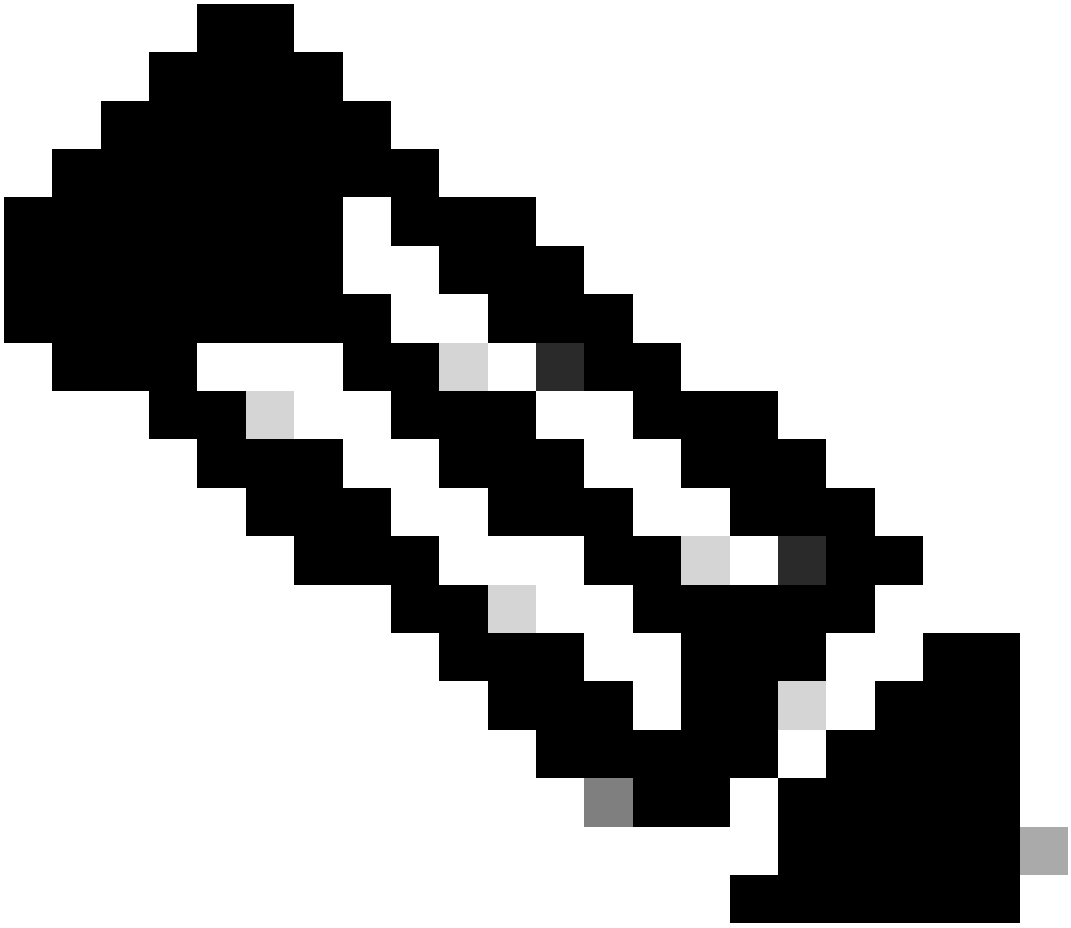
a.エンティティID

口。署名証明書

d.暗号証明書

d.ログアウトURL

e. URにログインします



注：証明書はx.509形式で、.CRT拡張子を付けて保存する必要があります。

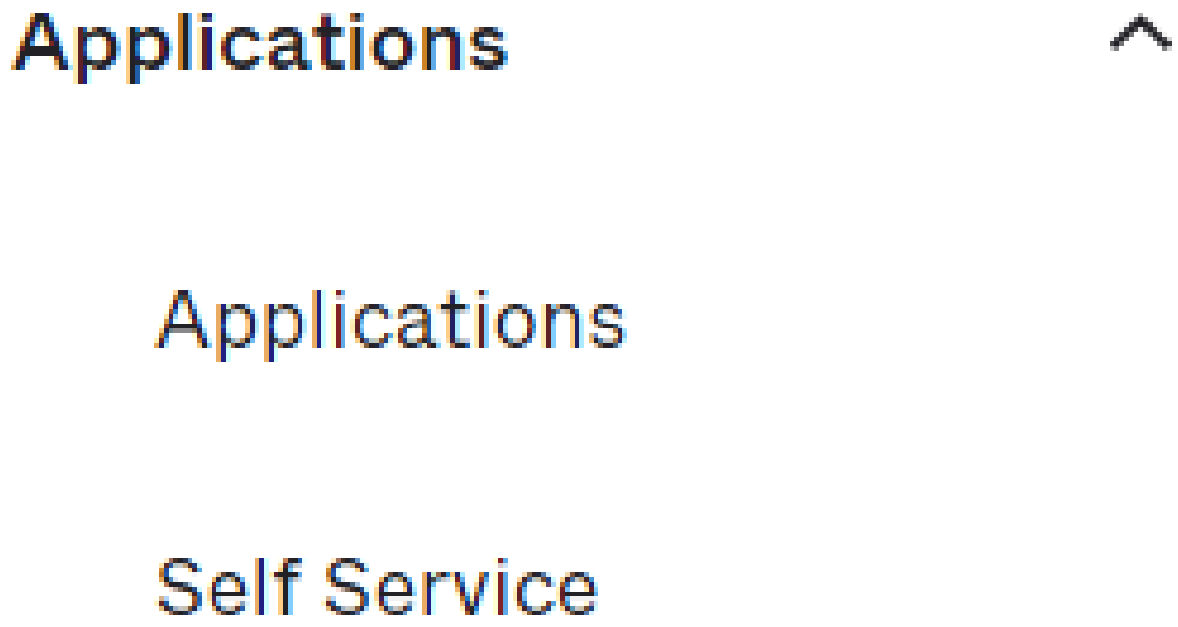
```
-----BEGIN CERTIFICATE-----
MIIDfTCCAmWgAwIBAgIhAM8T9QVLqX/lp1oK/q2XNUbJcGhRmGvqdXxGTUkrKUBhMA0GCSqGSIb3
DQEBCwUAMHIxDDAKBgNVBAYTA1VTQTELMAkGA1UECBMCQ0ExETAPBgNVBAcTCFNhbiBKb3NlMRQw
EgYDVQQKEwtDSVNDT1JUUExBQjEUMBIGA1UECxMLQ01lTQ09SVFBMQUIxFjAUBgNVBAMTDURlZmF1
bHRUZW5hbnQwHhcNMjAwNTI4MTQxMzQzWhcNMjUwNTI4MTQxMzQzWjByMQwwCgYDVQQGEwNVU0Ex
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証明書

OKTAの設定

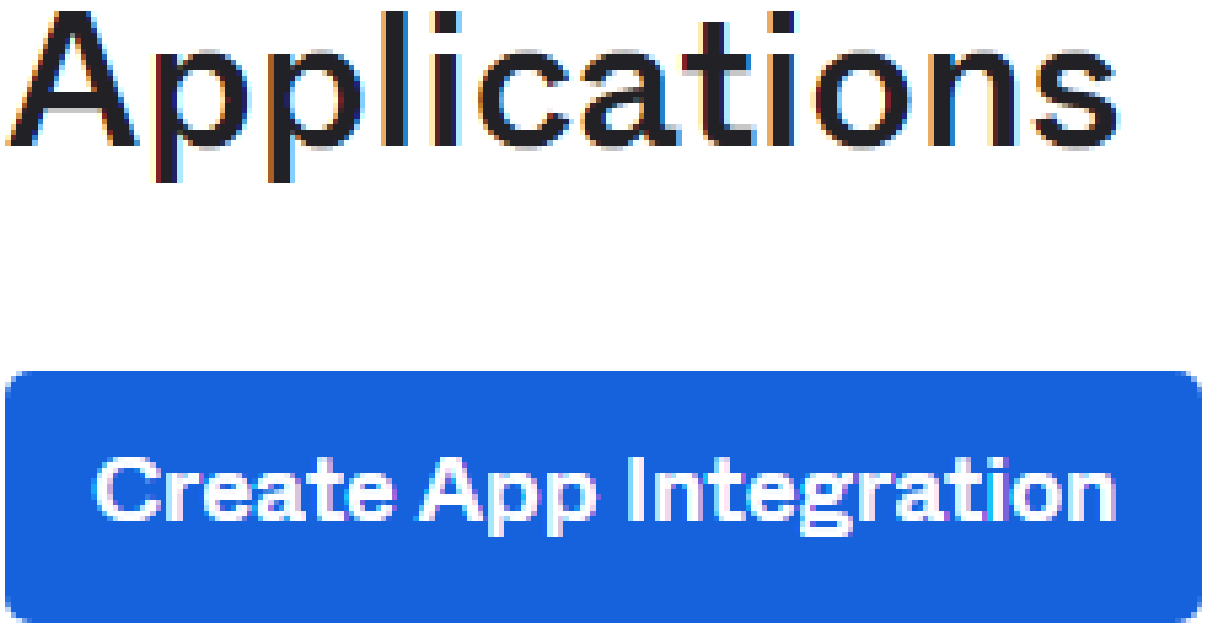
1. OKTAアカウントにログインします。

2. 「アプリケーション」> 「アプリケーション」にナビゲートします。



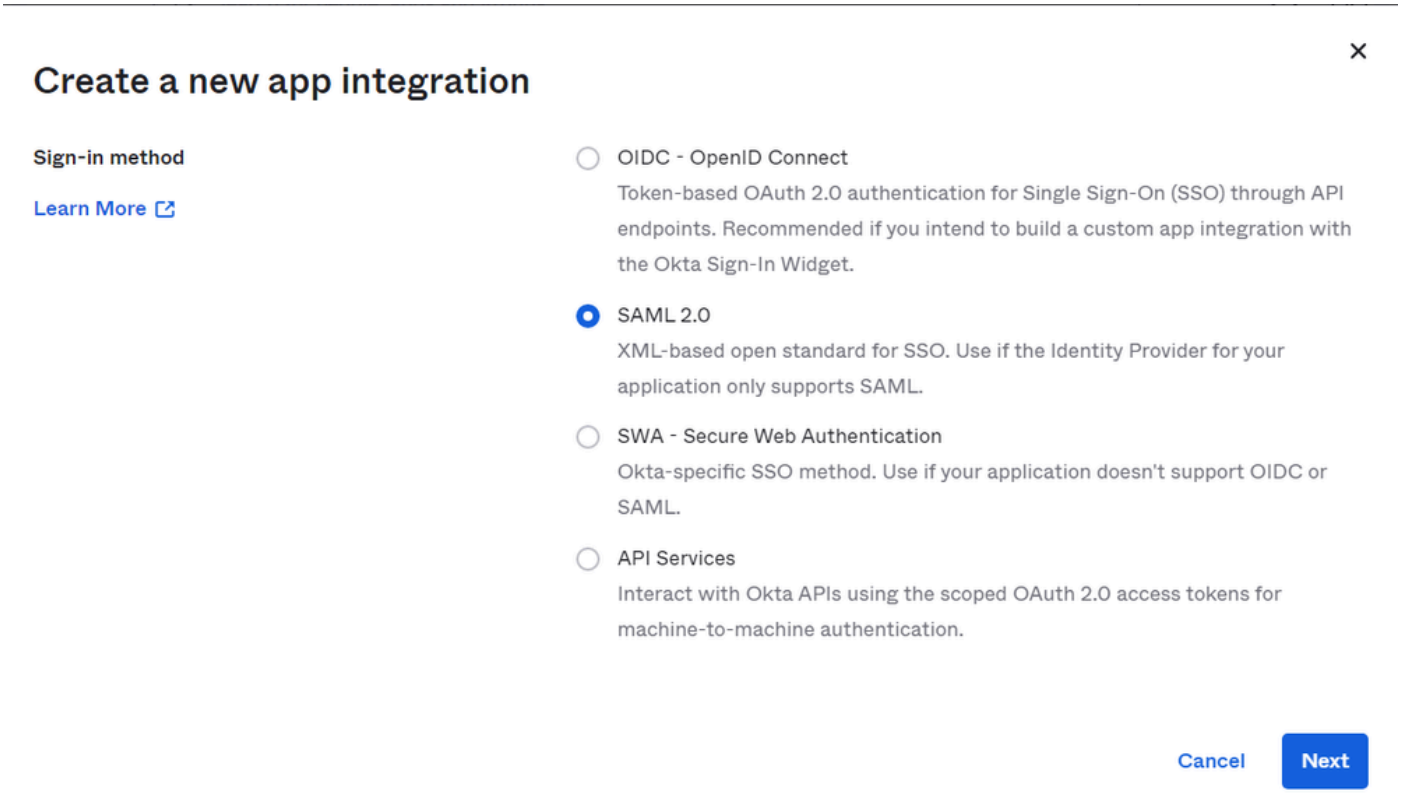
アプリケーション>アプリケーション

3. クリック アプリケーション統合の作成。



アプリケーションの作成

4. SAML 2.0をクリックし、nextをクリックします。



SAML2.0の設定

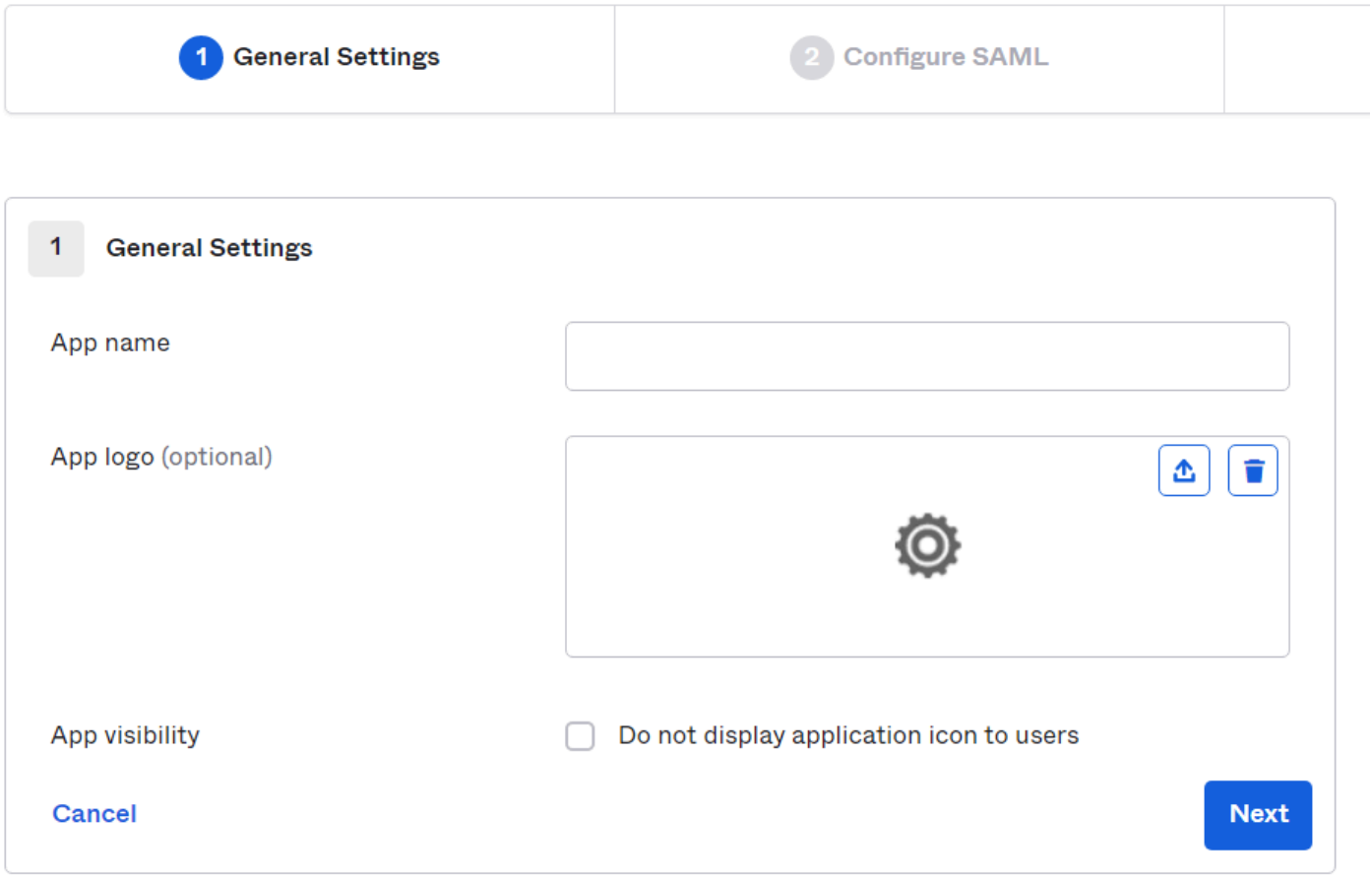
一般設定

1. アプリケーションの名前を入力します。

2. アプリケーションのロゴを追加します（オプション）。

3. アプリケーションの可視性（オプション）

4. NEXTをクリックします。



SAMLの一般設定

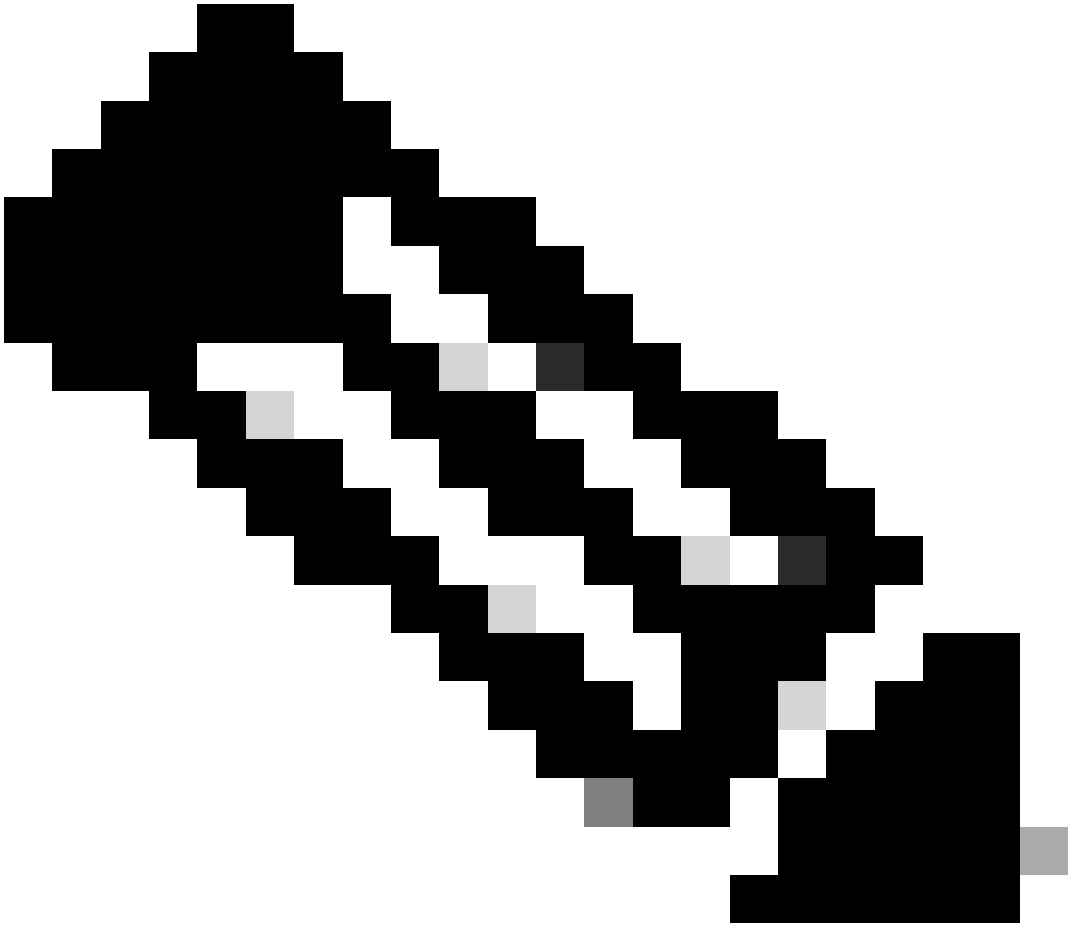
SAMLの設定

次の表では、このセクションで設定する必要があるパラメータについて説明します。

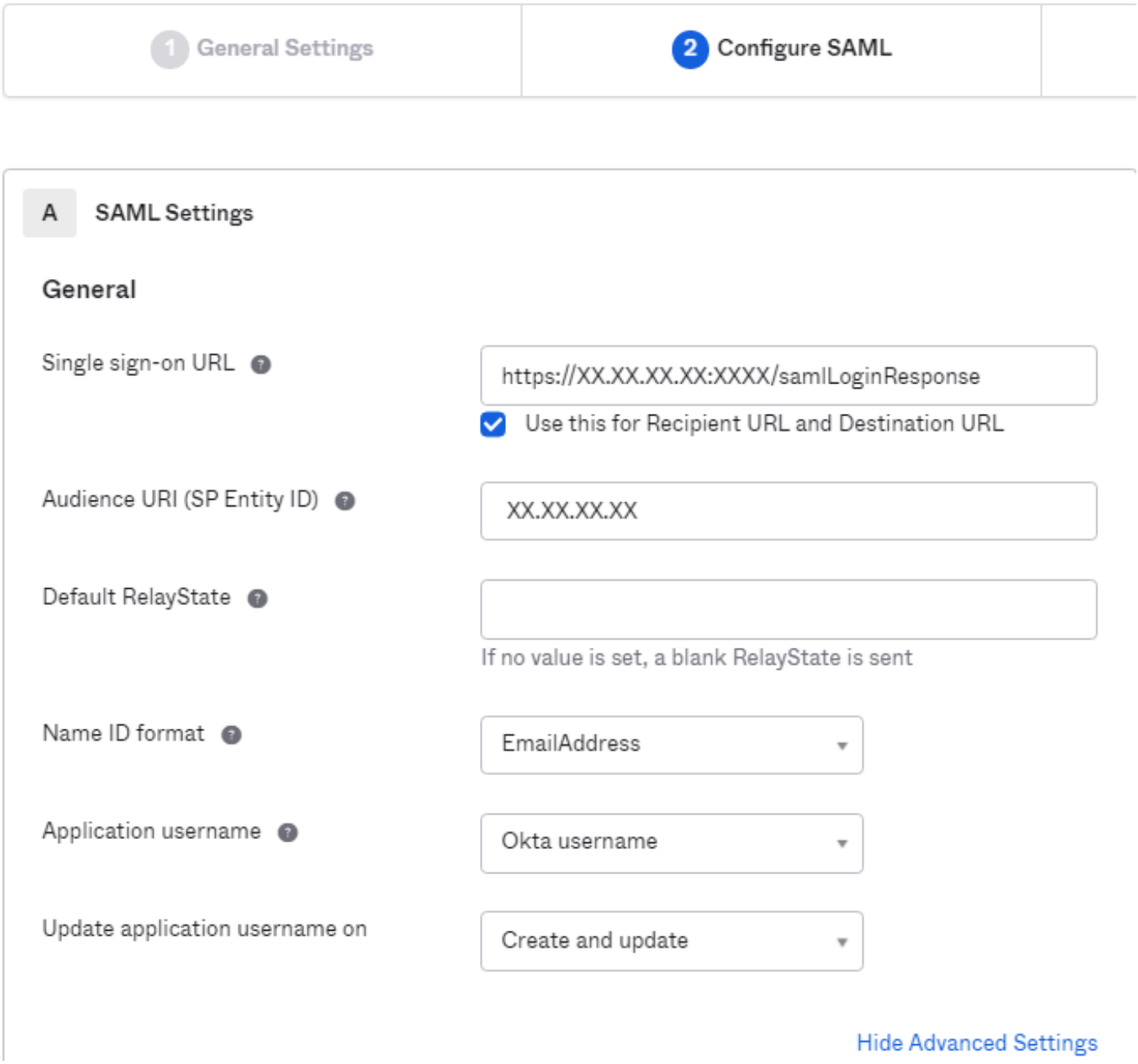
コンポーネント	値	コンフィギュレーション
シングルサインオンURL	https://XX.XX.XX.XX:XXXX/samlLoginResponse	メタデータから取得します。
対象ユーザーURI（SPエンティティID）	XX.XX.XX.XX	Cisco vManageのIPアドレスまたはDNS

コンポーネント	値	コンフィギュレーション
既定のRelayState		空
名前IDの形式		お客様の好みに応じて
アプリケーションユーザ名		お客様の好みに応じて
アプリケーションのユーザー名の更新	作成と更新	作成と更新
応答	署名済	署名済
アサーションシグニチャ	署名済	署名済
署名アルゴリズム	RSA-SHA256	RSA-SHA256
ダイジェストアルゴリズム	SHA256	SHA256
アサーション暗号化	[Encrypted]	[Encrypted]
暗号化アルゴリズム	AES256-CBC	AES256-CBC
キー転送アルゴリズム	RSA-OAEP	RSA-OAEP
暗号化証明書		メタデータからの暗号化証明書(x.509形式)を保持している必要があります。
シングルログアウトの有効化		確認する必要があります。

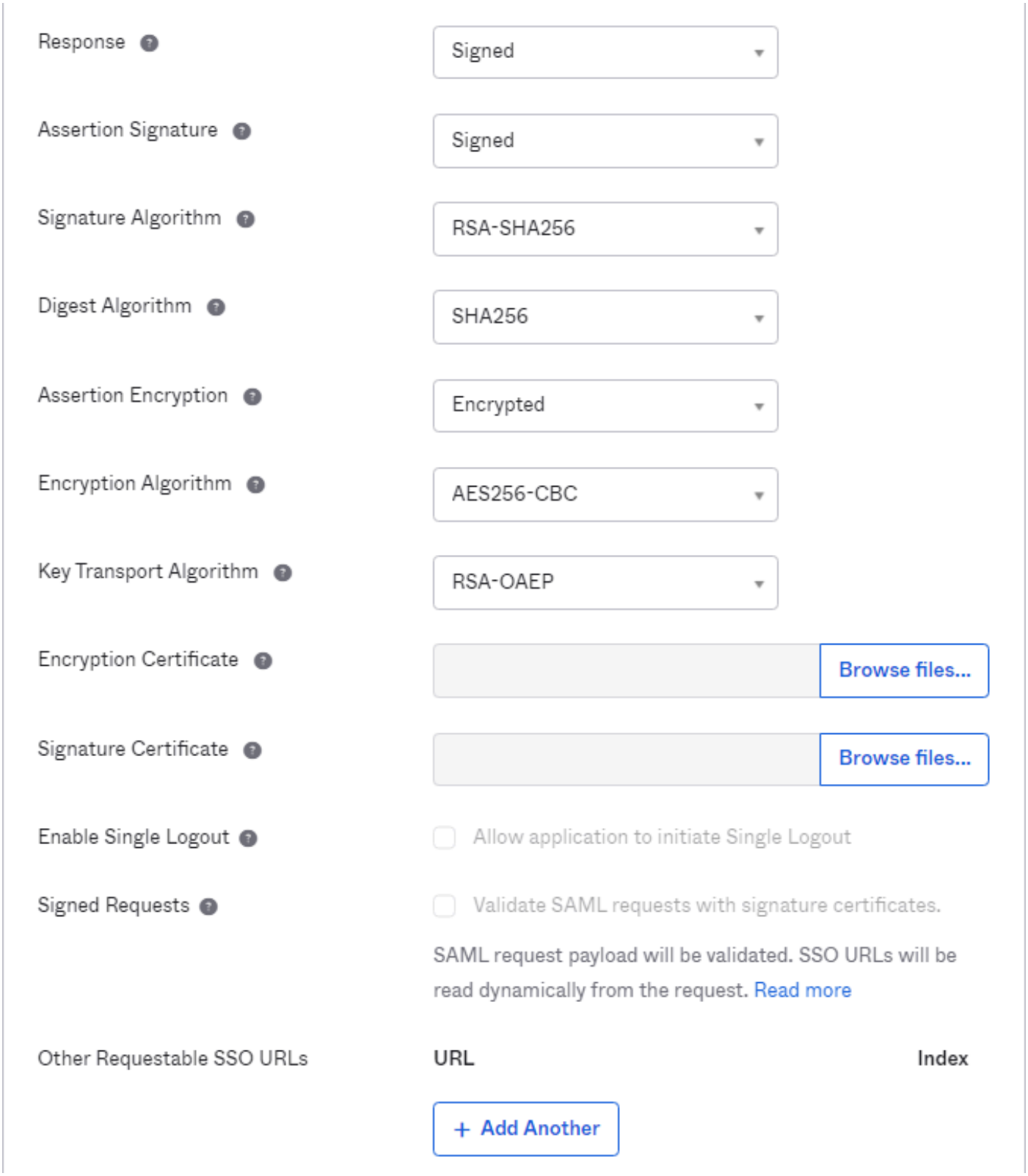
コンポーネント	値	コンフィギュレーション
シングルログアウトURL	https://XX.XX.XX.XX:XXXX/samlLogoutResponse	メタデータから取得します。
SP発行者	XX.XX.XX.XX	vManageのIPアドレスまたはDNS
署名証明書		メタデータからの暗号化証明書が、x.509形式である必要があります。
アサーションインラインフック	なし（無効）	なし（無効）
認証コンテキストクラス	X.509証明書	
認証の強制	Yes	Yes
SAML発行者ID文字列	SAML発行者ID文字列	文字列テキストを入力します
属性ステートメント（オプション）	名前▸ユーザ名 名前の形式（オプション）▸未指定 値▸user.login	名前▸ユーザ名 名前の形式（オプション）▸未指定 値▸user.login
グループ属性ステートメント（オプション）	グループ▸名前 名前の形式（オプション）▸未指定 フィルタ▸正規表現▸に一致します。*	グループ▸名前 名前の形式（オプション）▸未指定 フィルタ▸正規表現▸に一致します。*



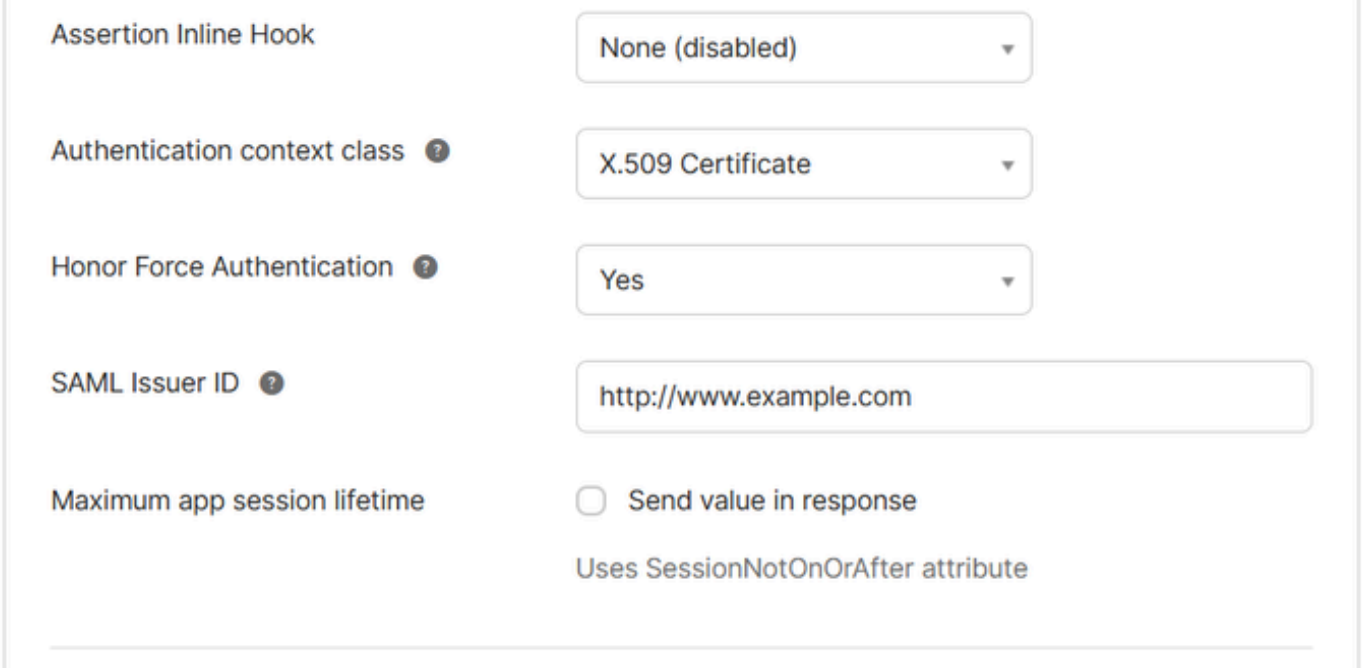
注:SAMLの設定の表に示されているとおりに、ユーザ名とグループを使用する必要があります。

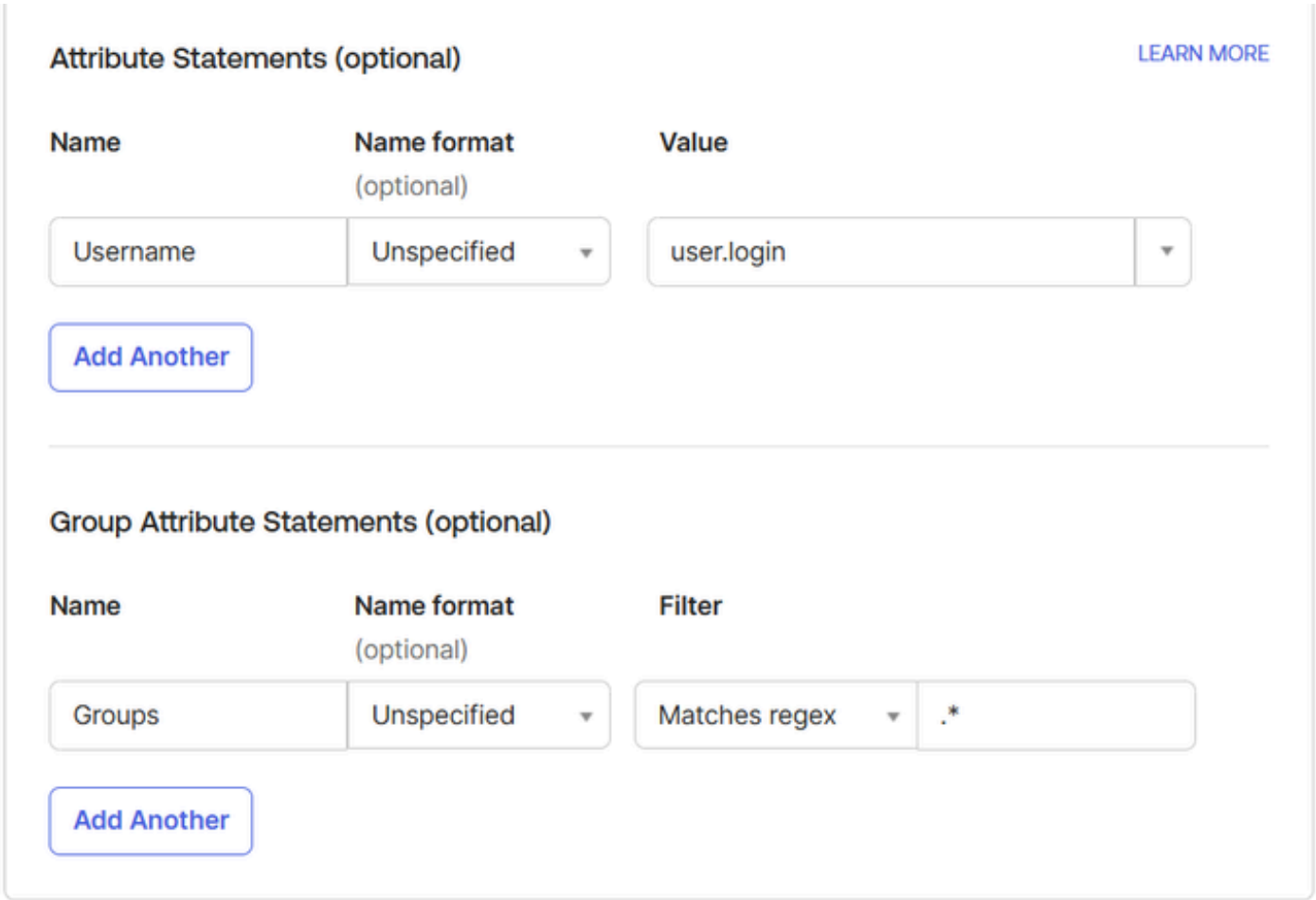


SAMLパート1の設定



SAMLパート2の設定



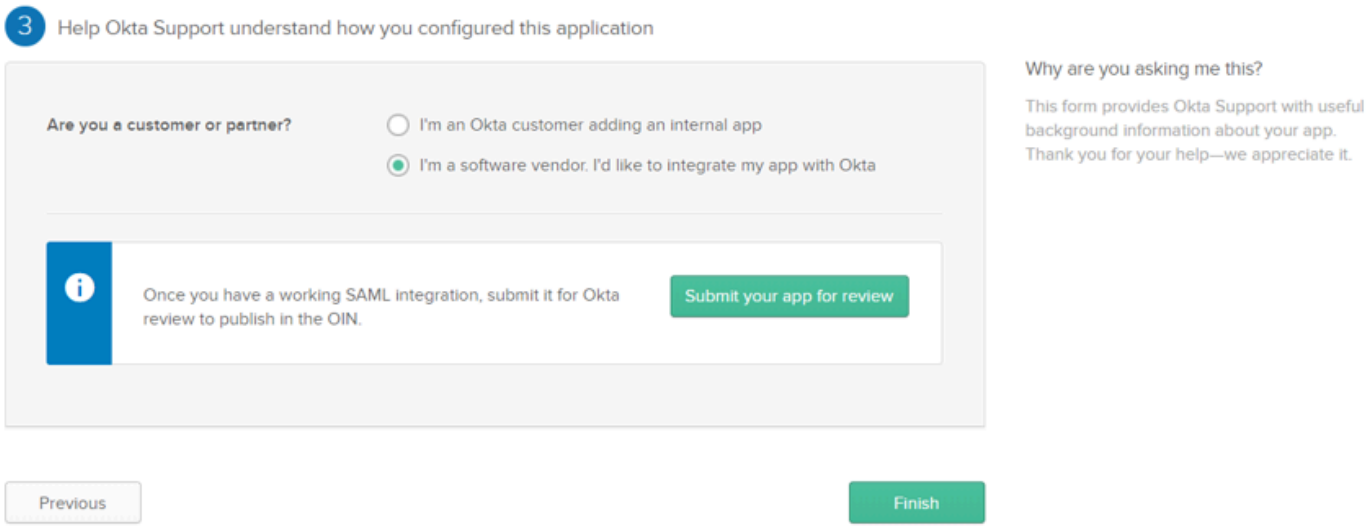


- [Next] をクリックします。

フィードバック

1. いずれかのオプションを選択します。

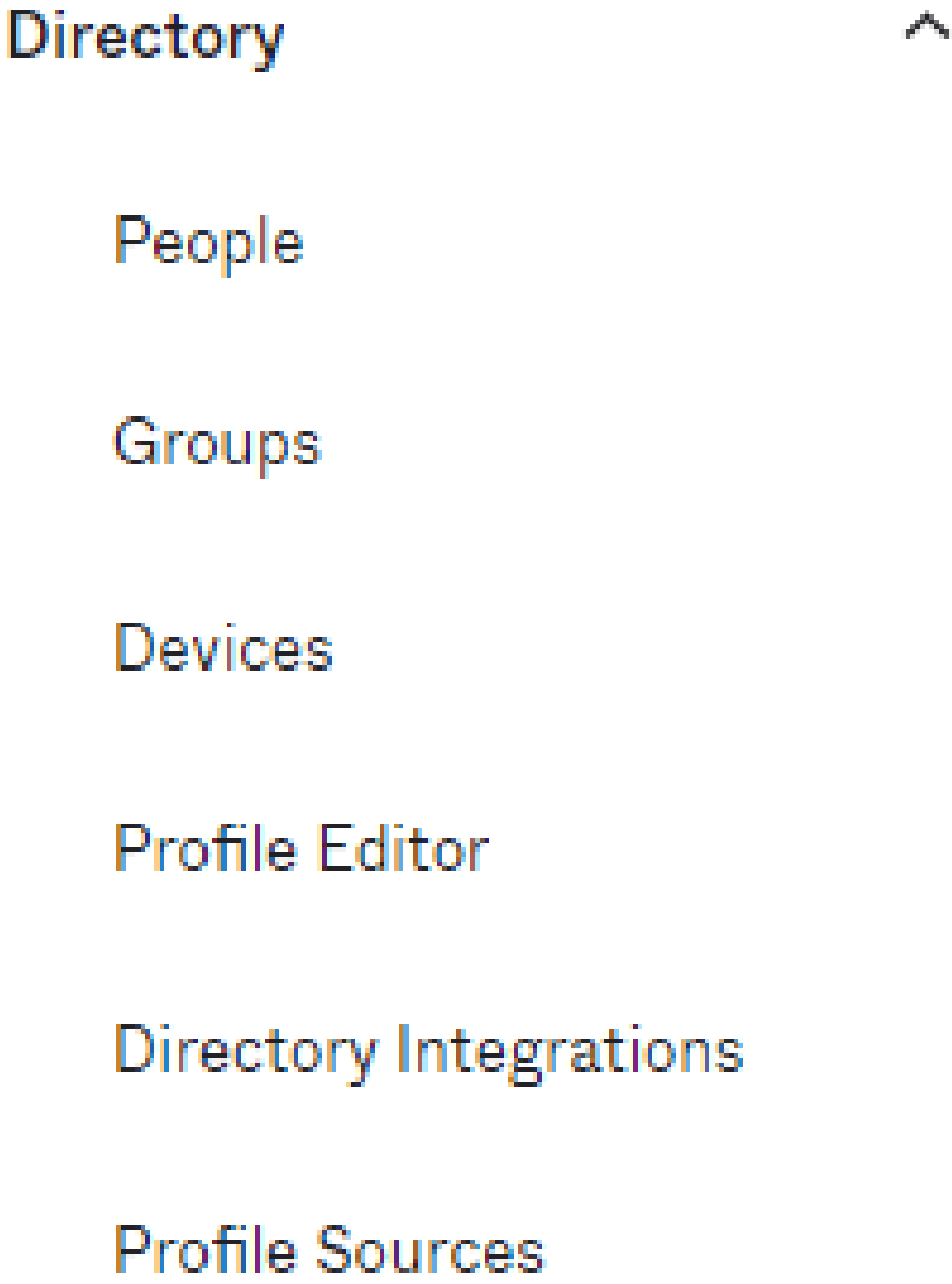
2. Finishをクリックします。



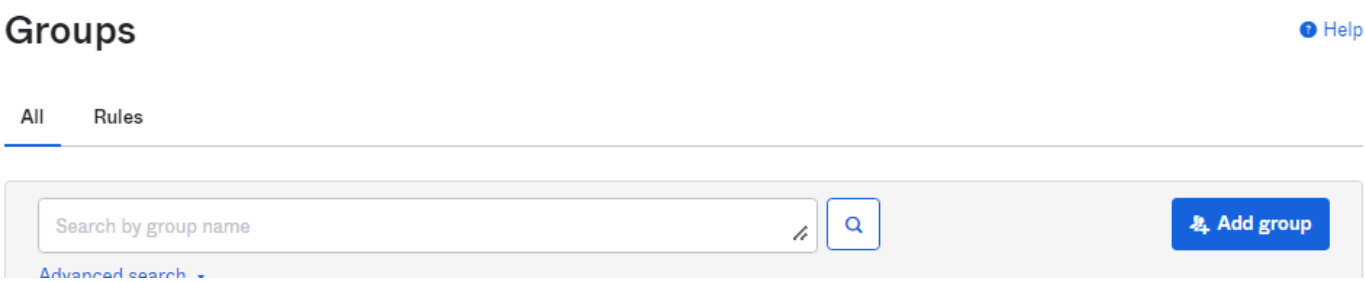
SMALフィードバック

OKTAでのグループの設定

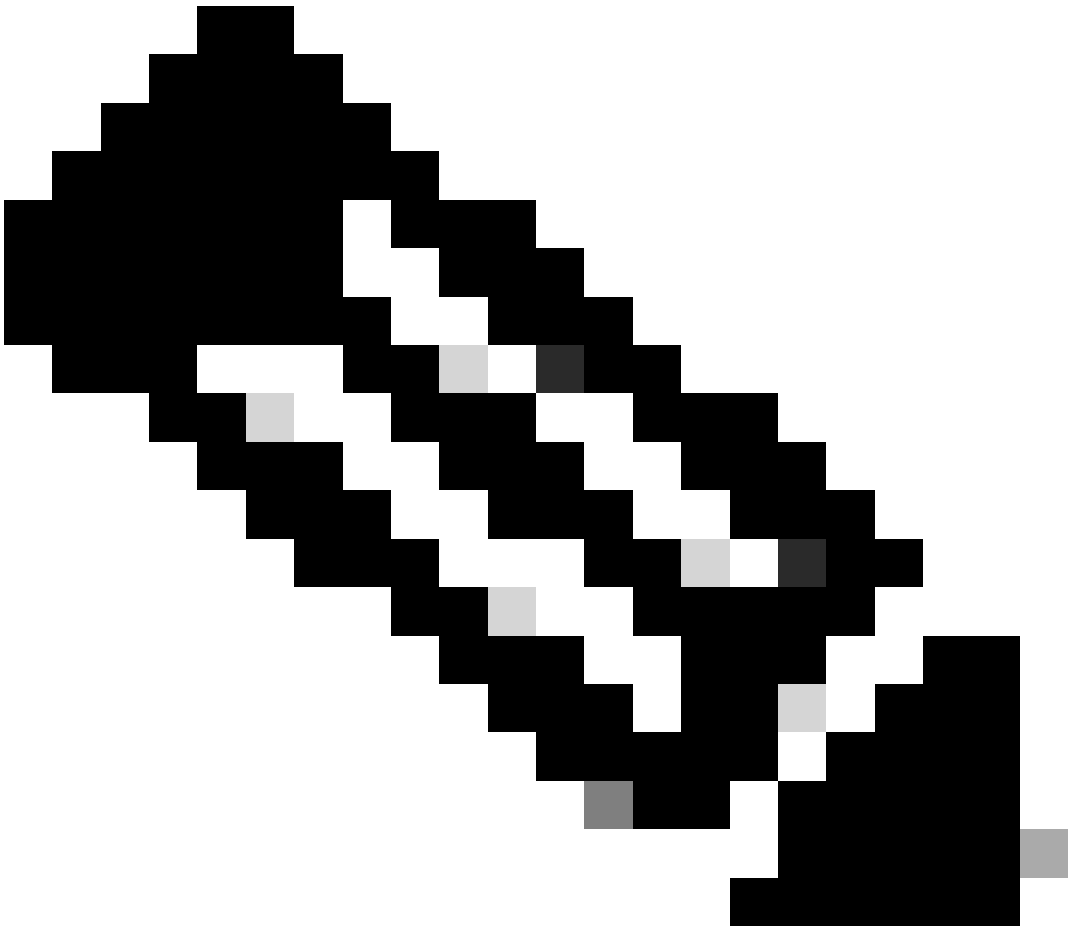
1. Directory > Groupsの順に移動します。


Directory
People
Groups
Devices
Profile Editor
Directory Integrations
Profile Sources

2. Add groupをクリックして、新しいグループを作成します。



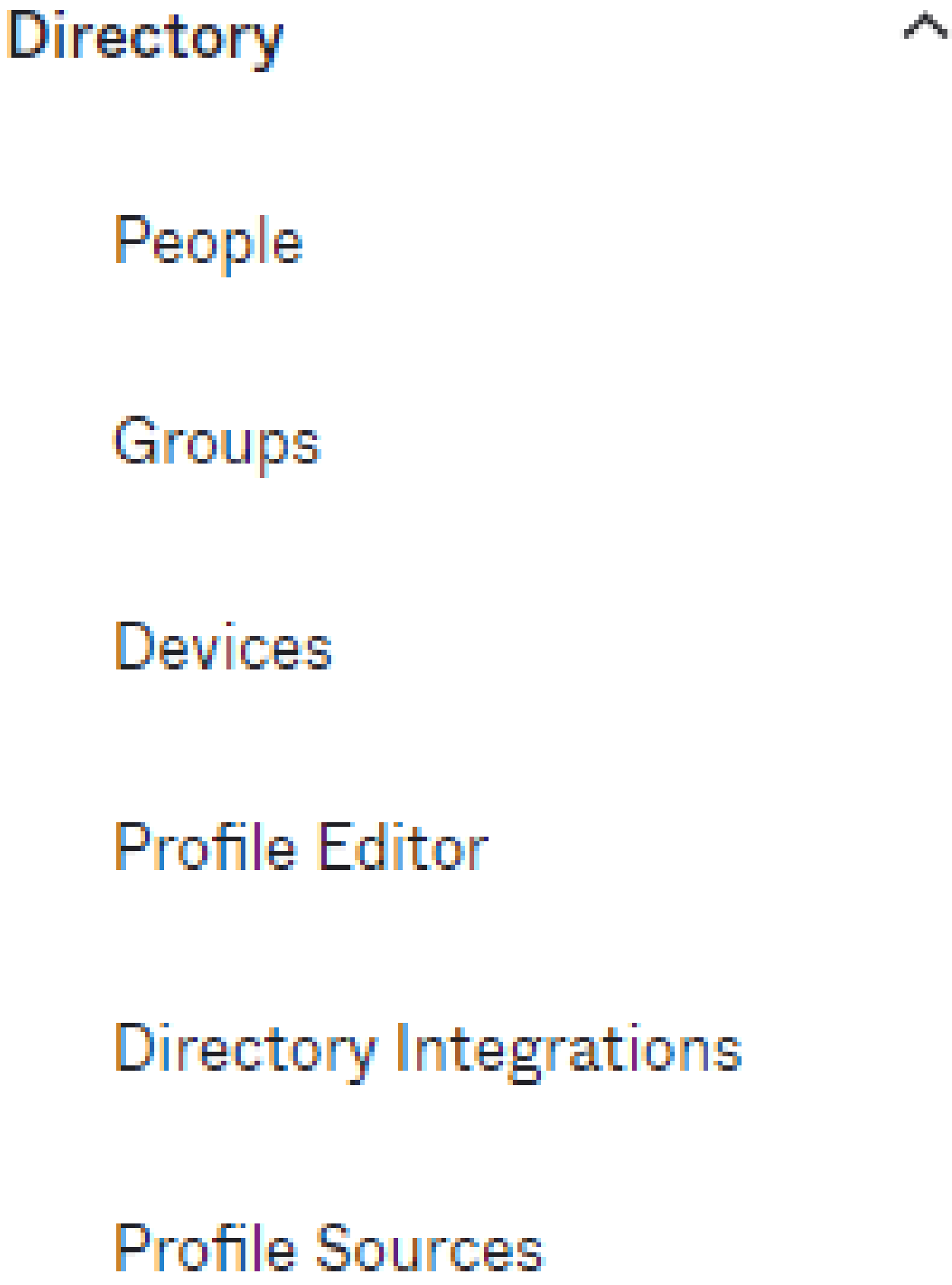
グループの追加



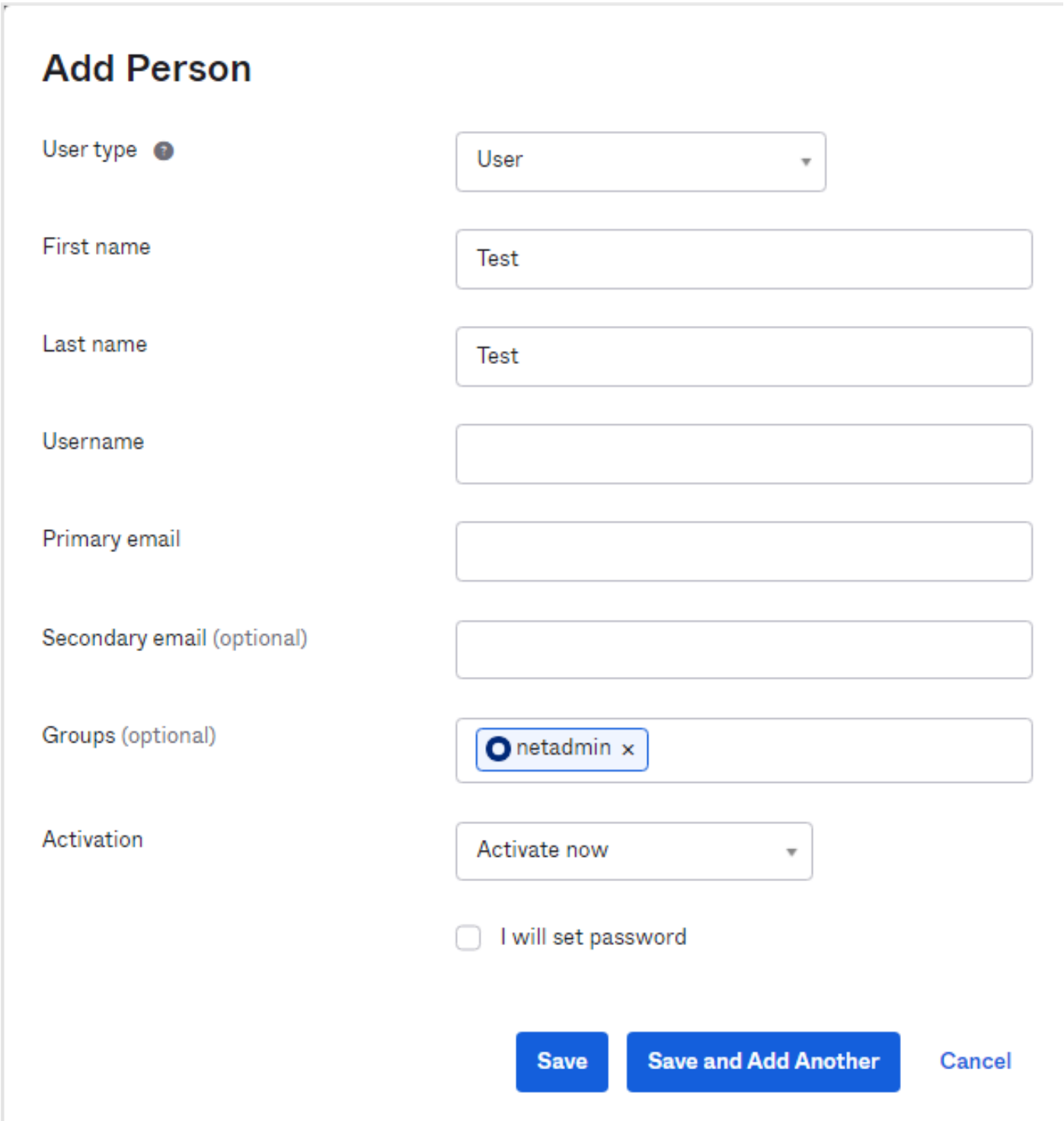
注：グループはCisco vManageグループと一致している必要があり、小文字にする必要があります。

OKTAでのユーザの設定

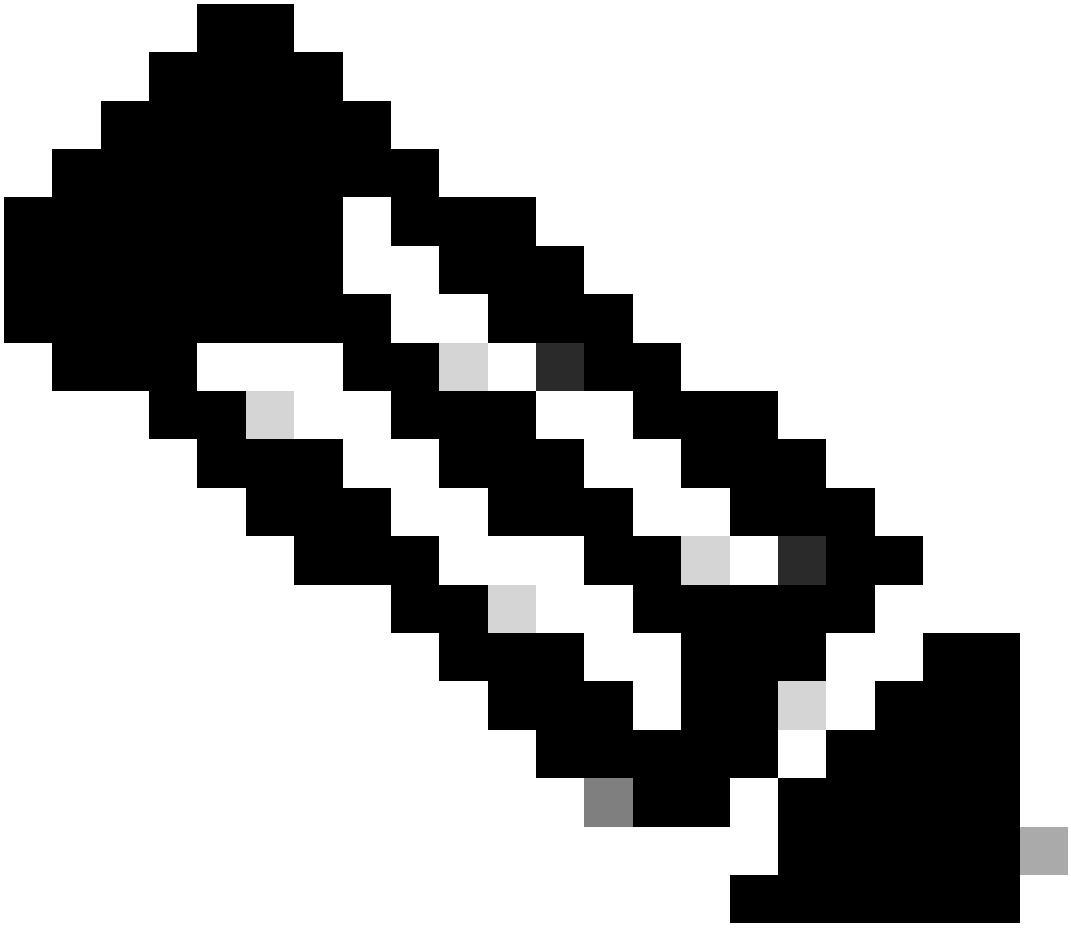
1. Directory > Peopleの順に移動します。


Directory
People
Groups
Devices
Profile Editor
Directory Integrations
Profile Sources

2. Add personをクリックし、新しいユーザを作成し、グループに割り当てて保存します。



ユーザの追加

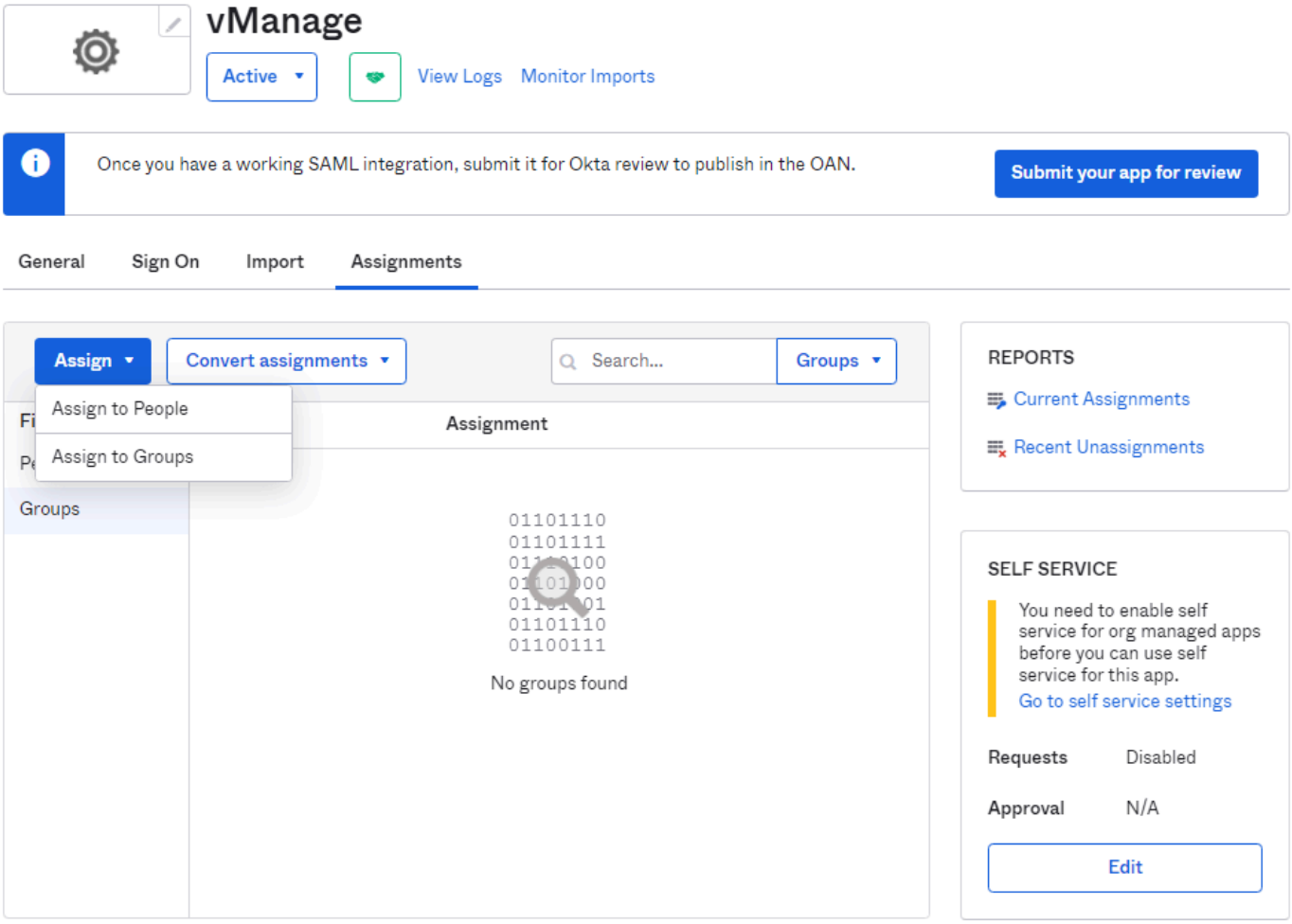


注:OKTAユーザの代わりにActive Directoryを使用できます。

アプリケーションでのグループとユーザの割り当て

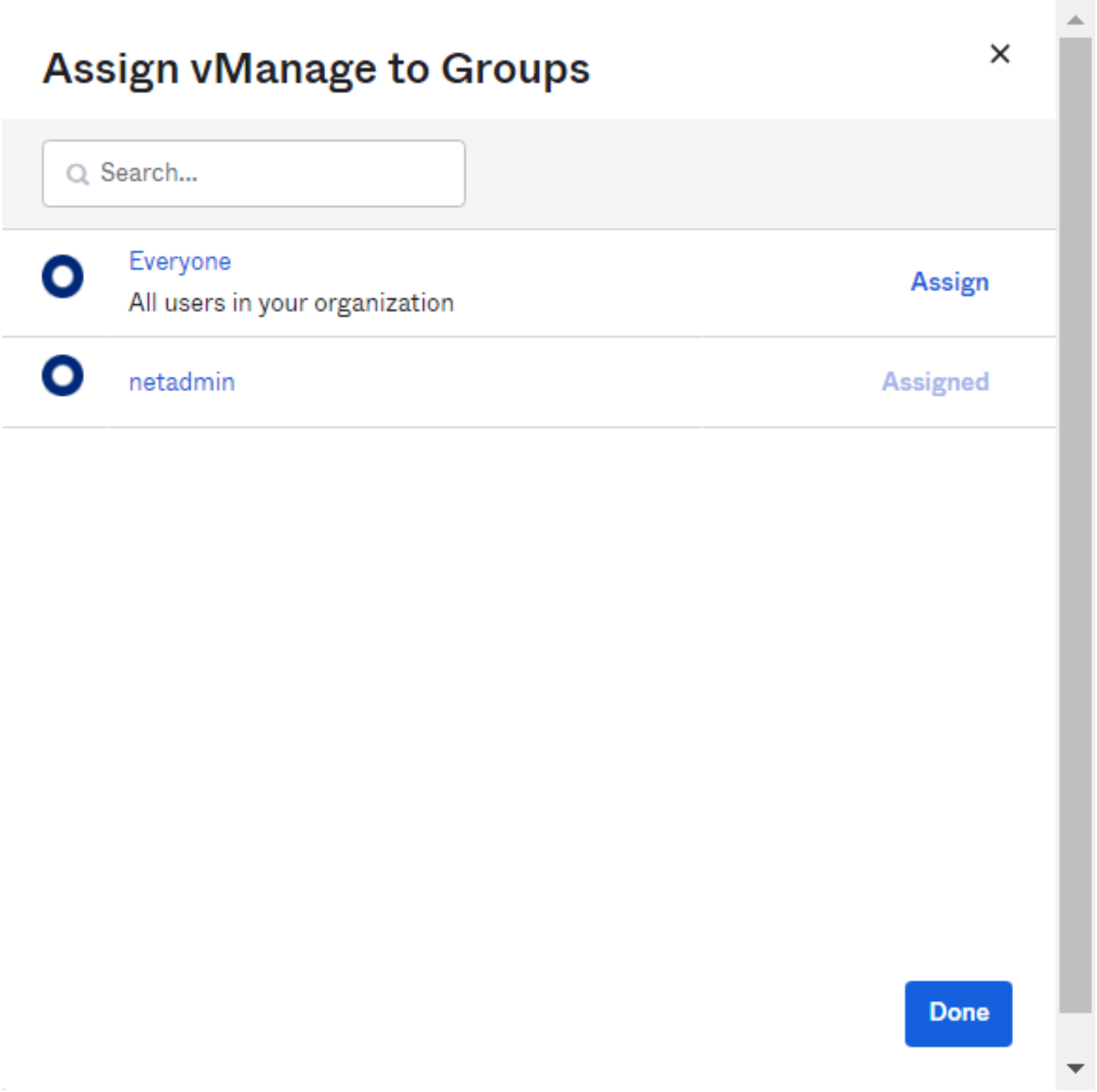
1. 「アプリケーション」>「アプリケーション」に移動し、新しいアプリケーションを選択します。

2. Assign > Assign to Groupsの順にクリックします。



アプリケーション>グループ

3. グループを識別し、「割り当て」>「完了」の順にクリックします。

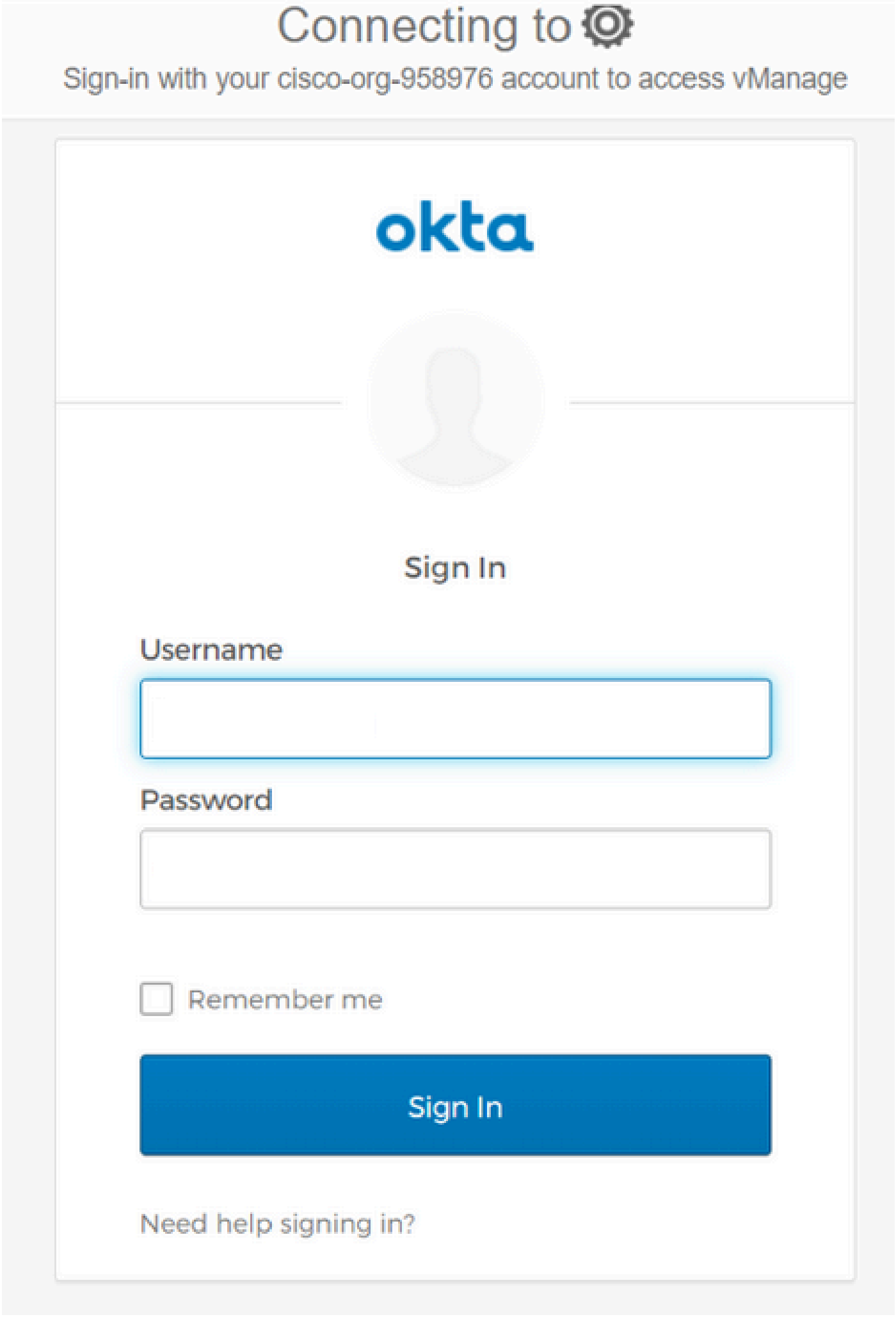


グループとユーザの割り当て

4. グループとユーザーをアプリケーションに割り当てる必要があります。

確認

設定が完了すると、OKTAからCisco vManageにアクセスできます。



SSOログインVmanage

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。