Configuration de l'authentification unique (SSO) OKTA sur SD-WAN

Table des matières

Introduction

Ce document décrit comment intégrer OKTA Single Sing-On (SSO) sur un réseau étendu défini par logiciel (SD-WAN).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Présentation générale du SD-WAN
- SAML (Security Assertion Markup Language)
- Fournisseur d'identité (IdP)
- Certificats

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de

logiciel suivantes :

- Cisco vManage version 18.3.X ou ultérieure
- 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Fond

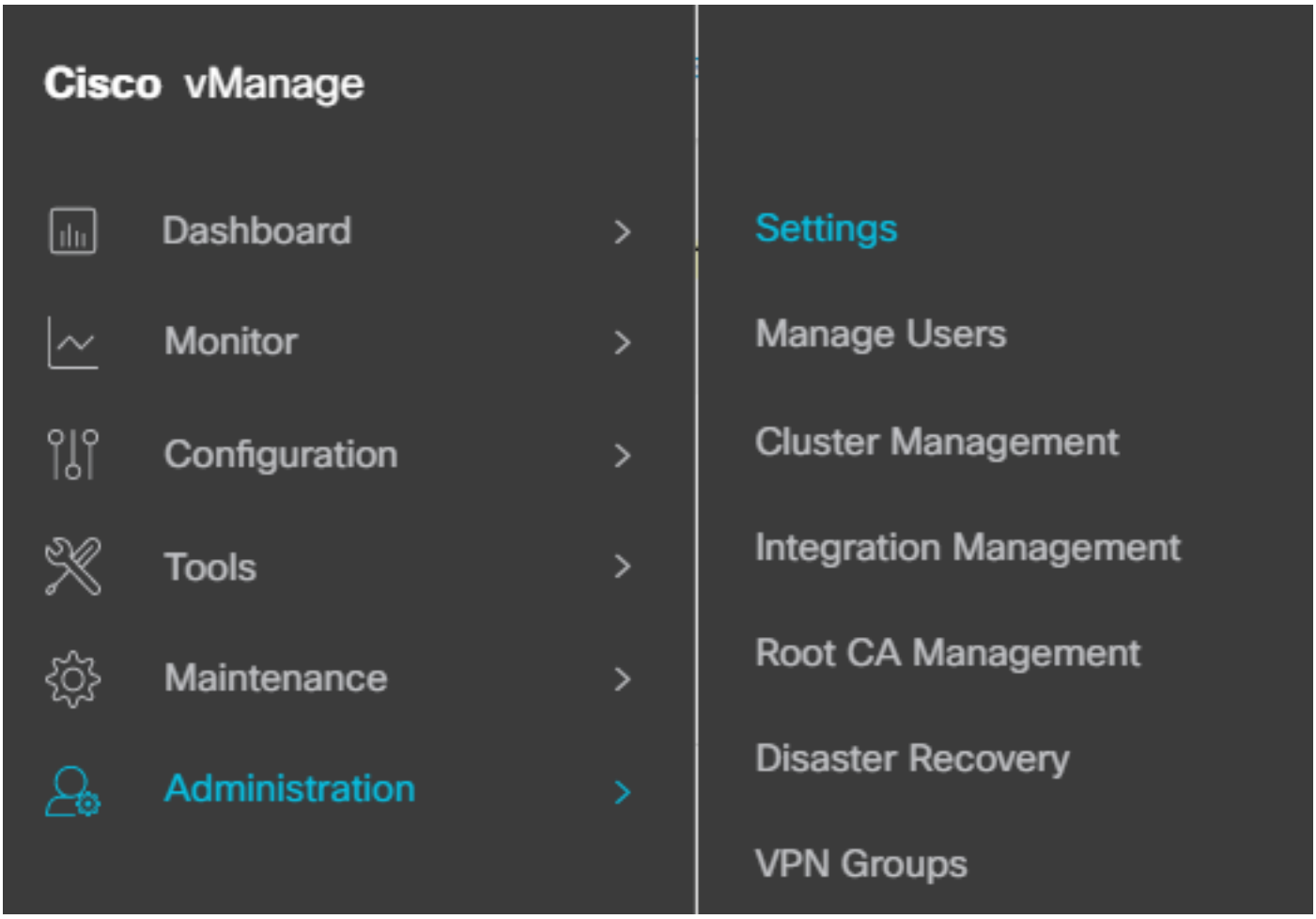
Le langage SAML (Security Assertion Markup Language) est une norme ouverte pour l'échange de données d'authentification et d'autorisation entre les parties, en particulier entre un fournisseur d'identité et un fournisseur de services. Comme son nom l'indique, SAML est un langage de balisage XML pour les assertions de sécurité (instructions que les fournisseurs de services utilisent pour prendre des décisions de contrôle d'accès).

Un fournisseur d'identité (IdP) est un fournisseur de confiance qui vous permet d'utiliser l'authentification unique (SSO) afin d'accéder à d'autres sites Web. SSO réduit la fatigue des mots de passe et améliore leur convivialité. Il réduit la surface d'attaque potentielle et offre une meilleure sécurité.

Configurer

Configuration vManage

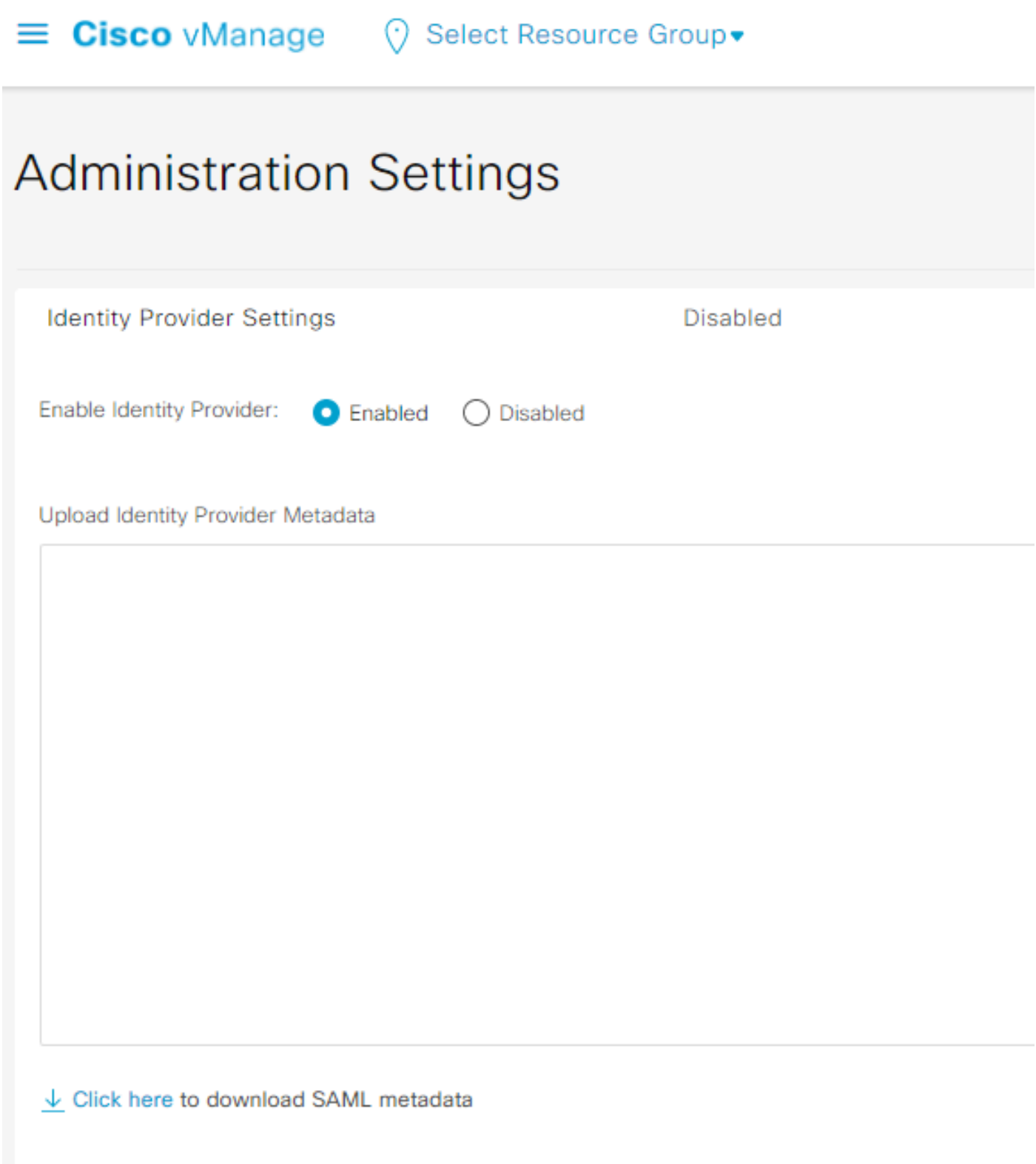
1. Dans Cisco vManage, accédez à Administration > Settings > Identity Provider Settings > Edit.



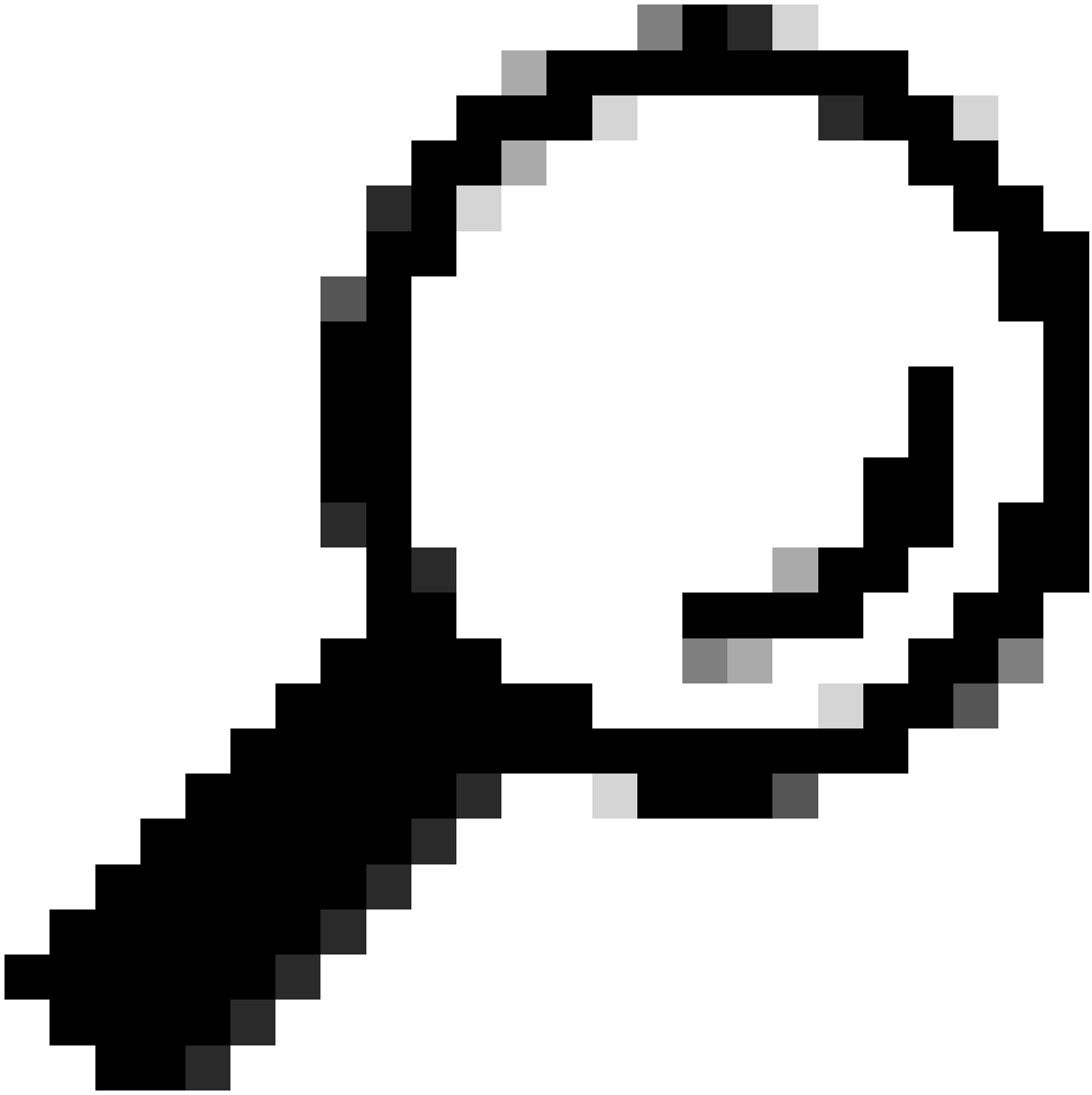
Configuration > Paramètres

2. Cliquez sur Activé.

3. Cliquez pour télécharger les métadonnées SAML et enregistrer le contenu dans un fichier. C'est nécessaire du côté de l'OKTA.



Télécharger SAML



Conseil : Vous avez besoin de ces informations de METADATA pour configurer OKTA avec Cisco vManage.

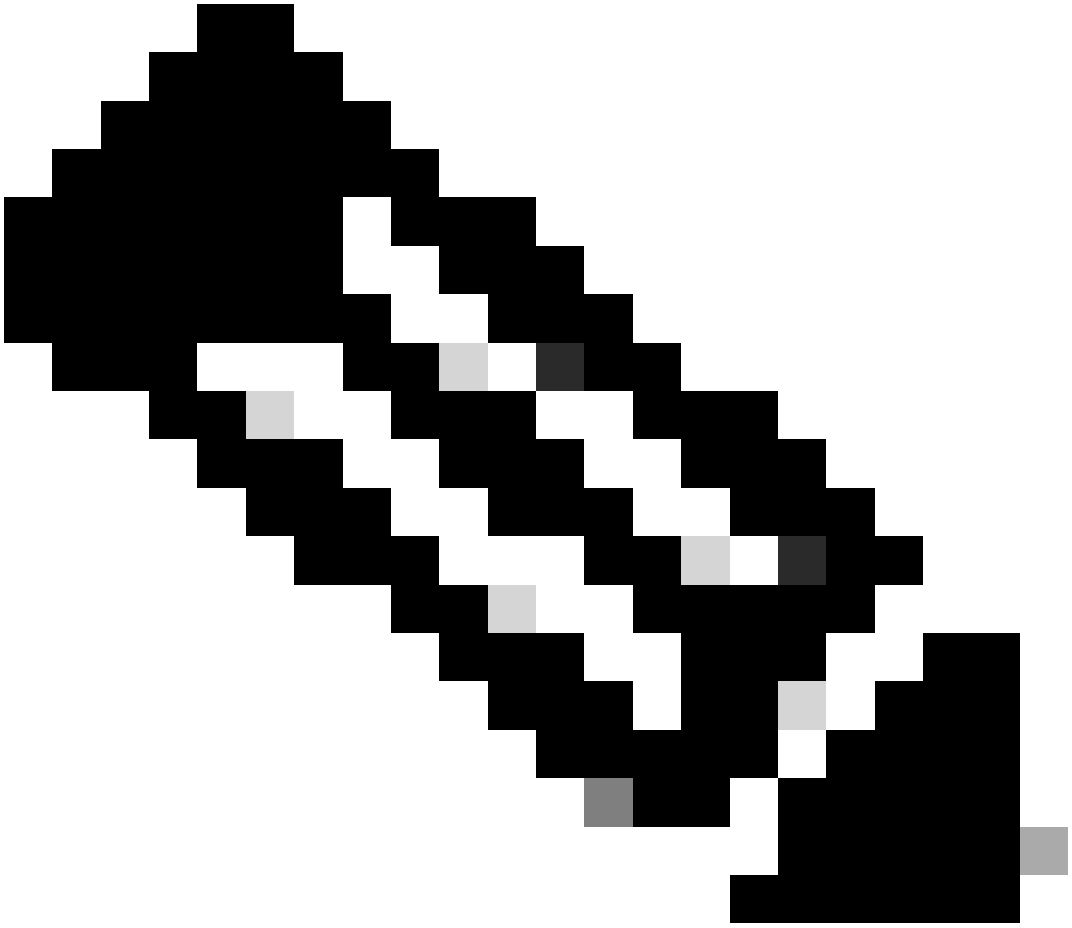
a. ID entité

b. Signer le certificat

c. Certificat de cryptage

d. URL de déconnexion

e. Se connecter UR



Remarque : Les certificats doivent être au format x.509 et les enregistrer avec l'extension .CRT.

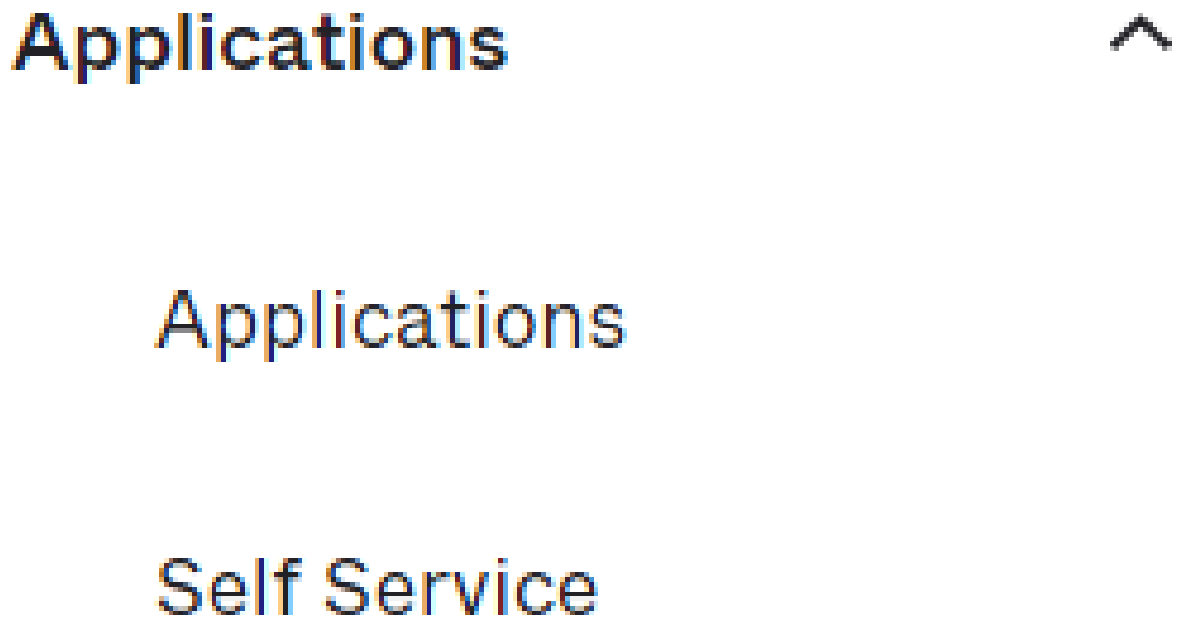
```
-----BEGIN CERTIFICATE-----
MIIDfTCCAmWgAwIBAgIhAM8T9QVLqX/lp1oK/q2XNUbJcGhRmGvqdXxGTUkrKUBhMA0GCSqGSIb3
DQEBCwUAMHIxDDAKBgNVBAYTA1VTQTELMAkGA1UECBMCQ0ExETAPBgNVBAcTCFNhbiBKb3NlMRQw
EgYDVQQKEwtDSVNDT1JUUExBQjEUMBIGA1UECxMLQ01lTQ09SVFBMQUIxFjAUBgNVBAMTDURlZmF1
bHRUZW5hbnQwHhcNMjAwNTI4MTQxMzQzWhcNMjUwNTI4MTQxMzQzWjByMQwwCgYDVQQGEwNVU0Ex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

Certificat X.509

Configuration OKTA

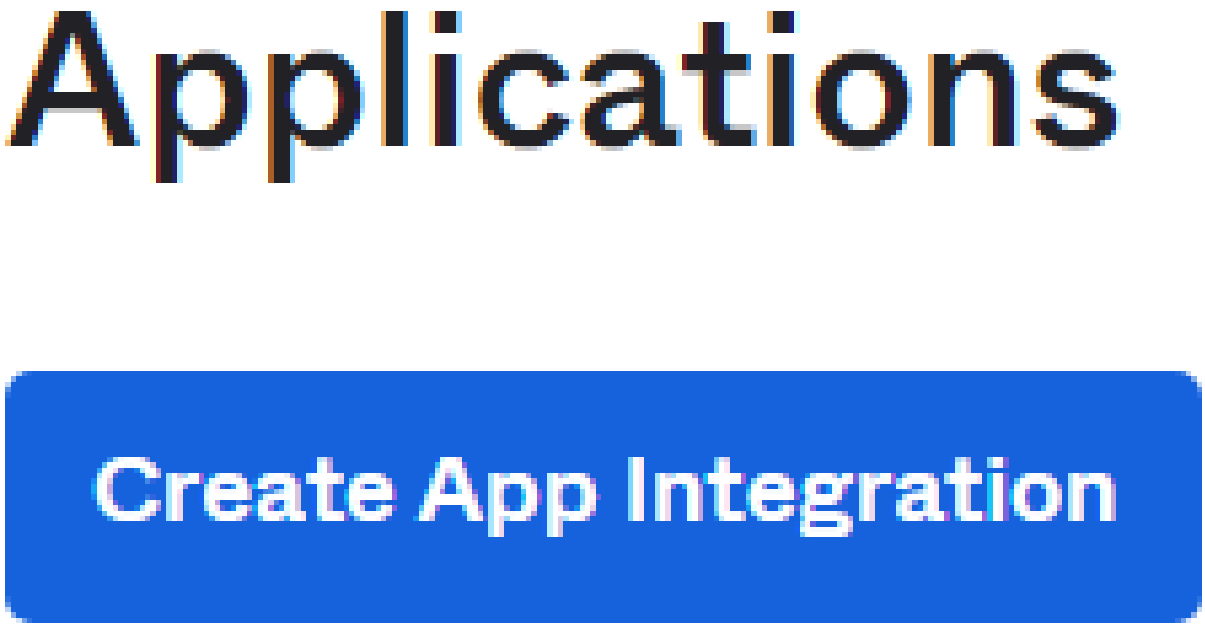
1. Connectez-vous au compte OKTA.

2. Accédez à Applications > Applications.



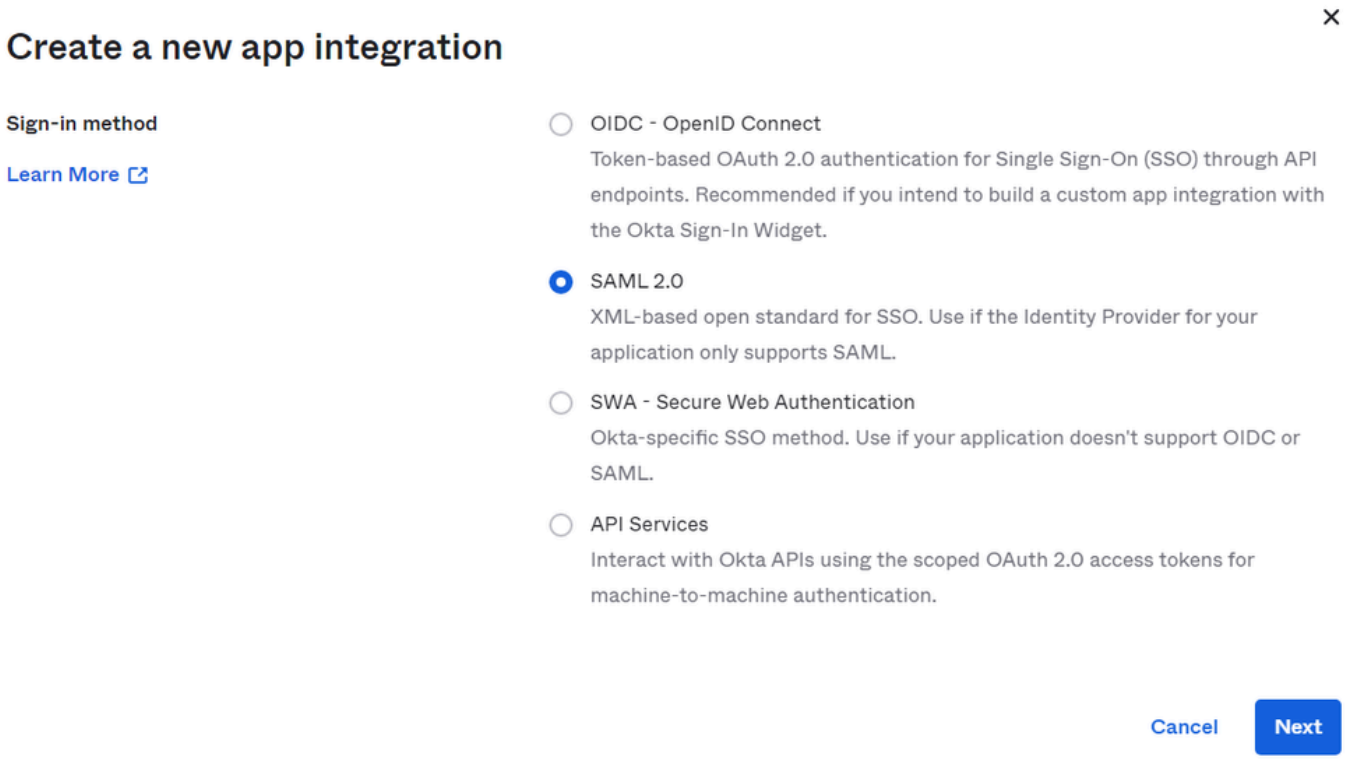
Applications > Applications

3. Cliquez sur Créer une intégration d'application.



Créer une application

4. Cliquez sur SAML 2.0 et sur next.



Configuration de SAML2.0

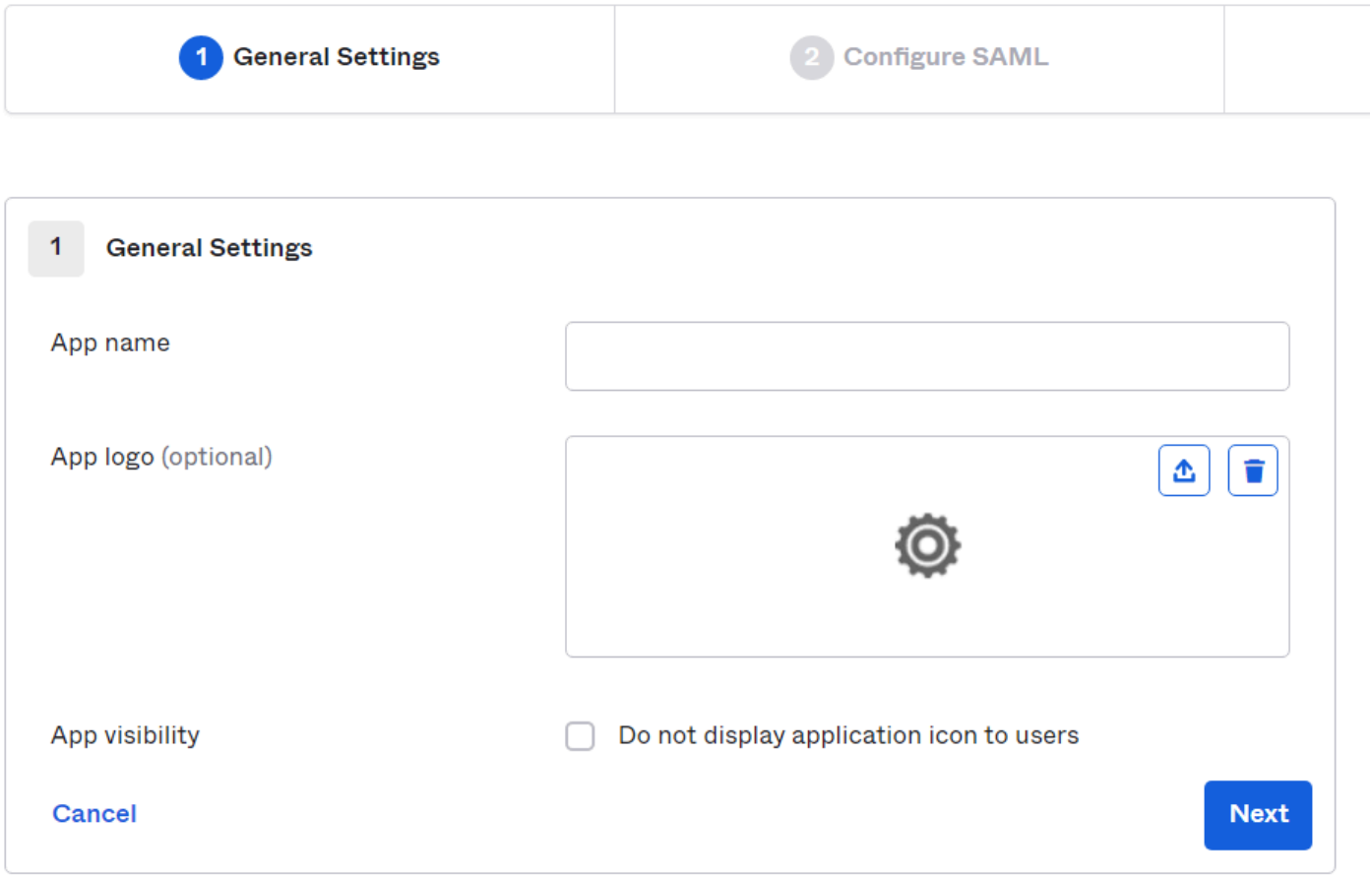
Paramètres généraux

1. Entrez le nom de l'application.

2. Ajoutez un logo pour l'application (facultatif).

3. Visibilité des applications (facultatif).

4. Cliquez sur SUIVANT.



Paramètres généraux SAML

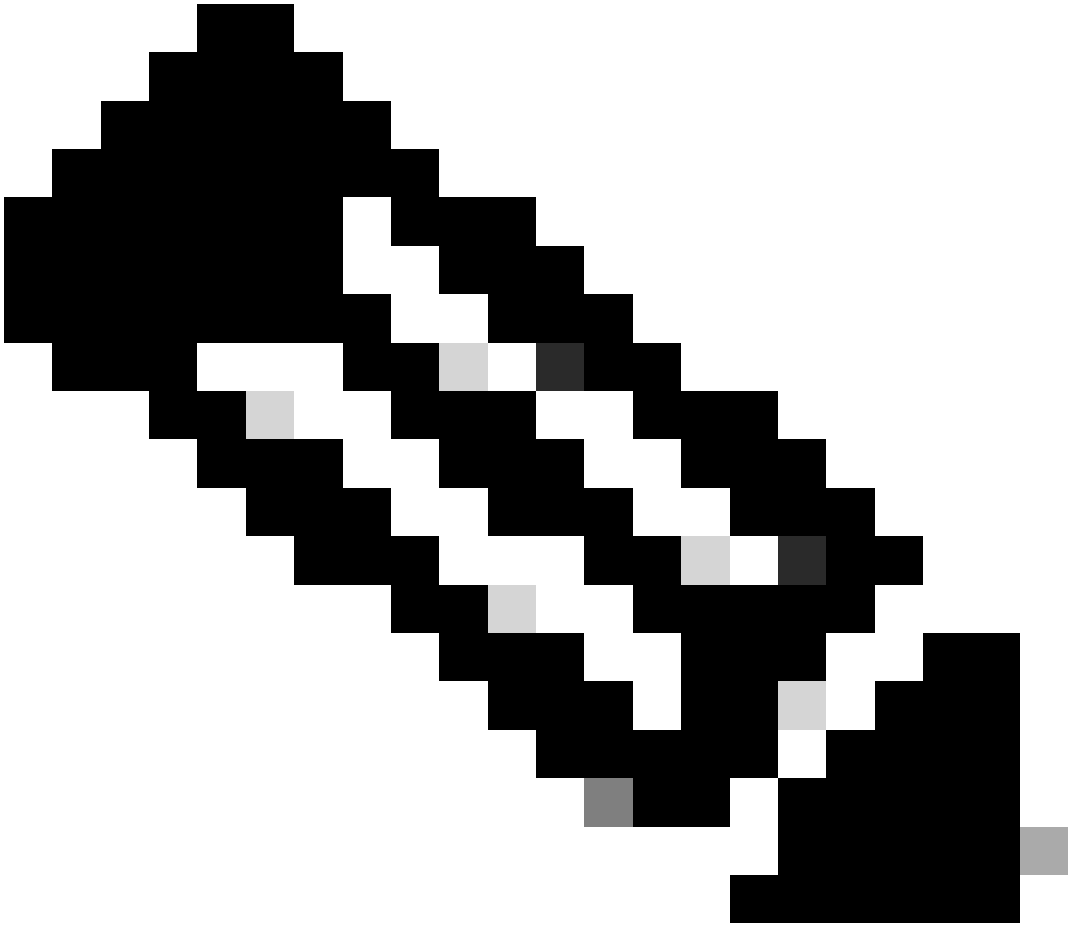
Configurer SAML

Ce tableau décrit les paramètres qui doivent être configurés dans cette section.

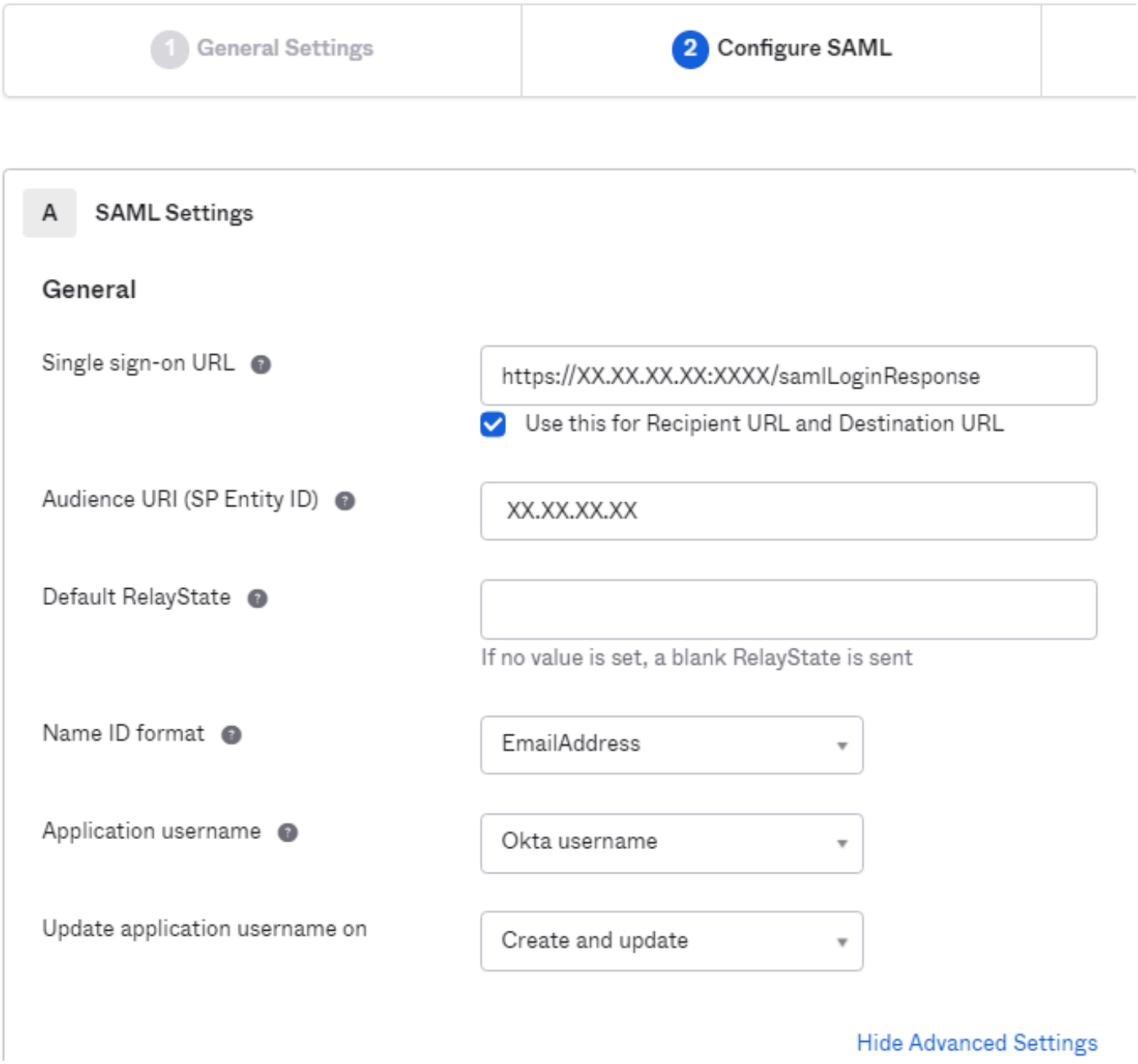
Composante	Valeur	Configuration
URL d'authentification unique	https://XX.XX.XX.XX:XXXX/samlLoginResponse	Tirez-le des métadonnées.
URI du public (ID d'entité SP)	XX.XX.XX.XX	Adresse IP ou DNS pour Cisco vManage

Composante	Valeur	Configuration
ÉtatRelais par défaut		VIDE
Format ID nom		Selon vos préférences
Nom d'utilisateur		Selon vos préférences
Mettre à jour le nom d'utilisateur	Créer et mettre à jour	Créer et mettre à jour
Réponse	Signé	Signé
Signature d'assertion	Signé	Signé
Algorithme de signature	RSA-SHA256	RSA-SHA256
Algorithme Digest	SHA256	SHA256
Chiffrement d'assertion	Chiffré	Chiffré
Algorithme de chiffrement	AES256-CBC	AES256-CBC
Algorithme de transport de clé	RSA-OAEP	RSA-OAEP
Certificat de chiffrement		Le certificat de chiffrement des métadonnées doit être au format x.509.
Activer la déconnexion unique		doit être vérifiée.

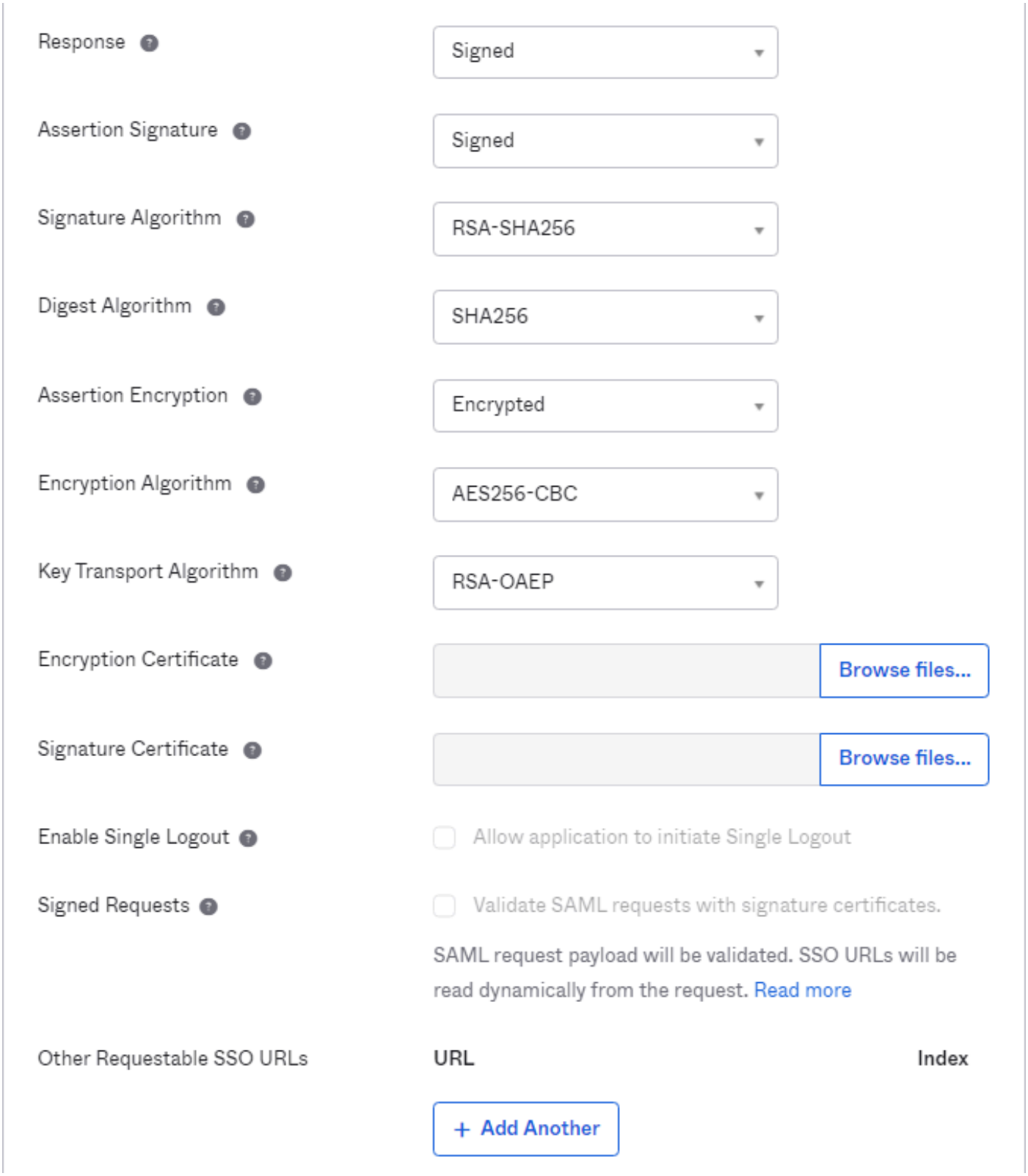
Composante	Valeur	Configuration
URL de déconnexion unique	https://XX.XX.XX.XX:XXXX/samlLogoutResponse	Obtenez des métadonnées.
Émetteur SP	XX.XX.XX.XX	Adresse IP ou DNS pour vManage
Certificat de signature		Le certificat de chiffrement des métadonnées doit être au format x.509.
Crochet En Ligne D'Assertion	Aucun(désactivé)	Aucun(désactivé)
Classe de contexte d'authentification	Certificat X.509	
Authentification Honor Force	Oui	Oui
Chaîne ID émetteur SAML	Chaîne ID émetteur SAML	Tapez un texte de chaîne
Instructions d'attributs (facultatif)	Nom ► Nom d'utilisateur Format du nom (facultatif) ► Non spécifié Valeur ►user.login	Nom ► Nom d'utilisateur Format du nom (facultatif) ► Non spécifié Valeur ►user.login
Instructions d'attribut de groupe (facultatif)	Nom ► Groupes Format du nom (facultatif) ► Non spécifié Filtre ►Correspond à regex ►.*	Nom ► Groupes Format du nom (facultatif) ►Non spécifié Filtre ►Correspond à regex ►.*



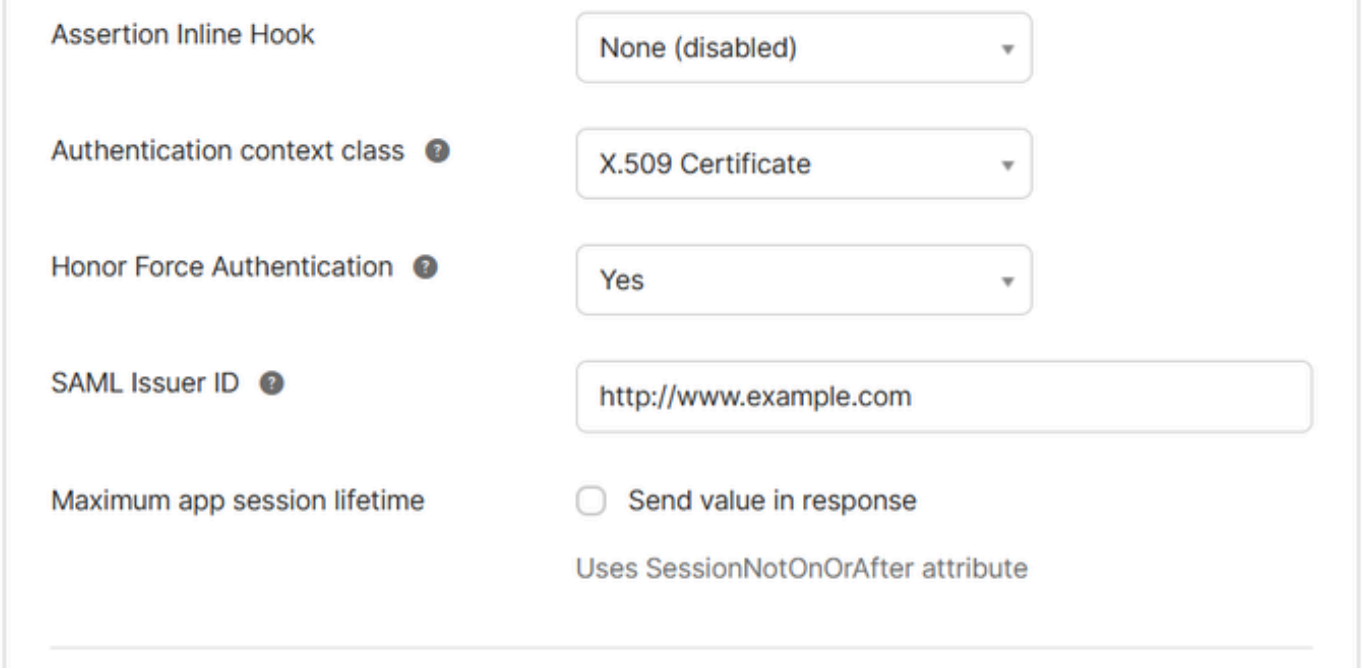
Remarque : Vous devez utiliser Username et Groups, exactement comme indiqué dans la table CONFIGURE SAML.

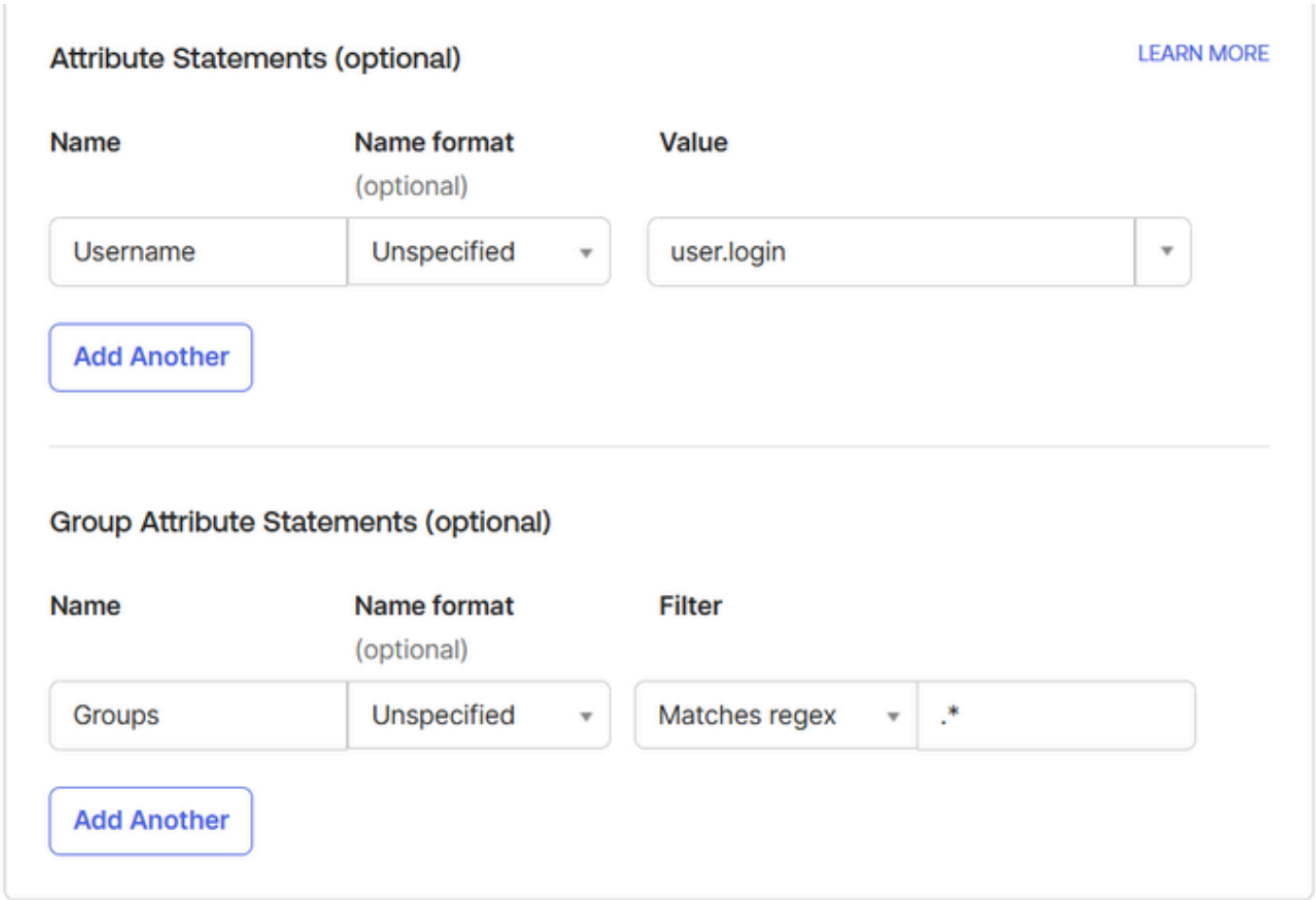


Configuration de SAML - Partie 1



Configuration de SAML - Partie 2



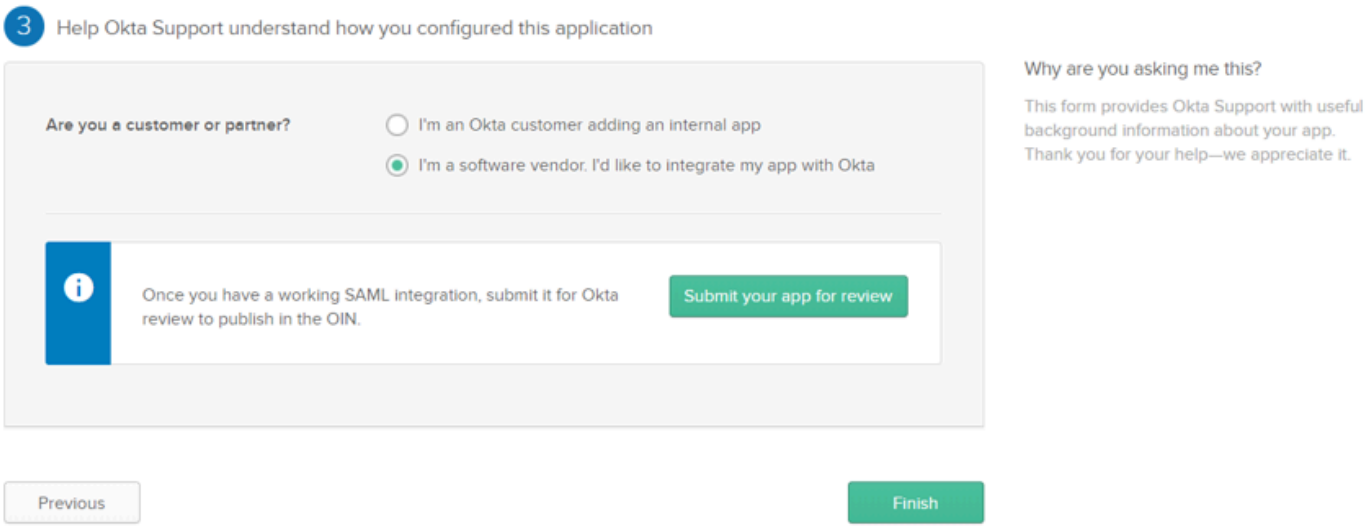


- Cliquez sur Next (Suivant).

Commentaires

1. Sélectionnez l'une des options de votre choix.

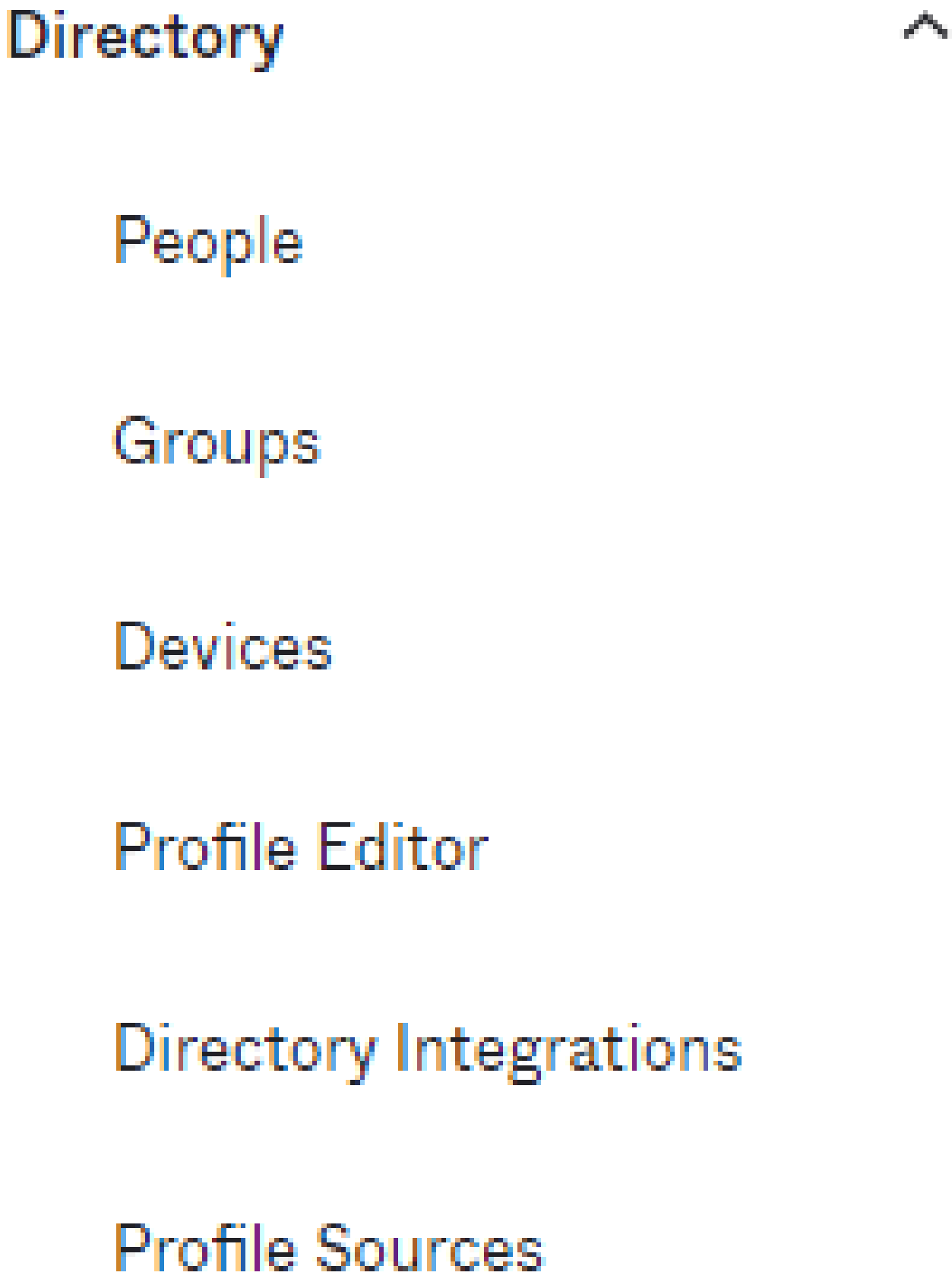
2. Cliquez sur Terminer.



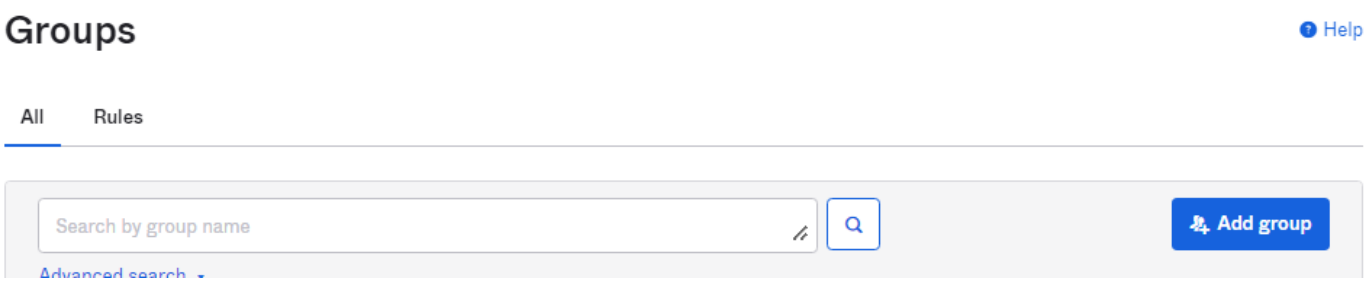
PETIT feedback

Configurer des groupes dans OKTA

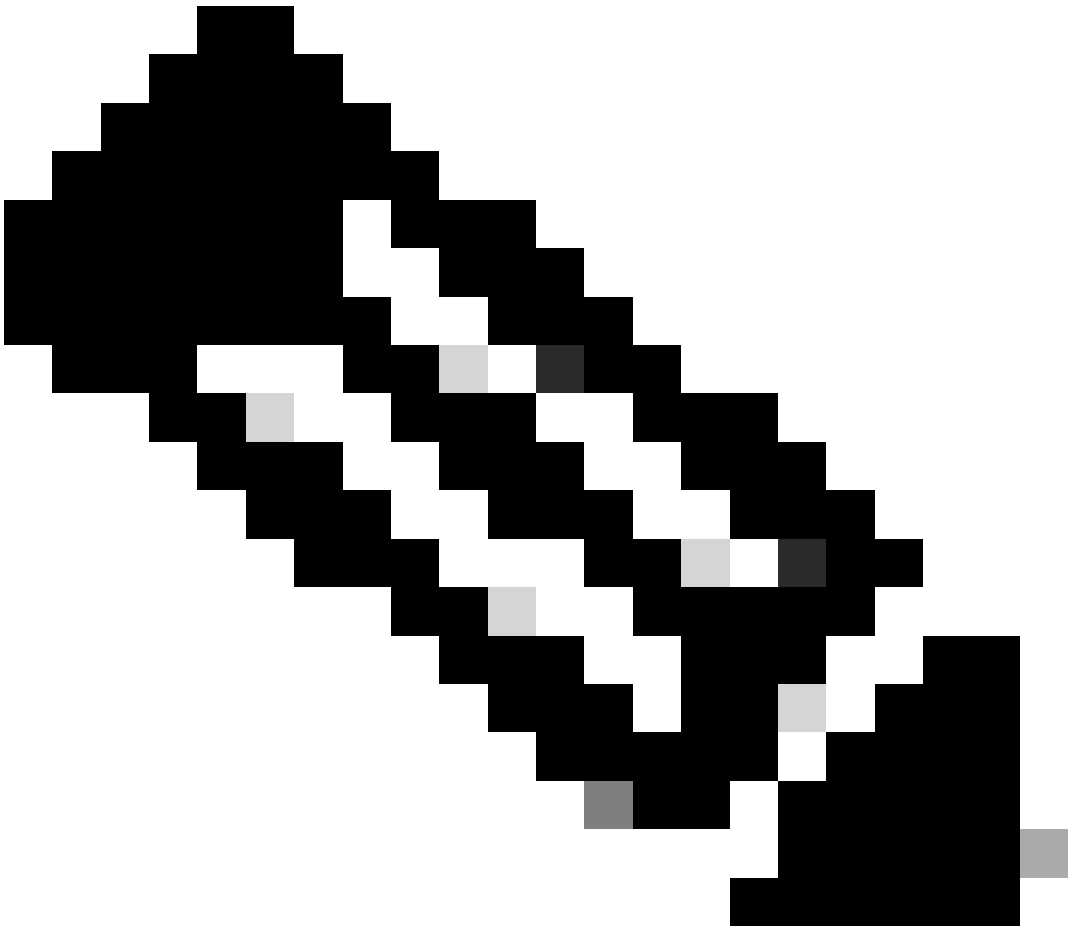
1. Accédez à Répertoire > Groupes.


Directory
People
Groups
Devices
Profile Editor
Directory Integrations
Profile Sources

2. Cliquez sur Ajouter un groupe et créez un nouveau groupe.



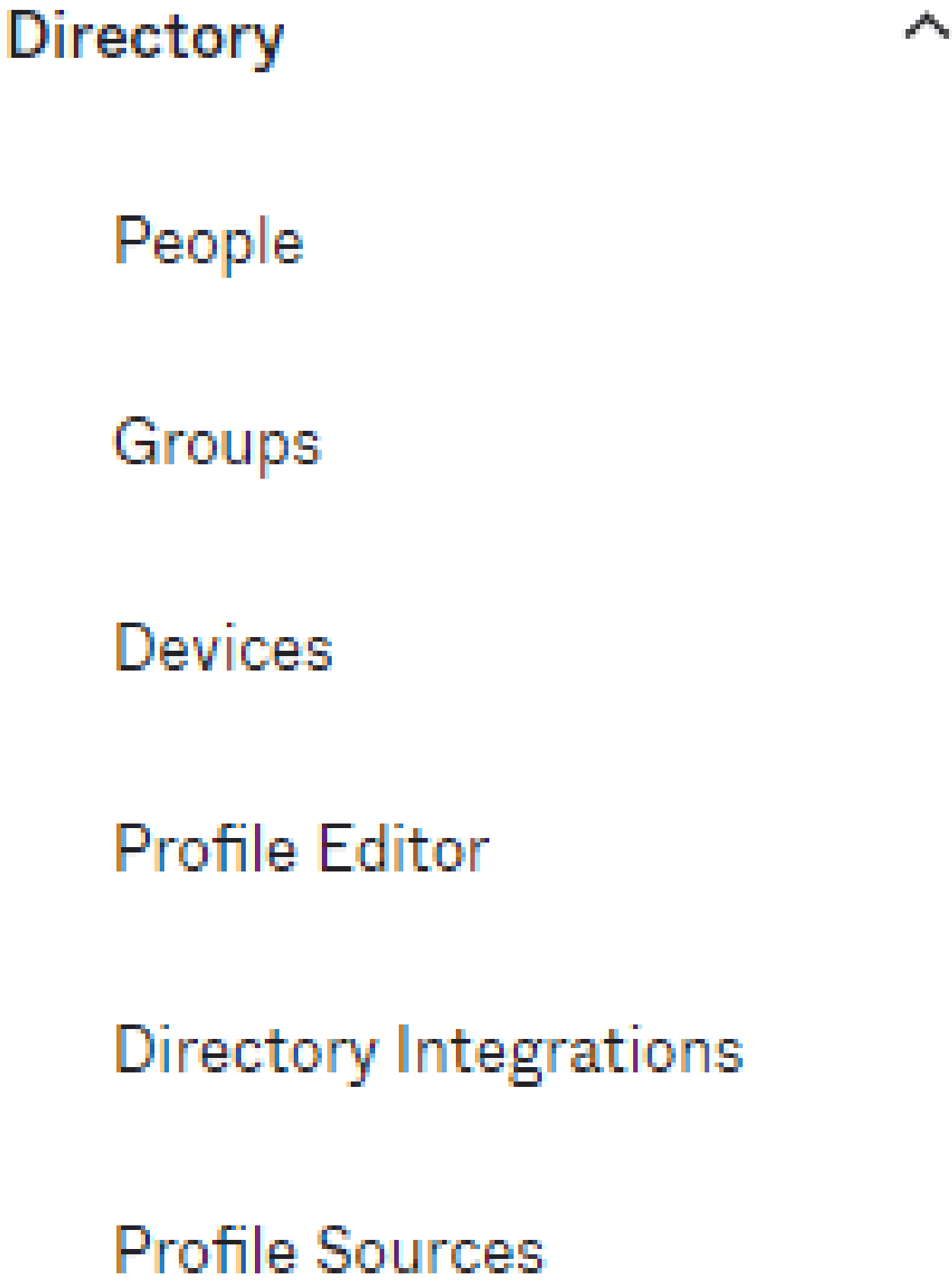
Ajouter un groupe



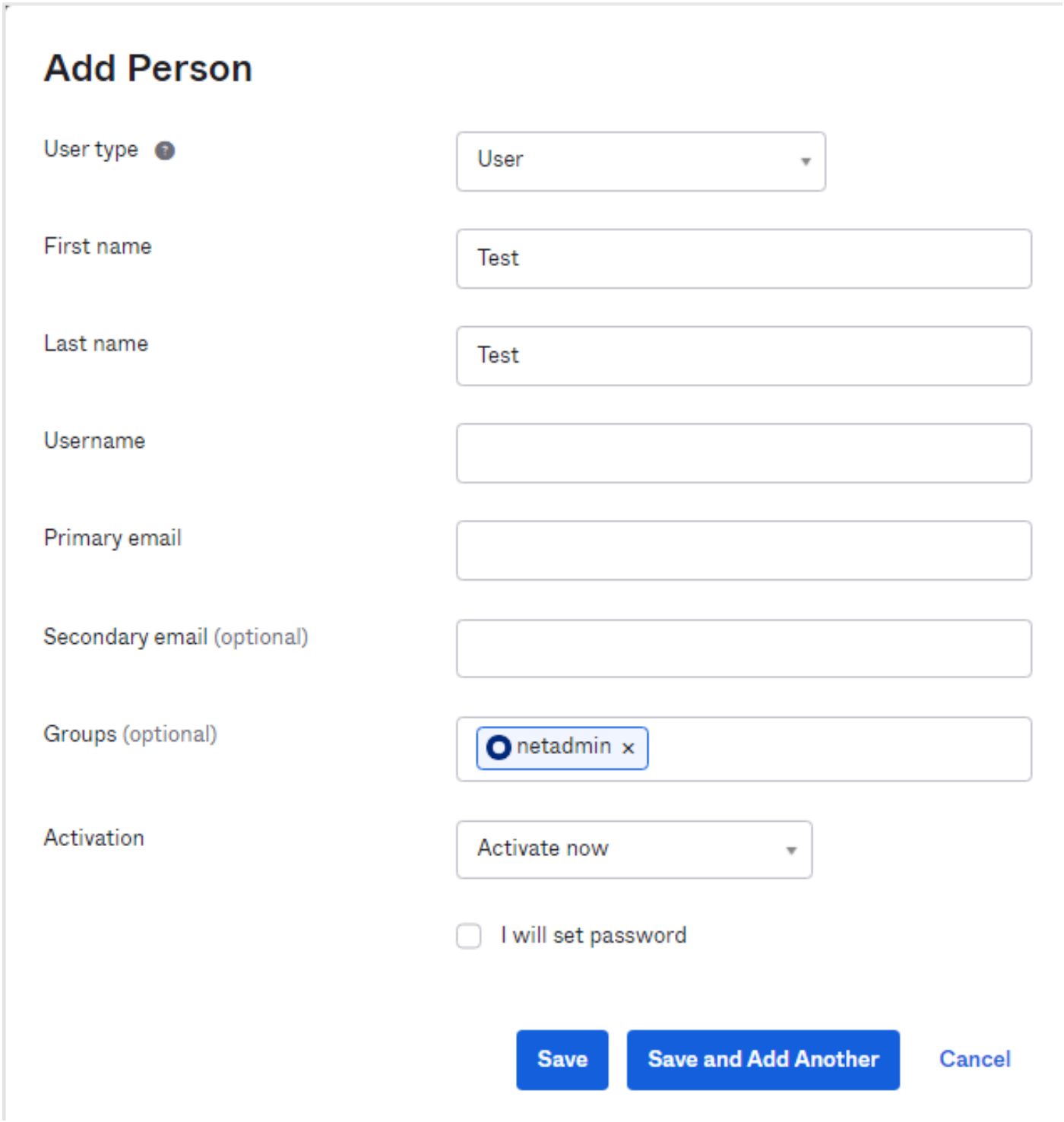
Remarque : Les groupes doivent correspondre aux groupes Cisco vManage et ils doivent être en minuscules.

Configurer des utilisateurs dans OKTA

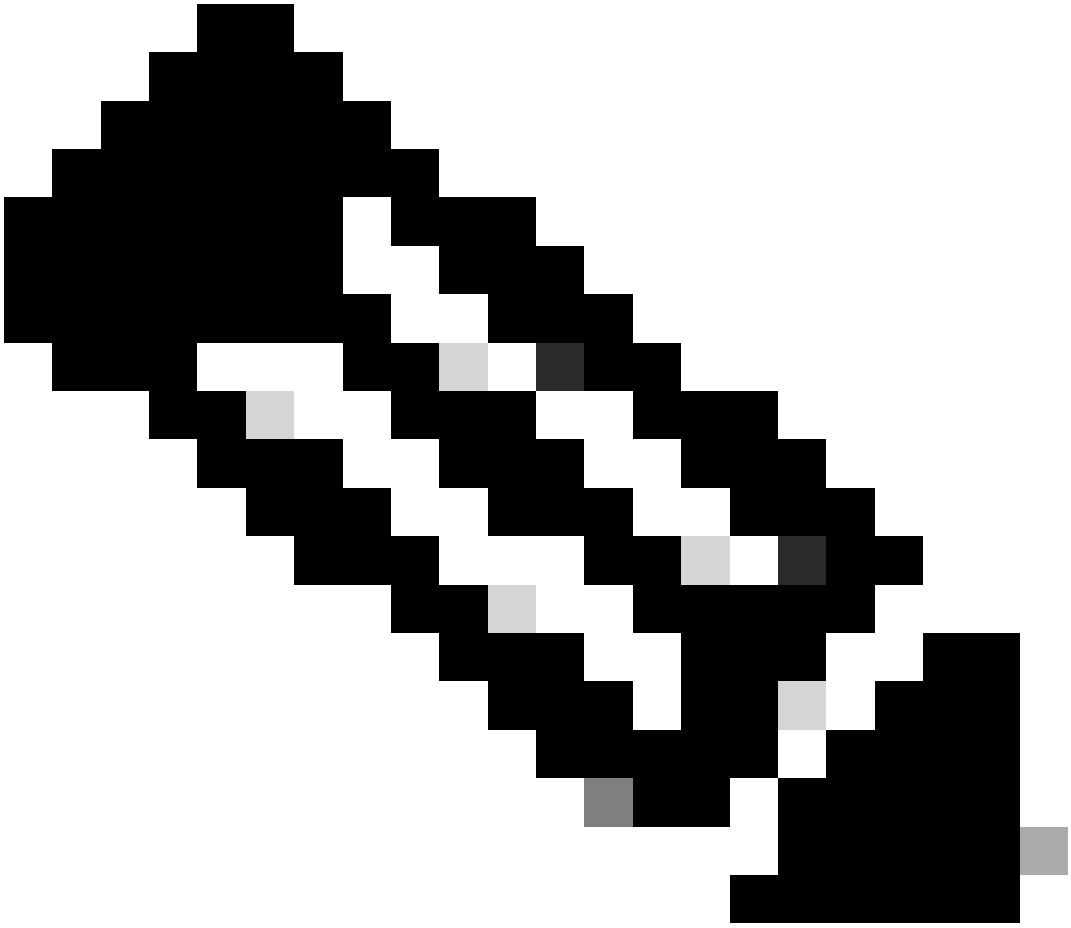
1. Accédez à Répertoire > Personnes.


Directory
People
Groups
Devices
Profile Editor
Directory Integrations
Profile Sources

2. Cliquez sur Ajouter une personne, créez un nouvel utilisateur, affectez-le au groupe et enregistrez-le.



Ajouter un utilisateur

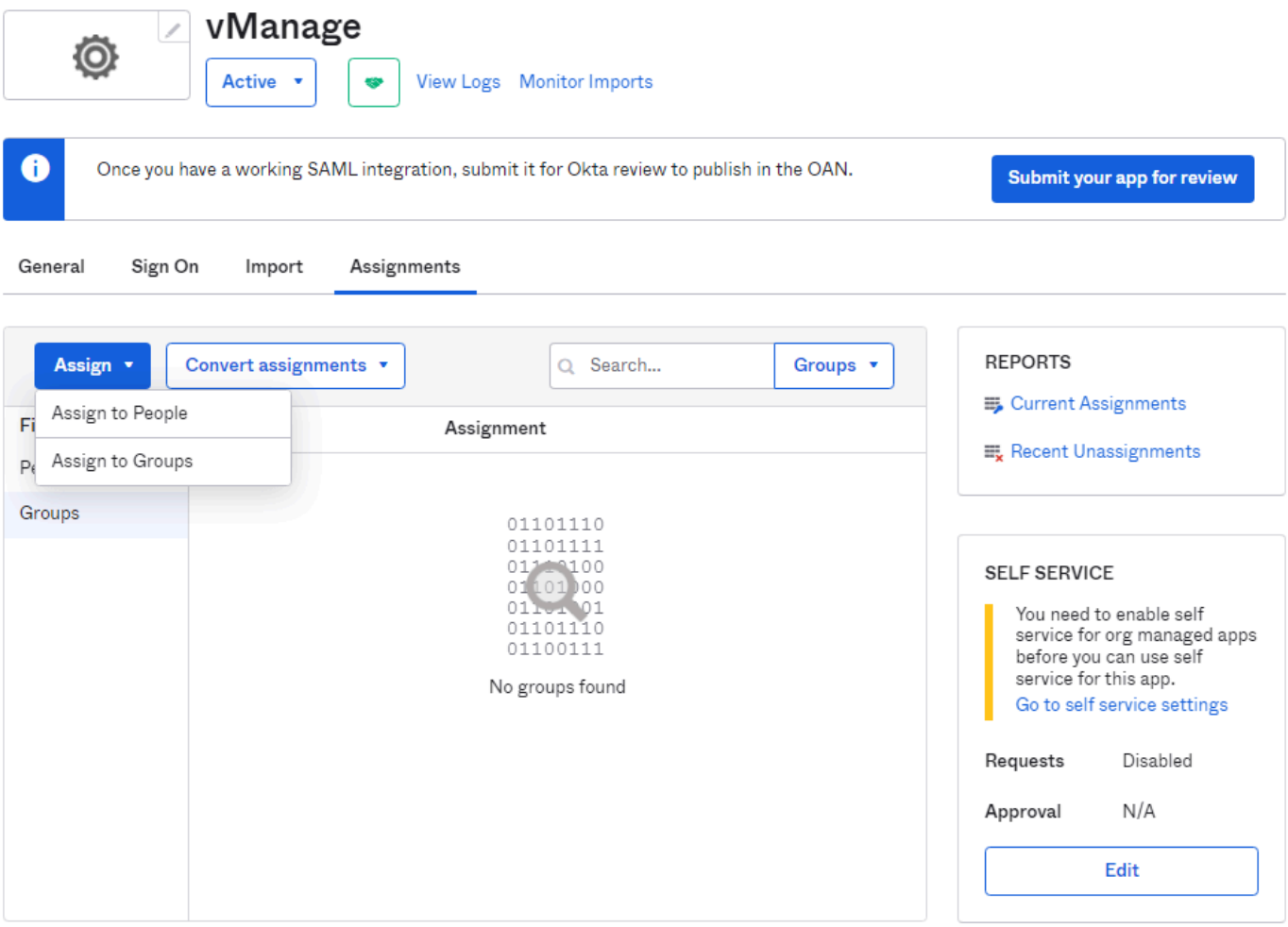


Remarque : Active Directory peut être utilisé à la place des utilisateurs OKTA.

Affecter des groupes et des utilisateurs dans l'application

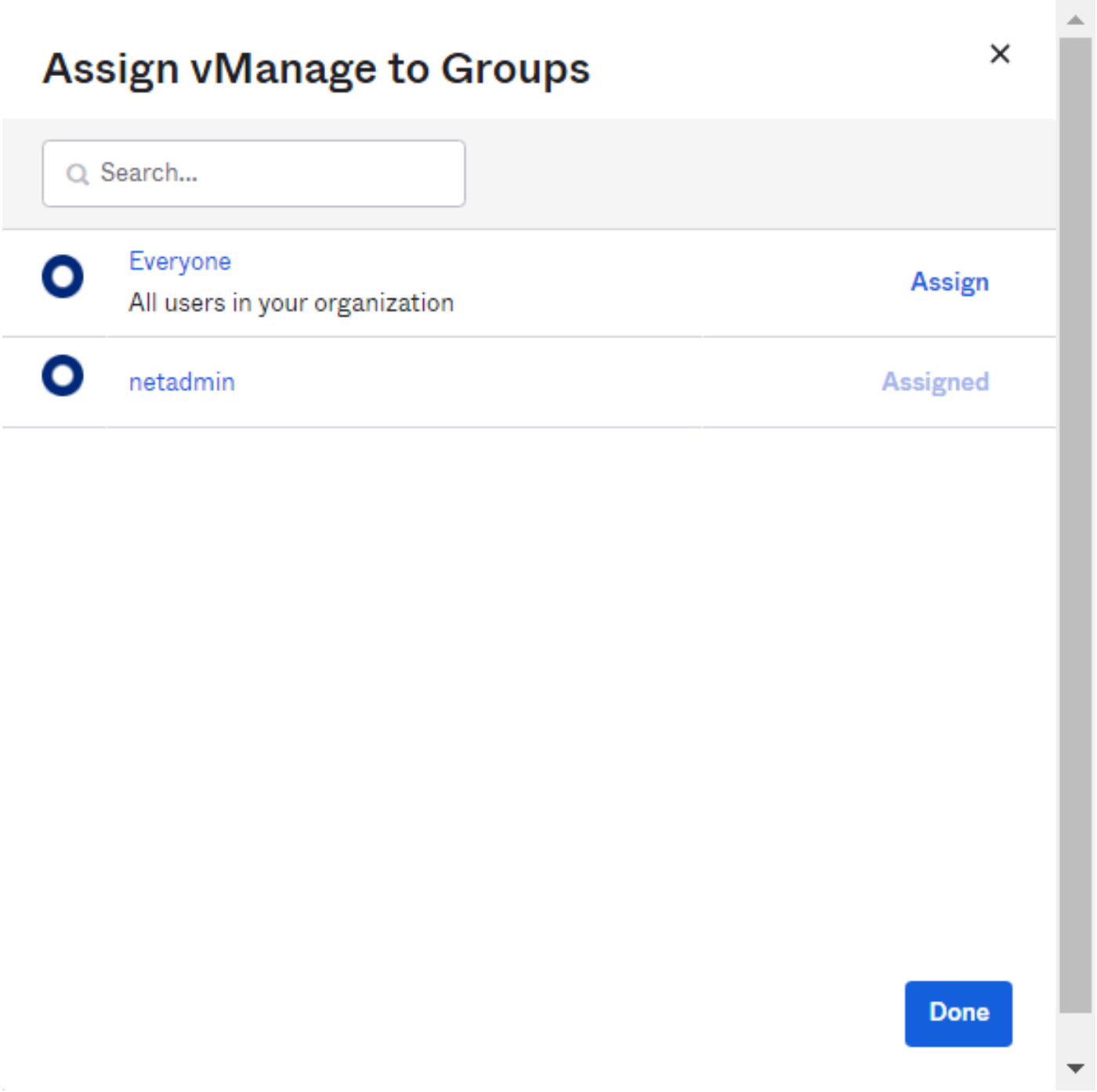
1. Accédez à Applications > Applications > Sélectionnez la nouvelle application.

2. Cliquez sur Assign > Assign to Groups.



Application > Groupes

3. Identifiez le groupe et cliquez sur Affecter > Terminé.

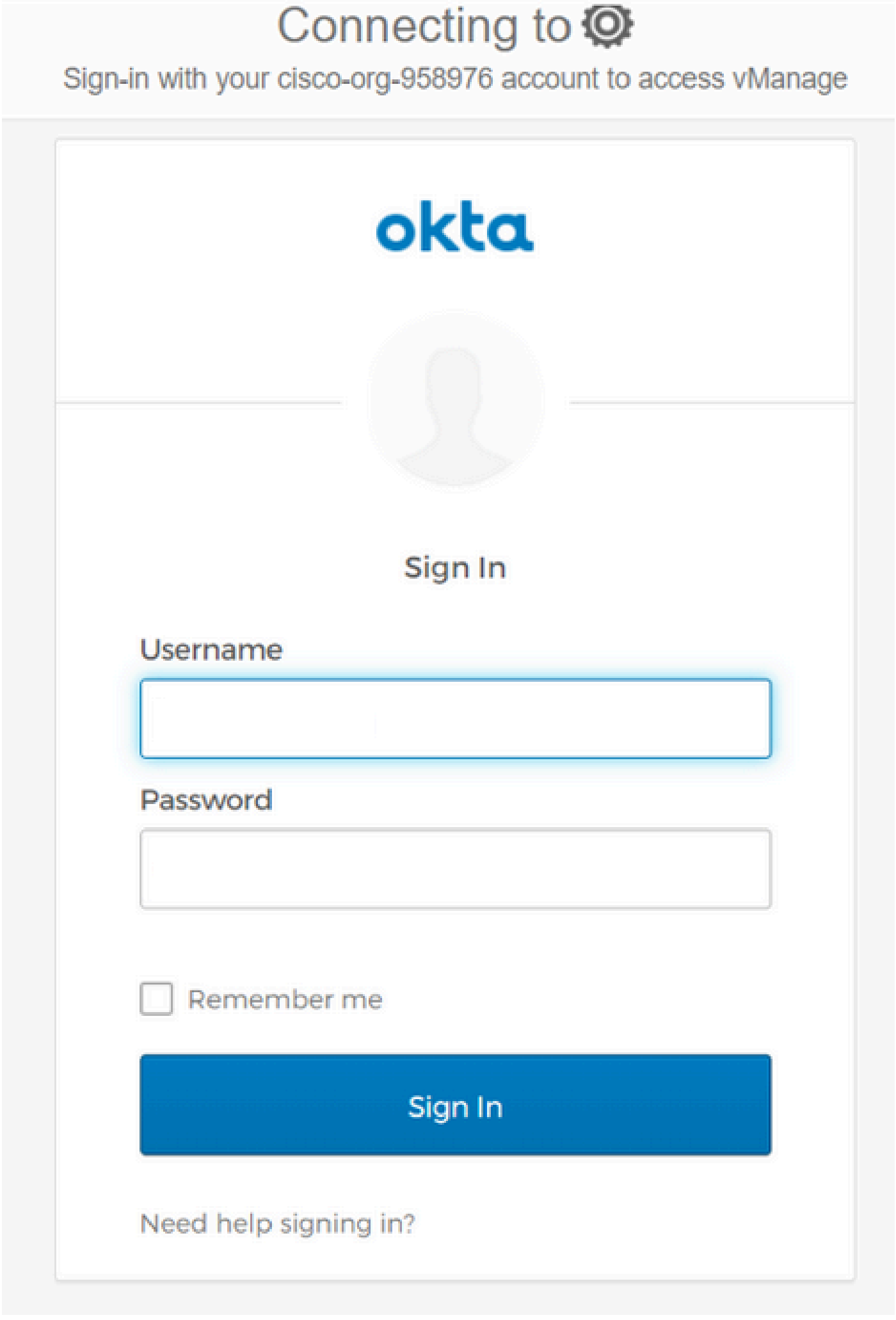


Affecter un groupe et un utilisateur

4. Le groupe et les utilisateurs doivent maintenant être affectés à l'application.

Vérifier

Une fois la configuration terminée, vous pouvez accéder à Cisco vManage via OKTA.



SSO Login Vmanage

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.