

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

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Fond](#)

[Configurer](#)

[Configuration vManage](#)

[Configuration OKTA](#)

[Paramètres généraux](#)

[Configurer SAML](#)

[Commentaires](#)

[Configurer des groupes dans OKTA](#)

[Configurer des utilisateurs dans OKTA](#)

[Affecter des groupes et des utilisateurs dans l'application](#)

[Vérifier](#)

[Dépannage](#)

[Informations connexes](#)

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

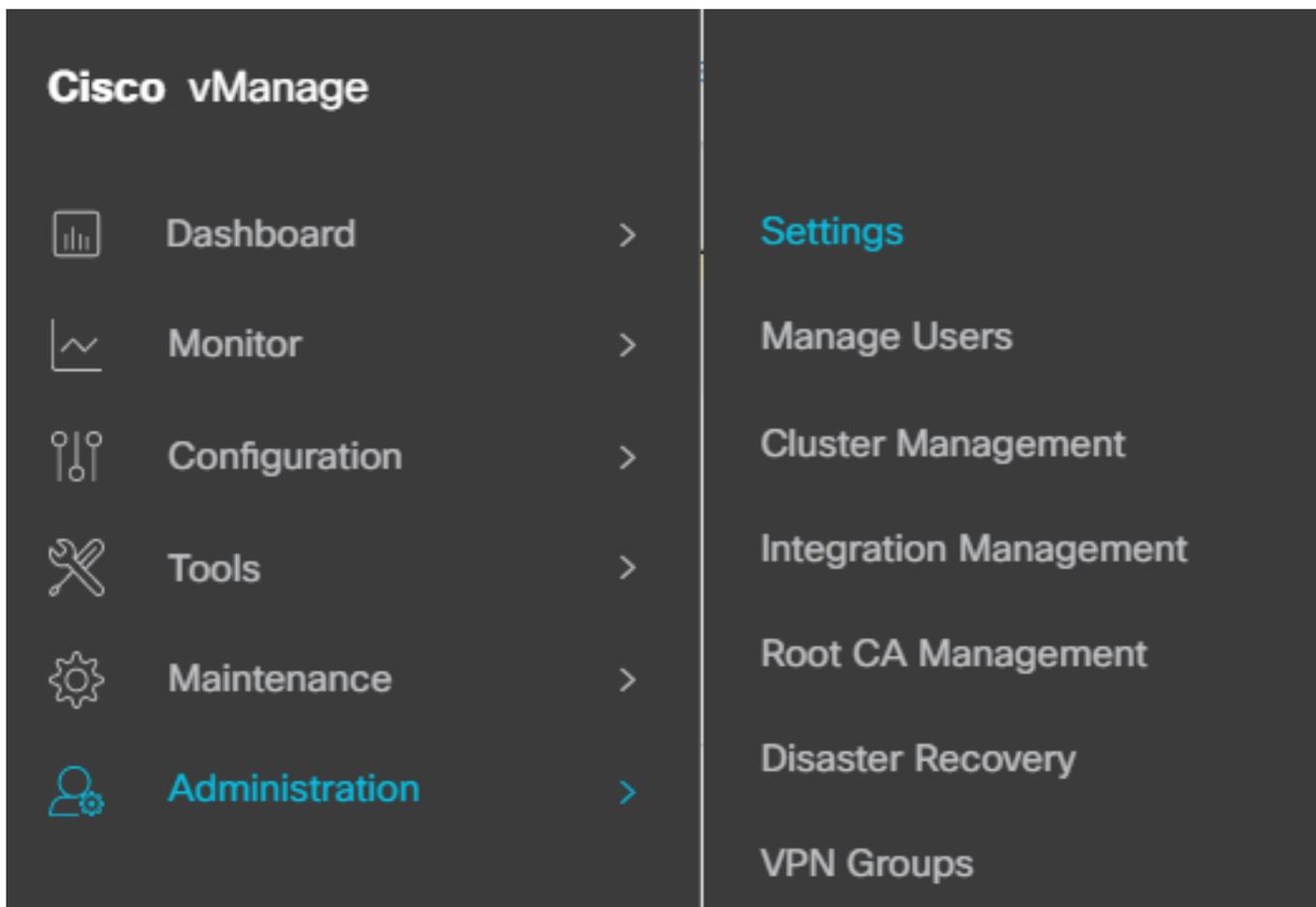
Le langage SAML (Security Assertion Markup Language) est une norme ouverte pour l'échange de données d'authentification et d'autorisation entre les parties, en particulier entre un fournisseur d'identité et un fournisseur de services. Comme son nom l'indique, SAML est un langage de balisage XML pour 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.

Administration Settings

Identity Provider Settings

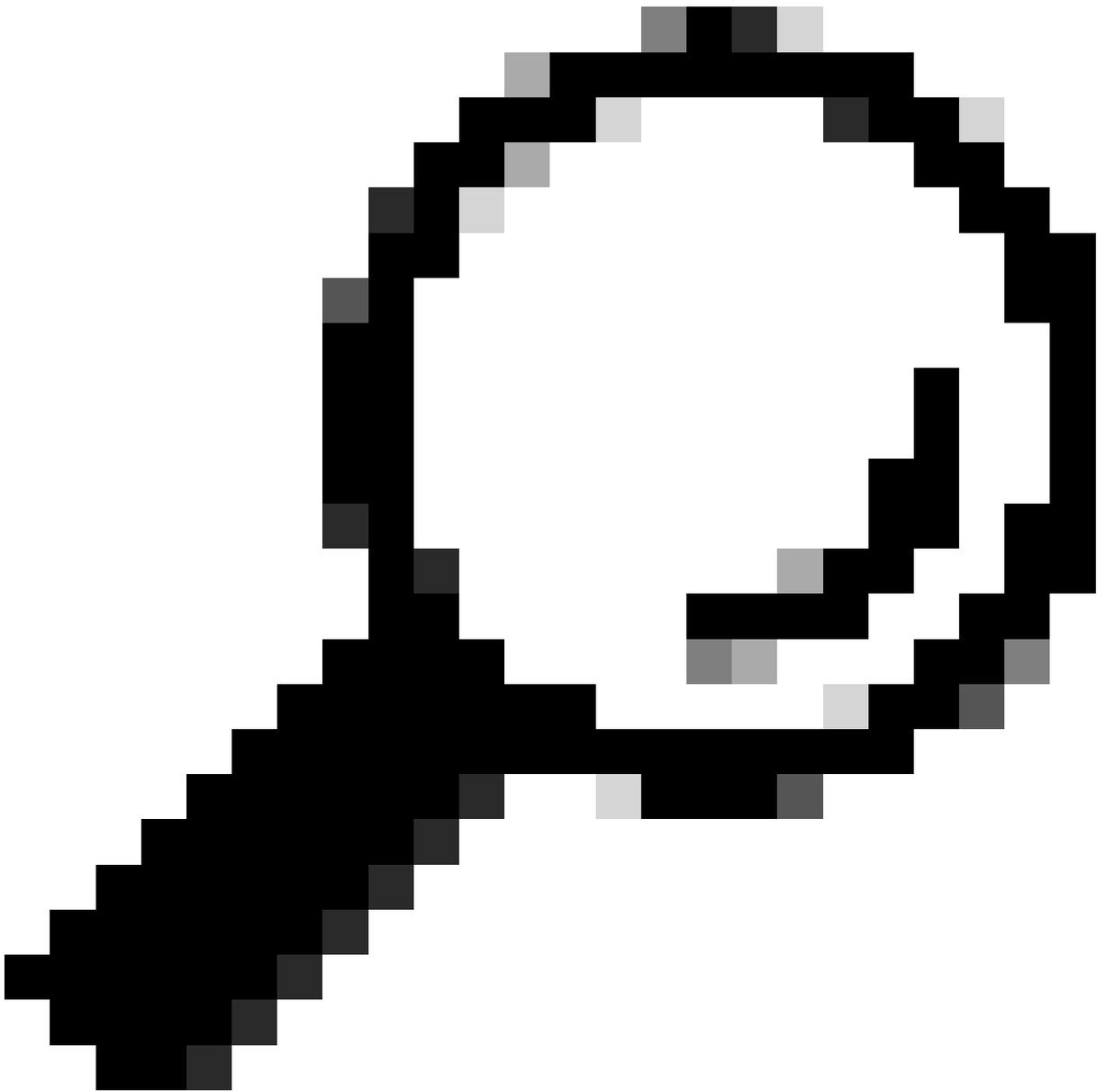
Disabled

Enable Identity Provider: Enabled Disabled

Upload Identity Provider Metadata

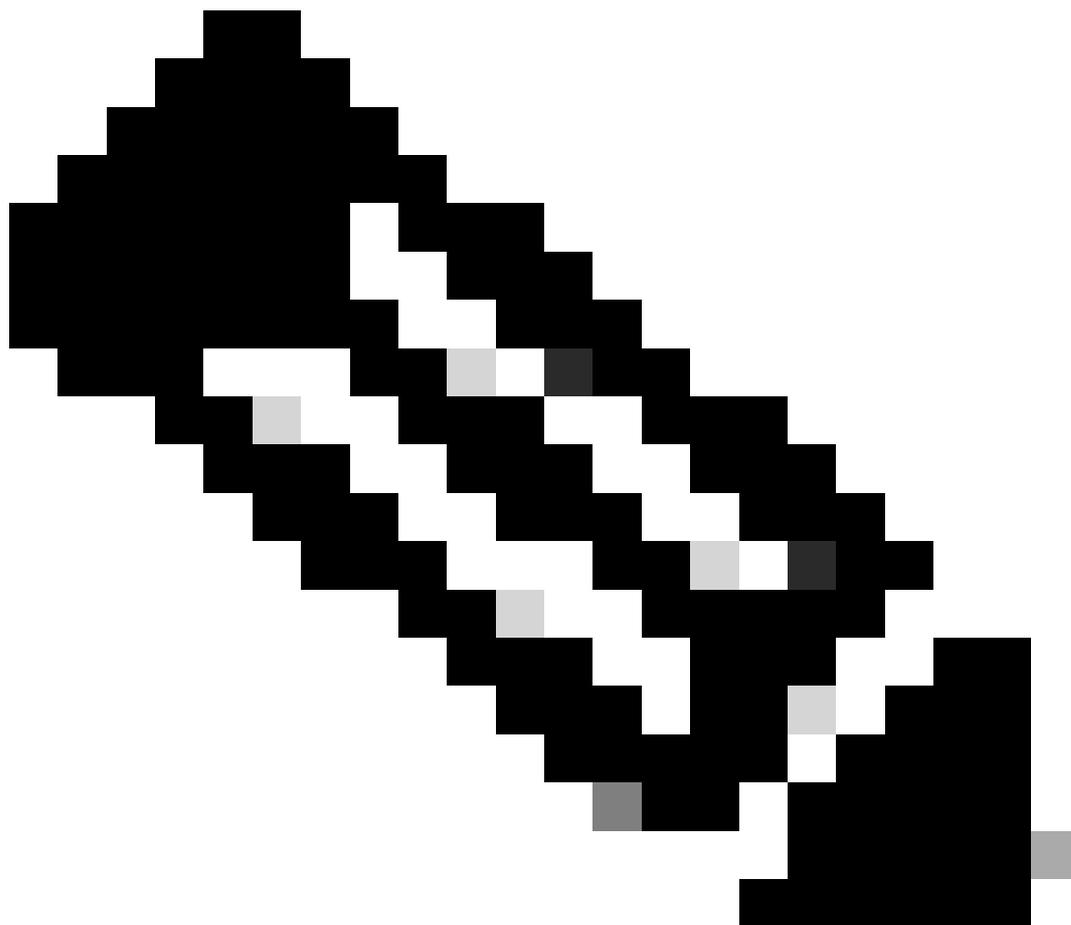
[↓ Click here to download SAML metadata](#)

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
DQEBCwUAMHlxDDAKBgNVBAYTA1VTQTELMakGA1UECBMCQ0ExETAPBgNVBACTCFNhbiBkb3NlMRQw
EgYDVQQKEwtDSVNDT1JUUExBQjEUMBIGA1UECXMlQ01TQ09SVFBMQUIxIjAUBgNVBAMTDURlZmF1
bHRUZW5hbnQwHhcNMjAwNTI4MTQxMzQzWWhcNMjUwNTI4MTQxMzQzWjByMQwwCgYDVQQGEwNVU0Ex
CzAJBgNVBAGTAkNBMRwDwYDVQQHEWhTYW4gSm9zZTEUMBIGA1UEChMLQ01TQ09SVFBMQUIxIjFAS
BgNVBAsTC0NlU0NPUlRQTEFCMRYwFAyDVQQDEw1EZWZhdWx0VGVuYW50MIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAg9HOIwjWHD3pbkCB3wRUsn01PTsNAhCqRKof5aY4QDWbu7U3+6gF
TzZgrB9189rLSkbb7cEzRcE7ZbZ1a3zICVw76ZN8jj2BZMYpuTlS9LSGRq2FClYMAg6JU4Yc9prg
T6IcmJKHPfuFM3izXKVsrzfn8tDZ7UDHGIUNPs2kntamU4ZB7BRTE1zJXp+Zh3CvnfLE9g3aXK9
SM9qRFDjAaC8GhWphOYyK3RisQZ/bIZJ2vWkVo91p+6/kQy7/oxFKznK/2oAXaAe26P8HYw+XC0b
mkCwb3e9a1vCGrCmPJwJPjn9j09dX426/LbjdmDAo6HudjTEoQMZduD3Z9GU5QIDAQABMA0GCSqG
SIb3DQEBCwUAA4IBAQBbO/FdHT365rzOHpgHo8YWbxbYdhjAMrHUBbuXLq6MEaHvm4GoTYsgJzc9
Scy/Iwoa6krjBXHJPPthtBwzYYXvK6CJxh8J/rlednlmai0z9growg/sSEgbXPpuQw6qT9hM8s2i
FHlFchPoqiaZFlDNF4iupuzFPTcD8kmzEC3mGlcxfm2TaVjLFDu7McRAMLZTV+yPY+WZXjuoMI8P
hXapKdUt0B6RrxzucBRac2ZB22g7HWDQuDZUzf966Q2k5Us1QxtNlpXLU5X+i+YDW011T2AP6+UUi
vrN1A6vFVPP3QtAd7ao7VziMeEvxfYTuK690b+ej4MntWIKdHneU+/YC
-----END CERTIFICATE-----
```

Certificat X.509

Configuration OKTA

1. Connectez-vous au compte [OKTA](#).
2. Accédez à Applications > Applications.

Applications



Applications

Self Service

Applications > Applications

3. Cliquez sur Créer une intégration d'application.

Applications

Create App Integration

Créer une application

4. Cliquez sur SAML 2.0 et sur next.

Create a new app integration ✕

Sign-in method

[Learn More](#) 

- OIDC - OpenID Connect**
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
- SAML 2.0**
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
- SWA - Secure Web Authentication**
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
- API Services**
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Cancel

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.

1 **General Settings**

2 **Configure SAML**

1
General Settings

App name

App logo (optional)

App visibility Do not display application icon to users

Cancel
Next

Paramètres généraux SAML

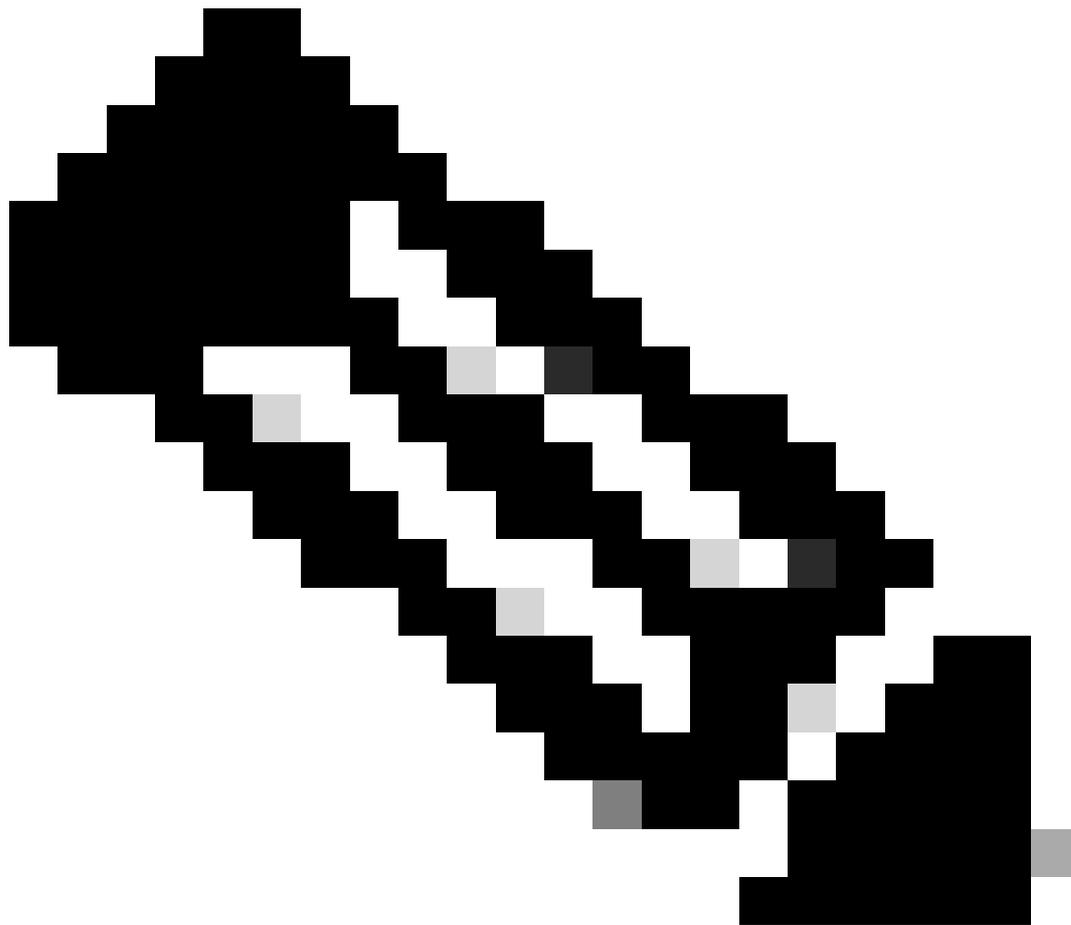
Configurer SAML

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
État Relais 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.

A SAML Settings

General

Single sign-on URL ⓘ

https://XX.XX.XX.XX:XXXX/samlLoginResponse

Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID) ⓘ

XX.XX.XX.XX

Default RelayState ⓘ

If no value is set, a blank RelayState is sent

Name ID format ⓘ

EmailAddress ▼

Application username ⓘ

Okta username ▼

Update application username on

Create and update ▼

[Hide Advanced Settings](#)

Response ⓘ Signed ▼

Assertion Signature ⓘ Signed ▼

Signature Algorithm ⓘ RSA-SHA256 ▼

Digest Algorithm ⓘ SHA256 ▼

Assertion Encryption ⓘ Encrypted ▼

Encryption Algorithm ⓘ AES256-CBC ▼

Key Transport Algorithm ⓘ RSA-OAEP ▼

Encryption Certificate ⓘ [Browse files...](#)

Signature Certificate ⓘ [Browse files...](#)

Enable Single Logout ⓘ Allow application to initiate Single Logout

Signed Requests ⓘ Validate SAML requests with signature certificates.

SAML request payload will be validated. SSO URLs will be read dynamically from the request. [Read more](#)

Other Requestable SSO URLs

URL

Index

[+ Add Another](#)

Assertion Inline Hook	<input type="text" value="None (disabled)"/>
Authentication context class ?	<input type="text" value="X.509 Certificate"/>
Honor Force Authentication ?	<input type="text" value="Yes"/>
SAML Issuer ID ?	<input type="text" value="http://www.example.com"/>
Maximum app session lifetime	<input type="checkbox"/> Send value in response Uses SessionNotOnOrAfter attribute

Attribute Statements (optional) [LEARN MORE](#)

Name	Name format (optional)	Value
<input type="text" value="Username"/>	<input type="text" value="Unspecified"/>	<input type="text" value="user.login"/>

Group Attribute Statements (optional)

Name	Name format (optional)	Filter
<input type="text" value="Groups"/>	<input type="text" value="Unspecified"/>	<input type="text" value="Matches regex"/> <input type="text" value=".*"/>

- Cliquez sur Next (Suivant).

Commentaires

1. Sélectionnez l'une des options de votre choix.
2. Cliquez sur Terminer.

3 Help Okta Support understand how you configured this application

Are you a customer or partner?

I'm an Okta customer adding an internal app

I'm a software vendor. I'd like to integrate my app with Okta

 Once you have a working SAML integration, submit it for Okta review to publish in the OIN. [Submit your app for review](#)

Why are you asking me this?

This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.

[Previous](#)

[Finish](#)

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.

Groups

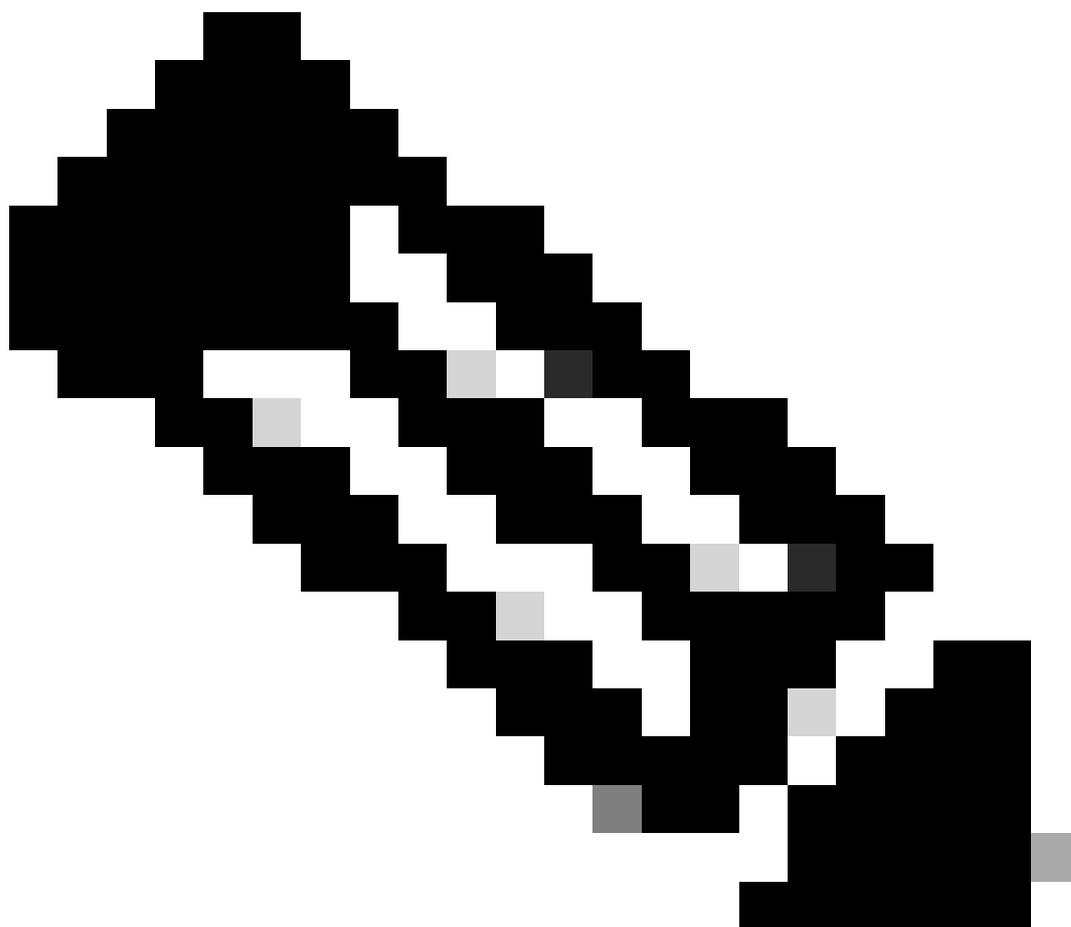
[Help](#)

All Rules

Search by group name

[Advanced search](#)

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.

Add Person

User type 

First name

Last name

Username

Primary email

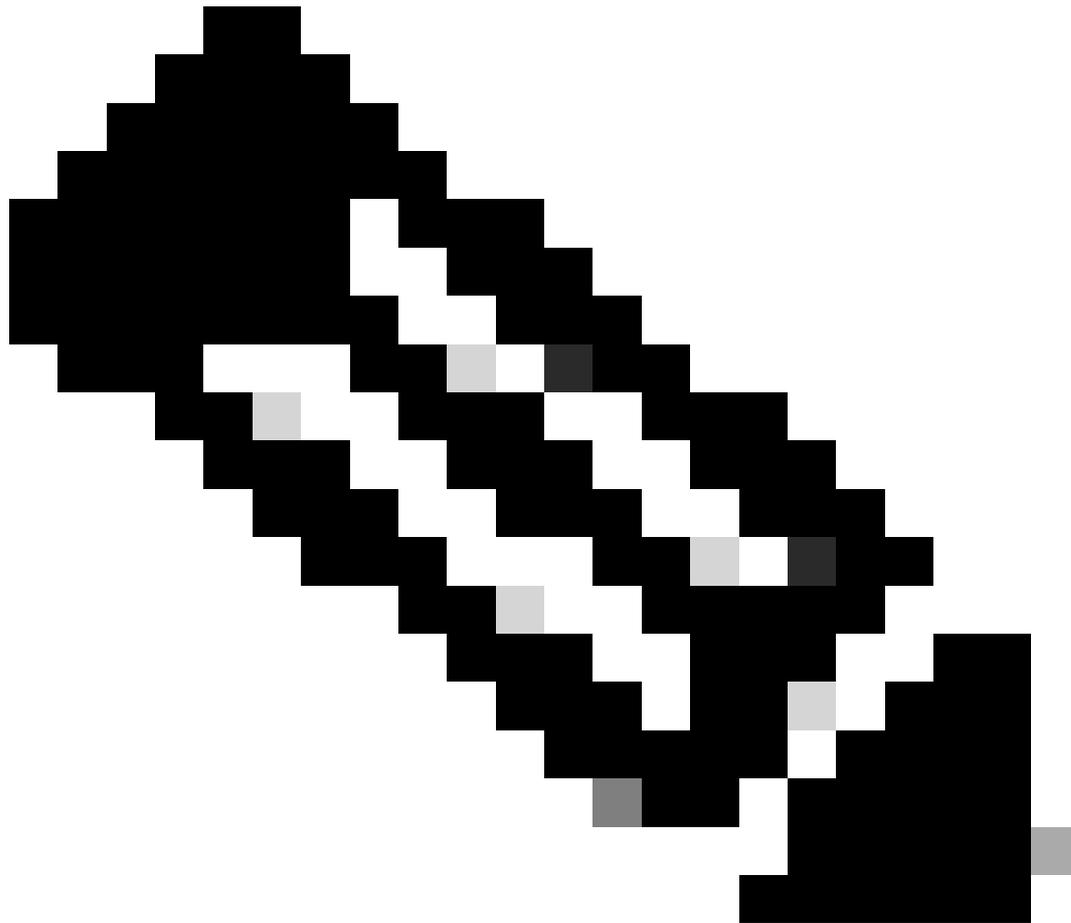
Secondary email (optional)

Groups (optional)

Activation

I will set password

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.



Once you have a working SAML integration, submit it for Okta review to publish in the OAN.

[Submit your app for review](#)

Assign ▾ Convert assignments ▾ Groups ▾

- Assign to People
- Assign to Groups

Groups	Assignment
	01101110
	01101111
	01101100
	01101000
	01101001
	01101110
	01100111
	No groups found

REPORTS

- [Current Assignments](#)
- [Recent Unassignments](#)

SELF SERVICE

You need to enable self service for org managed apps before you can use self service for this app.
[Go to self service settings](#)

Requests Disabled

Approval N/A

[Edit](#)

Application > Groups

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

Assign vManage to Groups



Everyone

All users in your organization

Assign



netadmin

Assigned

Done

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.

Connecting to

Sign-in with your cisco-org-958976 account to access vManage



Sign In

Username

Password

Remember me

Sign In

Need help signing in?

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.