

# Configureer OKTA Single Sign-On (SSO) op SD-WAN

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrond](#)

[Configureren](#)

[vManager-configuratie](#)

[OKTA-configuratie](#)

[Algemene instellingen](#)

[SAML configureren](#)

[Feedback](#)

[Groepen in OKTA configureren](#)

[Gebruikers in OKTA configureren](#)

[Wijs Groepen en Gebruikers in Toepassing toe](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

---

## Inleiding

Dit document beschrijft hoe OKTA Single Sing-On (SSO) kan worden geïntegreerd op een softwaregedefinieerde Wide Area Network (SD-WAN).

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- SD-WAN algemeen overzicht
- Security Assertion Markup Language (SAML)
- Identity Provider (IDP)
- Certificaten

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco vManager release 18.3.x of hoger
- Cisco vManager versie 20.6.3
- Cisco vBond versie 20.6.3
- Cisco vSmart versie 20.6.3

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Achtergrond

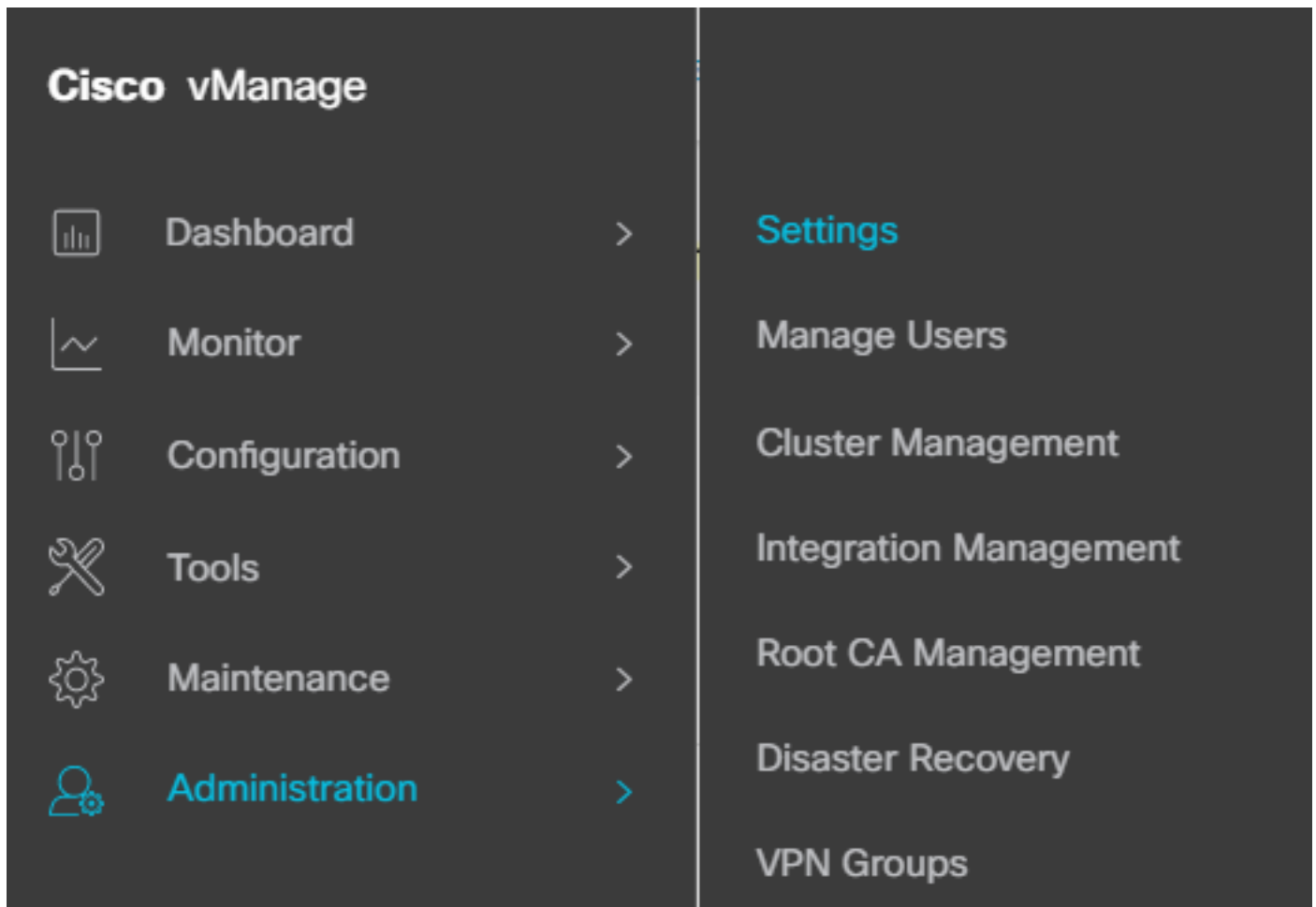
Security Assertion Markup Language (SAML) is een open standaard voor het uitwisselen van authenticatie- en autorisatiegegevens tussen partijen, in het bijzonder tussen een identiteitsprovider en een serviceprovider. Zoals de naam impliceert, is SAML een op XML-gebaseerde opmaaktaal voor beweringen over beveiliging (verklaringen die serviceproviders gebruiken om beslissingen over toegangscontrole te nemen).

Een Identity Provider (IDP) is een vertrouwde provider die u inlogt met een enkele aanmelding (SSO) om toegang te krijgen tot andere websites. SSO vermindert wachtwoordmoeheid en verbetert bruikbaarheid. Het vermindert het potentiële aanvalsoppervlak en verstrekt betere veiligheid.

## Configureren

### vManager-configuratie

1. In Cisco vManager, navigeer naar Beheer > Instellingen > Instellingen van provider identificeren > Bewerken.



Configuratie > Instellingen

2. Klik op Ingeschakeld.

3. Klik om de SAML metadata te downloaden en de inhoud op te slaan in een bestand. Dit is nodig aan de kant van OKTA.

# Administration Settings

Identity Provider Settings

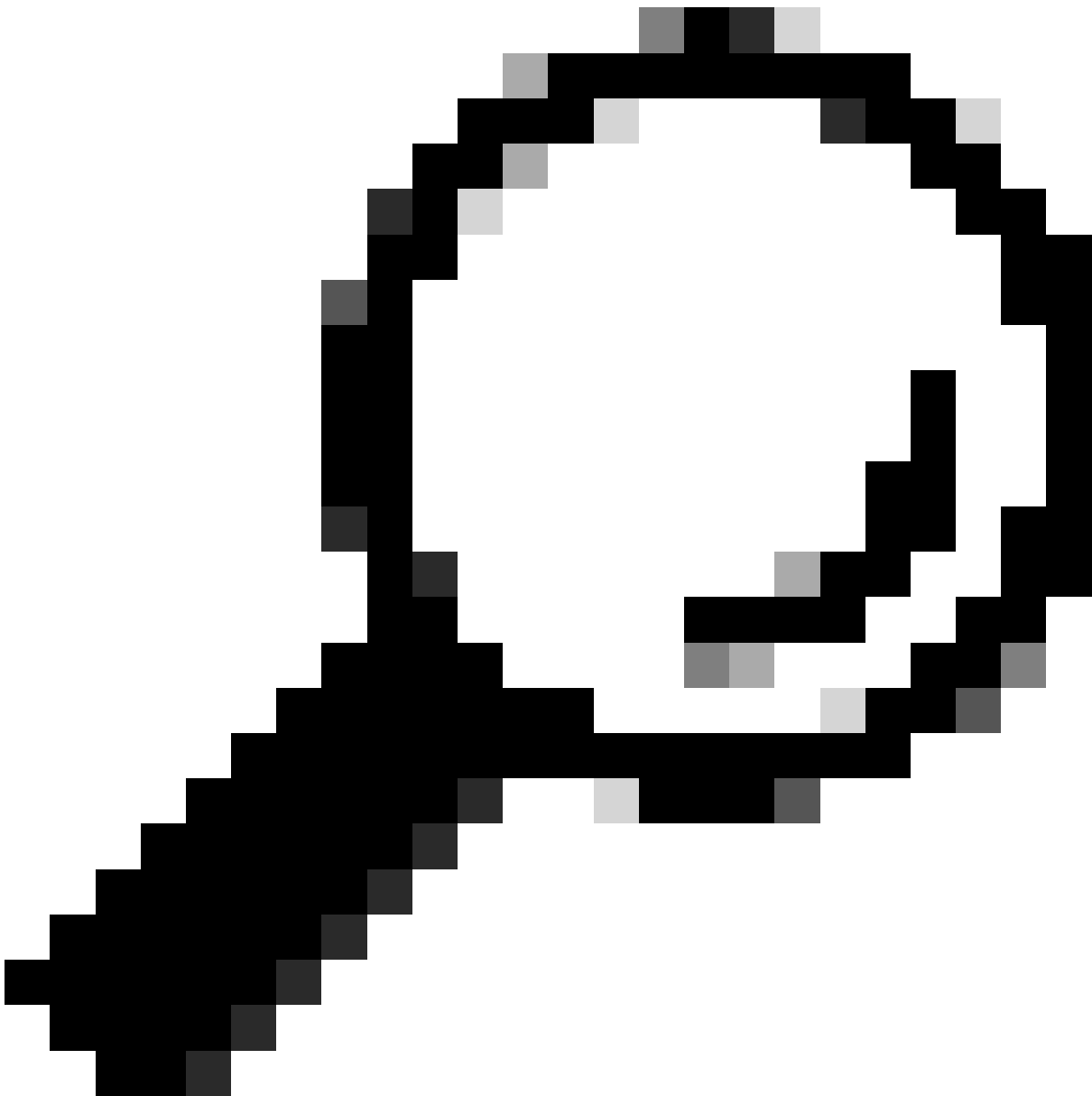
Disabled

Enable Identity Provider:  Enabled  Disabled

Upload Identity Provider Metadata

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

SAML downloaden



Tip: U hebt deze informatie van METADATA nodig om OKTA met Cisco vManager te kunnen configureren.

- a. Entiteits-ID
  - b. Certificaat van ondertekening
  - c. Encryptiecertificaat
  - d. URL voor uitloggen
  - e. Inloggen via URL
-



Opmerking: Certificaten moeten in x.509-formaat zijn opgeslagen en met de extensie .CRT zijn opgeslagen.

---

```
-----BEGIN CERTIFICATE-----
MIIDfTCCAmWgAwIBAgIhAM8T9QVLqX/lp1oK/q2XNUbJcGhRmGvqdXxGTUkrKUBhMA0GCSqGSIb3
DQEBCwUAMHixDDAKBgNVBAYTA1VTQTELMakGA1UECBMCQ0ExETAPBgNVBACTCFNhbiBkb3N1MRQw
EgYDVQQKEwtDSVNDT1JUUEXBQjEUMBIGA1UECXMLQ01TQ09SVFBMQUIxLjZmF1bHRUZW5hbnQw
HhcNMjAwNTI4MTQxMzQzWWhcNMjUwNTI4MTQxMzQzWjByMQwwCgYDVQQGEwNVU0ExCzAJBgNV
BAGTAkNBREwDwYDVQQHEwhTYW4gSm9zZTEUMBIGA1UEChMLQ01TQ09SVFBMQUIxFDASBgNVBAsTC0
NJU0NPUlRQTEFCMRYwFAyDVQQDEw1EZWZhdWx0VGVuYW50MIIBIjANBgkqhkiG9w0BAQEFAAO
CAQ8AMIIBCgKCAQEAg9HOIwjWHD3pbkCB3wRUsn01PTsNAhCqRKof5aY4QDWbu7U3+6gFTzZgr
B9189rLskkb7cEzRcE7ZbZ1a3zICVw76ZN8jj2BZMYpuTlS9LSGRq2FClYMAg6JU4Yc9prgT6I
cmJKHPfuFM3izXKVsrzfn8tDZ7UDHGIUNPs2kntamU4ZB7BRTE1zJXp+Zh3CvnfLE9g3aXK9SM9
qRFDjAaC8GhWphOYyK3RisQZ/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-----
```

X.509-certificaat

## OKTA-configuratie

1. Log in [OKTA](#) account.
2. Ga naar Toepassingen > Toepassingen.

# Applications



## Applications

## Self Service

Toepassingen > Toepassingen

3. Klik op App-integratie maken.

# Applications

## Create App Integration

Toepassing maken

4. Klik op SAML 2.0 en vervolgens op.

### 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

SAML2.0 configureren

Algemene instellingen






1. Voer een naam van de toepassing in.
2. Voeg het logo voor de toepassing toe (facultatief).
3. Zichtbaarheid van de app (facultatief).
4. Klik op VOLGENDE.



**1 General Settings**

App name

App logo (optional)   



App visibility  Do not display application icon to users

[Cancel](#) [Next](#)

Algemene instellingen van SAML

## SAML configureren

In deze tabel worden de parameters beschreven die in deze sectie moeten worden geconfigureerd.

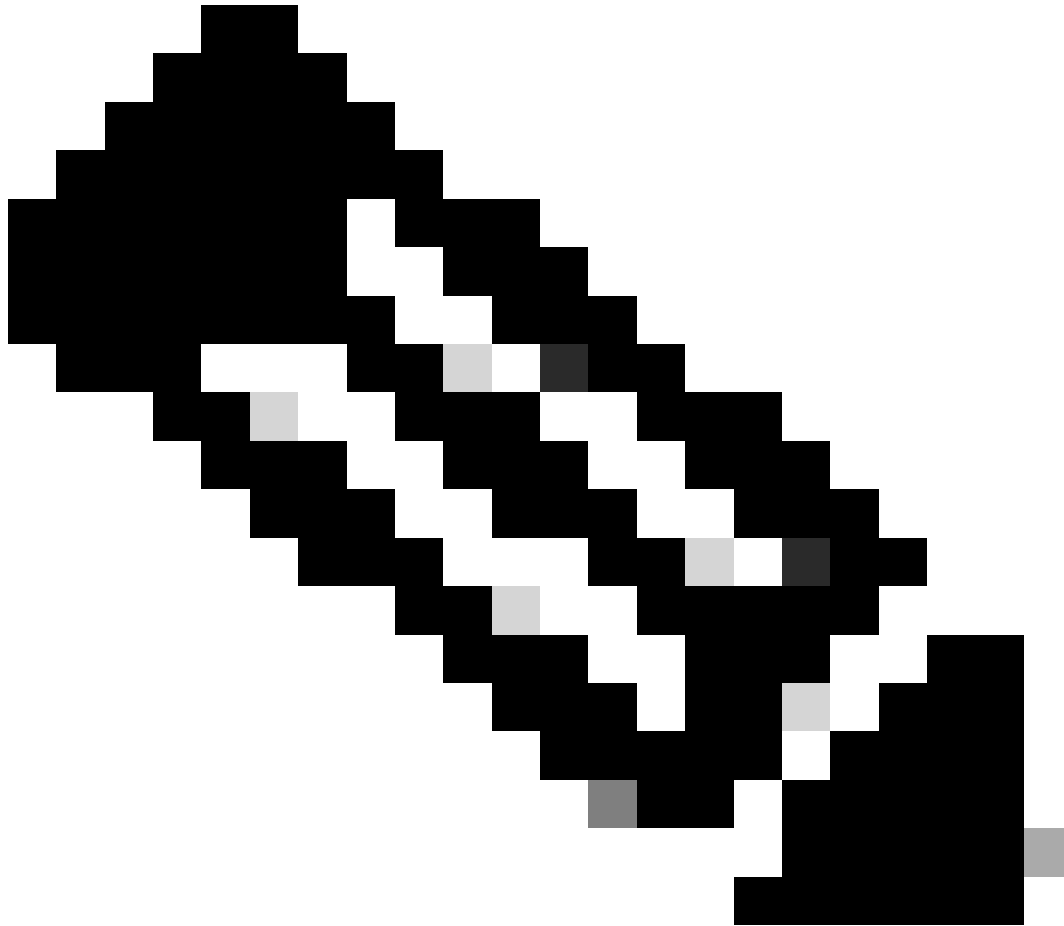
Samengesteld	Waarde	Configuratie
Enkelvoudige URL voor aanmelding	<a href="https://XX.XX.XX.XX:XXXX/samlLoginResponse">https://XX.XX.XX.XX:XXXX/samlLoginResponse</a>	Haal het uit de metadata.
URI publiek (SP entiteit-ID)	XX.XX.XX.XX	IP-adres of DNS voor Cisco

Samengesteld	Waarde	Configuratie
		vManager
Standaard Relay-status		LEEG
Formaat voor naam-ID		Zoals uw voorkeur
Gebruikersnaam voor toepassing		Zoals uw voorkeur
Gebruikersnaam voor toepassing bijwerken op	Creëer en update	Creëer en update
Reactie	Ondertekend	Ondertekend
Verklaring-handtekening	Ondertekend	Ondertekend
Algoritme voor handtekening	RSA-SHA256 router	RSA-SHA256 router
Digest-algoritme	SHA256-software	SHA256-software
Assertion-encryptie	Versleuteld	Versleuteld
Encryptiealgoritme	AES256-CBC switch	AES256-CBC switch
Toetsentransportalgoritme	RSA-OAEP	RSA-OAEP
Encryptiecertificaat		Het encryptie certificaat van metagegevens, moet op formaat x.509 zijn.
Enkelvoudige aanmelding		moet worden

Samengesteld	Waarde	Configuratie
inschakelen		gecontroleerd.
Enkelvoudige aanmelding-URL	<a href="https://XX.XX.XX.XX:XXXX/samlLogoutResponse">https://XX.XX.XX.XX:XXXX/samlLogoutResponse</a>	Haal uit de metadata.
SP-uitgever	XX.XX.XX.XX	IP-adres of DNS voor vManager
Handtekeningcertificaat		Het encryptie certificaat van de metagegevens, moet op formaat x.509 zijn.
Verklaring inline haak	Geen (uitschakelen)	Geen (uitschakelen)
Verificatiecontextklasse	X.509-certificaat	
Honor Force-verificatie	Ja	Ja
tekenreeks van SAML issuer-id	tekenreeks van SAML issuer-id	Typ een tekst in de string
Verklaringen van kenmerken (facultatief)	<p>Naam ► gebruikersnaam</p> <p>Naamnotatie (optioneel) ► Niet gespecificeerd</p> <p>Waarde ► user.login</p>	<p>Naam ► gebruikersnaam</p> <p>Naamnotatie (optioneel) ► Niet gespecificeerd</p> <p>Waarde ► user.login</p>
Verklaringen van groepskenmerken (optioneel)	<p>Naam ► groepen</p> <p>Naamnotatie (optioneel) ► Niet gespecificeerd</p> <p>Filter ► Overeenkomsten regex ►.*</p>	<p>Naam ► groepen</p> <p>Naamnotatie (optioneel) ► Niet gespecificeerd</p> <p>Filter</p>

Samengesteld	Waarde	Configuratie
		►Overeenkomsten regex ►.*

---



Opmerking: Moet Gebruikersnaam en Groepen gebruiken, precies zoals in de tabel SAML CONFIGUREREN wordt getoond.

---

1 General Settings

2 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 <sup>?</sup>

Signed

Assertion Signature <sup>?</sup>

Signed

Signature Algorithm <sup>?</sup>

RSA-SHA256

Digest Algorithm <sup>?</sup>

SHA256

Assertion Encryption <sup>?</sup>

Encrypted

Encryption Algorithm <sup>?</sup>

AES256-CBC

Key Transport Algorithm <sup>?</sup>

RSA-OAEP

Encryption Certificate <sup>?</sup>

[Browse files...](#)

Signature Certificate <sup>?</sup>

[Browse files...](#)

Enable Single Logout <sup>?</sup>

Allow application to initiate Single Logout

Signed Requests <sup>?</sup>

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 <span>?</span>	<input type="text" value="X.509 Certificate"/>
Honor Force Authentication <span>?</span>	<input type="text" value="Yes"/>
SAML Issuer ID <span>?</span>	<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=".*"/>

- Klik op Next (Volgende).

## Feedback

1. Selecteer een van de opties naar keuze.
2. Klik op Voltooien.


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

SMAL-feedback

## Groepen in OKTA configureren

1. Navigeren naar Directory > Groepen.



# Directory



People

Groups

Devices

Profile Editor

Directory Integrations

Profile Sources

2. Klik op Groep toevoegen en nieuwe groep maken.

## Groups

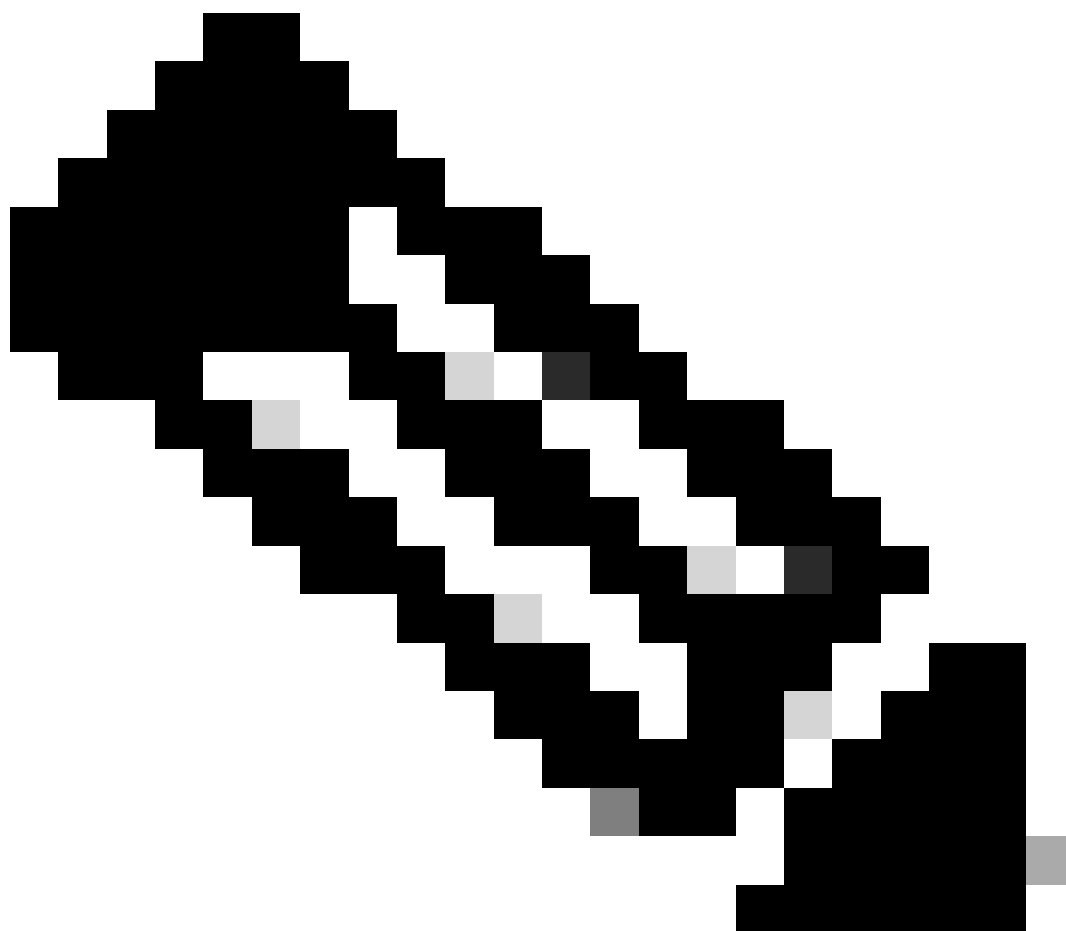
[Help](#)

All Rules

Search by group name

[Advanced search](#)

Groep toevoegen



Opmerking: Groepen moeten overeenkomen met de Cisco vManager-groepen en moeten in kleine letters worden weergegeven.

## Gebruikers in OKTA configureren

1. Navigeer naar Directory > People.

# Directory



People

Groups

Devices


Profile Editor

Directory Integrations

Profile Sources

2. Klik op Add person, maak een nieuwe gebruiker, wijs deze toe aan de groep en sla deze op.

## Add Person

User type 

First name

Last name

Username

Primary email

Secondary email (optional)

Groups (optional)

Activation

I will set password

Gebruiker toevoegen



Opmerking: Active Directory kan worden gebruikt in plaats van OKTA gebruikers.

---

## Wijs Groepen en Gebruikers in Toepassing toe

1. Ga naar Toepassingen > Toepassingen > Selecteer de nieuwe toepassing.
2. Klik op Toewijzen > Toewijzen aan groepen.



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

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](#)

Toepassing > Groepen

3. Identificeer de groep en klik op Toewijzen > Gereed.

## Assign vManage to Groups



Everyone

All users in your organization

Assign



netadmin

Assigned

Done

Toewijzen aan groep en gebruiker

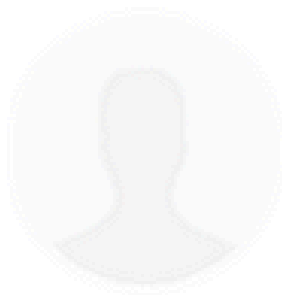
4. De groep en de gebruikers moeten nu aan de toepassing worden toegewezen.

## Verifiëren

Nadat de configuratie is voltooid, kunt u toegang tot Cisco vManager krijgen 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?



## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.