

# Konfigurieren von OKTA Single Sign-On (SSO) auf SD-WAN

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrund](#)

[Konfigurieren](#)

[vManage Konfiguration](#)

[OKTA-Konfiguration](#)

[Allgemeine Einstellungen](#)

[Konfigurieren von SAML](#)

[Feedback](#)

[Gruppen in OKTA konfigurieren](#)

[Benutzer in OKTA konfigurieren](#)

[Zuweisen von Gruppen und Benutzern in der Anwendung](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

---

## Einleitung

In diesem Dokument wird beschrieben, wie OKTA Single Sing-On (SSO) in ein Software-Defined Wide Area Network (SD-WAN) integriert wird.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- SD-WAN - Allgemeiner Überblick
- Security Assertion Markup Language (SAML)
- Identitätsanbieter (IdP)
- Zertifikate

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-

Versionen:

- Cisco vManage Version 18.3.X oder höher
- Cisco vManage Version 20.6.3
- Cisco vBond-Version 20.6.3
- Cisco vSmart Version 20.6.3

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Hintergrund

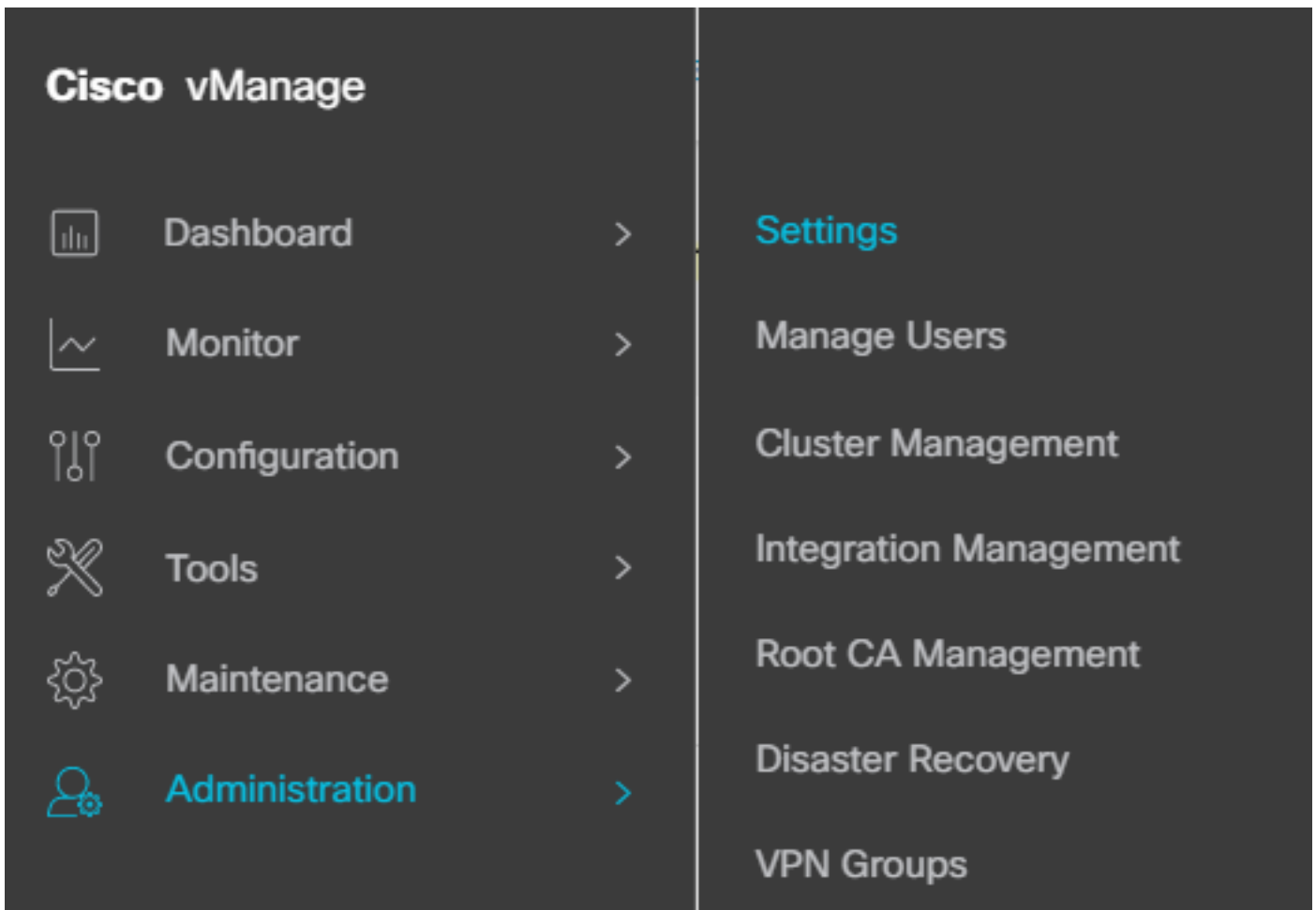
Security Assertion Markup Language (SAML) ist ein offener Standard für den Austausch von Authentifizierungs- und Autorisierungsdaten zwischen Parteien, insbesondere zwischen einem Identitätsanbieter und einem Dienstanbieter. Wie der Name bereits andeutet, ist SAML eine XML-basierte Markupsprache für Sicherheitsassertionen (Anweisungen, die Service Provider verwenden, um Zugriffskontrollentscheidungen zu treffen).

Ein Identity Provider (IdP) ist ein vertrauenswürdiger Anbieter, mit dem Sie sich mit einer einmaligen Anmeldung (Single Sign-on, SSO) auf andere Websites zugreifen können. SSO reduziert die Ermüdung von Passwörtern und verbessert die Benutzerfreundlichkeit. Sie verringert die potenzielle Angriffsfläche und bietet eine bessere Sicherheit.

## Konfigurieren

### vManage Konfiguration

1. Navigieren Sie in Cisco vManage zu Administration > Settings > Identify Provider Settings > Edit.



Konfiguration > Einstellungen

2. Klicken Sie auf Aktiviert.

3. Klicken Sie hier, um die SAML-Metadaten herunterzuladen und den Inhalt in einer Datei zu speichern. Dies ist auf der OKTA-Seite erforderlich.

# Administration Settings

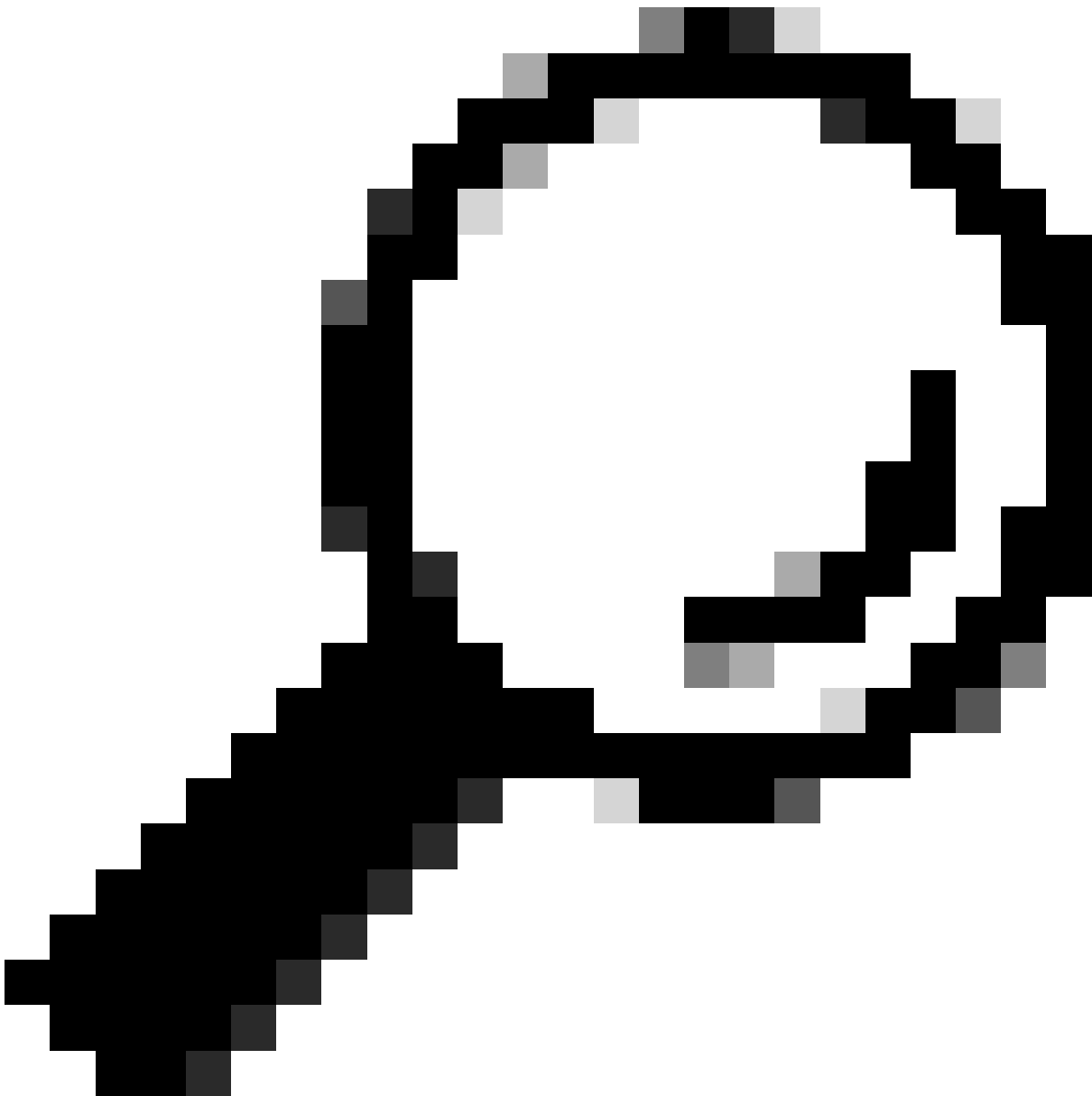
Identity Provider Settings

Disabled

Enable Identity Provider:  Enabled  Disabled

Upload Identity Provider Metadata

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



Tipp: Sie benötigen diese Informationen von METADATA, um OKTA mit Cisco vManage zu konfigurieren.

antwort: Entitäts-ID

b. Zertifikat signieren

c. Verschlüsselungszertifikat

d. Abmelde-URL

e. Anmeldung bei UR

---



Anmerkung: Zertifikate müssen im x.509-Format vorliegen und mit der .CRT-Erweiterung gespeichert werden.

---

```
-----BEGIN CERTIFICATE-----
MIIDfTCCAmWgAwIBAgIhAM8T9QVLqX/lp1oK/q2XNUbJcGhRmGvqdXxGTUkrKUBhMA0GCSqGSIb3
DQEBCwUAMHixDDAKBgNVBAYTA1VTQTELMakGA1UECBMCQ0ExETAPBgNVBACTCFNhbiBkb3NlMRQw
EgYDVQQKEwtDSVNDT1JUUExBQjEUMBIGA1UECMLQ01TQ09SVFBMQUIxLjZmF1bHRUZW5hbnQw
HhcNMjAwNTI4MTQxMzQzWjcNMjUwNTI4MTQxMzQzWjByMQwwCgYDVQQGEwNVU0ExCzAJBgNV
BAGTAkNBMRwDwYDVQQHEwhTYW4gSm9zZTEUMBIGA1UEChMLQ01TQ09SVFBMQUIxFDASBgNVBAsTC0
NJU0NPUlRQTEFCMRYwFAyDVQQDEw1EZWZhdWx0VGVuYW50MIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAg9HOIwjWHD3pbkCB3wRUsn01PTsNAhCqRKof5aY4QDWbu7U3+6gFTzZgrB9
189rLskkb7cEzRcE7ZbZ1a3zICVw76ZN8jj2BZMYpuTlS9LSGRq2FClYMAg6JU4Yc9prgT6Icm
JKHPfuFM3izXKVsrzfn8tDZ7UDHGIUNPs2kjtamU4ZB7BRTE1zJXp+Zh3CvnfLE9g3aXK9SM9qR
FDjAaC8GhWphOYyK3RisQZ/bIZJ2vWkVo91p+6/kQy7/oxFKznK/2oAXaAe26P8HYw+XC0bmkC
wb3e9a1vCGrCmPJwJPjn9j09dX426/LbjdmDAo6HudjTEoQMZduD3Z9GU5QIDAQABMA0GCSqG
SIb3DQEBCwUAA4IBAQBbO/FdHT365rzOHpgHo8YWbxbYdhjAMrHUBbuXLq6MEaHvm4GoTYsgJzc9
Scy/Iwoa6krjBXHJPPthtBwzYYXvK6CJxh8J/rlednlmai0z9growg/sSEgbXPpuQw6qT9hM8s2i
FHlFchPoqiaZFldNF4iupuzFPTcD8kmzEC3mGlcxfm2TaVjLFDu7McRAMLZTV+yPY+WZXjuoMI8P
hXapKdUt0B6RrxzucBRac2ZB22g7HWDQuDZUzf966Q2k5Us1QxtNlpXLU5X+i+YDW011T2AP6+UUi
vrN1A6vFVPP3QtAd7ao7VziMeEvxfYTuK690b+ej4MntWIKdHneU+/YC
-----END CERTIFICATE-----
```

X.509-Zertifikat

## OKTA-Konfiguration

1. Melden Sie sich bei [OKTA](#) an.
2. Navigieren Sie zu Anwendungen > Anwendungen.

# Applications



## Applications

## Self Service

Anwendungen > Anwendungen

3. Klicken Sie Anwendungsintegration erstellen.

# Applications

## Create App Integration

Anwendung erstellen

4. Klicken Sie auf SAML 2.0 und dann auf Weiter.

### 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

Konfigurieren von SAML2.0

Allgemeine Einstellungen



1. Geben Sie einen Namen für die Anwendung ein.
2. Logo für Anwendung hinzufügen (optional).
3. Anwendungstransparenz (optional)
4. Klicken Sie auf WEITER.



**1 General Settings**

App name

App logo (optional)

App visibility  Do not display application icon to users

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

Allgemeine SAML-Einstellungen

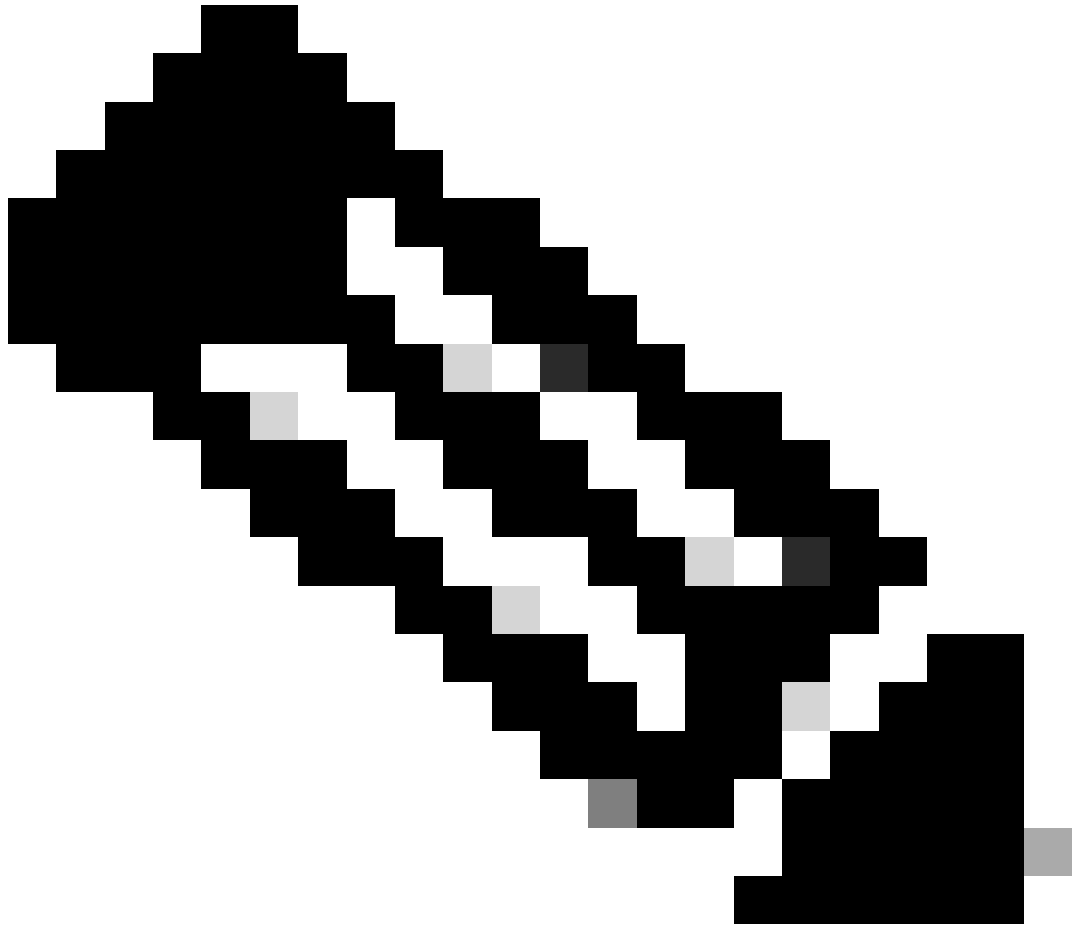
## Konfigurieren von SAML

In dieser Tabelle werden die Parameter beschrieben, die in diesem Abschnitt konfiguriert werden müssen.

Komponente	Wert	Konfiguration
URL für einmalige Anmeldung	<a href="https://XX.XX.XX.XX:XXXX/samlLoginResponse">https://XX.XX.XX.XX:XXXX/samlLoginResponse</a>	Holen Sie es aus den Metadaten.
Zielgruppen-URI (SP-Element-ID)	XX.XX.XX.XX	IP-Adresse oder DNS f Cisco vManage

Komponente	Wert	Konfiguration
Standard-Relaystatus		LEER
Name ID-Format		Je nach Ihren Wünschen
Anwendungsbenutzername		Je nach Ihren Wünschen
Anwendungsbenutzername aktualisieren auf	Erstellen und aktualisieren	Erstellen und aktualisieren
Antwort	Unterzeichnet	Unterzeichnet
Unterschrift der Behauptung	Unterzeichnet	Unterzeichnet
Signaturalgorithmus	RSA-SHA256	RSA-SHA256
Digest-Algorithmus	SHA 256	SHA 256
Assertion Encryption	Verschlüsselt	Verschlüsselt
Verschlüsselungsalgorithmus	AES256-CBC	AES256-CBC
Schlüsseltransportalgorithmus	RSA-OAEP	RSA-OAEP
Verschlüsselungszertifikat		Das Verschlüsselungszertifikat aus Metadaten muss das Format x.509 haben.
Single Logout aktivieren		muss überprüft werden
URL für einzelne Abmeldung	<a href="https://XX.XX.XX.XX:XXXX/samlLogoutResponse">https://XX.XX.XX.XX:XXXX/samlLogoutResponse</a>	Abrufen aus den Metadaten.
SP-Aussteller	XX.XX.XX.XX	IP-Adresse oder DNS f

Komponente	Wert	Konfiguration
		vManage
Signaturzertifikat		Das Verschlüsselungszertifikat aus den Metadaten muss das Format x.509 haben
Assertion Inline-Hook	None (Deaktivierung)	None (Deaktivierung)
Authentifizierungskontextklasse	X.509-Zertifikat	
Ehrenauthentifizierung erzwingen	Ja	Ja
SAML-Aussteller-ID-Zeichenfolge	SAML-Aussteller-ID-Zeichenfolge	Geben Sie einen Zeichenfolgentext ein
Attributanweisungen (optional)	Name ▶ Benutzername Namensformat (optional) ▶ Nicht angegeben Wert ▶user.login	Name ▶ Benutzername Namensformat (optional) ▶ Nicht angegeben Wert ▶user.login
Gruppenattribut-Anweisungen (optional)	Name ▶ Gruppen Namensformat (optional) ▶ Nicht angegeben Filter ▶Passt zu regulären Ausdrücken ▶.*	Name ▶ Gruppen Namensformat (optional) ▶Nicht angegeben Filter ▶Passt zu regulären Ausdrücken ▶.*



Anmerkung: Benutzername und Gruppen müssen genau wie in der SAML-Tabelle CONFIGURE verwendet werden.

---

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 ⓘ

Assertion Signature ⓘ

Signature Algorithm ⓘ

Digest Algorithm ⓘ

Assertion Encryption ⓘ

Encryption Algorithm ⓘ

Key Transport Algorithm ⓘ

Encryption Certificate ⓘ

Signature Certificate ⓘ

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

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

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

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

---

**Group Attribute Statements (optional)**

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

- Klicken Sie auf Next (Weiter).

## Feedback

1. Wählen Sie eine der Optionen aus.
2. Klicken Sie auf Fertig stellen.


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

SAML-Feedback

## Gruppen in OKTA konfigurieren

1. Navigieren Sie zu Verzeichnis > Gruppen.



# Directory



People

Groups

Devices

Profile Editor

Directory Integrations

Profile Sources

2. Klicken Gruppe hinzufügen und neue Gruppe erstellen.

## Groups

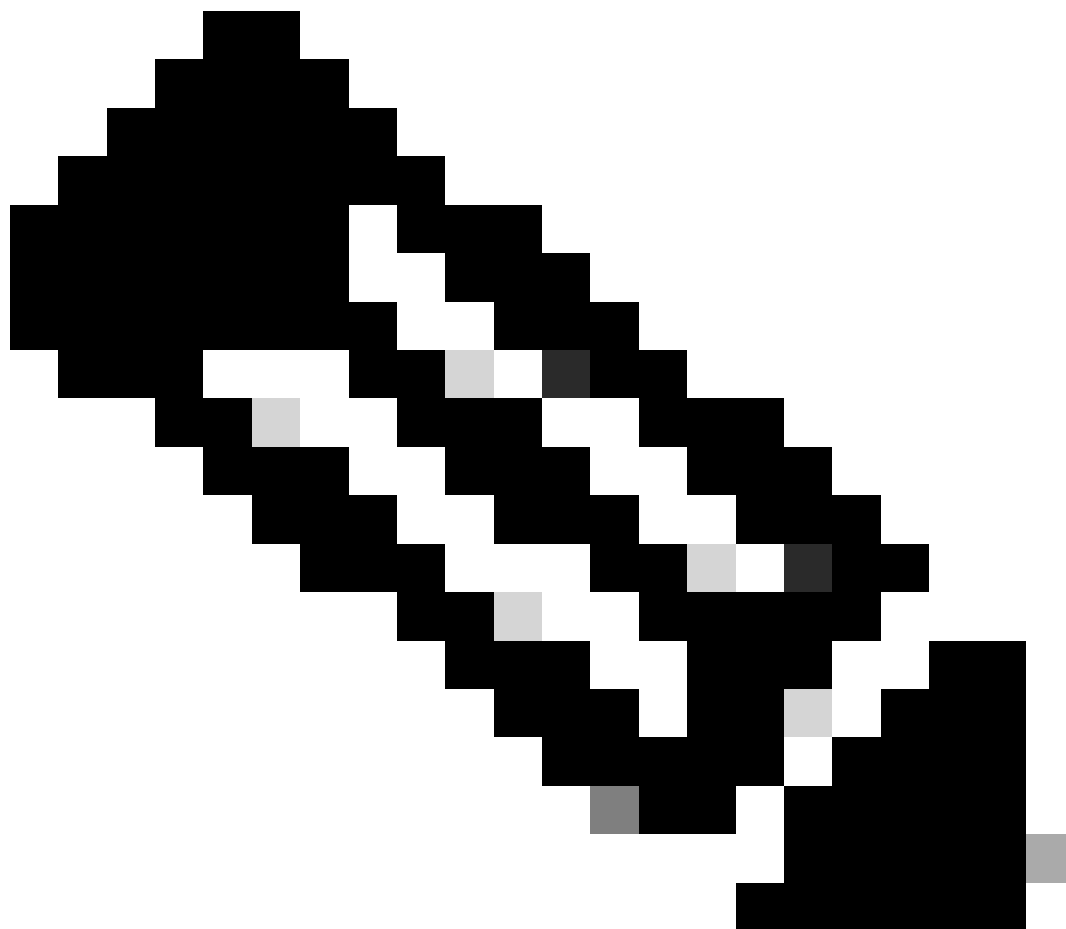
[Help](#)

All Rules

Search by group name

[Advanced search](#)

Gruppe hinzufügen



Anmerkung: Die Gruppen müssen mit den Cisco vManage-Gruppen übereinstimmen und in Kleinbuchstaben geschrieben sein.

## Benutzer in OKTA konfigurieren

1. Navigieren Sie zu Verzeichnis > Personen.

# Directory



People

Groups

Devices


Profile Editor

Directory Integrations

Profile Sources

2. Klicken Sie auf Person hinzufügen, erstellen Sie einen neuen Benutzer, weisen Sie ihn der Gruppe zu und speichern Sie ihn.

## Add Person

User type 

First name

Last name

Username

Primary email

Secondary email (optional)

Groups (optional)

Activation

I will set password

Benutzer hinzufügen



Anmerkung: Active Directory kann anstelle von OKTA-Benutzern verwendet werden.

---

## Zuweisen von Gruppen und Benutzern in der Anwendung

1. Navigieren Sie zu Anwendungen > Anwendungen > Wählen Sie die neue Anwendung aus.
2. Klicken Sie auf Zuweisen > Gruppen zuweisen.



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](#)

Anwendung > Gruppen

3. Identifizieren Sie die Gruppe, und klicken Sie auf Zuweisen > Fertig.

# Assign vManage to Groups



Everyone

All users in your organization

Assign



netadmin

Assigned

Done

Gruppe und Benutzer zuweisen

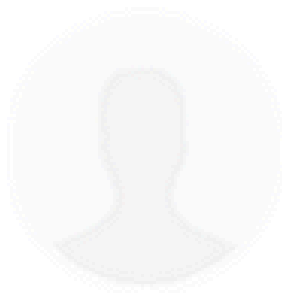
4. Gruppe und Benutzer müssen jetzt der Anwendung zugewiesen werden.

## Überprüfung

Nach Abschluss der Konfiguration können Sie über OKTA auf Cisco vManage zugreifen.

# 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?



## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.