

# 在SD-WAN上配置OKTA单点登录(SSO)

## 目录

---

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景](#)

[配置](#)

[vManage配置](#)

[OKTA配置](#)

[常规设置](#)

[配置SAML](#)

[反馈](#)

[在OKTA中配置组](#)

[在OKTA中配置用户](#)

[在应用程序中分配组 and 用户](#)

[验证](#)

[故障排除](#)

[相关信息](#)

---

## 简介

本文档介绍如何在软件定义广域网(SD-WAN)上集成OKTA单点登录(SSO)。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- SD-WAN概述
- 安全断言标记语言(SAML)
- 身份提供程序(IdP)
- 证书

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco vManage版本18.3.X或更高版本
- 思科vManage版本20.6.3

- 思科vBond版本20.6.3
- 思科vSmart版本20.6.3

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 背景

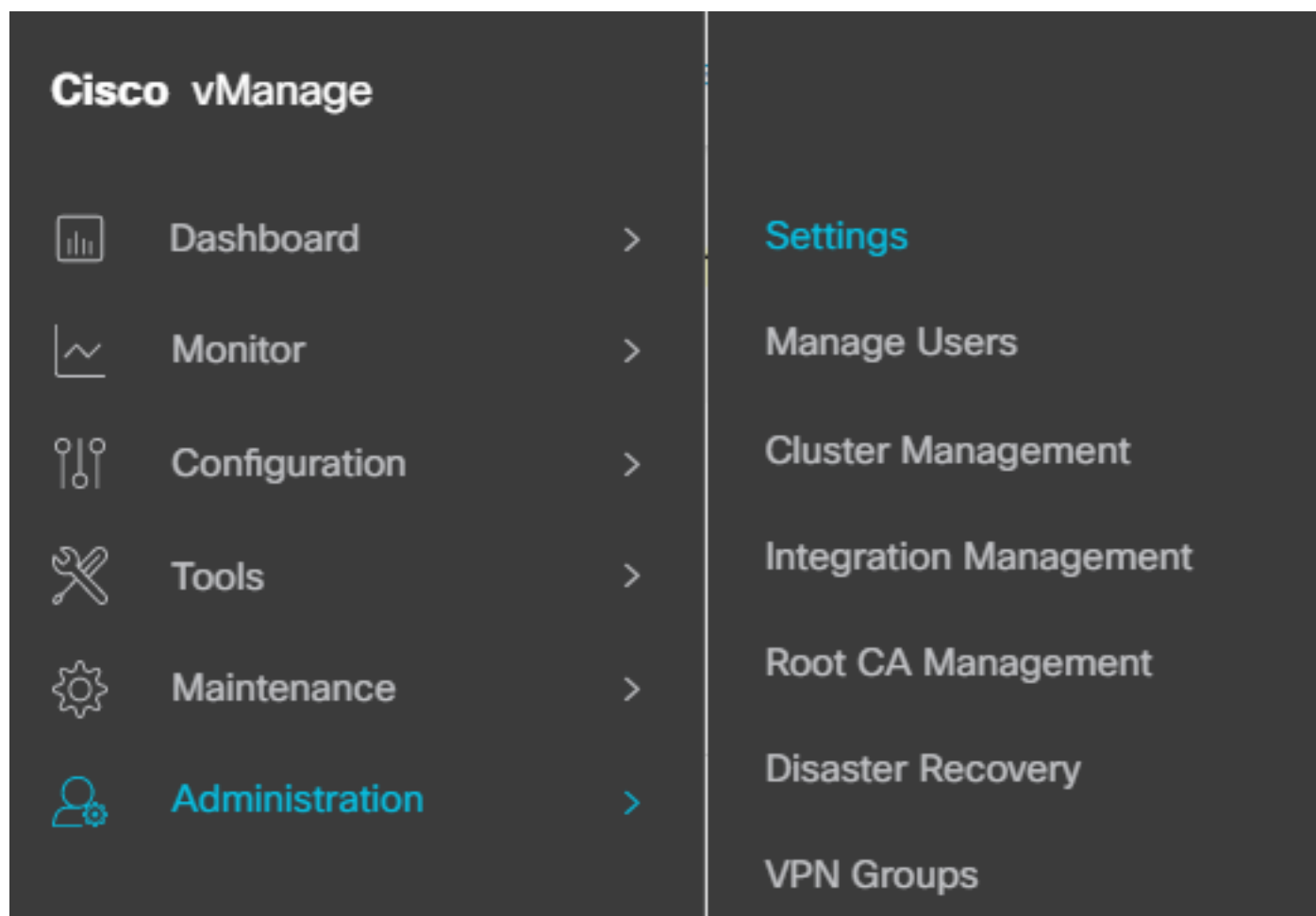
安全断言标记语言(SAML)是用于在各方之间，特别是在身份提供方和服务提供商之间交换身份验证和授权数据的开放标准。顾名思义，SAML是基于XML的安全断言（服务提供商用于制定访问控制决策的语句）标记语言。

身份提供程序(IdP)是一个受信任的提供程序，可用于使用单点登录(SSO)访问其他网站。SSO减少了密码疲劳，增强了可用性。它可以减小潜在攻击面，并提供更好的安全性。

## 配置

### vManage配置

1. 在Cisco vManage中，导航到Administration > Settings > Identify Provider Settings > Edit。



Configuration > Settings

2.单击Enabled。

3.单击以下载SAML元数据并将内容保存在文件中。OKTA端需要此功能。

 **Cisco** vManage

 Select Resource Group▼

## Administration Settings

Identity Provider Settings

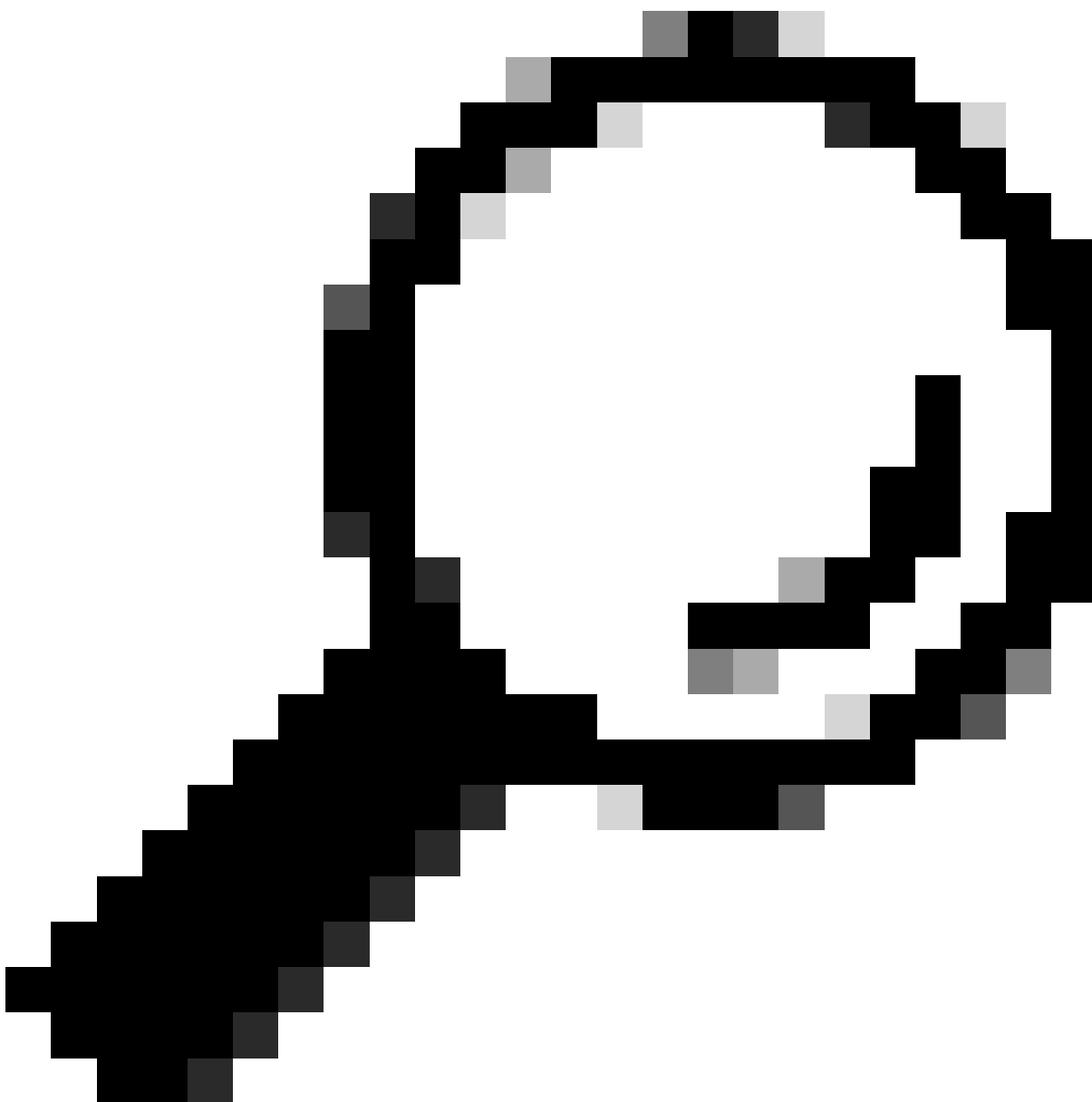
Disabled

Enable Identity Provider: ☒ Enabled ☐ Disabled

Upload Identity Provider Metadata

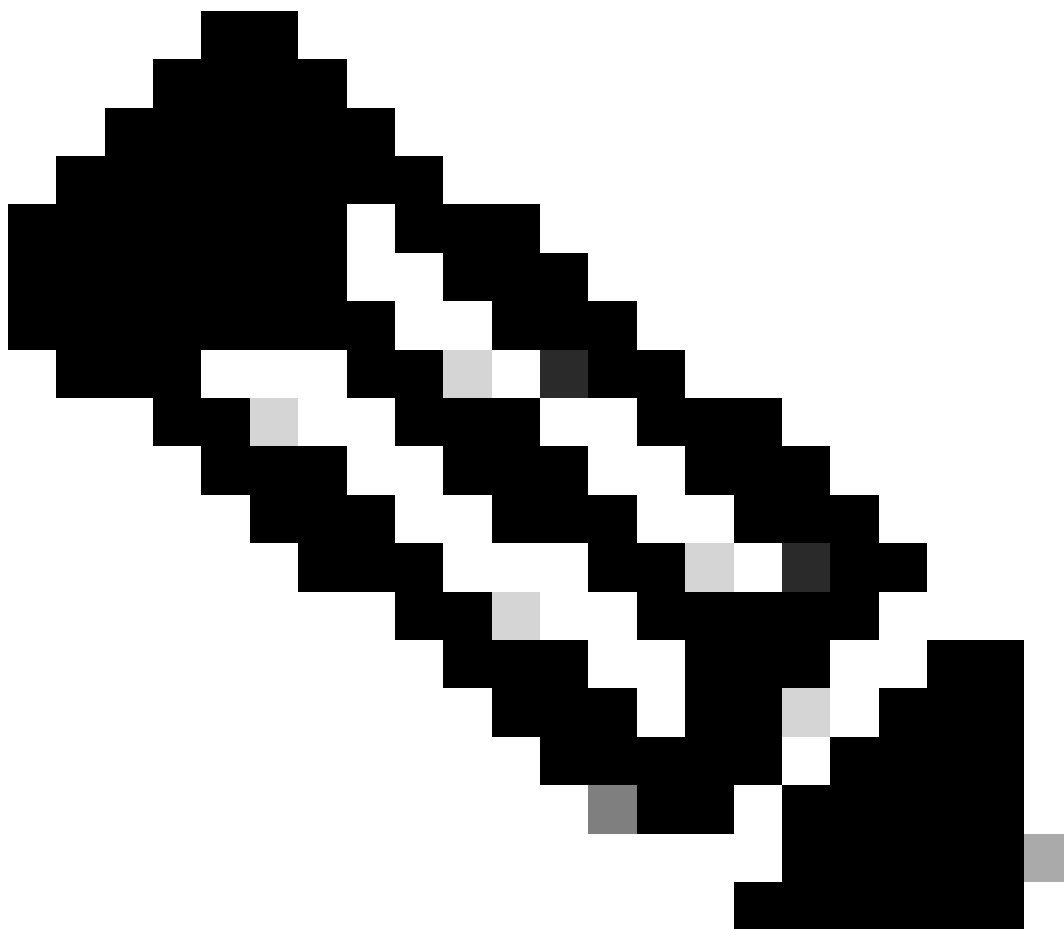
[!\[\]\(870f5d5e9c0d57485634be3ecf52f3ca\_img.jpg\) Click here to download SAML metadata](#)

下载SAML



提示：您需要来自METADATA的这些信息才能使用Cisco vManage配置OKTA。

- a. 实体Id
  - b. 签名证书
  - c. 加密证书
  - d. 注销URL
  - e. 登录UR
-



注意：证书必须采用x.509格式，并使用.CRT扩展名保存这些证书。

---

```
-----BEGIN CERTIFICATE-----
MIIDftCCAmWgAwIBAgIhAM8T9QVLqX/lp1oK/q2XNUbJcGhRmGvqdXxGTUkrKUBhMA0GCSqGSIb3
DQEBCwUAMHixDDAKBgNVBAYTA1VTQTELMakGA1UECBMCQ0ExETAPBgNVBACTCFNhbiBkb3NlMRQw
EgYDVQQKEwtDSVNDT1JUUExBQjEUMBIGA1UECXMlQ01TQ09SVFBMQUIxFTjAUBgNVBAMTDURLZmF1
bHRUZW5hbnQwHhcNMjAwNTI4MTQxMzQzWWhcNMjUwNTI4MTQxMzQzWjByMQwwCgYDVQQGEwNVU0Ex
CzAJBgNVBAgTAkNBMRwDwYDVQQHEWhTYW4gSm9zZTEUMBIGA1UEChMLQ01TQ09SVFBMQUIxFDAS
BgNVBASTC0NJU0NPULRQTEFCMRYwFAYDVQQDEw1EZWZhdWx0VGluYW50MIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAg9H0IwjWHD3pbkCB3wRUsn01PTsNAhCqRKOf5aY4QDWbu7U3+6gF
TzZgrB9189rLskkb7cEzRcE7ZbZ1a3zICVw76ZN8jj2BZMYpuTLS9LSGRq2FC1YMAg6JU4Yc9prg
T6IcmJKHPfuFM3izXKVsrzfn8tDZ7UDHGIUNPs2kjtamU4ZB7BRTE1zJXp+Zh3CvnfLE9g3aXK9
SM9qRFDjAac8GhWphOYyK3RisQZ/bIZJ2vWkVo91p+6/kQy7/oxFKznK/2oAXaAe26P8HYw+XC0b
mkCwb3e9a1vCGrCmPJwJPjn9j09dX426/LbjdmDAo6HudjTEoQMZduD3Z9GU5QIDAQABMA0GCSqG
SIb3DQEBCwUAA4IBAQBbO/FdHT365rzOHpgHo8YWbxbYdhjAMrHUBbuXLq6MEaHvm4GoTYsgJzc9
Scy/Iwoa6krjBXHJPPthtBwzYYXvK6CJxh8J/rlednlmai0z9growg/sSEgbXPpuQw6qT9hM8s2i
FhlFchPoqiaZFldNF4iupuzFPTcd8kmzEC3mGlcxfm2TaVjLFDu7McRAmLZTV+yPY+WZXjuoMI8P
hXapKdUt0B6RxzuCBRac2ZB22g7HWDQuDZUzf966Q2k5Us1QxtNlpXLU5X+i+YDW011T2AP6+UUi
vrN1A6vFVFP3QtAd7ao7VziMeEvxfYTuk690b+ej4MNtWIKdHneU+/YC
-----END CERTIFICATE-----
```

X.509证书

## OKTA配置

1. 登录[OKTA](#)帐户。
2. 定位至“应用”>“应用”。

# Applications



## Applications

## Self Service

Applications ( 应用 ) > Applications ( 应用 )

3. 单击 创建应用集成。

# Applications

## Create App Integration

创建应用程序

4. 单击SAML 2.0和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

配置SAML2.0

常规设置

- 1.输入申请名称。
- 2.为应用程序添加徽标（可选）。
- 3.应用可视性（可选）。
- 4.单击下一步。

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

SAML 常规设置

配置SAML

此表说明了本节中必须配置的参数。

组件	价值	配置
单点登录URL	<a href="https://XX.XX.XX.XX:XXXX/samlLoginResponse">https://XX.XX.XX.XX:XXXX/samlLoginResponse</a>	从元数据中获取数据。
受众URI（SP实体ID）	XX.XX.XX.XX	Cisco vManage的IP地址或DNS



组件	价值	配置
默认RelayState		空
名称ID格式		根据您的偏好
应用程序用户名		根据您的偏好
更新应用程序用户名	创建和更新	创建和更新
回复	已签名	已签名
断言签名	已签名	已签名
签名算法	RSA-SHA256	RSA-SHA256
摘要算法	SHA256	SHA256
断言加密	已加密	已加密
加密算法	AES256-CBC	AES256-CBC
密钥传输算法	RSA-OAEP	RSA-OAEP
加密证书		来自元数据的加密证书的格式必须为x.509。
启用单一注销		必须检查。
单一注销URL	<a href="https://XX.XX.XX.XX:XXXX/samlLogoutResponse">https://XX.XX.XX.XX:XXXX/samlLogoutResponse</a>	从元数据获取。
SP颁发者	XX.XX.XX.XX	vManage的IP地址或DNS
签名证书		来自元数据的加密证书的格式必须为x.509。

组件	价值	配置
断言内联挂接	无（禁用）	无（禁用）
身份验证上下文类	X.509证书	
执行强制身份验证	Yes	Yes
SAML颁发者ID字符串	SAML颁发者ID字符串	键入字符串文本
属性语句（可选）	名称▶用户名 名称格式（可选）▶未指定 值▶user.login	名称▶用户名 名称格式（可选）▶未指定 值▶user.login
组属性语句（可选）	组▶称 名称格式（可选）▶未指定 过滤▶匹配regex ▶。*	组▶称 名称格式（可选）▶未指定 过滤▶匹配regex ▶。*



注意：必须使用用户名和组，具体如配置SAML表中所示。

---

1 General Settings

2 Configure SAML

A SAML Settings

General

Single sign-on URL ?

https://XX.XX.XX.XX:XXXXX/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](#)

配置SAML第1部分

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

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

Name	Name format (optional)	Value
<div>Username</div>	<div>Unspecified ▾</div>	<div>user.login ▾</div>
<div>Add Another</div>		

Group Attribute Statements (optional)

Name	Name format (optional)	Filter
<div>Groups</div>	<div>Unspecified ▾</div>	<div>Matches regex ▾ .*</div>
<div>Add Another</div>		

- 单击 Next。

## 反馈

- 1.选择选项之一作为首选项。
- 2.单击完成。


### 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反馈

## 在OKTA中配置组

1.导航至目录>组。

# Directory



People

Groups

Devices

Profile Editor

Directory Integrations

Profile Sources



2.单击Add group并创建新组。

Groups

Help

AllRules

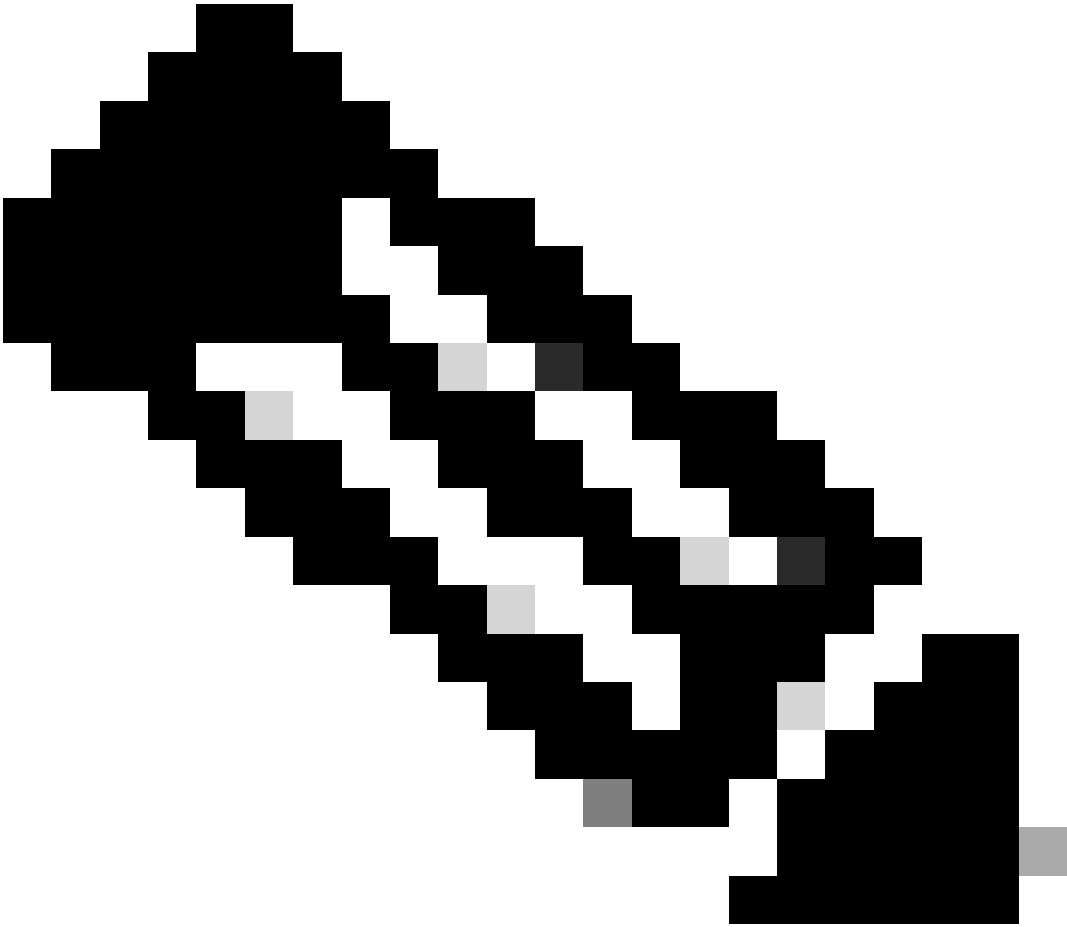
Search by group name

Q

Add group

Advanced search

添加组



注意：组必须与Cisco vManage组匹配，且它们需要小写。

在OKTA中配置用户

1.定位至目录>人员。

# Directory



People

Groups

Devices


Profile Editor

Directory Integrations

Profile Sources

2.单击添加人员，创建新用户，将其分配给组并保存。

## Add Person

User type 

User ▼

First name

Test

Last name


Test

Username

Primary email

Secondary email (optional)

Groups (optional)

 netadmin x

Activation

Activate now ▼

☐ I will set password

Save

Save and Add Another

Cancel

添加用户



注意：可使用Active Directory代替OKTA用户。

---

## 在应用程序中分配组 和用户

- 1.定位至应用>应用>选择新应用。
- 2.单击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

Search...

Groups

Assign to People

Assign to Groups

Assignment
01101110
01101111
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

应用>组

3.标识组，然后单击分配>完成。

# Assign vManage to Groups

Q Search...

Everyone

All users in your organization

Assign

netadmin

Assigned

Done

分配组 and 用户

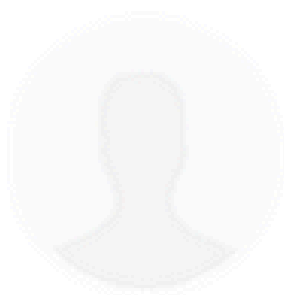
4.现在必须将组和用户分配给应用程序。

## 验证

完成配置后，您可以通过OKTA访问Cisco vManage。

# 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?](#)

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。