

Configure OKTA Single Sign-On (SSO) on SD-WAN

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background](#)

[Configure](#)

[vManage Configuration](#)

[OKTA Configuration](#)

[General Settings](#)

[Configure SAML](#)

[Feedback](#)

[Configure Groups in OKTA](#)

[Configure Users in OKTA](#)

[Assign Groups and Users in Application](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

Introduction

This document describes how to integrate OKTA Single Sign-On (SSO) on a Software-Defined Wide Area Network (SD-WAN).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- SD-WAN general overview
- Security Assertion Markup Language (SAML)
- Identity Provider (IdP)
- Certificates

Components Used

The information in this document is based on these software and hardware versions:

- Cisco vManage Release 18.3.X or later
- 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. If your network is live, ensure that you understand the potential impact of any command.

Background

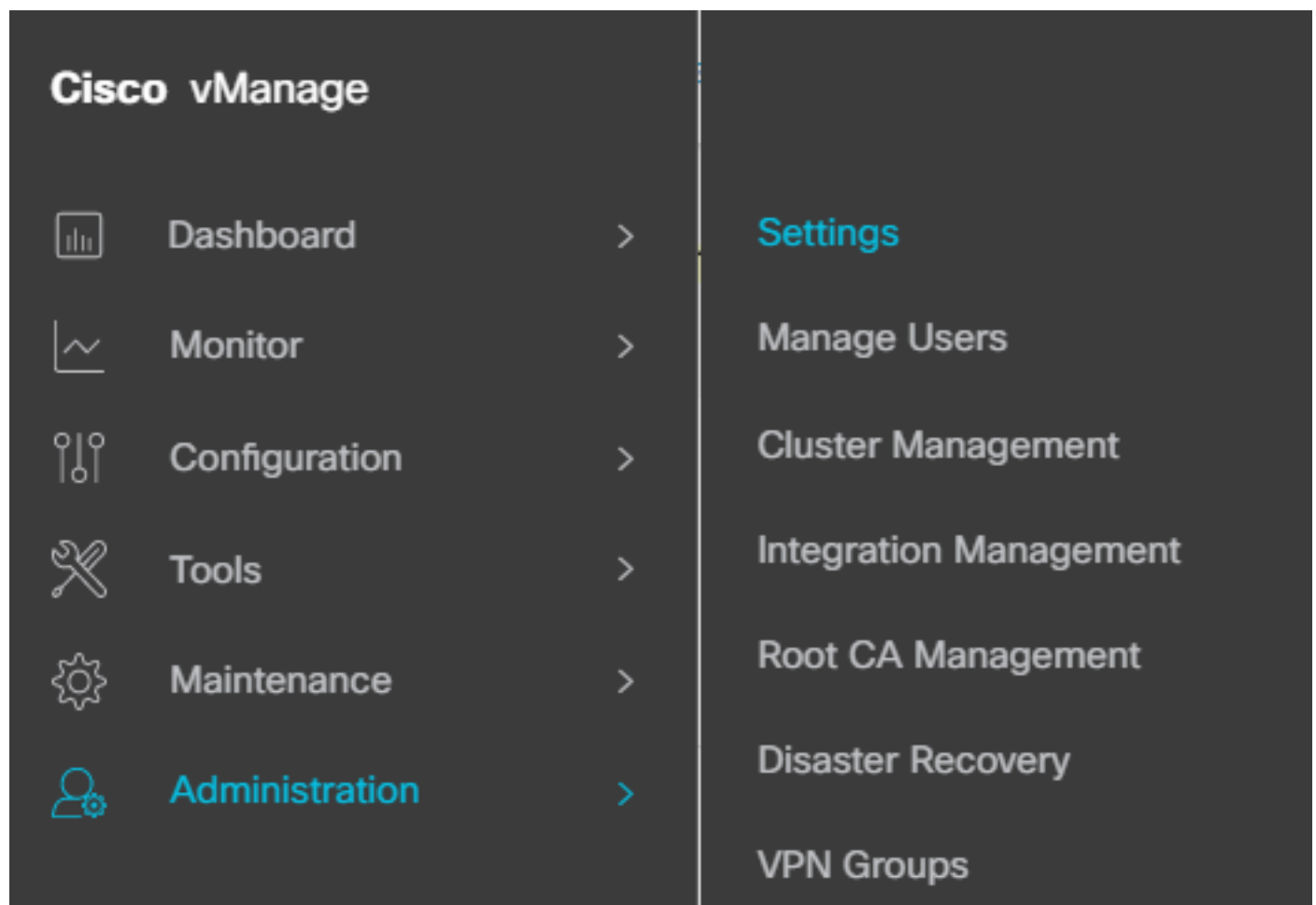
Security Assertion Markup Language (SAML) is an open standard for exchange authentication and authorization data between parties, in particular, between an identity provider and a service provider. As its name implies, SAML is an XML-based markup language for security assertions (statements that service providers use to make access-control decisions).

An Identity Provider (IdP) is a trusted provider that lets you use single sign-on (SSO) in order to access other websites. SSO reduces password fatigue and enhances usability. It decreases the potential attack surface and provides better security.

Configure

vManage Configuration

1. In Cisco vManage, navigate to **Administration** > **Settings** > **Identify Provider Settings** > **Edit**.



2. Click **Enabled**.

3. Click to **download the SAML metadata** and save the content in a file. This is needed on the OKTA side.

Administration Settings

Identity Provider Settings

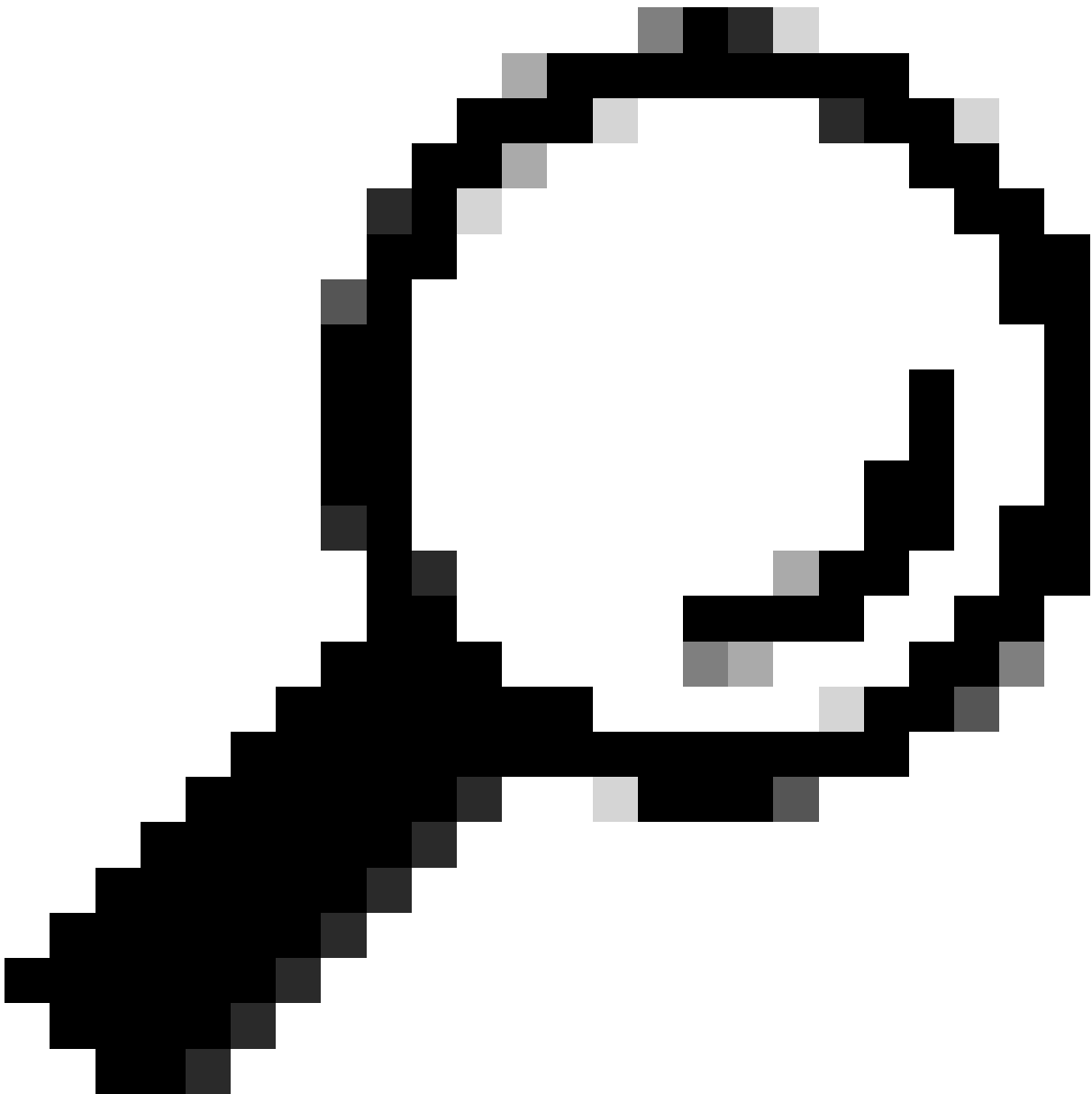
Disabled

Enable Identity Provider: ☒ Enabled ☐ Disabled

Upload Identity Provider Metadata

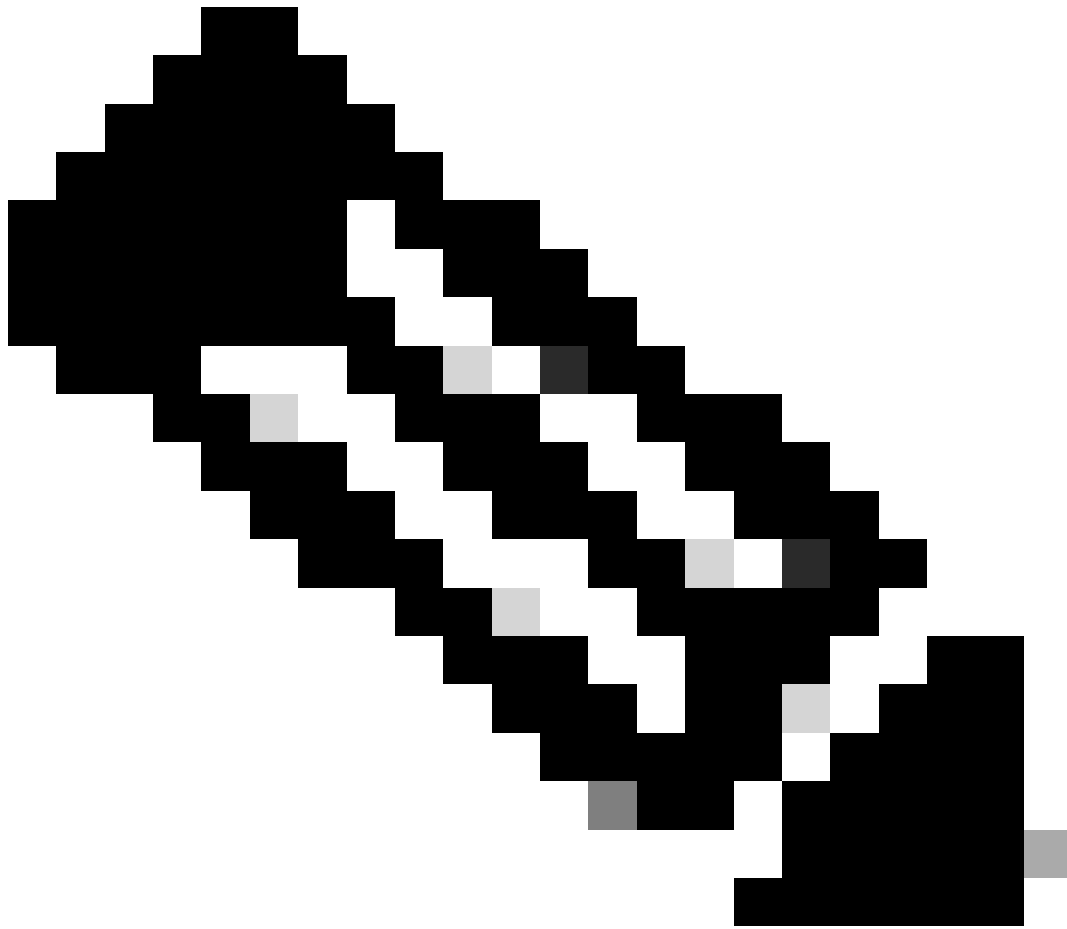
[↓ Click here](#) to download SAML metadata

Download SAML



Tip: You need these information from **METADATA** to configure OKTA with Cisco vManage.

- a. Entity ID**
 - b. Sign certificate**
 - c. Encryption certificate**
 - d. Log out URL**
 - e. Log in UR**
-



Note: Certificates must be in **x.509** format and save them with **.CRT** extension.

```
-----BEGIN CERTIFICATE-----
MIIDfTCCAmWgAwIBAgIhAM8T9QVLqX/lp1oK/q2XNUbJcGhRmGvqdXxGTUkrKUBhMA0GCSqGSIb3
DQEBCwUAMHixDDAKBgNVBAYTA1VTQTELMakGA1UECBMCQ0ExETAPBgNVBACTCFNhbiBkb3NlMRQw
EgYDVQQKEwtDSVNDTlJUUExBQjEUMBIGA1UECMLQ01TQ09SVFBMQUIxFTJlZmF1bHRUZW5hbnQw
HhcnMjAwNTI4MTQxMzQzWWhcnMjUwNTI4MTQxMzQzWjByMQwwCgYDVQQGEwNVU0ExCzAJBgNV
BAGTAkNBMRwDwYDVQQHEwhTYW4gSm9zZTEUMBIGA1UEChMLQ01TQ09SVFBMQUIxFDASBgNVBAS
TC0NJU0NPULRQTEFCMRYwFAYDVQQDEw1EZWZhdWx0VGluYW50MIIBIjANBgkqhkiG9w0BAQE
FAAOCAQ8AMIIBCgKCAQEAg9H0IwjWHD3pbkCB3wRUsn01PTsNAhCqRKOf5aY4QDWbu7U3+6gF
TzZgrB9189rLskkb7cEzRcE7ZbZ1a3zICVw76ZN8jj2BZMYpuTSL9LSGRq2FC1YMAg6JU4Yc9
prgT6IcmJKHPfuFM3izXKVsrzfn8tDZ7UDHGIUNPs2kjntamU4ZB7BRTE1zJXp+Zh3CvnfLE9g3a
XK9SM9qRFDjAac8GhWphOYyK3RisQZ/bIZJ2vWkVo91p+6/kQy7/oxFKznK/2oAXaAe26P8HYw
+XC0bmkCwb3e9a1vCGrCmPJwJPjn9j09dX426/LbjdmDAo6HudjTEoQMZduD3Z9GU5QIDAQA
BMA0GCSqGSIb3DQEBCwUAA4IBAQBbO/FdHT365rzOHpgHo8YWbxbYdhjAMrHUBbuXLq6MEaH
vm4GoTYsgJzc9Scy/Iwoa6krjBXHJPPthtBwzYYXvK6CJxh8J/rlednlmai0z9growg/sSEgb
XPpuQw6qT9hM8s2iFhlFchPoqiaZFldNF4iupuzFPTcd8kmzEC3mGlcxfm2TaVjLFdu7McRAm
LZTV+yPY+WZXjuoMI8PhXapKdUt0B6RxzuCBRac2ZB22g7HWDQuDZUzf966Q2k5Us1QxtNlpX
LU5X+i+YDW011T2AP6+UUiVrN1A6vFVPP3QtAd7ao7VziMeEvxfYTuk690b+ej4MNtWIKdHneU
+/YC
-----END CERTIFICATE-----
```

X.509 Certificate

OKTA Configuration

1. Log in [OKTA](#) account.
2. Navigate to **Applications > Applications**.

Applications



Applications

Self Service

Applications > Applications

3. Click **Create App Integration**.

Applications

Create App Integration

Create Application

4. Click **SAML 2.0** and **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

Configure SAML2.0

General Settings

1. Enter a name of application.
2. Add logo for application (optional).
3. App visibility (optional).
4. Click **NEXT**.

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 General Settings

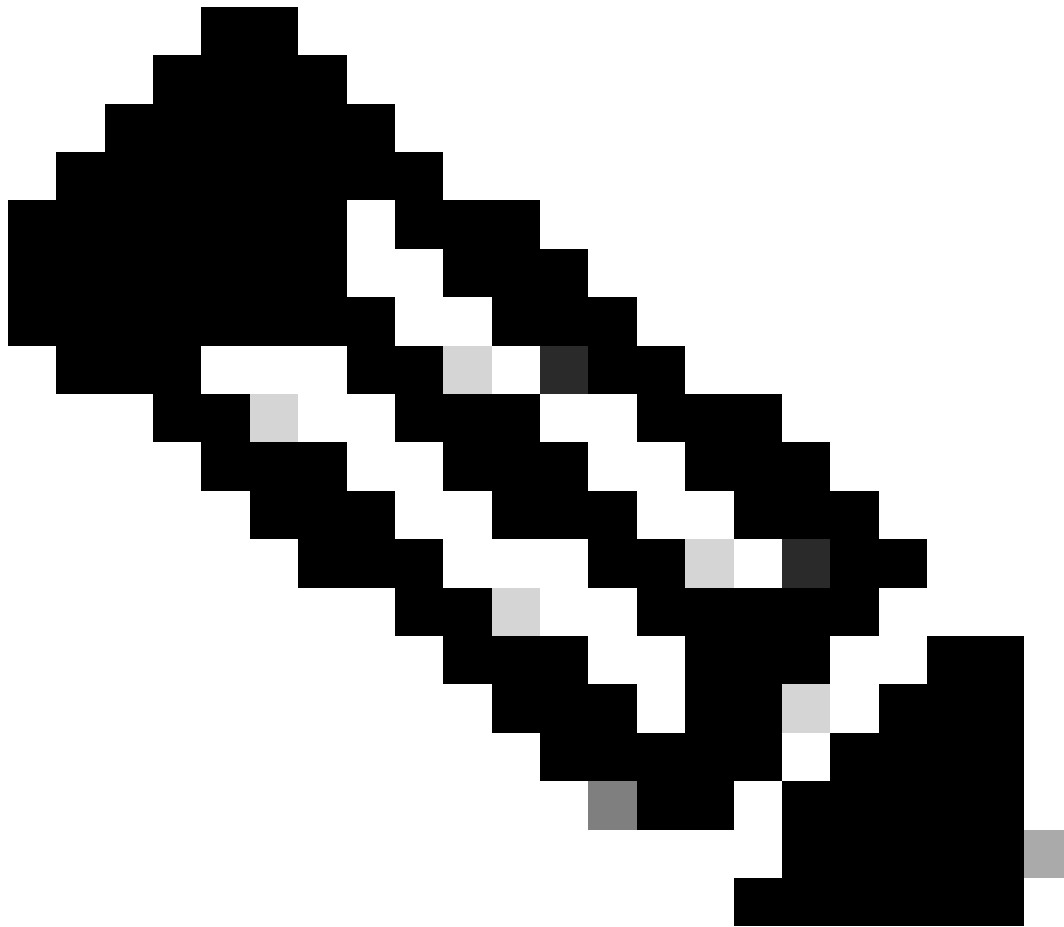
Configure SAML

This table describe the parameters must need configure on this section.

Component	Value	Configuration
Single sign on URL	https://XX.XX.XX.XX:XXXX/samlLoginResponse	Get it from the metadata.
Audience URI (SP Entity ID)	XX.XX.XX.XX	Ip address or DNS for Cisco vManage
Default RelayState		EMPTY

Component	Value	Configuration
Name ID format		As per your preference
Application username		As per your preference
Update application username on	Create and update	Create and update
Response	Signed	Signed
Assertion Signature	Signed	Signed
Signature Algorithm	RSA-SHA256	RSA-SHA256
Digest Algorithm	SHA256	SHA256
Assertion Encryption	Encrypted	Encrypted
Encryption Algorithm	AES256-CBC	AES256-CBC
Key Transport Algorithm	RSA-OAEP	RSA-OAEP
Encryption Certificate		Encryption certificate from metadata, must be on format x.509 .
Enable Single Logout		must be checked.
Single Logout URL	https://XX.XX.XX.XX:XXXX/samlLogoutResponse	Get from the metadata.
SP Issuer	XX.XX.XX.XX	Ip address or DNS for vManage
Signature		Encryption certificate from the

Component	Value	Configuration
Certificate		metadata, must be on format x.509 .
Assertion Inline Hook	None(disable)	None(disable)
Authentication context class	X.509 Certificate	
Honor Force Authentication	Yes	Yes
SAML issuer ID string	SAML issuer ID string	Type an string text
Attributes Statements (optional)	Name ► Username Name format (optional) ► Unspecified Value ► user.login	Name ► Username Name format (optional) ► Unspecified Value ► user.login
Group Attribute Statements (optional)	Name ► Groups Name format (optional) ► Unspecified Filter ► Matches regex ► .*	Name ► Groups Name format (optional) ► Unspecified Filter ► Matches regex ► .*



Note: Must use **Username** and **Groups**, exactly as shown in **CONFIGURE SAML** table.

A SAML Settings

General

Single sign-on URL ?

☒ Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID) ?

Default RelayState ?

If no value is set, a blank RelayState is sent

Name ID format ?

Application username ?

Update application username on

[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	None (disabled) ▾
Authentication context class ?	X.509 Certificate ▾
Honor Force Authentication ?	Yes ▾
SAML Issuer ID ?	http://www.example.com
Maximum app session lifetime	☐ Send value in response Uses SessionNotOnOrAfter attribute

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

Name	Name format (optional)	Value
Username	Unspecified ▾	user.login ▾
Add Another		

Group Attribute Statements (optional)

Name	Name format (optional)	Filter
Groups	Unspecified ▾	Matches regex ▾ .*
Add Another		

- Click **Next**.

Feedback

1. Select one of the option as your preference.
2. Click **Finish**.

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

Configure Groups in OKTA

1. Navigate to **Directory > Groups**.

Directory



People

Groups

Devices

Profile Editor

Directory Integrations

Profile Sources

2. Click **Add group** and creat new group.

Groups

[Help](#)

All Rules

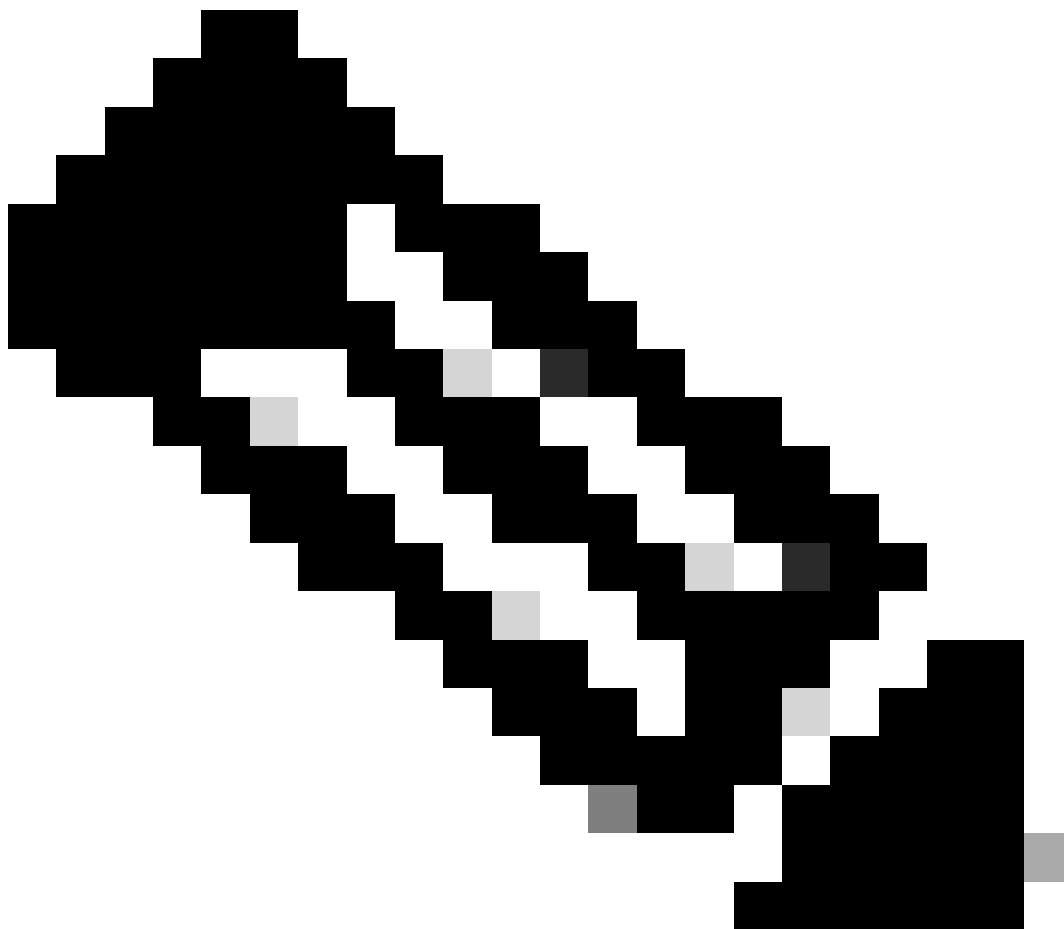
Search by group name



[Add group](#)

[Advanced search](#)

Add Group



Note: Groups must match with the Cisco vManage groups and they need to be in lower case.

Configure Users in OKTA

1. Navigate to **Directory > People**.

Directory



People

Groups

Devices

Profile Editor

Directory Integrations

Profile Sources

2. Click **Add person**, create a new user, assigne it to the group and save it.

Add Person

User type 

User ▼

First name

Test

Last name

Test

Username

Primary email

Secondary email (optional)

Groups (optional)

 netadmin ×

Activation

Activate now ▼

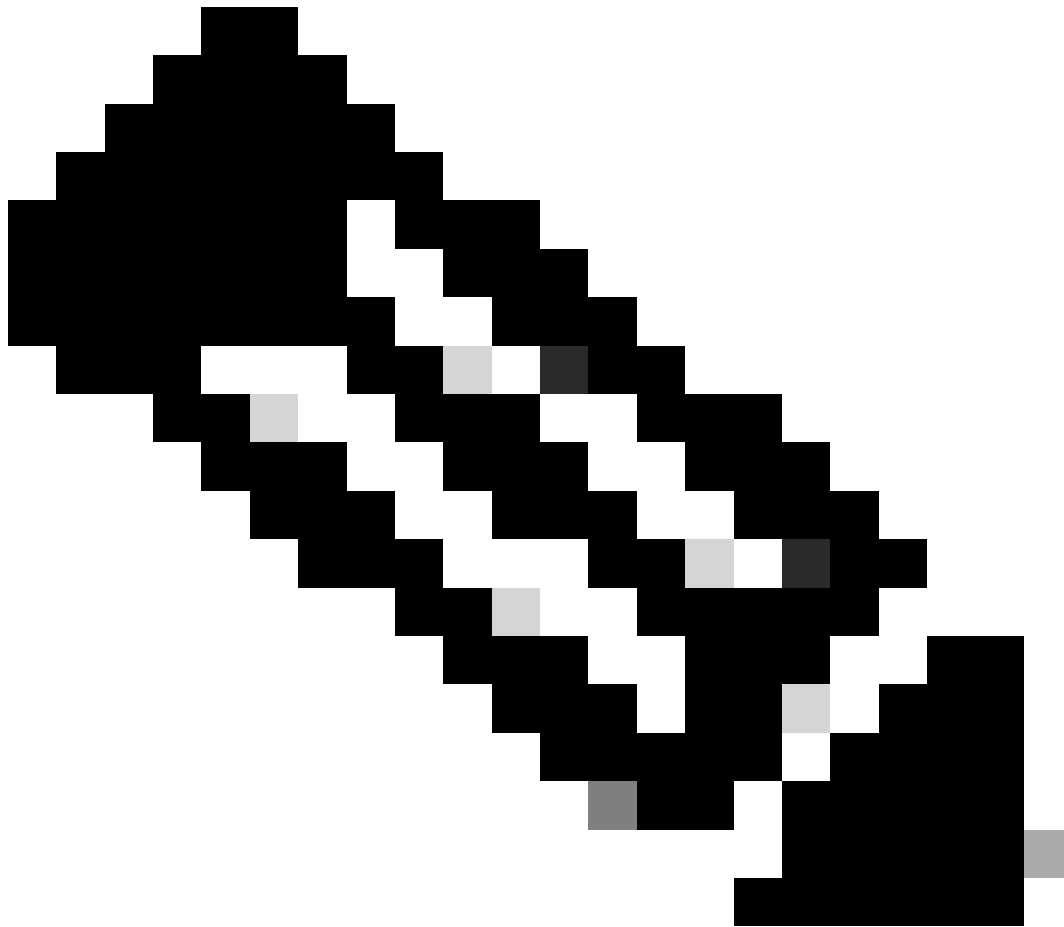
☐ I will set password

Save

Save and Add Another

Cancel

Add User



Note: Active Directory can be use instead of OKTA users.

Assign Groups and Users in Application

1. Navigate to **Applications > Applications** > Select the new application.
2. Click **Assign > Assign to Groups**.



Active



[View Logs](#)

[Monitor Imports](#)



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

[Submit your app for review](#)

General

Sign On

Import

Assignments

Assign

Convert assignments

Assign to People

Assign to Groups

Search...

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. Identify the group and click **Assign** > **Done**.

Assign vManage to Groups



Everyone

All users in your organization

Assign



netadmin

Assigned

Done

Assign Group and User

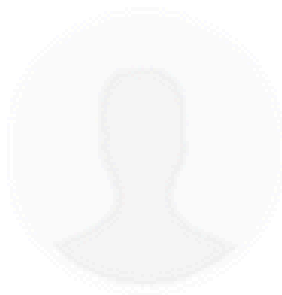
4. Group and Users now must be assigned to application.

Verify

Once the configuration be completed, you can get access to Cisco vManage through 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?](#)