

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

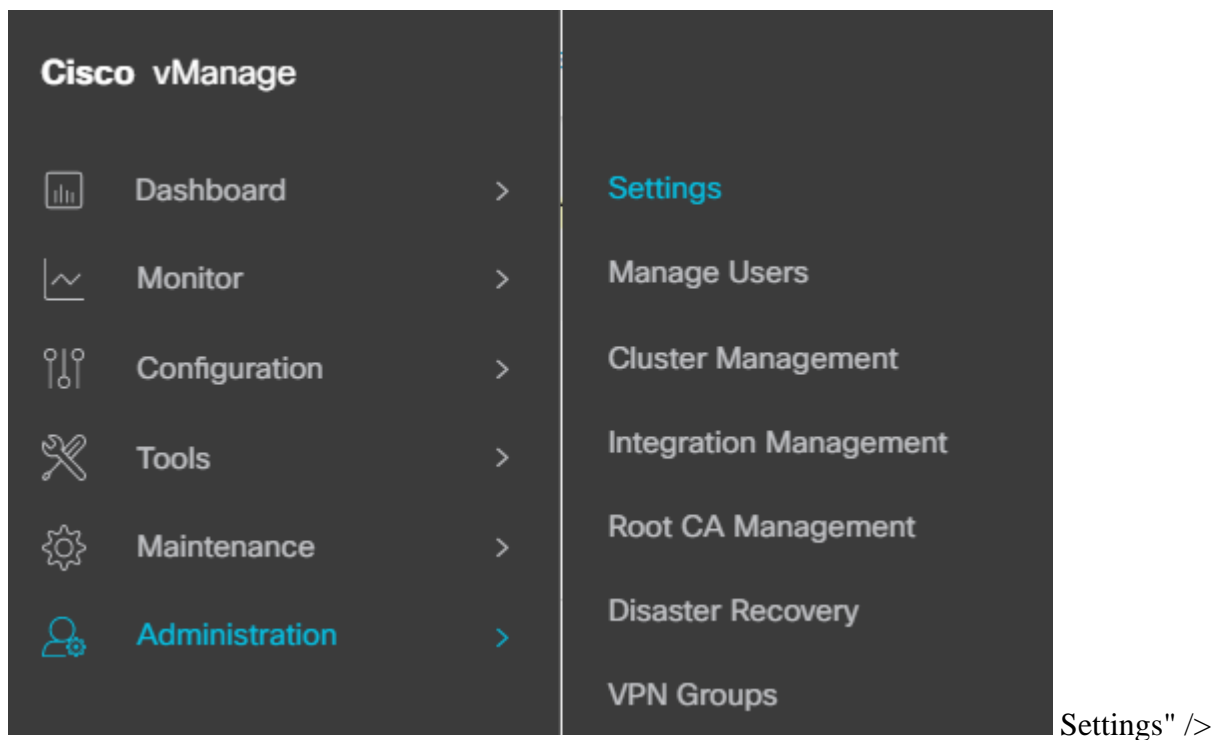
Security Assertion Markup Language (SAML) is an open standard for exchange authentication and authorization data between parties, in particular, between an identity provider and a service provider. As its name implies, SAML is an XML-based markup language for security assertions (statements that service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



Configuration > Settings

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/q2XNUbJcGhRmGvqdXxGTU
DQEBCwUAMHIXDDAKBgNVBAYTA1VTQTELMakGA1UECBMCQ0ExETAPBgNVBA
EgYDVQQKEwtDSVNDT1JUUEXBQjEUMBIGA1UECXMLQ01TQ09SVFBMQUIxXj
bHRUZW5hbnQwHhcNMjAwNTI4MTQxMzQzWWhcNMjUwNTI4MTQxMzQzWjByMQ
CzAJBgNVBAgTAkNBMRwDwYDVQQHEwhTYW4gSm9zZTEUMBIGA1UEChMLQ0
BgNVBAsTC0NJU0NPUlRQTEFCMRYwFAyDVQQDEw1EZWZhdWx0VGVuYW50MI
AQEFAAOCAQ8AMIIBCgKCAQEAg9HOIwjWHD3pbkCB3wRUsn01PTsNAhCqRK
TzZgrB9189rLSkkb7cEzRcE7ZbZ1a3zICVw76ZN8jj2BZMYpuTLS9LSGRQ
T6IcmJKHPfuFM3izXKVsrzfn8tDZ7UDHGIUNPs2kjntamU4ZB7BRTE1zJX
SM9qRFDjAaC8GhWphOYyK3RisQZ/bIZJ2vWkVo91p+6/kQy7/oxFKznK/2
mkCwb3e9a1vCGrCmPJwJPjn9j09dX426/LbjdmDAo6HudjTEoQMZduD3Z9
SIb3DQEBCwUAA4IBAQBbO/FdHT365rzOHpgHo8YWbxbYdhjAMrHUBbuXLQ
Scy/Iwoa6krjBXHJPphtBwzYYXvK6CJxh8J/rlednlmai0z9growg/sSE
FHLfCHPoqiaZFldNF4iupuzFPTcD8kmzEC3mGlcxfm2TaVjLFDu7McRAML
hXapKdUt0B6RxzuCBRac2ZB22g7HWDQuDZUzf966Q2k5Us1QxtNlpXLU5X
vrN1A6vFVPP3QtAd7ao7VziMeEvxfYTuK690b+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 > Applications

3. Click **Create App Integration**.

Applications

Create App Integration

Create Application

Component	Value	Configuration
Audience URI (SP Entity ID)	XX.XX.XX.XX	Ip address or DNS for Cisco vManage
Default RelayState		EMPTY
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 .

Component	Value	Configuration
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 Certificate		Encryption certificate from the 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 â-° Username Name format (optional) â-° Unspecified Value â-° user.login	Name â-° Username Name format (optional) â-° Unspecified Value â-° user.login
Group Attribute Statements (optional)	Name â-° Groups Name format (optional) â-° Unspecified Filter â-° .*	Name â-° Groups Name format (optional) â-° Unspecified Filter â-° .*

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

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

None (disabled) ▼

Authentication context class ⓘ

X.509 Certificate ▼

Honor Force Authentication ⓘ

Yes ▼

SAML Issuer ID ⓘ

http://example

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 ▼

Starts with ▼

.*

[Add Another](#)

Configure SAML Part 3

- 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 form provides Okta
background information
Thank you for your help-

Previous

Finish

SAML Feedback

Configure Groups in OKTA

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


- Directory ^
- People
- Groups
- Devices
- Profile Editor
- Directory Integrations
- Profile Sources


OKTA Groups

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

Groups

All Rules

Search by group name 

Advanced search 

Add Group