

SD-WANでのOKTAシングルサインオン(SSO)の設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景](#)

[設定](#)

[vManageの設定](#)

[OKTAの設定](#)

[一般設定](#)

[SAMLの設定](#)

[フィードバック](#)

[OKTAでのグループの設定](#)

[OKTAでのユーザの設定](#)

[アプリケーションでのグループとユーザの割り当て](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

はじめに

このドキュメントでは、ソフトウェア定義型ワイドエリアネットワーク(SD-WAN)でOKTAシングルサインオン(SSO)を統合する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- SD-WANの概要
- Security Assertion Markup Language(SAML)
- アイデンティティプロバイダー(IdP)
- 証明書

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco vManageリリース18.3.X以降
- Cisco vManageバージョン20.6.3
- Cisco vBondバージョン20.6.3
- Cisco vSmartバージョン20.6.3

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景

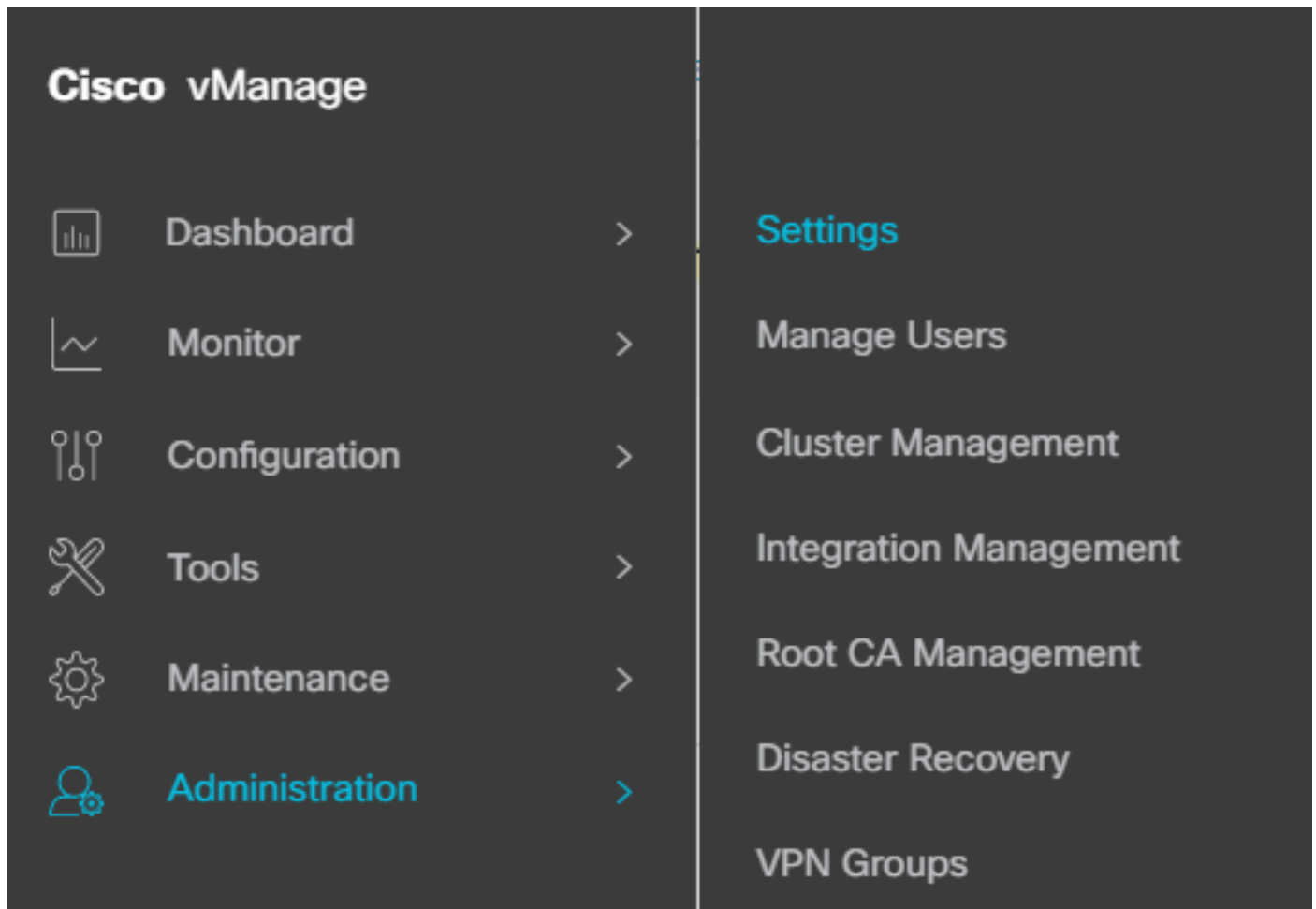
Security Assertion Markup Language(SAML)は、パーティ間、特にアイデンティティプロバイダーとサービスプロバイダーの間で認証および許可データを交換するためのオープンスタンダードです。その名前が示すように、SAMLはセキュリティアサーション（サービスプロバイダーがアクセス制御の決定に使用するステートメント）用のXMLベースのマークアップ言語です。

アイデンティティプロバイダー(IdP)は、シングルサインオン(SSO)を使用して他のWebサイトにアクセスできる信頼されたプロバイダーです。SSOは、パスワードの疲労を軽減し、使いやすさを向上させます。潜在的な攻撃対象領域が減少し、セキュリティが向上します。

設定

vManageの設定

1. Cisco vManageで、Administration > Settings > Identify Provider Settings > Editの順に移動します。



設定>設定

2. Enabledをクリックします。

3. SAMLメタデータをダウンロードしてファイルに保存する場合をクリックします。これはOKTA側で必要です。

Administration Settings

Identity Provider Settings

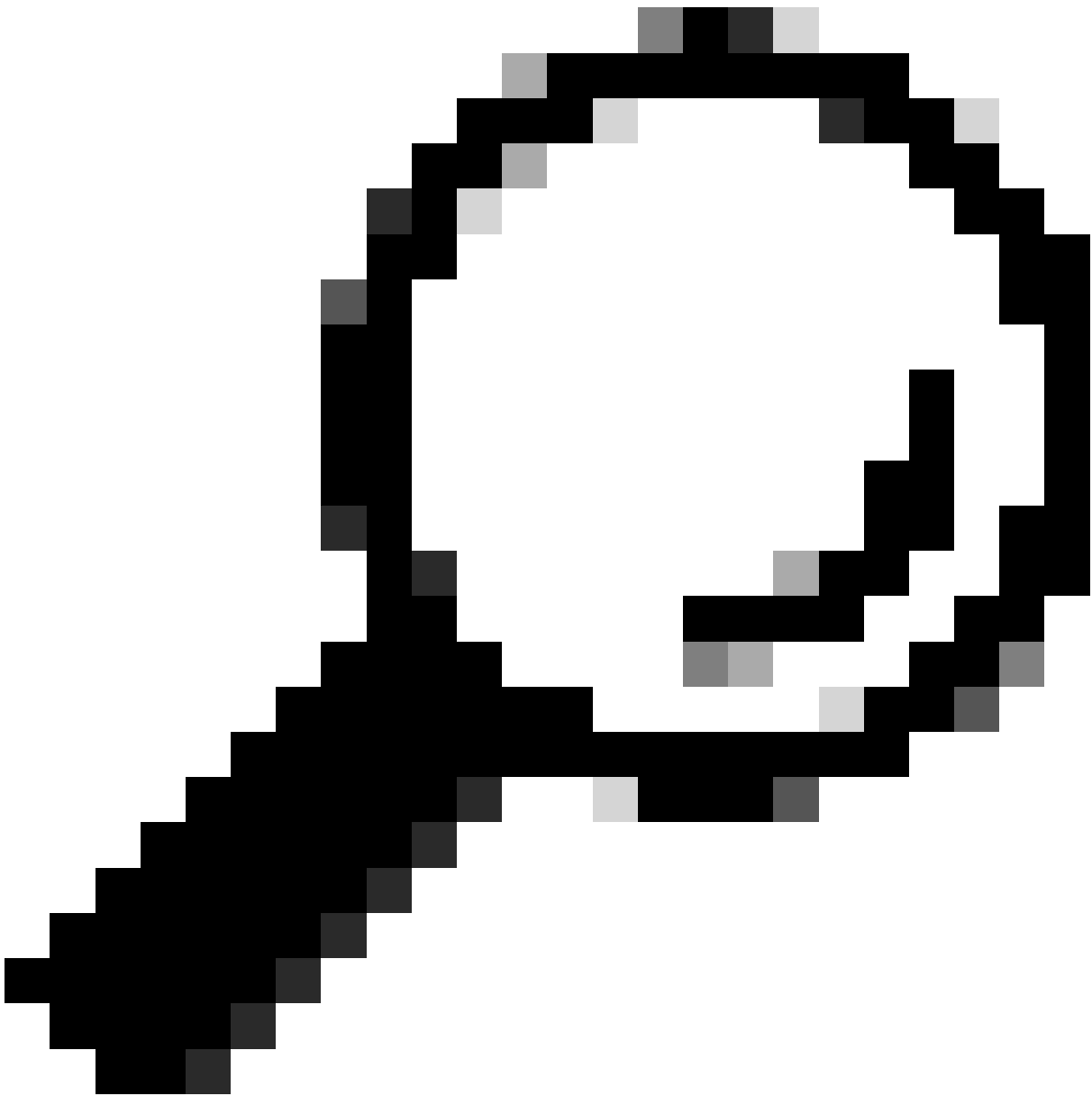
Disabled

Enable Identity Provider: Enabled Disabled

Upload Identity Provider Metadata

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

SAMLのダウンロード



ヒント: Cisco vManageでOKTAを設定するには、METADATAの次の情報が必要です。

a. エンティティID

□。署名証明書

d. 暗号証明書

d. ログアウトURL

e. URにログインします



注：証明書はx.509形式で、.CRT拡張子を付けて保存する必要があります。

```
-----BEGIN CERTIFICATE-----
MIIDfTCCAmWgAwIBAgIhAM8T9QVLqX/lp1oK/q2XNUbJcGhRmGvqdXxGTUkrKUBhMA0GCSqGSIb3
DQEBCwUAMHlxDDAKBgNVBAYTA1VTQTELMakGA1UECBMCQ0ExETAPBgNVBACTCFNhbiBkb3NlMRQw
EgYDVQQKEwtDSVNDT1JUUEXBQjEUMBIGA1UECXMlQ01TQ09SVFBMQUIxLjZmF1bHRUZW5hbnQw
HhcNMjAwNTI4MTQxMzQzWWhcNMjUwNTI4MTQxMzQzWjByMQwwCgYDVQQGEwNVU0ExCzAJBgNV
BAGTAKNBMRwDwYDVQQHEWhTYW4gSm9zZTEUMBIGA1UEChMLQ01TQ09SVFBMQUIxFDASBgNVBAsTC0
NJU0NPUlRQTEFCMRYwFAyDVQQDEw1EZWZhdWx0VGVuYW50MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8
AMIIBCgKCAQEAg9HOIwjWHD3pbkCB3wRUsn01PTsNAhCqRKof5aY4QDWbu7U3+6gFTzZgrB9189r
Lskkb7cEzRcE7ZbZ1a3zICVw76ZN8jj2BZMYpuTlS9LSGRq2FClYMAg6JU4Yc9prgT6IcmJKHPfu
FM3izXKVsrzfn8tDZ7UDHGIUNPs2kntamU4ZB7BRTE1zJXp+Zh3CvnfLE9g3aXK9SM9qRFDjAaC8
GhWphOYyK3RisQZ/bIZJ2vWkVo91p+6/kQy7/oxFKznK/2oAXaAe26P8HYw+XC0bmkCwb3e9a1v
CGrCmPJwJPjn9j09dX426/LbjdmDAo6HudjTEoQMZduD3Z9GU5QIDAQABMA0GCSqGSIb3DQEBCw
UAA4IBAQBbO/FdHT365rzOHpgHo8YWbxbYdhjAMrHUBbuXLq6MEaHvm4GoTYsgJzc9Scy/Iwoa6kRj
BXHJPPthtBwzYYXvK6CJxh8J/rlednlmai0z9growg/sSEgbXPpuQw6qT9hM8s2iFHlFchPoqiaZ
FldNF4iupuzFPTcD8kmzEC3mGlcxfm2TaVjLFDu7McRAMLZTV+yPY+WZXjuoMI8PhXapKdUt0B6R
xzuCBRac2ZB22g7HWDQuDZUzf966Q2k5Us1QxtNlpXLU5X+i+YDW011T2AP6+UUiVrN1A6vFVPP3
QtAd7ao7VziMeEvxfYTuK690b+ej4MntWIKdHneU+/YC
-----END CERTIFICATE-----
```

X.509証明書

OKTAの設定

1. [OKTA](#)アカウントにログインします。
2. 「アプリケーション」 > 「アプリケーション」にナビゲートします。

Applications



Applications

Self Service

アプリケーション > アプリケーション

3. クリック アプリケーション統合の作成。

Applications

Create App Integration

アプリケーションの作成

4. SAML 2.0をクリックし、nextをクリックします。

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の設定

一般設定

1. アプリケーションの名前を入力します。
2. アプリケーションのロゴを追加します (オプション)。
3. アプリケーションの可視性 (オプション)
4. NEXTをクリックします。

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の一般設定

SAMLの設定

次の表では、このセクションで設定する必要があるパラメータについて説明します。

コンポーネント	値	コンフィギュレーション
シングルサインオンURL	https://XX.XX.XX.XX:XXXX/samlLoginResponse	メタデータから取得します。
対象ユーザーURI (SPエンティティID)	XX.XX.XX.XX	Cisco vManageのIPアドレスまたはDNS

コンポーネント	値	コンフィギュレーション
既定のRelayState		空
名前IDの形式		お客様の好みに応じて
アプリケーション ユーザ名		お客様の好みに応じて
アプリケーション のユーザー名の更 新	作成と更新	作成と更新
応答	署名済	署名済
アサーションシグ ニチャ	署名済	署名済
署名アルゴリズム	RSA-SHA256	RSA-SHA256
ダイジェストアル ゴリズム	SHA256	SHA256
アサーション暗号 化	[Encrypted]	[Encrypted]
暗号化アルゴリズム	AES256-CBC	AES256-CBC
キー転送アルゴリ ズム	RSA-OAEP	RSA-OAEP
暗号化証明書		メタデータからの暗号化証 明書(x.509形式)を保持して いる必要があります。
シングルログアウトの有効化		確認する必要があります。

コンポーネント	値	コンフィギュレーション
シングルログアウトURL	https://XX.XX.XX.XX:XXXX/samlLogoutResponse	メタデータから取得します。
SP発行者	XX.XX.XX.XX	vManageのIPアドレスまたはDNS
署名証明書		メタデータからの暗号化証明書が、x.509形式である必要があります。
アサーションインラインフック	なし (無効)	なし (無効)
認証コンテキストクラス	X.509証明書	
認証の強制	Yes	Yes
SAML発行者ID文字列	SAML発行者ID文字列	文字列テキストを入力します
属性ステートメント (オプション)	名前▶ユーザ名 名前の形式 (オプション) ▶未指定値▶user.login	名前▶ユーザ名 名前の形式 (オプション) ▶未指定値▶user.login
グループ属性ステートメント (オプション)	グループ▶名前 名前の形式 (オプション) ▶未指定 フィルタ▶正規表現▶に一致します。*	グループ▶名前 名前の形式 (オプション) ▶未指定 フィルタ▶正規表現▶に一致します。*



注:SAMLの設定の表に示されているとおりに、ユーザ名とグループを使用する必要があります。

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](#)

SAMLパート1の設定

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 [?]	X.509 Certificate ▼
Honor Force Authentication [?]	Yes ▼
SAML Issuer ID [?]	<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=".*"/>

- [Next] をクリックします。

フィードバック

1. いずれかのオプションを選択します。
2. Finishをクリックします。

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

i 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フィードバック

OKTAでのグループの設定

1. Directory > Groupsの順に移動します。

Directory



People

Groups

Devices

Profile Editor

Directory Integrations

Profile Sources

2. Add groupをクリックして、新しいグループを作成します。

Groups

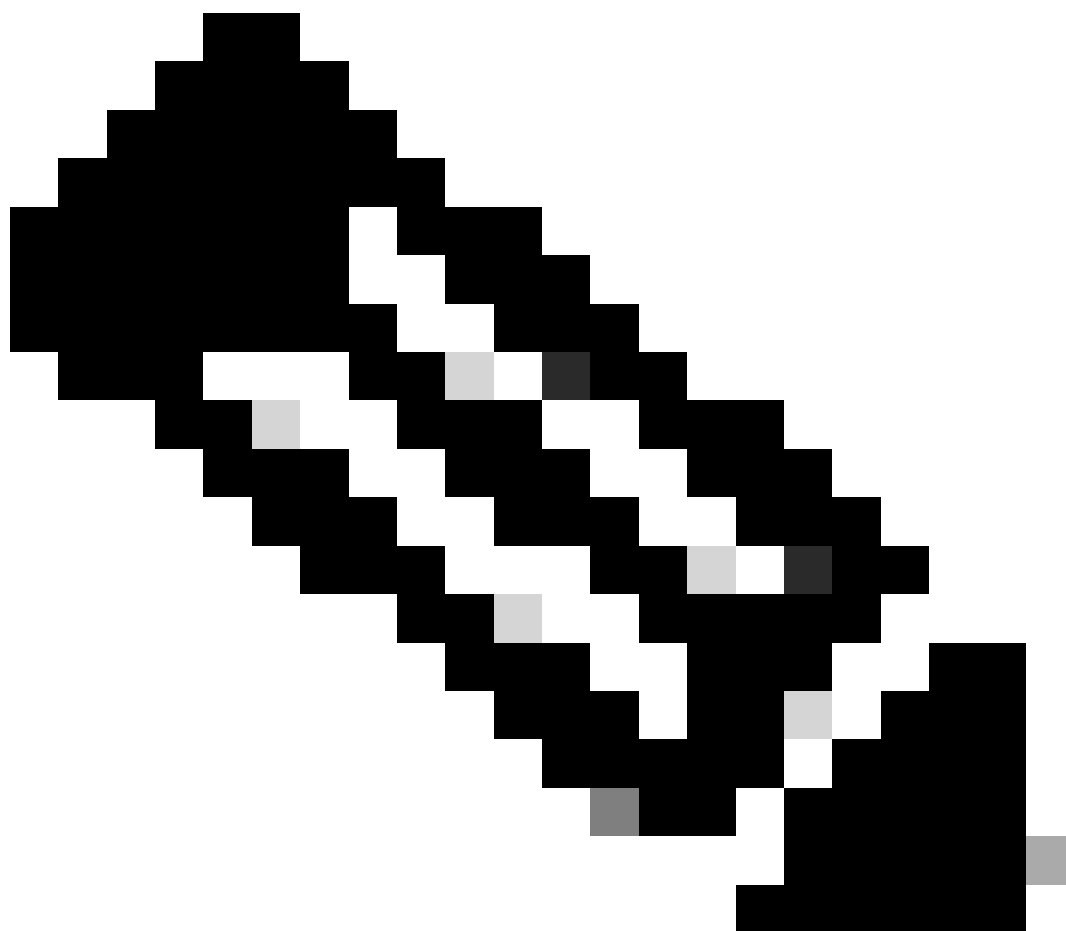
[Help](#)

All Rules

Search by group name

[Advanced search](#)

グループの追加



注：グループはCisco vManageグループと一致している必要があり、小文字にする必要があります。

OKTAでのユーザの設定

1. Directory > Peopleの順に移動します。

Directory



People

Groups

Devices

Profile Editor

Directory Integrations

Profile Sources

2. Add personをクリックし、新しいユーザを作成し、グループに割り当てて保存します。

Add Person

User type ⓘ

First name

Last name

Username

Primary email

Secondary email (optional)

Groups (optional)

Activation

I will set password

ユーザの追加



注:OKTAユーザの代わりにActive Directoryを使用できます。

アプリケーションでのグループとユーザの割り当て

1. 「アプリケーション」 > 「アプリケーション」に移動し、新しいアプリケーションを選択します。
2. Assign > Assign to Groupsの順にクリックします。



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 ▾ 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](#)

アプリケーション>グループ

3. グループを識別し、「割り当て」>「完了」の順にクリックします。

Assign vManage to Groups



Everyone

All users in your organization

Assign



netadmin

Assigned

Done

グループとユーザの割り当て

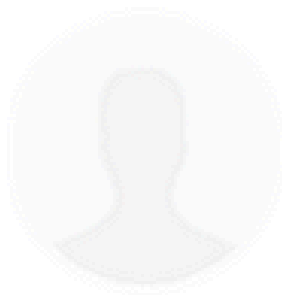
4. グループとユーザーをアプリケーションに割り当てる必要があります。

確認

設定が完了すると、OKTAからCisco vManageにアクセスできます。

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?

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。