

Configurar o Logon Único OKTA (SSO) na SD-WAN

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Background](#)

[Configurar](#)

[Configuração do vManage](#)

[Configuração do OKTA](#)

[Configurações gerais](#)

[Configurar SAML](#)

[Feedback](#)

[Configurar grupos no OKTA](#)

[Configurar usuários no OKTA](#)

[Atribuir grupos e usuários no aplicativo](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como integrar OKTA Single Sing-On (SSO) em uma rede de longa distância definida por software (SD-WAN).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Visão geral da SD-WAN
- SAML (Security Assertion Markup Language, Linguagem de marcação de asserção de segurança)
- Provedor de identidade (IdP)
- Certificados

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco vManage versão 18.3.X ou posterior
- Cisco vManage versão 20.6.3
- Cisco vBond versão 20.6.3
- Cisco vSmart Versão 20.6.3

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Background

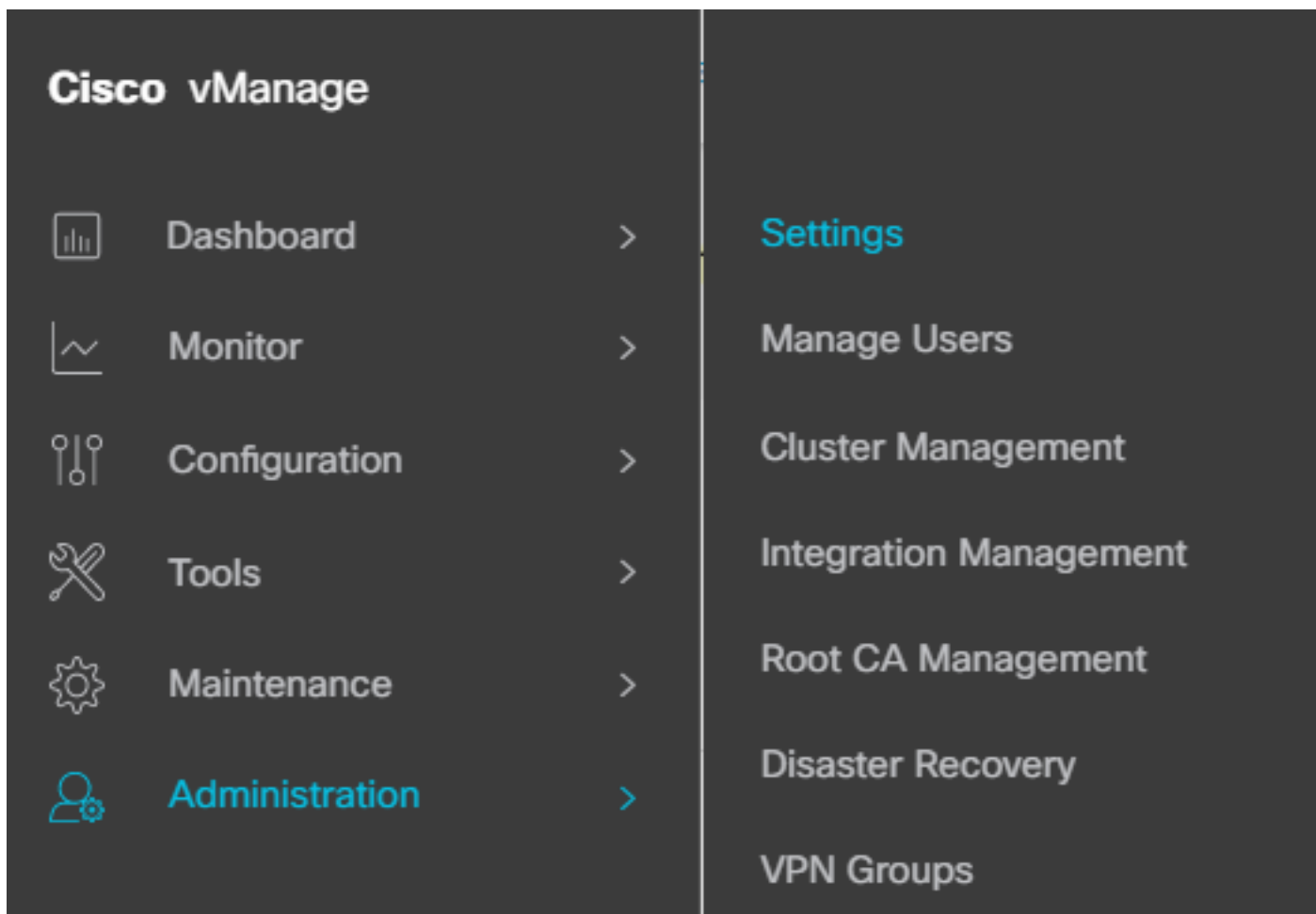
A SAML (Security Assertion Markup Language) é um padrão aberto para o intercâmbio de dados de autenticação e autorização entre as partes, em particular entre um provedor de identidade e um provedor de serviços. Como o nome indica, a SAML é uma linguagem de marcação baseada em XML para asserções de segurança (instruções que os provedores de serviços usam para tomar decisões de controle de acesso).

Um Provedor de Identidade (IdP) é um provedor confiável que permite usar o logon único (SSO) para acessar outros sites. O SSO reduz o cansaço de senhas e melhora a usabilidade. Ele reduz a superfície de ataque potencial e fornece melhor segurança.

Configurar

Configuração do vManage

1. No Cisco vManage, navegue até Administration > Settings > Identify Provider Settings > Edit.



Configuração > Configurações

2. Clique em Enabled.

3. Clique para baixar os metadados SAML e salvar o conteúdo em um arquivo. Isso é necessário no lado OKTA.

Administration Settings

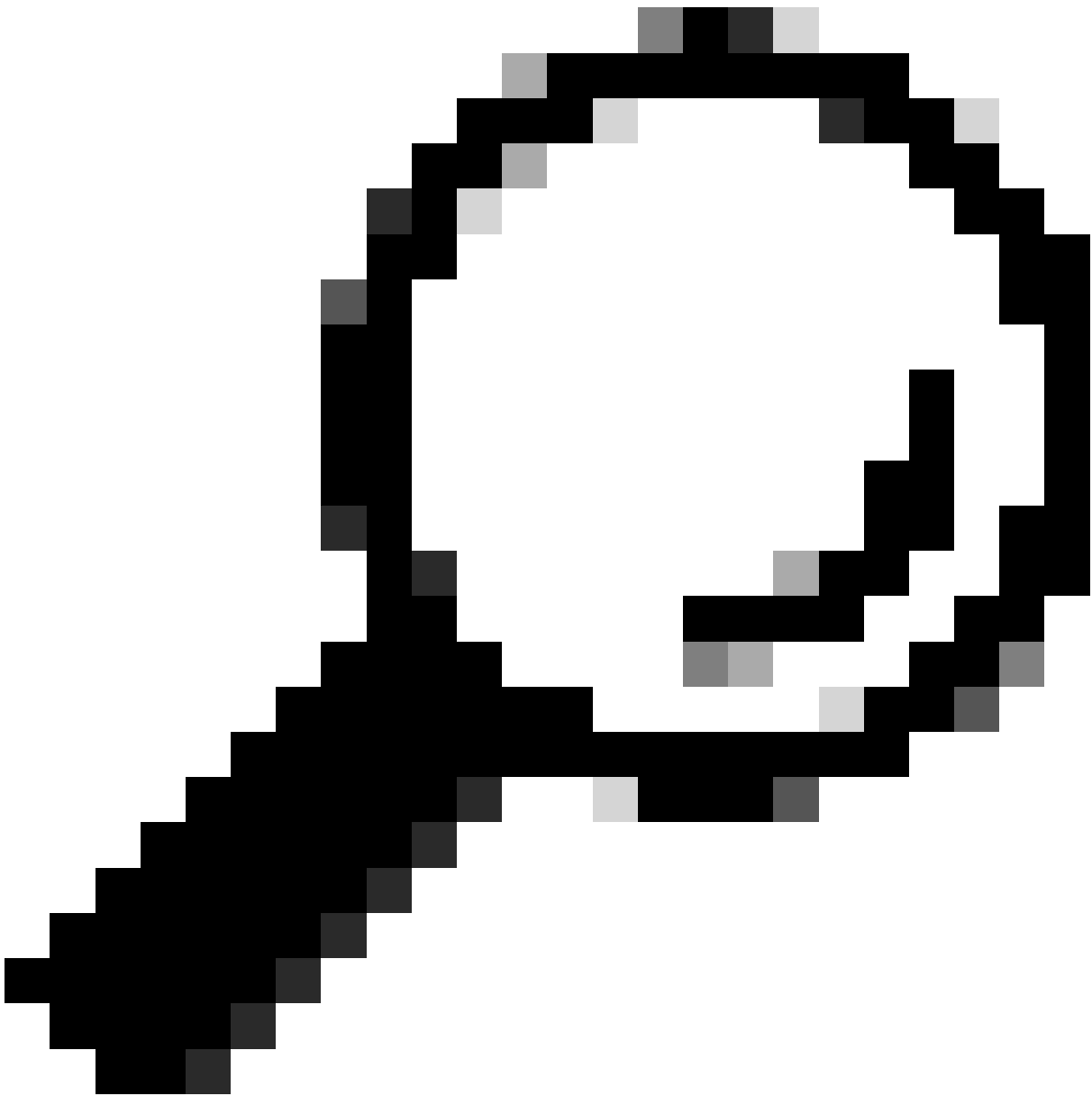
Identity Provider Settings

Disabled

Enable Identity Provider: Enabled Disabled

Upload Identity Provider Metadata

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



Tip: Essas informações são necessárias em METADATA para configurar o OKTA com o Cisco vManage.

- a. ID da entidade
 - b. Assinar certificado
 - c. Certificado de criptografia
 - d. URL de logoff
 - e. URL de logon
-



Note: Os certificados devem estar no formato x.509 e devem ser salvos com a extensão .CRT.

```
-----BEGIN CERTIFICATE-----
MIIDfTCCAmWgAwIBAgIhAM8T9QVLqX/lp1oK/q2XNUbJcGhRmGvqdXxGTUkrKUBhMA0GCSqGSIb3
DQEBCwUAMHlxDDAKBgNVBAYTA1VTQTELMakGA1UECBMCQ0ExETAPBgNVBACTCFNhbiBkb3NlMRQw
EgYDVQQKEwtDSVNDT1JUUExBQjEUMBIGA1UECXMlQ01TQ09SVFBMQUIxVjAUBG9NVBAMTDURlZmF1
bHRUZW5hbnQwHhcNMjAwNTI4MTQxMzQzWWhcNMjUwNTI4MTQxMzQzWjByMQwwCgYDVQQGEwNVU0Ex
CzAJBG9NVBAGTAKNBMRwDwYDVQQHEWhTYW4gSm9zZTEUMBIGA1UEChMLQ01TQ09SVFBMQUIxFDAS
BgNVBAsTC0NlU0NPUlRQTEFCMRYwFAyDVQQDEw1EZWZhdWx0VGVuYW50MIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAg9HOIwjWHD3pbkCB3wRUsn01PTsNAhCqRKof5aY4QDWbu7U3+6gF
TzZgrB9189rLSkbb7cEzRcE7ZbZ1a3zICVw76ZN8jj2BZMYpuTlS9LSGRq2FClYMAg6JU4Yc9prg
T6IcmJKHPfuFM3izXKVsrzfn8tDZ7UDHGIUNPs2kntamU4ZB7BRTE1zJXp+Zh3CvnfLE9g3aXK9
SM9qRFDjAaC8GhWphOYyK3RisQZ/bIZJ2vWkVo91p+6/kQy7/oxFKznK/2oAXaAe26P8HYw+XC0b
mkCwb3e9a1vCGrCmPJwJPjn9j09dX426/LbjdmDAo6HudjTEoQMZduD3Z9GU5QIDAQABMA0GCSqG
SIb3DQEBCwUAA4IBAQBbO/FdHT365rzOHpgHo8YWbxbYdhjAMrHUBbuXLq6MEaHvm4GoTYsgJzc9
Scy/Iwoa6krjBXHJPPthtBwzYYXvK6CJxh8J/rlednlmai0z9growg/sSEgbXPpuQw6qT9hM8s2i
FHlFchPoqiaZFlDNF4iupuzFPTcD8kmzEC3mGlcxfm2TaVjLFDu7McRAMLZTV+yPY+WZXjuoMI8P
hXapKdUt0B6RrxzucBRac2ZB22g7HWDQuDZUzf966Q2k5Us1QxtNlpXLU5X+i+YDW011T2AP6+UUi
vrN1A6vFVPP3QtAd7ao7VziMeEvxfYTuK690b+ej4MntWIKdHneU+/YC
-----END CERTIFICATE-----
```

Certificado X.509

Configuração do OKTA

1. Efetue login na conta [OKTA](#).
2. Navegue até Aplicações > Aplicações.

Applications



Applications

Self Service

Aplicativos > Aplicativos

3. Clique em Criar Integração de Aplicativo.

Applications

Create App Integration

Criar Aplicativo

4. Clique em SAML 2.0 e em 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

Configurar SAML2.0



Configurações gerais


1. Informe um nome de aplicação.
2. Adicione o logotipo para o aplicativo (opcional).
3. Visibilidade do aplicativo (opcional).
4. Clique em PRÓXIMO.



1 General Settings

App name

App logo (optional)  



App visibility Do not display application icon to users

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

Configurações gerais de SAML

Configurar SAML

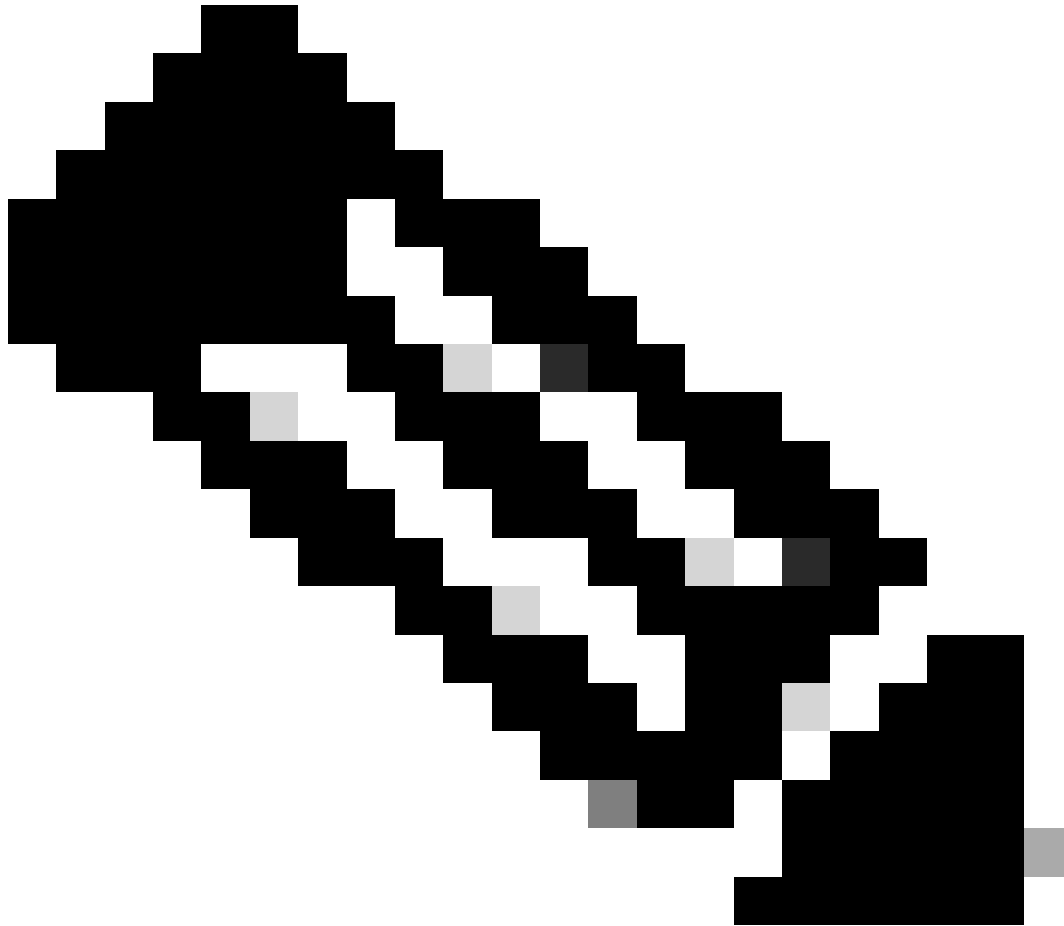
Esta tabela descreve os parâmetros que devem ser configurados nesta seção.

Componente	Valor	Configuração
URL de logon único	https://XX.XX.XX.XX:XXXX/samlLoginResponse	Obtenha-o dos metadados.
URI da Audiência (ID da Entidade SP)	XX.XX.XX.XX	Endereço IP ou DNS para o Cisco vManage

Componente	Valor	Configuração
RelayState padrão		VAZIO
Formato de ID do nome		De acordo com sua preferência
Nome de usuário do aplicativo		De acordo com sua preferência
Atualizar nome de usuário do aplicativo em	Criar e atualizar	Criar e atualizar
Resposta	Assinado	Assinado
Assinatura de Asserção	Assinado	Assinado
Algoritmo de assinatura	RSA-SHA256	RSA-SHA256
Algoritmo Digest	SHA256	SHA256
Criptografia de Asserção	Criptografado	Criptografado
Algoritmo de Criptografia	AES256-CBC	AES256-CBC
Algoritmo de Transporte de Chave	RSA-OAEP	RSA-OAEP
Certificado de criptografia		O certificado de criptografia dos metadados deve estar no formato x.509.

Componente	Valor	Configuração
Habilitar logoff único		deve ser verificado.
URL de logoff único	https://XX.XX.XX.XX:XXXX/samlLogoutResponse	Obter dos metadados.
Emissor SP	XX.XX.XX.XX	Endereço IP ou DNS para vManage
Certificado de assinatura		O certificado de criptografia dos metadados deve estar no formato x.509.
Gancho em linha de asserção	Nenhum(desabilitar)	Nenhum(desabilitar)
Classe de contexto de autenticação	Certificado X.509	
Autenticação da força de honra	Yes	Yes
Cadeia de caracteres de ID do emissor SAML	Cadeia de caracteres de ID do emissor SAML	Digite um texto de cadeia de caracteres
Instruções de Atributos (opcional)	Nome ▶ Nome de usuário Formato do nome (opcional) ▶ Não especificado Valor ▶user.login	Nome ▶ Nome de usuário Formato do nome (opcional) ▶ Não especificado Valor ▶user.login
Declarações de Atributos do Grupo (opcional)	Nome ▶ grupos Formato do nome (opcional) ▶ Não especificado Filtro ▶Corresponde a ▶ regex.*	Nome ▶ grupos Formato do nome (opcional) ▶Não especificado

Componente	Valor	Configuração
		Filtro ▶Corresponde a ▶ regex.*



Note: Deve usar Username e Groups, exatamente como mostrado na tabela 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](#)

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 [?]	<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"/> ▼

[Add Another](#)

Group Attribute Statements (optional)

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

[Add Another](#)

- Clique em Next.

Feedback


1. Selecione uma das opções como sua preferência.
2. Clique em Finalizar.

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](#)

Comentários SMAL

Configurar grupos no OKTA

1. Navegue até Diretório > Grupos.

Directory



People

Groups

Devices

Profile Editor

Directory Integrations

Profile Sources

2. Clique em Adicionar grupo e crie um novo grupo.

Groups

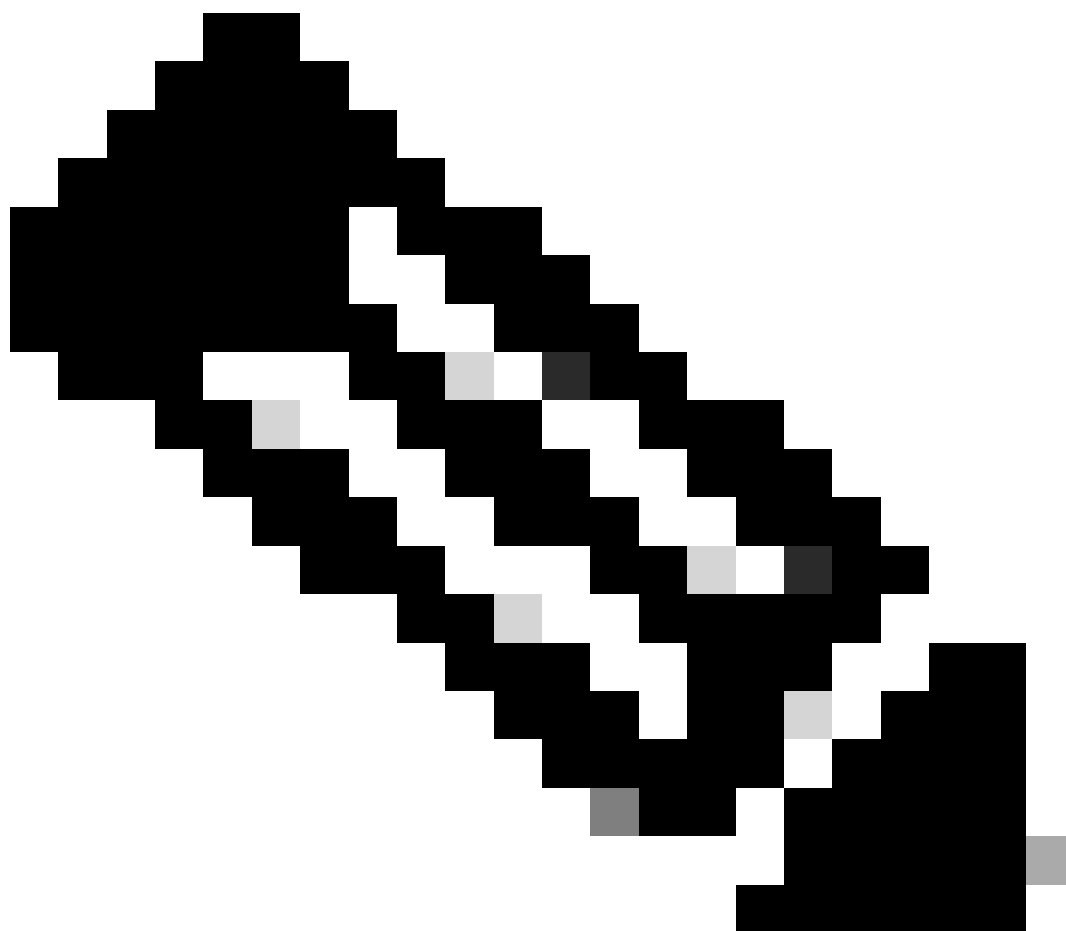
[Help](#)

All Rules

Search by group name

[Advanced search](#)

Adicionar grupo



Note: Os grupos devem corresponder aos grupos do Cisco vManage e devem estar em letras minúsculas.

Configurar usuários no OKTA

1. Navegue até Diretório > Pessoas.

Directory



People

Groups

Devices


Profile Editor

Directory Integrations

Profile Sources

2. Clique em Adicionar pessoa, crie um novo usuário, atribua-o ao grupo e salve-o.

Add Person

User type 

First name

Last name

Username

Primary email

Secondary email (optional)

Groups (optional)

Activation

I will set password

Adicionar usuário



Note: O Ative Directory pode ser usado em vez de usuários OKTA.

Atribuir grupos e usuários no aplicativo

1. Navegue até Aplicações > Aplicações > Selecione a nova aplicação.
2. Clique em Atribuir > Atribuir a Grupos.



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](#)

Assignment

Groups

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](#)

Aplicativo > Grupos

3. Identifique o grupo e clique em Atribuir > Concluído.

Assign vManage to Groups



Everyone

All users in your organization

Assign



netadmin

Assigned

Done

Atribuir grupo e usuário

4. O Grupo e os Usuários agora devem ser atribuídos ao aplicativo.

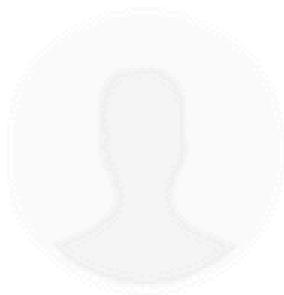
Verificar

Depois que a configuração for concluída, você poderá acessar o Cisco vManage por meio do OKTA.

Connecting to

Sign-in with your cisco-org-958976 account to access vManage

okta



Sign In

Username

Password

Remember me

Sign In

Need help signing in?

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.