

Configuración de OKTA Single Sign-On (SSO) en SD-WAN

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Background](#)

[Configurar](#)

[Configuración de vManage](#)

[Configuración de OKTA](#)

[Configuración general](#)

[Configurar SAML](#)

[Comentarios](#)

[Configurar grupos en OKTA](#)

[Configurar usuarios en OKTA](#)

[Asignar grupos y usuarios en la aplicación](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo integrar OKTA Single Sign-On (SSO) en una red de área extensa definida por software (SD-WAN).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Descripción general de SD-WAN
- Lenguaje de marcado de aserción de seguridad (SAML)
- Proveedor de identidad (IdP)
- Certificados

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y

hardware.

- Cisco vManage versión 18.3.X o posterior
- Cisco vManage versión 20.6.3
- Cisco vBond versión 20.6.3
- Cisco vSmart versión 20.6.3

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Background

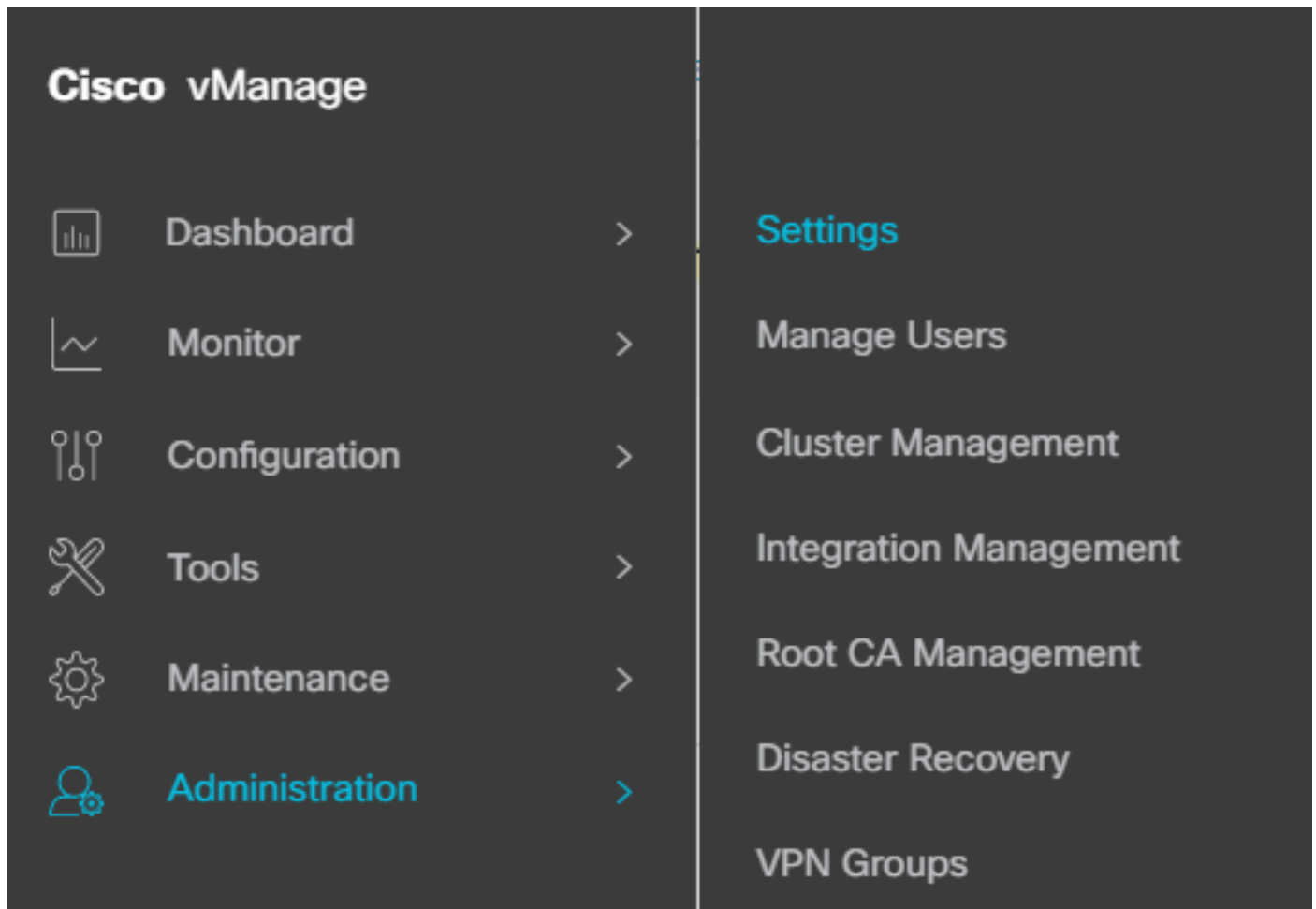
El lenguaje de marcado de aserción de seguridad (SAML) es un estándar abierto para intercambiar datos de autenticación y autorización entre partes, en particular, entre un proveedor de identidad y un proveedor de servicios. Como su nombre indica, SAML es un lenguaje de marcado basado en XML para las afirmaciones de seguridad (instrucciones que utilizan los proveedores de servicios para tomar decisiones de control de acceso).

Un proveedor de identidad (IdP) es un proveedor de confianza que le permite utilizar el inicio de sesión único (SSO) para acceder a otros sitios web. SSO reduce la fatiga de las contraseñas y mejora la facilidad de uso. Reduce la superficie de ataque potencial y proporciona una mayor seguridad.

Configurar

Configuración de vManage

1. En Cisco vManage, navegue hasta Administration > Settings > Identity Provider Settings > Edit.



Configuración > Configuración

2. Haga clic en Habilitado.

3. Haga clic para descargar los metadatos SAML y guardar el contenido en un archivo. Esto es necesario en el lado de OKTA.

Administration Settings

Identity Provider Settings

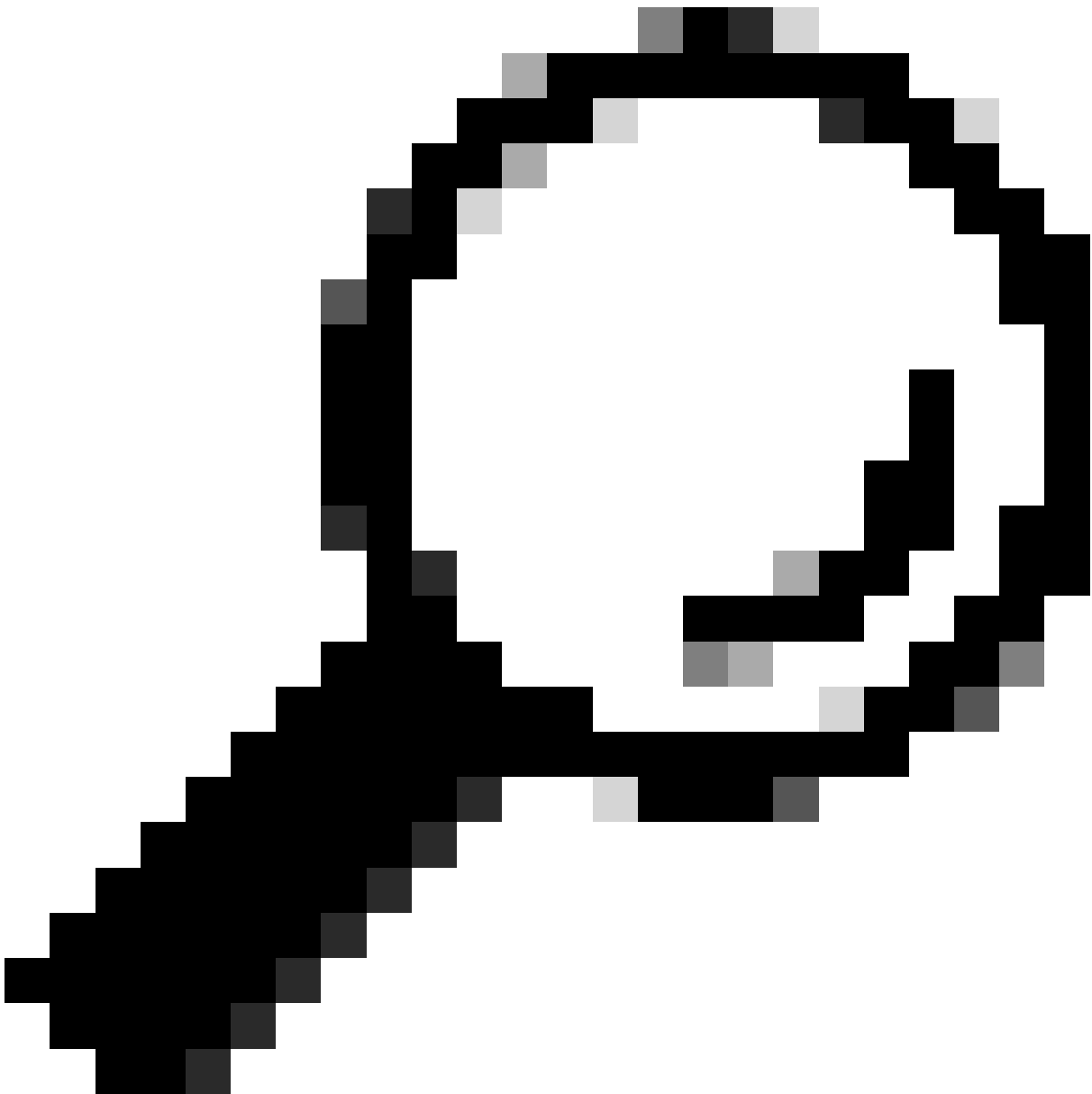
Disabled

Enable Identity Provider: Enabled Disabled

Upload Identity Provider Metadata

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

Descargar SAML



Consejo: Necesita esta información de METADATA para configurar OKTA con Cisco vManage.

- a. ID de entidad
 - b. Firmar certificado
 - c. Certificado de cifrado
 - d. URL de cierre de sesión
 - e. URL de inicio de sesión
-



Nota: Los certificados deben estar en formato x.509 y deben guardarse con la extensión .CRT.

```
-----BEGIN CERTIFICATE-----  
MIIDfTCCAmWgAwIBAgIhAM8T9QVLqX/lp1oK/q2XNUbJcGhRmGvqdXxGTUkrKUBhMA0GCSqGSIb3  
DQEBCwUAMHIxDDAKBgNVBAYTA1VTQTELMakGA1UECBMCQ0ExETAPBgNVBACTCFNhbiBkb3NlMRQw  
EgYDVQQKEwtDSVNDT1JUUExBQjEUMBIGA1UECXMlQ01TQ09SVFBMQUIxIjANBgkqhkiG9w0B  
bHRUZW5hbnQwHhcNMjAwNTI4MTQxMzQzWWhcNMjUwNTI4MTQxMzQzWjByMQwwCgYDVQQGEwNVU0Ex  
CzAJBGNVBAGTAkNBREwDwYDVQQHEWhTYW4gSm9zZTEUMBIGA1UEChMLQ01TQ09SVFBMQUIxFDAS  
BgNVBAsTC0NlU0NPUlRQTEFCMRyYwFAyDVQQDEw1EZWZhdWw0VGVuYW50MIIBIjANBgkqhkiG9w0B  
AQEFAAOCAQ8AMIIBCgKCAQEAg9HOIwjWHD3pbkCB3wRUsn01PTsNAhCqRKof5aY4QDWbu7U3+6gF  
TzZgrB9189rLskkb7cEzRcE7ZbZ1a3zICVw76ZN8jj2BZMYpuTLS9LSGRq2FC1YMAg6JU4Yc9prg  
T6IcmJKHPfuFM3izXKVsrzfn8tDZ7UDHGIUNPs2kjtamU4ZB7BRTE1zJXp+Zh3CvnfLE9g3aXK9  
SM9qRFDjAaC8GhWphOYyK3RisQZ/bIZJ2vWkVo91p+6/kQy7/oxFKznK/2oAXaAe26P8HYw+XC0b  
mkCwb3e9a1vCGrCmPJwJPjn9j09dX426/LbjdmDAo6HudjTEoQMZduD3Z9GU5QIDAQABMA0GCSqG  
SIb3DQEBCwUAA4IBAQBbO/FdHT365rzOHpgHo8YWbxbYdhjAMrHUBbuXLq6MEaHvm4GoTYsgJzc9  
Scy/Iwoa6krjBXHJPPthtBwzYYXvK6CJxh8J/rlednlmai0z9growg/sSEgbXPpuQw6qT9hM8s2i  
FHlFchPogiazFldNF4iupuzFPTcD8kmzEC3mGlcfm2TaVjLFdu7McRAMLZTV+yPY+WZXjuoMI8P  
hXapKdUt0B6RrxzucBRac2ZB22g7HWDQuDZUzf966Q2k5Us1QxtNlpXLU5X+i+YDW011T2AP6+UUi  
vrN1A6vFVPP3QtAd7ao7VziMeEvxfYTuK690b+ej4MntWIKdHneU+/YC  
-----END CERTIFICATE-----
```

Certificado X.509

Configuración de OKTA

1. Inicie sesión en la cuenta [OKTA](#).
2. Acceda a Aplicaciones > Aplicaciones.

Applications



Applications

Self Service

Aplicaciones > Aplicaciones

3. Haga clic Crear integración de aplicaciones.

Applications

Create App Integration

Crear aplicación

4. Haga clic en SAML 2.0 y siguiente.

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

Configuración de SAML2.0

Configuración general

1. Introduzca un nombre de aplicación.
2. Añadir logotipo para la aplicación (opcional).
3. Visibilidad de la aplicación (opcional).
4. Haga clic en NEXT.



1 General Settings

App name

App logo (optional)

App visibility Do not display application icon to users

[Cancel](#) Next

Configuración general de SAML

Configurar SAML

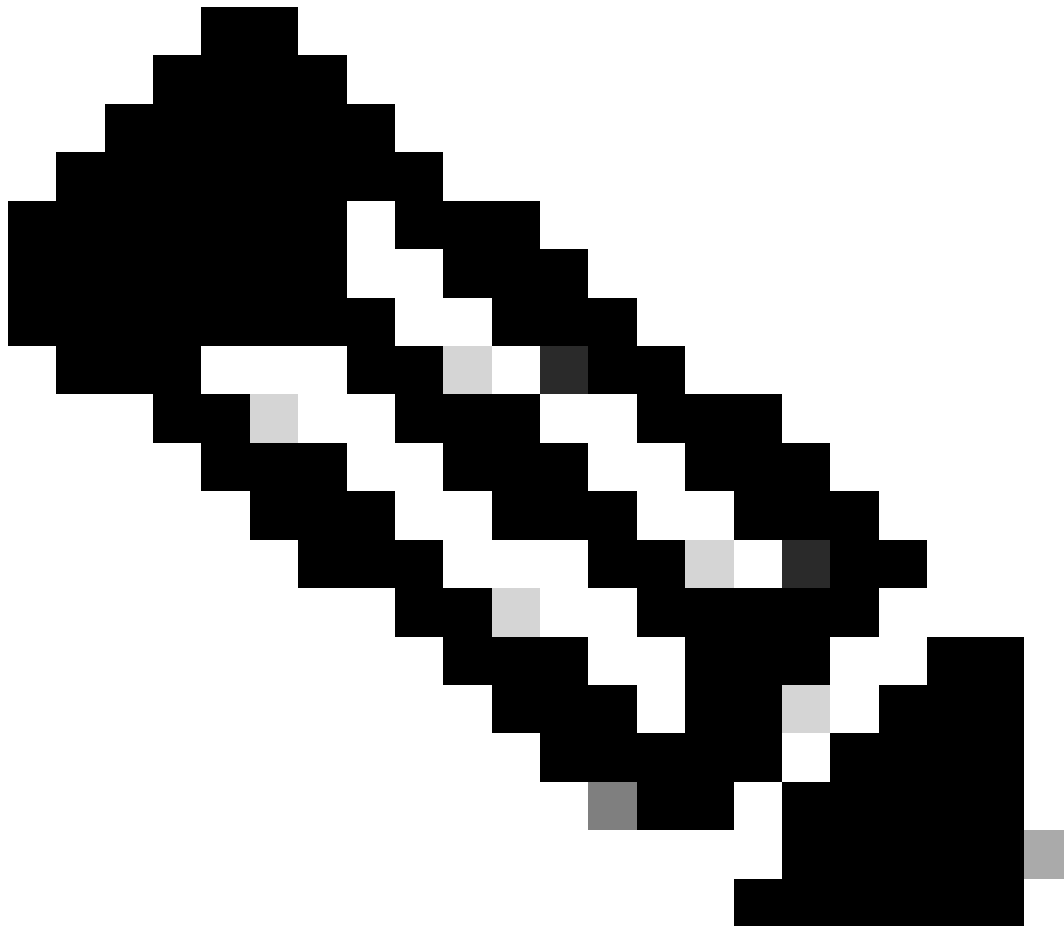
Esta tabla describe los parámetros que deben configurarse en esta sección.

Componente	Valor	Configuración
URL de inicio de sesión único	https://XX.XX.XX.XX:XXXX/samlLoginResponse	Consígalo a partir de los metadatos.
URI de público (ID de entidad SP)	XX.XX.XX.XX	Dirección IP o DNS para Cisco vManage

Componente	Valor	Configuración
Estado de retransmisión predeterminado		EMPTY
Formato de ID de nombre		Según sus preferencias
Nombre de usuario de aplicación		Según sus preferencias
Actualizar nombre de usuario de aplicación en	Crear y actualizar	Crear y actualizar
Respuesta	Firmado	Firmado
Firma de aserción	Firmado	Firmado
Algoritmo de firma	RSA-SHA256	RSA-SHA256
Algoritmo de resumen	SHA256	SHA256
Cifrado de aserción	Cifrados	Cifrados
Algoritmo de encriptación	AES256-CBC	AES256-CBC
Algoritmo de transporte de claves	RSA-OAEP	RSA-OAEP
Certificado de cifrado		El certificado de cifrado de los metadatos debe estar en el formato x.509.
Activar cierre de		debe estar comprobado.

Componente	Valor	Configuración
sesión único		
URL de cierre de sesión único	https://XX.XX.XX.XX:XXXX/samlLogoutResponse	Obtenga de los metadatos.
Emisor SP	XX.XX.XX.XX	Dirección IP o DNS para vManage
Certificado de firma		El certificado de cifrado de los metadatos debe estar en el formato x.509.
Gancho en línea de aserción	Ninguno (deshabilitar)	Ninguno (deshabilitar)
Clase de contexto de autenticación	Certificado X.509	
Autenticación de fuerza de honor	Yes	Yes
cadena de ID del emisor SAML	cadena de ID del emisor SAML	Escriba un texto de cadena
Sentencias Attributes (opcional)	Nombre ▶ Nombre de usuario Formato de nombre (opcional) ▶ No especificado Valor ▶ usuario.login	Nombre ▶ Nombre de usuario Formato de nombre (opcional) ▶ No especificado Valor ▶ usuario.login
Sentencias de atributo de grupo (opcional)	Nombre ▶ Grupos Formato de nombre (opcional) ▶ No especificado Filtro ▶ Coincide con regex ▶.*	Nombre ▶ Grupos Formato de nombre (opcional) ▶ Sin especificar Filtro ▶ Coincide con regex

Componente	Valor	Configuración
		▶.*



Nota: Debe utilizar Username y Groups, exactamente como se muestra en la tabla 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](#)

- Haga clic en Next (Siguiente).

Comentarios


1. Seleccione una de las opciones que prefiera.
2. Haga clic en 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

Comentarios sobre SMALL

Configurar grupos en OKTA

1. Navegue hasta Directorio > Grupos.

Directory



People

Groups

Devices

Profile Editor

Directory Integrations

Profile Sources

2. Haga clic en Agregar grupo y cree un nuevo grupo.

Groups

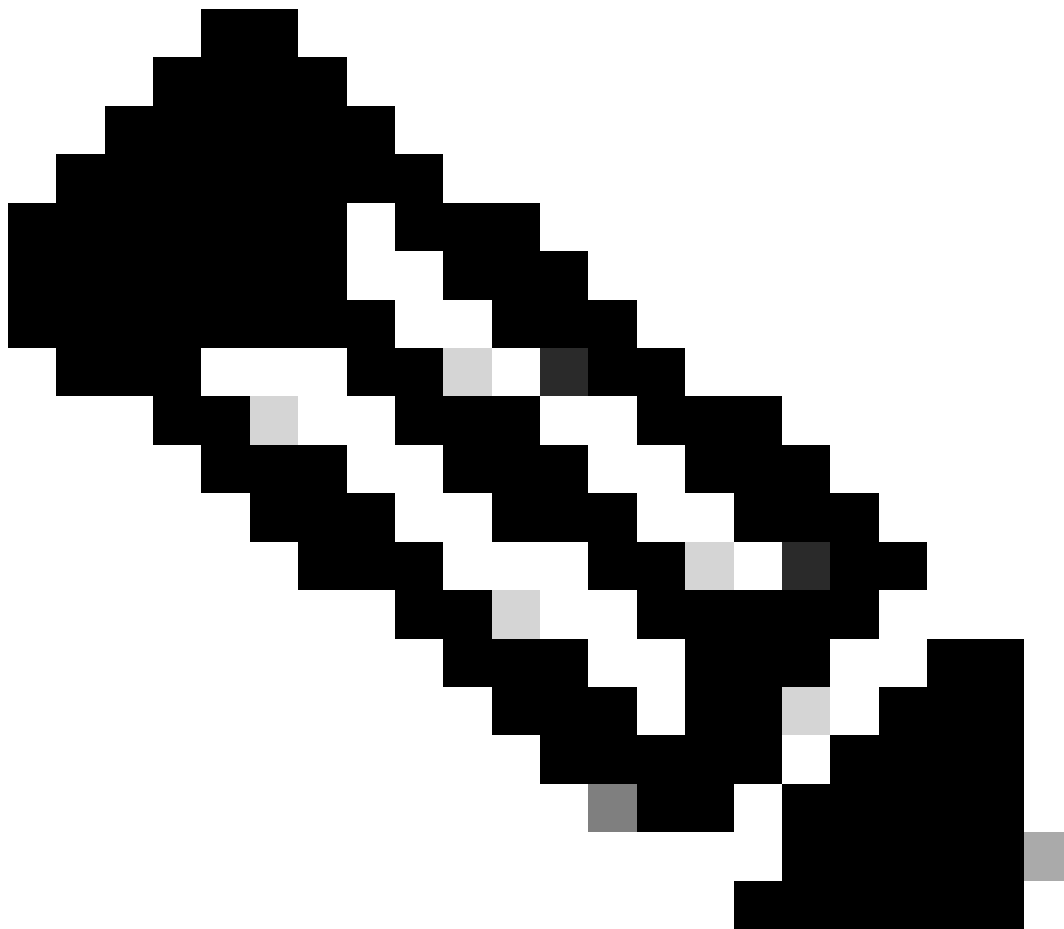
[Help](#)

All Rules

Search by group name

[Advanced search](#)

Agregar grupo



Nota: Los grupos deben coincidir con los grupos de Cisco vManage y deben estar en minúsculas.

Configurar usuarios en OKTA

1. Acceda a Directorio > Personas.

Directory



People

Groups

Devices


Profile Editor

Directory Integrations

Profile Sources

2. Haga clic en Agregar persona, cree un nuevo usuario, asígnelo al grupo y guárdelo.

Add Person

User type 

First name

Last name

Username

Primary email

Secondary email (optional)

Groups (optional)

Activation

I will set password

Agregar usuario



Nota: Se puede utilizar Active Directory en lugar de usuarios de OKTA.

Asignar grupos y usuarios en la aplicación

1. Acceda a Aplicaciones > Aplicaciones > Seleccione la nueva aplicación.
2. Haga clic en Asignar > Asignar a grupos.



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** ▾ **Groups** ▾

Assign to People
Assign to 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](#)

Aplicación > Grupos

3. Identifique el grupo y haga clic en Asignar > Finalizado.

Assign vManage to Groups



Everyone

All users in your organization

Assign



netadmin

Assigned

Done

Asignar grupo y usuario

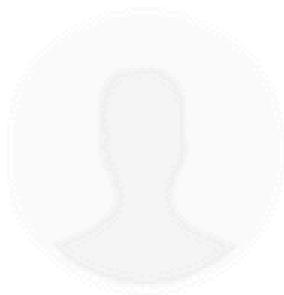
4. El grupo y los usuarios ahora deben ser asignados a la aplicación.

Verificación

Una vez completada la configuración, puede obtener acceso a Cisco vManage a través de 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?

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).