

Configurazione di OKTA Single Sign-On (SSO) su SD-WAN

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Introduzione](#)

[Configurazione](#)

[Configurazione vManage](#)

[Configurazione OKTA](#)

[Impostazioni generali](#)

[Configura SAML](#)

[Feedback](#)

[Configura gruppi in OKTA](#)

[Configura utenti in OKTA](#)

[Assegna gruppi e utenti nell'applicazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive come integrare OKTA Single Sign-On (SSO) su una rete Wide Area Network (SD-WAN) definita dal software.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Panoramica generale su SD-WAN
- SAML (Security Assertion Markup Language)
- Provider di identità (IdP)
- Certificati

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e

hardware:

- Cisco vManage release 18.3.X o successive
- Cisco vManage versione 20.6.3
- Cisco vBond versione 20.6.3
- Cisco vSmart versione 20.6.3

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Introduzione

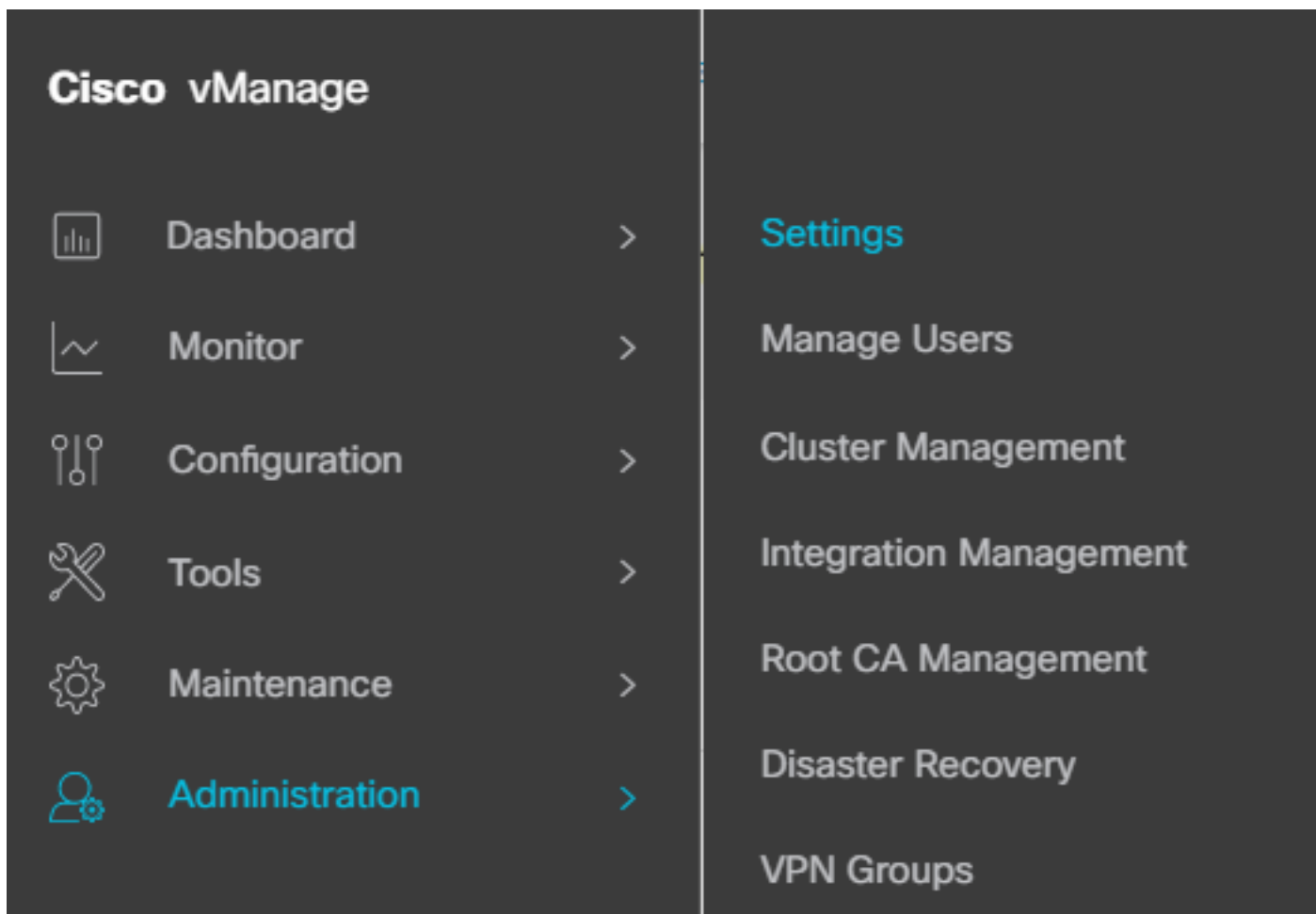
Il linguaggio SAML (Security Assertion Markup Language) è uno standard aperto per lo scambio di dati di autenticazione e autorizzazione tra parti, in particolare tra un provider di identità e un provider di servizi. Come indica il nome, SAML è un linguaggio di markup basato su XML per le asserzioni di sicurezza (istruzioni utilizzate dai provider di servizi per prendere decisioni sul controllo dell'accesso).

Un provider di identità (IdP) è un provider attendibile che consente di utilizzare Single Sign-On (SSO) per accedere ad altri siti Web. L'SSO riduce l'usura delle password e migliora la fruibilità. Diminuisce la superficie di attacco potenziale e fornisce una migliore sicurezza.

Configurazione

Configurazione vManage

1. In Cisco vManage, selezionare Administration > Settings > Identify Provider Settings > Edit (Amministrazione > Impostazioni > Identifica impostazioni provider).



Configurazione > Impostazioni

2. Fare clic su Abilitato.

3. Fare clic per scaricare i metadati SAML e salvare il contenuto in un file. Ciò è richiesto dalla parte dell'OKTA.

Administration Settings

Identity Provider Settings

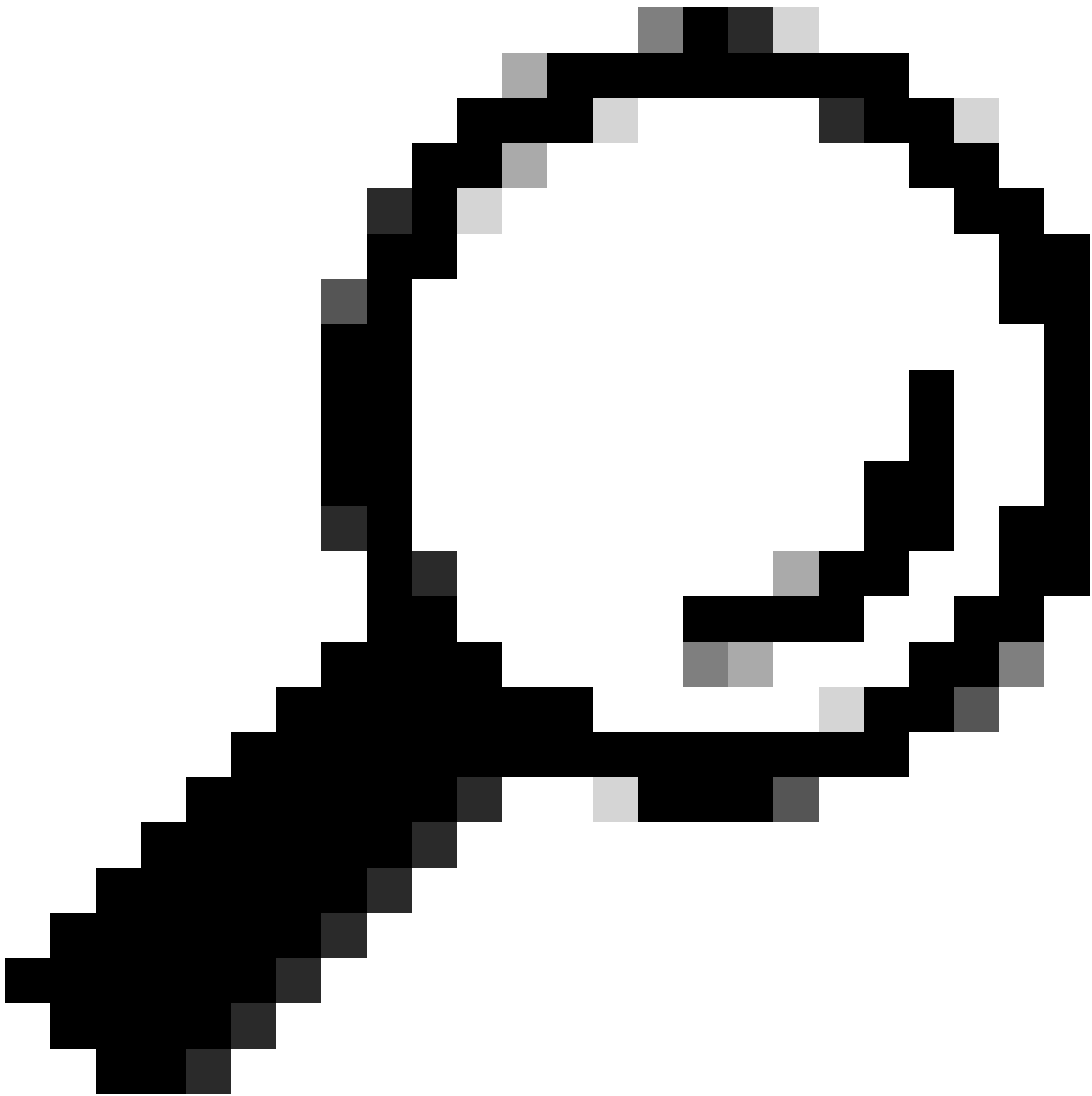
Disabled

Enable Identity Provider: Enabled Disabled

Upload Identity Provider Metadata

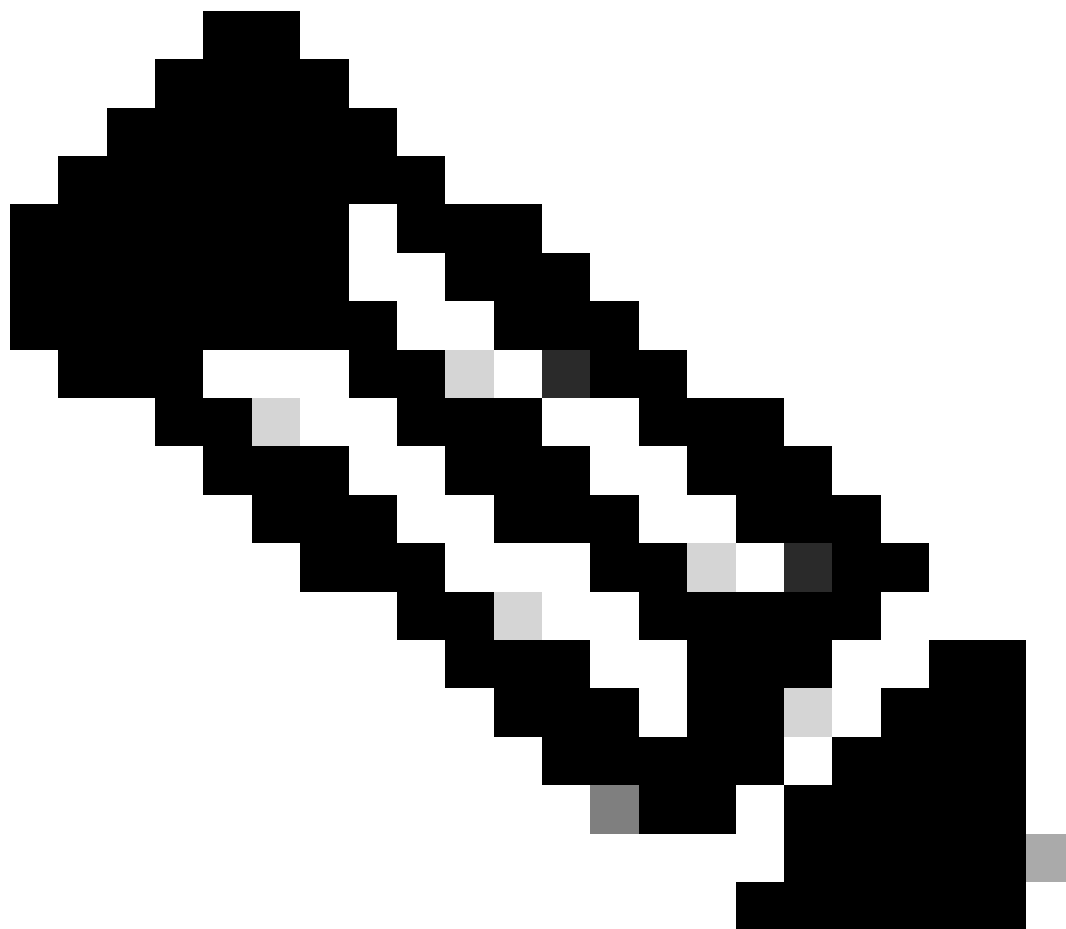
[↓ Click here to download SAML metadata](#)

Scarica SAML



Suggerimento: Queste informazioni provenienti da METADATA sono necessarie per configurare OKTA con Cisco vManage.

- r. ID entità
 - b. Firma certificato
 - c. Certificato di crittografia
 - d. URL di disconnessione
 - e. URL di accesso
-



Nota: I certificati devono essere nel formato x.509 e devono essere salvati con estensione .CRT.

```
-----BEGIN CERTIFICATE-----
MIIDfTCCAmWgAwIBAgIhAM8T9QVLqX/lp1oK/q2XNUbJcGhRmGvqdXxGTUkrKUBhMA0GCSqGSIb3
DQEBCwUAMHlxDDAKBgNVBAYTA1VTQTELMakGA1UECBMCQ0ExETAPBgNVBACTCFNhbiBkb3NlMRQw
EgYDVQQKEwtDSVNDT1JUUExBQjEUMBIGA1UECXMlQ01TQ09SVFBMQUIxLjZmF1bHRUZW5hbnQw
HhcNMjAwNTI4MTQxMzQzWWhcNMjUwNTI4MTQxMzQzWjByMQwwCgYDVQQGEwNVU0ExCzAJBgNV
BAGTAkNBREwDwYDVQQHEwhTYW4gSm9zZTEUMBIGA1UEChMLQ01TQ09SVFBMQUIxFDASBgNVBAsTC0
NJU0NPUlRQTEFCMRYwFAyDVQQDEw1EZWZhdWx0VGVuYW50MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8
AMIIBCgKCAQEAg9HOIwjWHD3pbkCB3wRUsn01PTsNAhCqRKof5aY4QDWbu7U3+6gFTzZgrB9189r
LSkbb7cEzRcE7ZbZ1a3zICVw76ZN8jj2BZMYpuTlS9LSGRq2FClYMAg6JU4Yc9prgT6IcmJKHPfu
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-----
```

Certificato X.509

Configurazione OKTA

1. Accedere all'account [OKTA](#).
2. Passare a Applicazioni > Applicazioni.

Applications



Applications

Self Service

Applicazioni > Applicazioni

3. Fare clic su Creare l'integrazione delle applicazioni.

Applications

Create App Integration

Crea applicazione

4. Fare clic su SAML 2.0 e avanti.

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

Configurazione di SAML2.0

Impostazioni generali

1. Inserire il nome dell'applicazione.
2. Aggiungere il logo per l'applicazione (facoltativo).
3. Visibilità dell'app (opzionale).
4. Fare clic su NEXT (AVANTI).



1 General Settings

2 Configure SAML

App name

App logo (optional)

App visibility Do not display application icon to users

Cancel
Next

Impostazioni generali SAML

Configura SAML

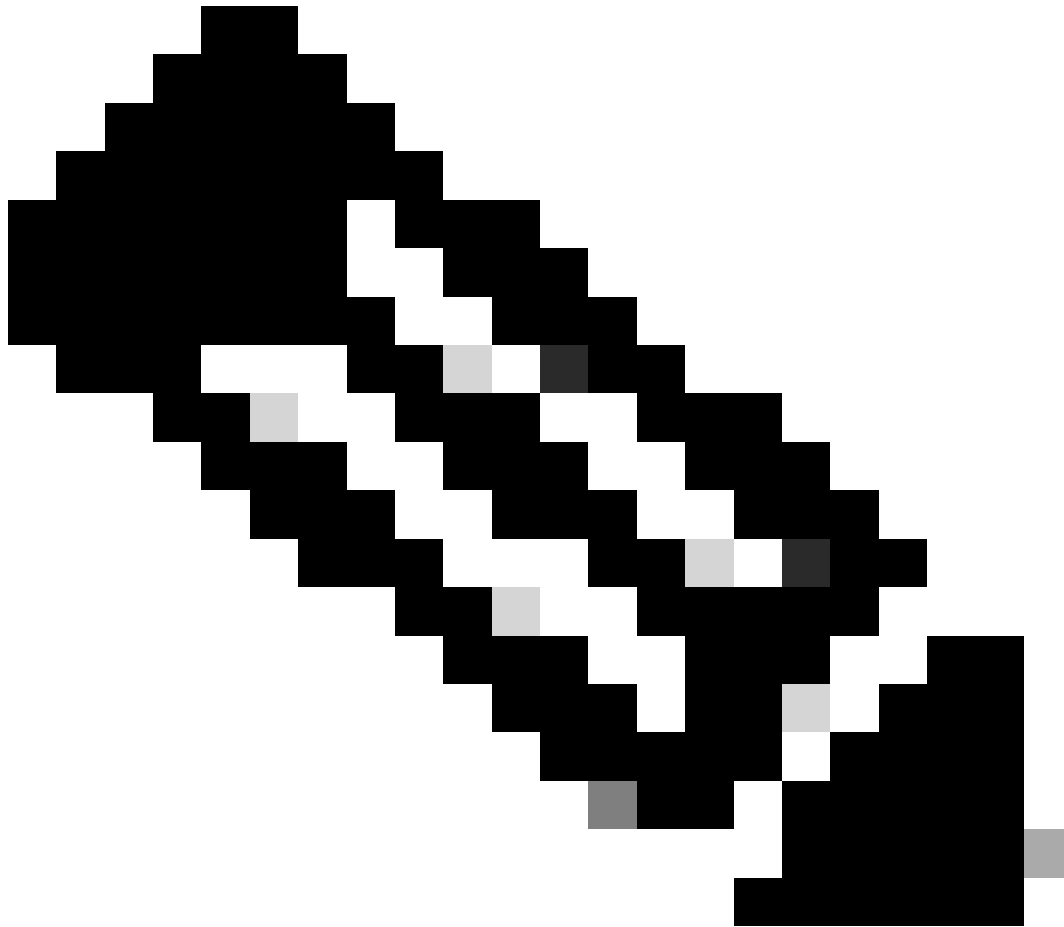
Questa tabella descrive i parametri che devono essere configurati in questa sezione.

Componente	Valore	Configurazione
URL Single Sign-On	https://XX.XX.XX.XX:XXXX/samlLoginResponse	Ottenetelo dai metadati.
URI gruppo di destinatari (ID entità SP)	XX.XX.XX.XX	Indirizzo IP o DNS per Cisco vManage

Componente	Valore	Configurazione
RelayState predefinito		VUOTO
Formato ID nome		In base alle tue preferenze
Nome utente applicazione		In base alle tue preferenze
Aggiorna nome utente applicazione in	Crea e aggiorna	Crea e aggiorna
Risposta	Firmato	Firmato
Firma asserzione	Firmato	Firmato
Algoritmo della firma	RSA-SHA256	RSA-SHA256
Algoritmo con classificazione	SHA256	SHA256
Assertion Encryption	Crittografia	Crittografia
Algoritmo di crittografia	AES256-CBC	AES256-CBC
Algoritmo di trasporto chiave	RSA-OAEP	RSA-OAEP
Certificato di crittografia		Il certificato di crittografia dai metadati deve essere nel formato x.509.
Abilita		devono essere controllate.

Componente	Valore	Configurazione
disconnessione singola		
URL di disconnessione singolo	https://XX.XX.XX.XX:XXXX/samlLogoutResponse	Ottieni dai metadati.
Emittente SP	XX.XX.XX.XX	Indirizzo IP o DNS per vManage
Certificato di firma		Il certificato di crittografia dai metadati deve essere nel formato x.509.
Hook inline asserzione	Nessuno(disabilita)	Nessuno(disabilita)
Classe contesto di autenticazione	Certificato X.509	
Rispetta autenticazione forzata	Sì	Sì
Stringa ID autorità emittente SAML	Stringa ID autorità emittente SAML	Digitare una stringa di testo
Istruzioni Attributes (facoltativo)	Nome ► Nome utente Formato del nome (facoltativo) ► Non specificato Valore ► user.login	Nome ► Nome utente Formato del nome (facoltativo) ► Non specificato Valore ► user.login
Istruzioni attributi gruppo (facoltativo)	Nome ► Gruppi Formato del nome (facoltativo) ► Non specificato	Nome ► Gruppi Formato del nome (facoltativo) ► Non

Componente	Valore	Configurazione
	Filter ▶ Corrisponde a regex ▶.*	specificato Filter ▶ Corrisponde a regex ▶.*



Nota: È necessario utilizzare Username e Groups, esattamente come mostrato nella tabella 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 ⓘ

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"/> ▼

[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](#)

- Fare clic su Next (Avanti).

Feedback


1. Selezionare una delle opzioni come preferenza.
2. Fare clic su Fine.

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

Feedback di piccole dimensioni

Configura gruppi in OKTA

1. Passare a Directory > Gruppi.

Directory



People

Groups

Devices

Profile Editor

Directory Integrations

Profile Sources

2. Fare clic su Aggiungi gruppo e creare un nuovo gruppo.

Groups

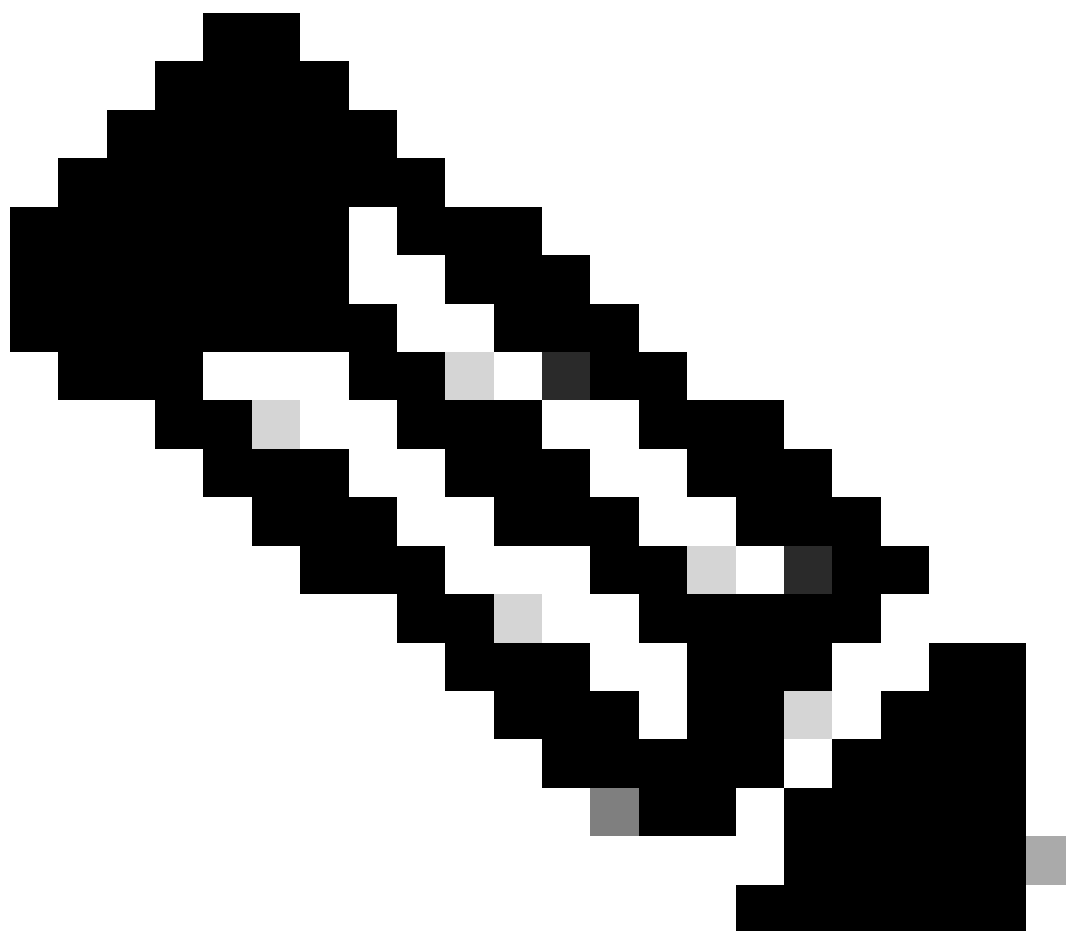
[Help](#)

All Rules

Search by group name

[Advanced search](#)

Aggiungi gruppo



Nota: I gruppi devono corrispondere ai gruppi Cisco vManage e devono essere scritti in minuscolo.

Configura utenti in OKTA

1. Selezionare Directory > Persone.

Directory



People

Groups

Devices


Profile Editor

Directory Integrations

Profile Sources

2. Fare clic su Aggiungi persona, creare un nuovo utente, assegnarlo al gruppo e salvarlo.

Add Person

User type 

First name

Last name

Username

Primary email

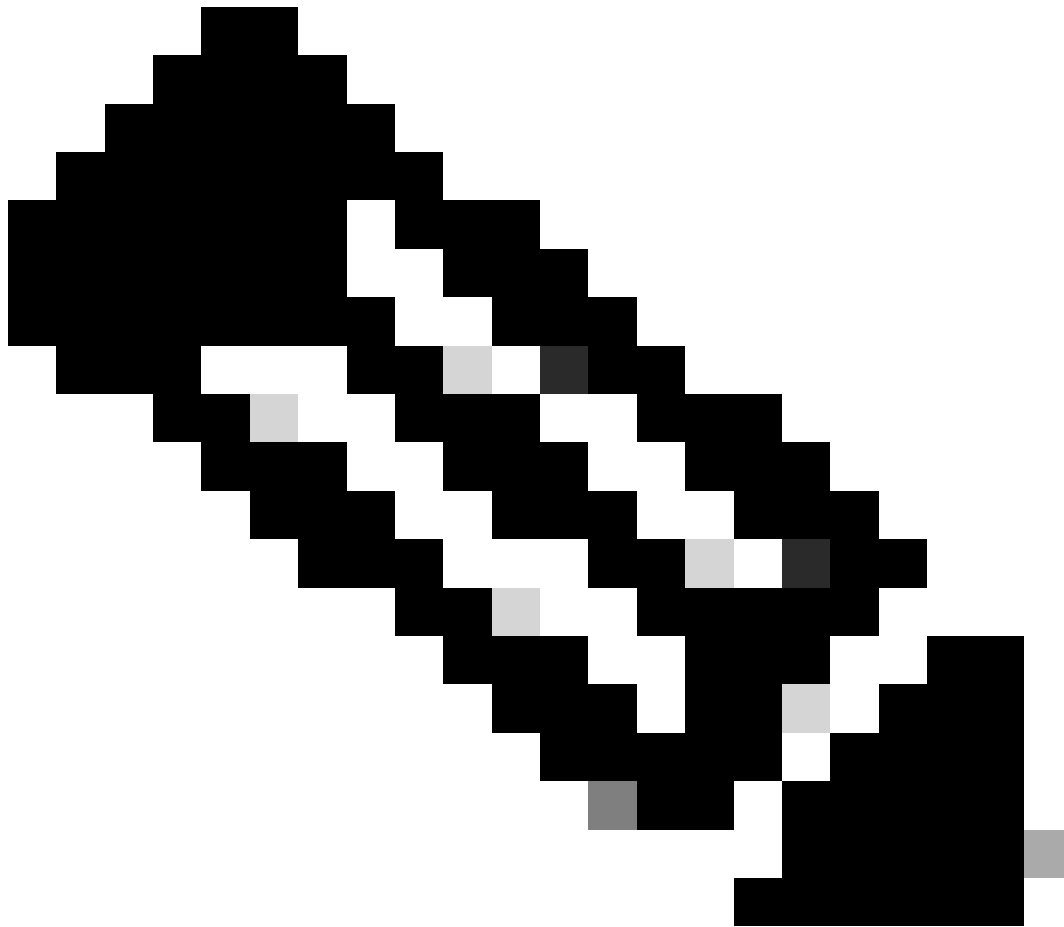
Secondary email (optional)

Groups (optional)

Activation

I will set password

Aggiungi utente



Nota: È possibile utilizzare Active Directory al posto degli utenti OKTA.

Assegna gruppi e utenti nell'applicazione

1. Passare a Applicazioni > Applicazioni > Selezionare la nuova applicazione.
2. Fare clic su Assegna > Assegna a gruppi.



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

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](#)

Applicazione > Gruppi

3. Identificate il gruppo e fate clic su Assegna (Assign) > Fatto (Done).

Assign vManage to Groups



Everyone

All users in your organization

Assign



netadmin

Assigned

Done

Assegna gruppo e utente

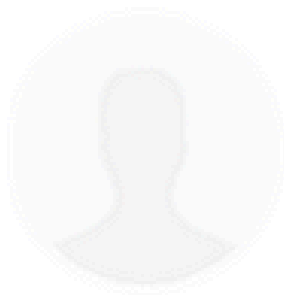
4. A questo punto, Gruppo e Utenti devono essere assegnati all'applicazione.

Verifica

Una volta completata la configurazione, è possibile accedere a Cisco vManage tramite 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?

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).