

---

## Configure Single Sign-On Using Director

 For supported software information, click [here](#).

This article describes how to configure single sign-on (SSO) on Director nodes.

SSO is a session and user authentication service that allows a user to use a single set of login credentials to access multiple applications. The service authenticates all the applications for which the user has the required rights and eliminates further prompts when you switch applications during the same session. On the backend, SSO logs user activities and monitors user accounts. In the context of Versa Director, the service provider offers SSO as a login mechanism to different integrators and clients.

For SSO, Versa Director supports the following:

- Security Assertion Markup Language (for Releases 20.2 and later)—SAML is an XML-based, open standard data format for exchanging authentication data and authorization data between an identity provider and a service provider.
- OpenID connect SSO methods

Versa Director enables identity provider (IDP)-based and local user authentication.

Versa Director supports two types of SSO:

- Service provider (SP)-initiated SSO—Allows you to access the Versa Director when you click on the Login with Single Sign-On link on the Director login page. This redirects you to the IDP page for authentication and then redirects you to the Director node.
- IDP-initiated SSO— Allows you to access Versa Director after authenticating on the customer's portal and redirects you directly to the Director node.

Director and Analytics SSO have been tested tested with the ADFS, Okta, OneLogin, and Ping Identity IDPs.

To configure SSO on a Director node, you do the following:

1. Configure Director SP-initiated SSO, or configure Director IDP-initiated SSO.
2. Configure an IDP.
3. Access the Director node using SSO.

For SSO to work properly, you must enable clock synchronization on the Director node. For more information, see [Configure an NTP Server](#) and [Configure the Time Zone](#) in [Configure Systemwide Functions](#).

---

## Configure SAML-Based SSO

*For Releases 20.2 and later.*

A service provider–initiated SSO flow operation is started from the service provider and is performed in the following sequence:

1. The service provider creates an authentication request and redirects you to the IDP.
2. The IDP requests your credentials, validates you, and redirects you to service provider with the login response.
3. The service provider validates the login response and, if the validation is successful, logs you in.

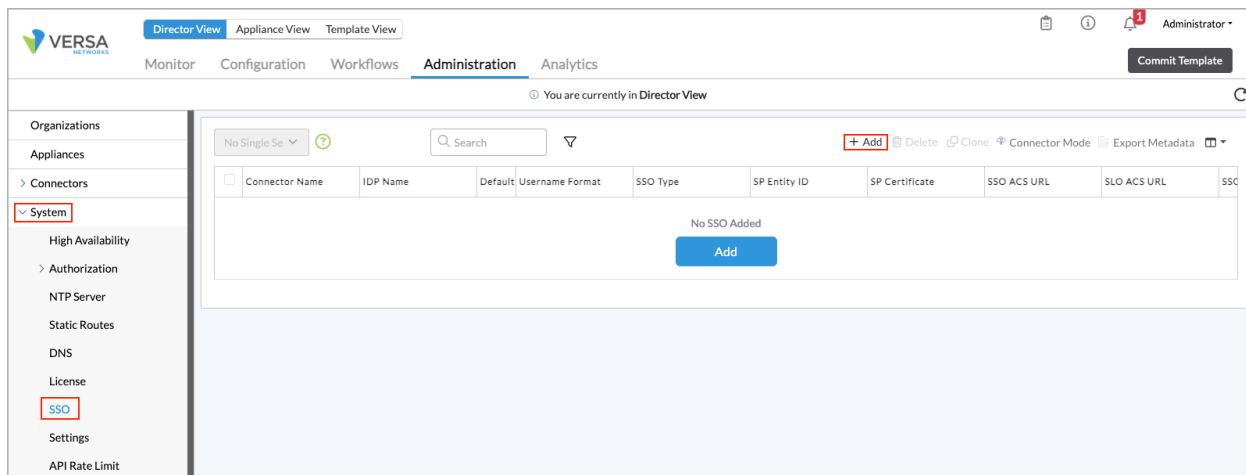
An IDP-initiated SSO flow operation is started from the IDP and is performed in the following sequence:

1. The IDP creates an SSO response.
2. The IDP redirects you to the service provider with the login response.
3. The service provider validates the login response and, if the validation is successful, provides access to the requested resource.

---

## Configure Service Provider–Initiated SSO

1. In Director view, select the Administration tab in the top menu bar.
2. Select System > SSO in the left menu bar. The main pane displays the SSO details.



3. Click the **+** Add icon to modify the SSO configuration and add IDP metadata and other configurations required to configure the SSO. In the Add SSO popup window, enter information for the following fields.

Add SSO

Connector Name \*

IDP Name \*

Organization

SSO Initiated Type

SSO Type

SSO Signout Type

Username Format

Versa Director FQDN/IP Address \*

SP Entity ID

Auth Context Comparison

Logout Success Redirect URL

IDP Metadata XML

Browse

☐ SSO Enabled

Analytics Client

SSO User Attributes

Director Client

Concerto Client




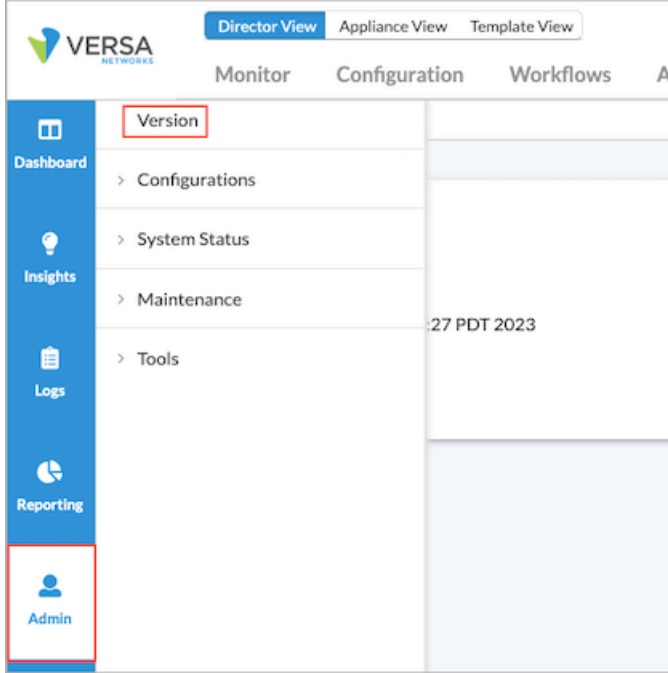
Metadata

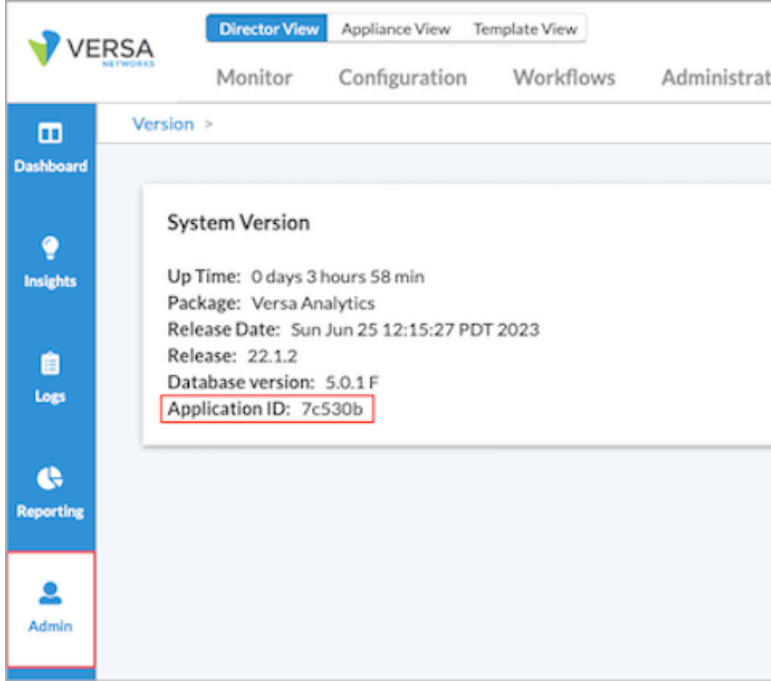

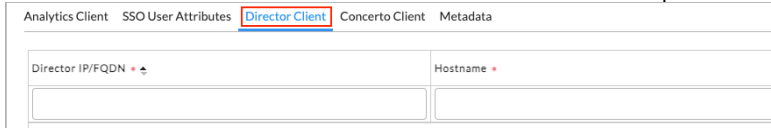
VAN IP/FQDN *	VAN APP ID *	
		+
No Records to Display		


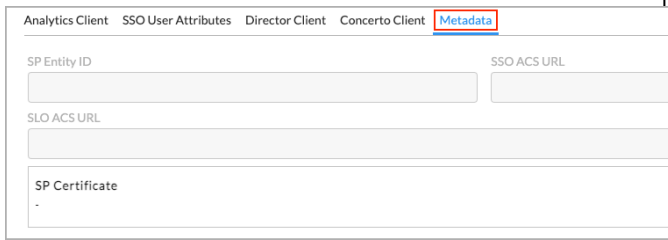
OK

Cancel

Field	Description
Connector Name	Enter a name for the connector.
IDP Name	Enter a name for the IDP service.
Organization	Select an organization.
SSO-Initiated Type	<p>Select the single sign-on initiator:</p> <ul style="list-style-type: none"> <li>◦ All</li> <li>◦ IDP Initiated</li> <li>◦ SP Initiated</li> </ul>
SSO Type	<p>Select the SSO markup language:</p> <ul style="list-style-type: none"> <li>◦ SAML-based SSO</li> </ul>
SSO Signout Type	<p>Enter the SSO signout type:</p> <ul style="list-style-type: none"> <li>◦ IDP</li> <li>◦ Local</li> </ul>
Versa Director FQDN/IP Address	Enter the FQDN or IP address of the Director host.
Username Format	<p>(For Releases 22.1.2 and later.) Enter the format for the username:</p> <ul style="list-style-type: none"> <li>◦ Email</li> <li>◦ String</li> </ul>
IDP Metadata XML	Click Browse, and then select the IDP metadata, in this case, Okta. For more information, see <a href="#">Configure an IDP</a> , below.
SP EntityID	Enter the URL that identifies the authentication request, for example, http://versa-networks.com/sp.
Authorization Context Comparison	Enter Exact for the authorization context comparison.
Logout Success Redirect URL	Enter the URL to be redirected to when the logout is success successful.
IDP Metadata XML	Click Browse, and then select the IDP metadata, in this case, Okta. For more information, see <a href="#">Configure an IDP</a> , below.

SSO Enabled	Click to enable SSO.
Analytics Client (Tab)	
<ul style="list-style-type: none"> <li>Versa Analytics IP/FQDN</li> </ul>	Enter the IP address of the Analytics node, and then click the  Add icon.
<ul style="list-style-type: none"> <li>Versa Analytics Application ID</li> </ul>	<p>Enter the Analytics application ID, and then click the  Add icon. To determine the Analytics application ID, select the Analytics tab in the top menu bar, and then select Administration &gt; Version in the left menu bar.</p>  <p>For example, here, the application ID is 7c530b:</p>

	
SSO User Attributes (Tab)	
◦ Email	Enter the attribute name, which is configured in the IDP.
◦ Organization	Enter the organization name, which is configured in the IDP.
◦ Roles	Enter the role, which is configured in the IDP.
◦ Idle Timeout	Enter the idle timeout, which is configured in the IDP.
◦ Concerto Role	(For Releases 22.1.2 and later.) Enter the name of the Concerto role, which is configured in the IDP.
Director Client (Tab)	

◦ Director IP/FQDN	Enter the IP address of the FQDN of the Director client.
◦ Hostname	Enter the hostname of the Director client (for central authorization only).
Concerto Client (Tab)	
◦ Concerto IP/FQDN	Enter the IP address of the FQDN of the Concerto client.
◦ Concerto Application ID	Enter Concerto.
Metadata (Tab)	

4. Click OK. The main pane displays the IDP details that the service provider requires for SSO.

For service provider–initiated SSO, configure the IDP with the service provider–related details, as described in [Configure an IDP](#), below.

For IDP-initiated SSO, you are redirected to the Director login page. The login page does not display the login with the SSO link on it.

## Configure an IDP

To generate the IDP metadata, you must first configure, or partially configure, basic details about the IDP. The following procedure shows an example of how to configure an IDP using Okta:

1. Configure the IDP using the details generated in the previous section. Check for the following four values in the certificate: SSO ACS URL, SLO ACS URL, SP Entity ID, and SP Certificate.

Single Sign On URL	https://192.168.135.130/versa/sso/loginConsumer	
Recipient URL	https://192.168.135.130/versa/sso/loginConsumer	
Destination URL	https://192.168.135.130/versa/sso/loginConsumer	
Audience Restriction	http://versa-networks.com/sp	
Default Relay State		
Name ID Format	Unspecified	
Response	Signed	
Assertion Signature	Signed	
Signature Algorithm	RSA_SHA1	
Digest Algorithm	SHA1	
Assertion Encryption	Unencrypted	
SAML Single Logout	Enabled	
Signature Certificate	vnms_sso_public2.cert (CN=L=Santa Clara, ST=California, C=US, OU=VersaDirector, O=versa-networks, CN=ranganatha-vm)	
authnContextClassRef	PasswordProtectedTransport	
Honor Force Authentication	No	
SAML Issuer ID	http://www.okta.com/\${org.externalKey}	
ATTRIBUTE STATEMENTS		
Name	Name Format	Value
role	Unspecified	appuser.role
org	Unspecified	appuser.org
IdleTimeOut	Unspecified	appuser.IdleTimeOut

Note: When you use an IDP-initiated authentication flow, RelayState mapping is required to complete the IDP-initiated configuration. The default relay state for enabling SSO in the parent organization is vd-ui::system, and for enabling SSO in any tenant organization it is vd-ui::TENANT1.

[https://docs.versa-networks.com/Management\\_and\\_Orchestration/Versa\\_Director/Configuration/Configure\\_Single\\_Sign-On\\_...](https://docs.versa-networks.com/Management_and_Orchestration/Versa_Director/Configuration/Configure_Single_Sign-On_...)

Updated: Thu, 24 Oct 2024 10:46:10 GMT

Copyright © 2024, Versa Networks, Inc.



2. To add users in the IDP, enter information for the following fields in the Edit User Assignment window. A user is classified as either a Provider User or a Tenant User.

Edit User Assignment

User Name

user1@acompany.com

Role

TenantSuperAdmin

idleTimeOut

15

org

org1

Save

Cancel

Field	Description
Username	Enter a name for the provider or tenant user.
Role	Enter the role for the provider or tenant user. The screenshot above show a tenant user with the TenantSuperAdmin role.
Idle Timeout	Enter the session idle timeout limit for the provider or tenant user.
Org	For a tenant user only, enter the organization name.

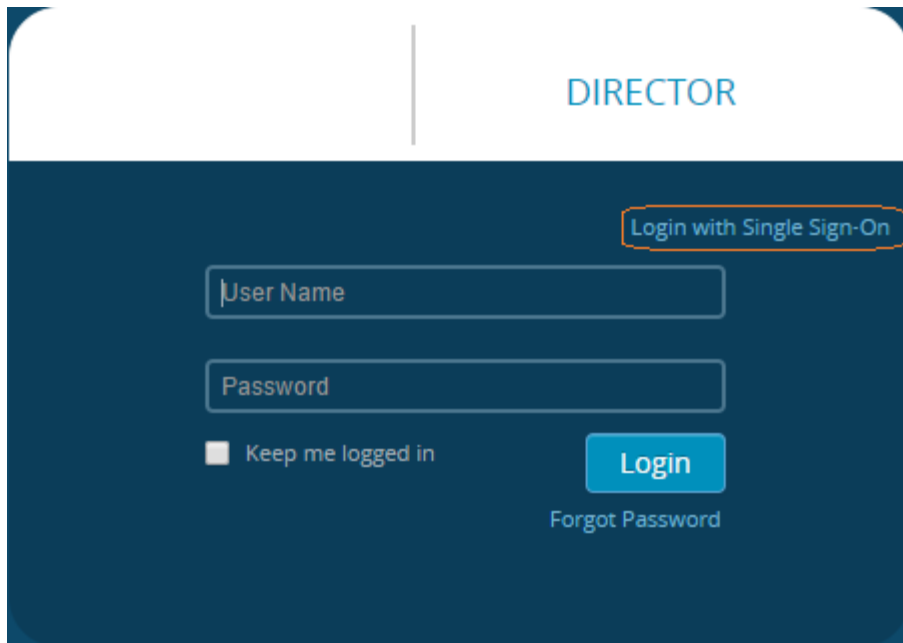
3. Click Save to commit the IDP configuration. You can now access the Versa Director page with the single sign-on option in it. For more information, see [Access a Director Using Service Provider-Initiated SSO](#), below.

### Access a Director Node Using Service Provider–Initiated SSO

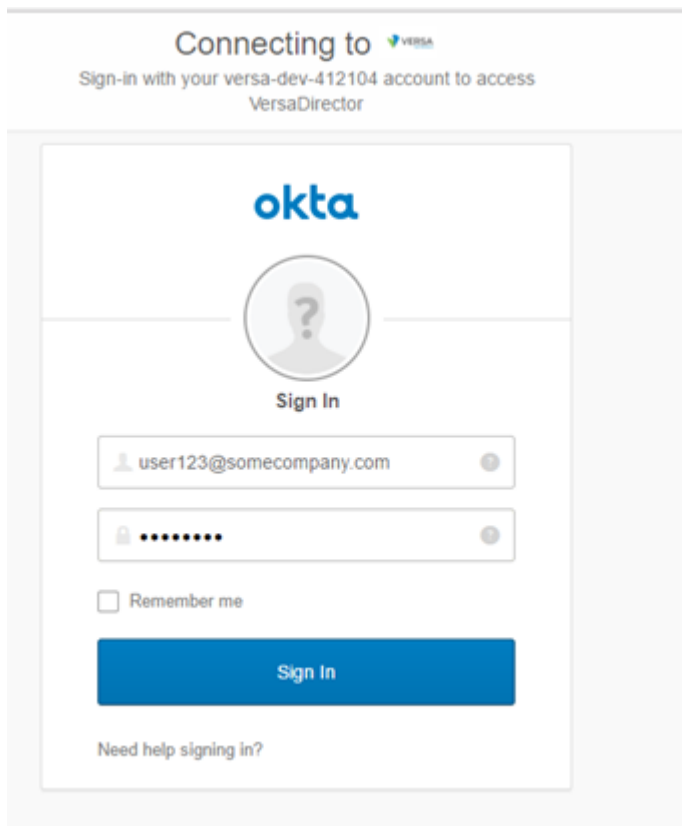
If you enable the SSO Enabled option in the Edit SSO popup window, the Director login page displays the Login with Single Sign-On link.

To access a Director node using SSO:

1. On the Director login page, click Login with Single Sign-On. The IDP (Okta) login page displays.



2. On the IDP (Okta) login page, enter your credentials and then click Sign In.



IDP validates your credentials and then displays the Director home page.

Organization Name	Parent Organization	CMS Connectors	CMS Organizations	Subscription Profile	Global Organization ID
<input type="checkbox"/> Customer1	Provider		-	Default-All-Services-Plan	3
<input type="checkbox"/> Customer2	Provider		-	Default-All-Services-Plan	6
<input type="checkbox"/> Customer3	Provider		-	Default-All-Services-Plan	4
<input type="checkbox"/> Customer4	Provider		-	Default-All-Services-Plan	2
<input type="checkbox"/> Provider	none		NewOrg	Default-All-Services-Plan	1

If a certificate issue occurs while the SAML login request is being verified, and if the certificate has expired, regenerate the SSO certificate on the Director node:

1. Regenerate the SSO certificate. Note that you should type this command on a single line.

```
# sudo openssl req -newkey rsa:2048 -nodes -keyout vnms_sso_private.key -x509
-days 365 -out vnms_sso_public.crt
-subj "/CN=director-hostname/O=organization-name/OU=organizational-unit-name/C=country/ST=state or
province/L=location"
```

For example:

```
# sudo openssl req -newkey rsa:2048 -nodes -keyout vnms_sso_private.key -x509
-days 365 -out vnms_sso_public.crt -subj "/CN=vm/O=versa-networks/OU=VersaDirector/C=US/
ST=California/L=Santa Clara"
```

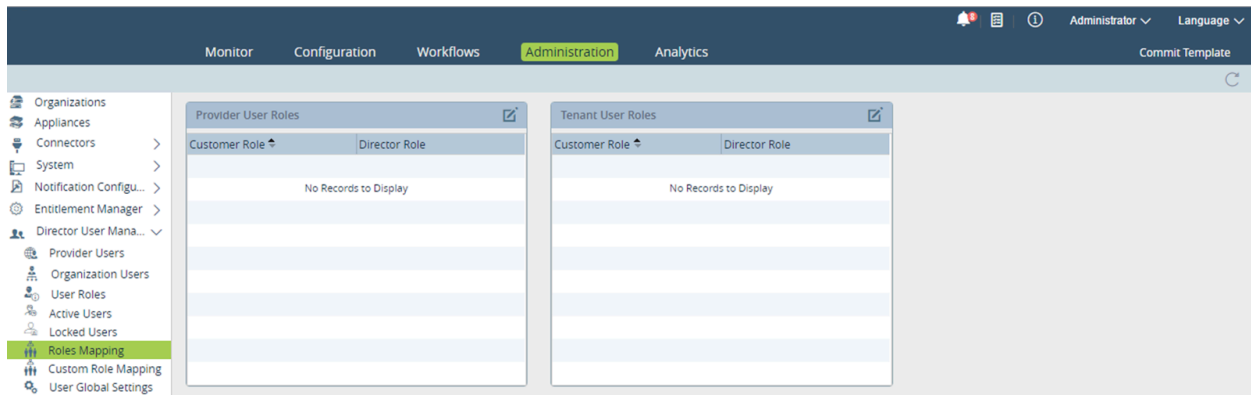
2. Copy the generated vnms\_sso\_public.crt certificate to the /var/versa/vnms/data/certs directory.
3. Upload the vnms\_sso\_public.crt certificate to the IDP, as described in [Configure an IDP](#), above.



## Configure Role Mapping

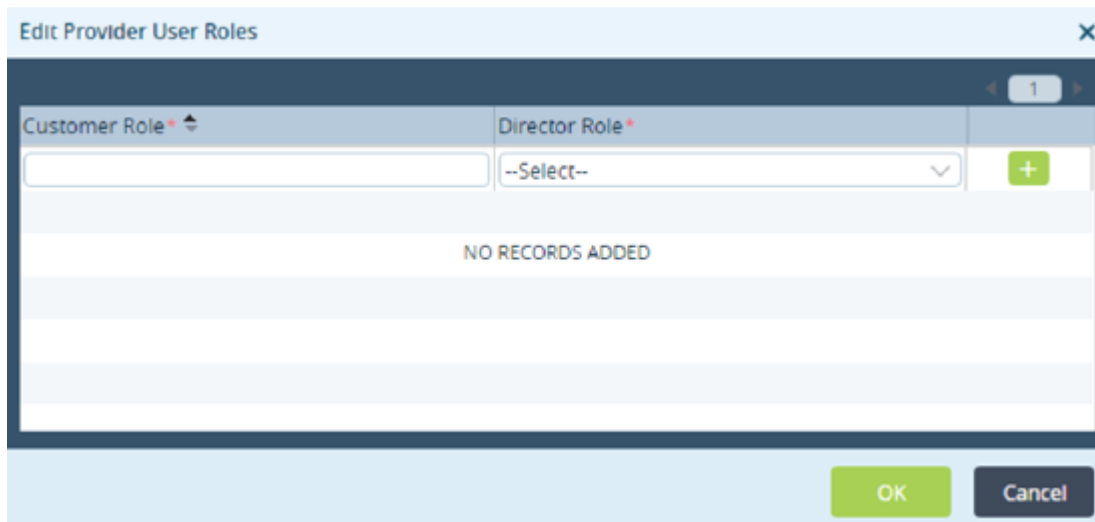
When the customer portal roles are different from the Director roles, you can map the customer portal roles to the Director roles.



To configure role mapping:

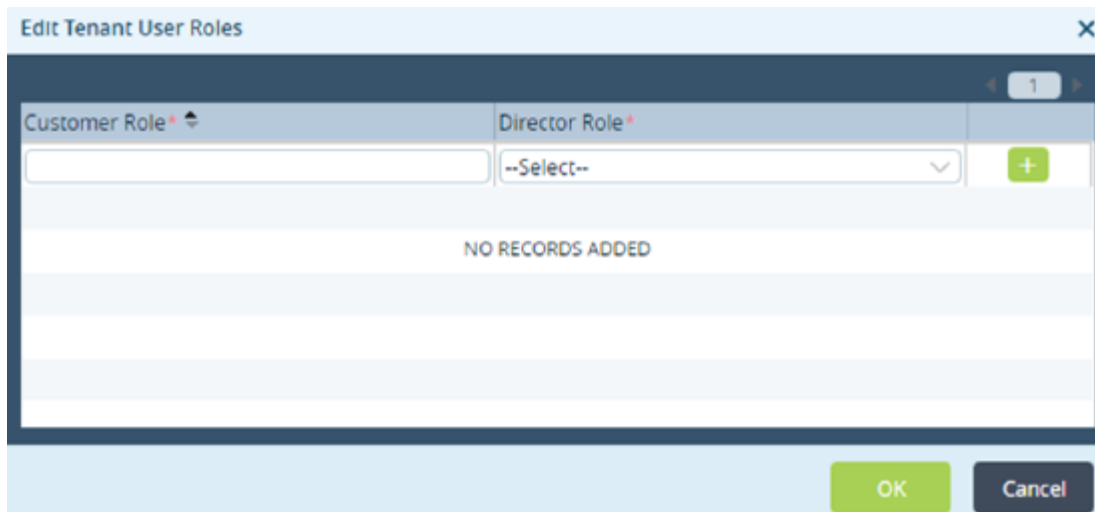
1. In Director view, select the Administration tab in the top menu bar.
2. Select Director User Management > Roles Mapping in the left menu bar. The main pane displays the existing roles of the provider and tenant users.



3. In the Provider User Roles pane, click the  Edit icon to map Director roles with provider roles. The Edit Provider User Roles popup window displays. Select the customer custom role defined in the IDP, select the Director role to map to, and then click the  Add icon.



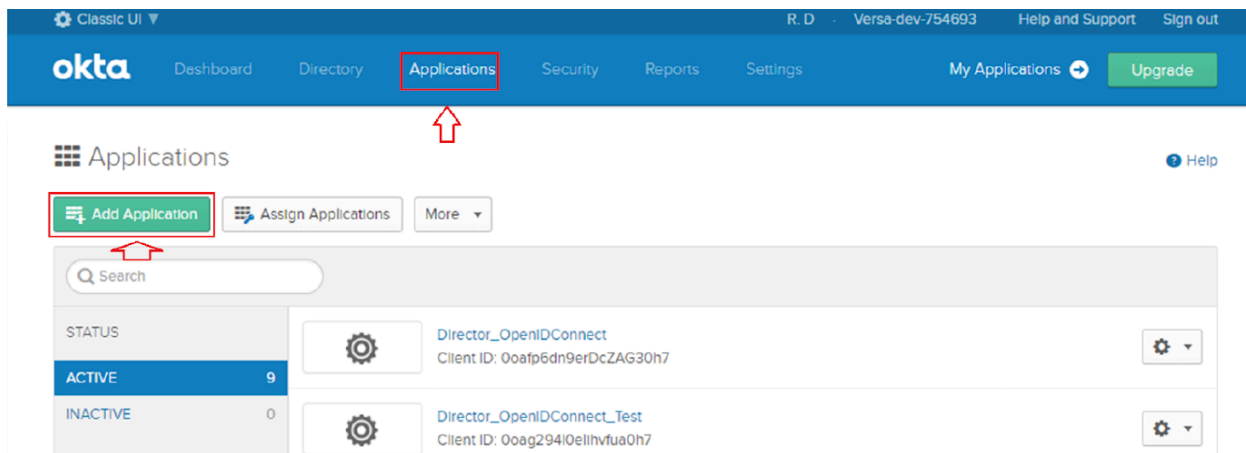
4. Click OK.
5. In the Tenant User Roles pane, click the  Edit icon to map Director roles with tenant roles. The Edit Tenant User Roles popup window displays. Select the customer custom role defined in the IDP, select the Director role to map to, and then click the  Add icon.



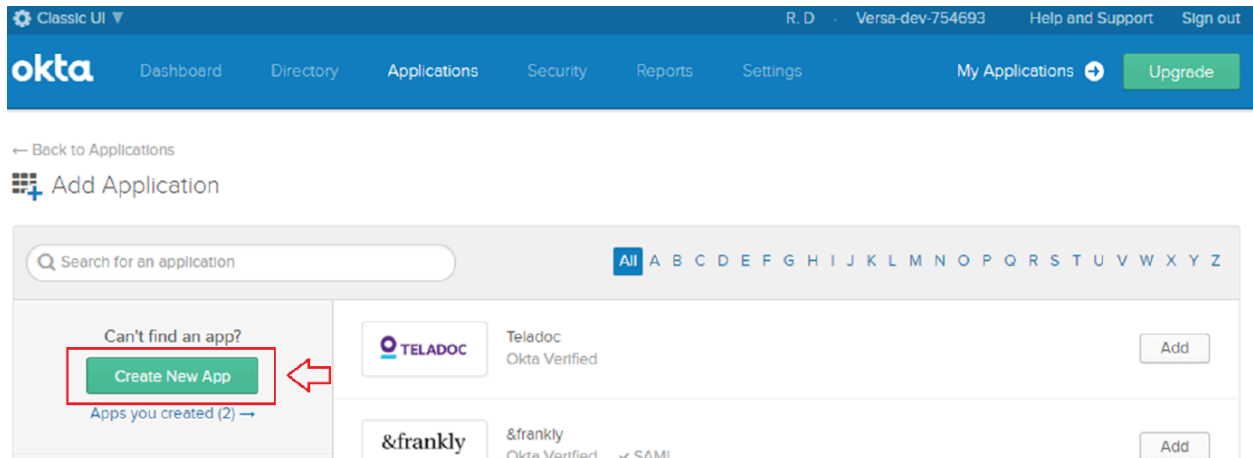
6. Click OK.

## Configure OpenID-Based SSO Using Okta

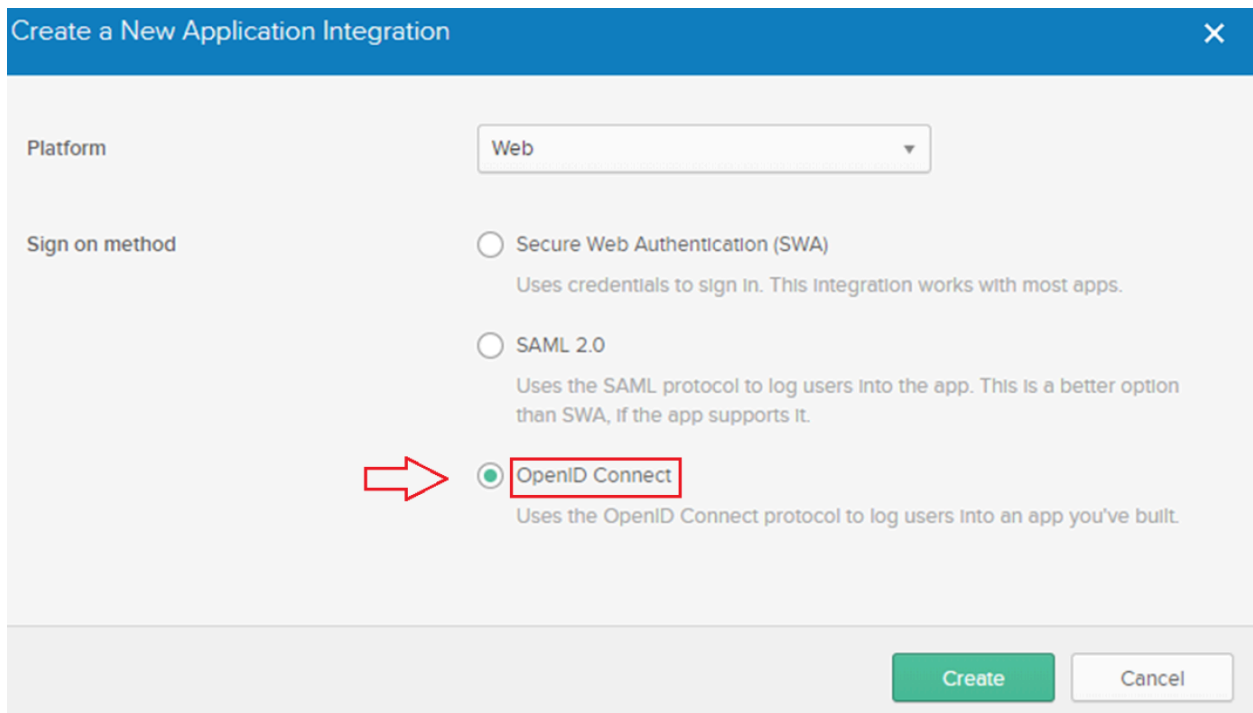
1. Create an account at [www.okta.com](https://www.okta.com).
2. Log in to Okta with your credentials.
3. Select the Applications tab in the top menu bar, and then click Add Application to create a new OpenID Connect application.



4. Click Create New App to create a new OpenID application. The Create New Application Integration page displays.



5. Select OpenID Connect, and then click Create. The Create OpenID Connect Integration page displays.



6. On the Create OpenID Connect Integration page, enter information for the following fields.

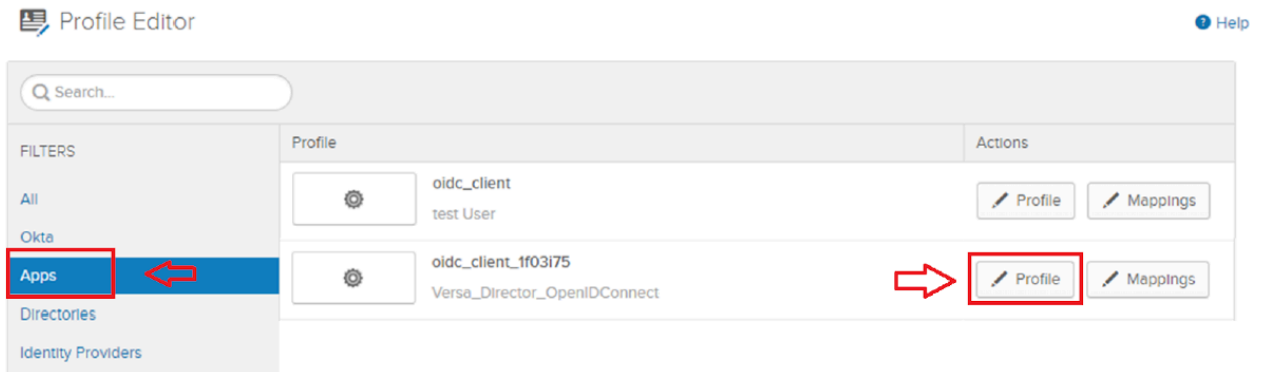
Field	Description
General Setting (Group of Fields)	
◦ Application Name	Enter a name for the OpenID Connect application.

Field	Description
◦ Application Logo	Browse and select a logo to represent the OpenID Connect.
Configure OpenID Connect (Group of Fields)	
◦ Login Redirect URIs	Enter the URI to which Okta sends OAuth responses.
◦ Logout Redirect URIs	Enter the URI to which Okta sends relying party-initiated logouts.

7. Click Save.
8. Select General tab on the new OpenID Connect preview page, and then copy the Client ID and Client Secret keys from the Client Credentials section.








- b. Select Add Attribute on the next page that displays.

Attributes

[+ Add Attribute](#) [Map Attributes](#)


FILTERS 


All  
Base  
Custom

### Add Attribute

\* Local app attributes are only stored on Okta and not created in Versa\_Director\_OpenIDConnect-TechDoc. Use local attributes if you plan to add the attribute to Versa\_Director\_OpenIDConnect-TechDoc or only want to store the mapped value in Okta.

Data type:

Display name :

Variable name :

Description:

Enum: ☐ Define enumerated list of values







Attribute Length:   
  
 and

Attribute required: ☐ Yes

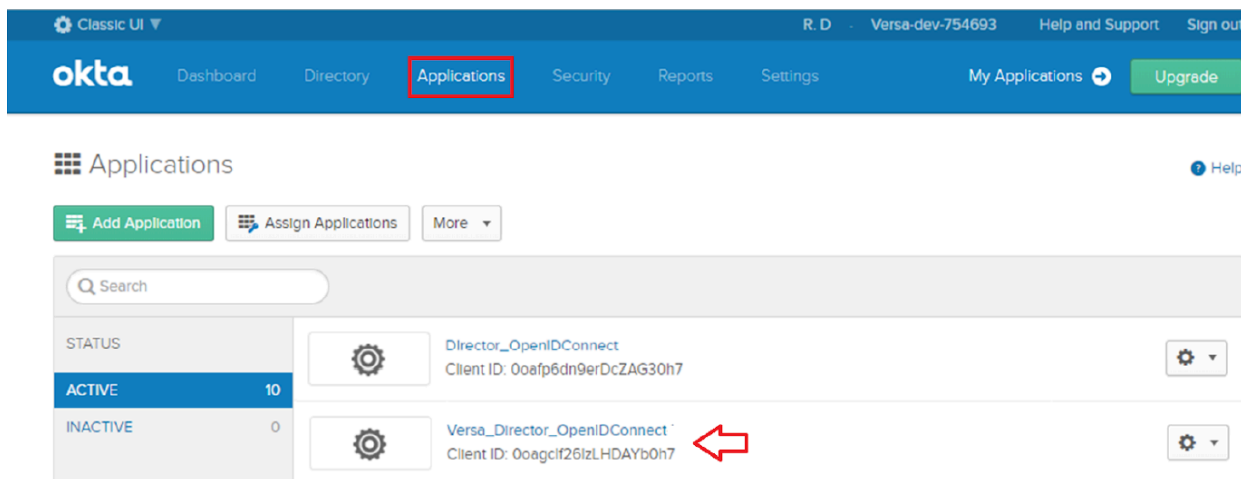
Scope: ☐ User personal

[Cancel](#) [Save](#) [Save and Add Another](#)

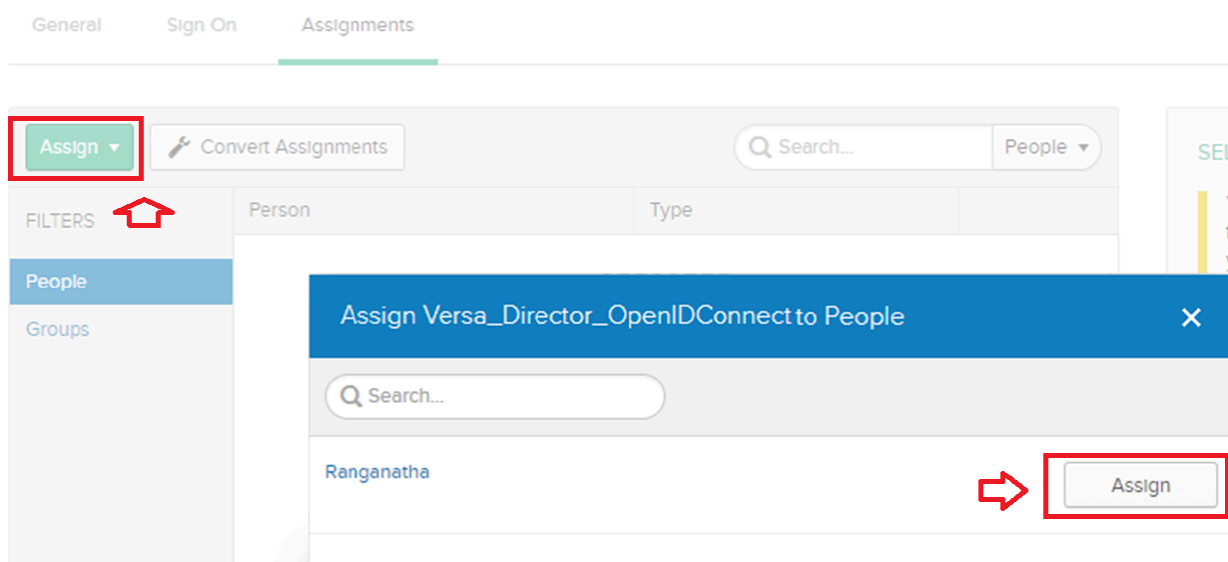
- c. In the Add Attribute popup window, add roles, organization, and idle timeout attributes. These display in the attribute dashboard.

roles	roles	string	Custom		
org	org	string	Custom		
idleTimeOut	idleTimeOut	number	Custom		

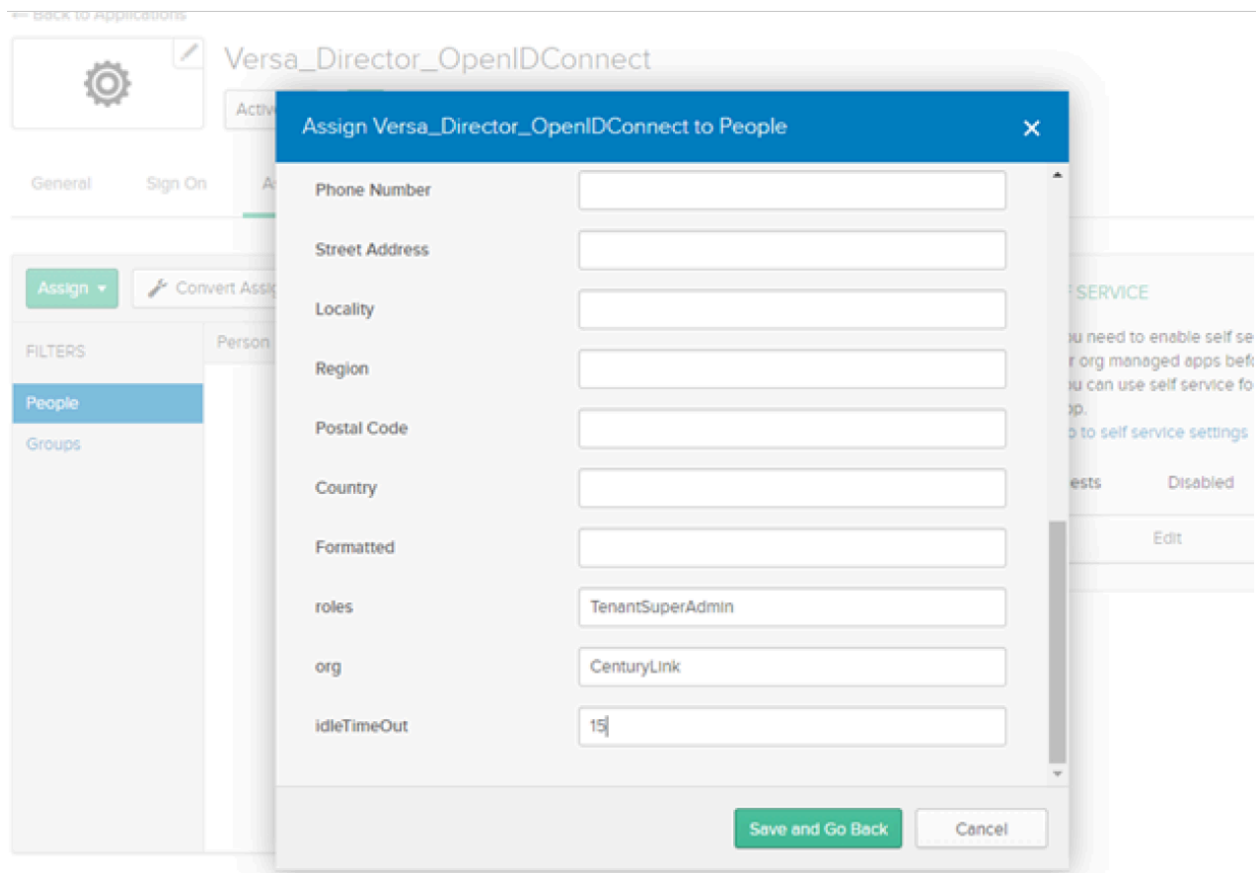
10. In the top menu bar, select Applications > Applications > Newly Created OpenID Connect to assign users to the Versa Director.




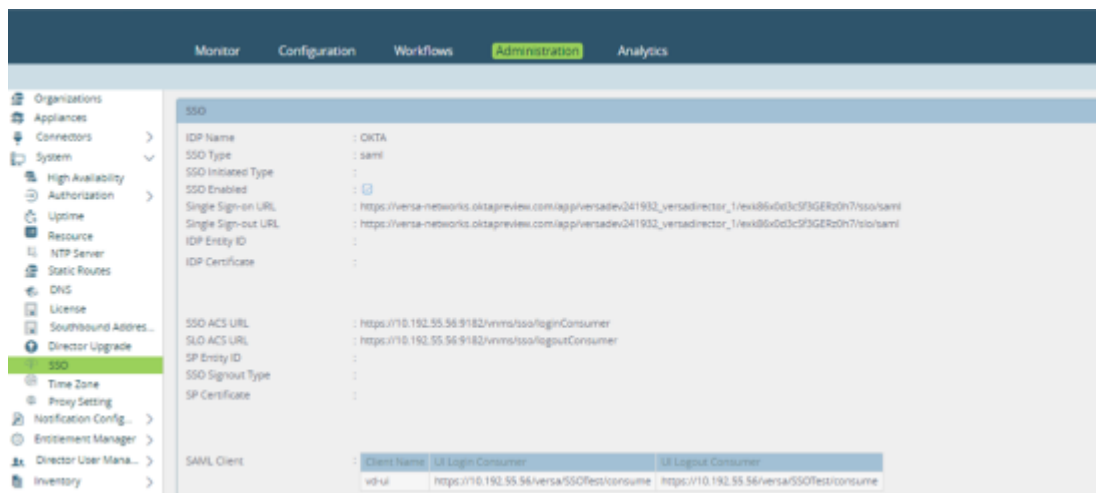
- a. Select Assign > Assign to People in the next page that displays.



- b. Select a person, and click Assign.
- c. In the preview page that displays next, enter the roles, organization, and idle timeout for the assigned user. Then click Save and Go Back.



11. On the Director node, select the Administration tab in the top menu bar, and then select System > SSO in the left menu bar. Click the  Edit icon to modify the SSO configuration.



12. In the Edit SSO popup window, enter information for the following fields.

[https://docs.versa-networks.com/Management\\_and\\_Orchestration/Versa\\_Director/Configuration/Configure\\_Single\\_Sign-On\\_...](https://docs.versa-networks.com/Management_and_Orchestration/Versa_Director/Configuration/Configure_Single_Sign-On_...)

Updated: Thu, 24 Oct 2024 10:46:10 GMT

Copyright © 2024, Versa Networks, Inc.

Edit SSO

IDP Name

OKTA

SSO Initiated Type

IDP Initiated

SSO Type

openid

Versa Director Host\*

10.192.55.56:9182

VAN IP\*

VAN APP ID\*

+

No Records to Display

SSO Signout Type

--Select--

☒ SSO Enabled

Authorize Endpoint\*

Token Endpoint\*

User Info Endpoint\*

Revoke Endpoint\*

Client Id\*

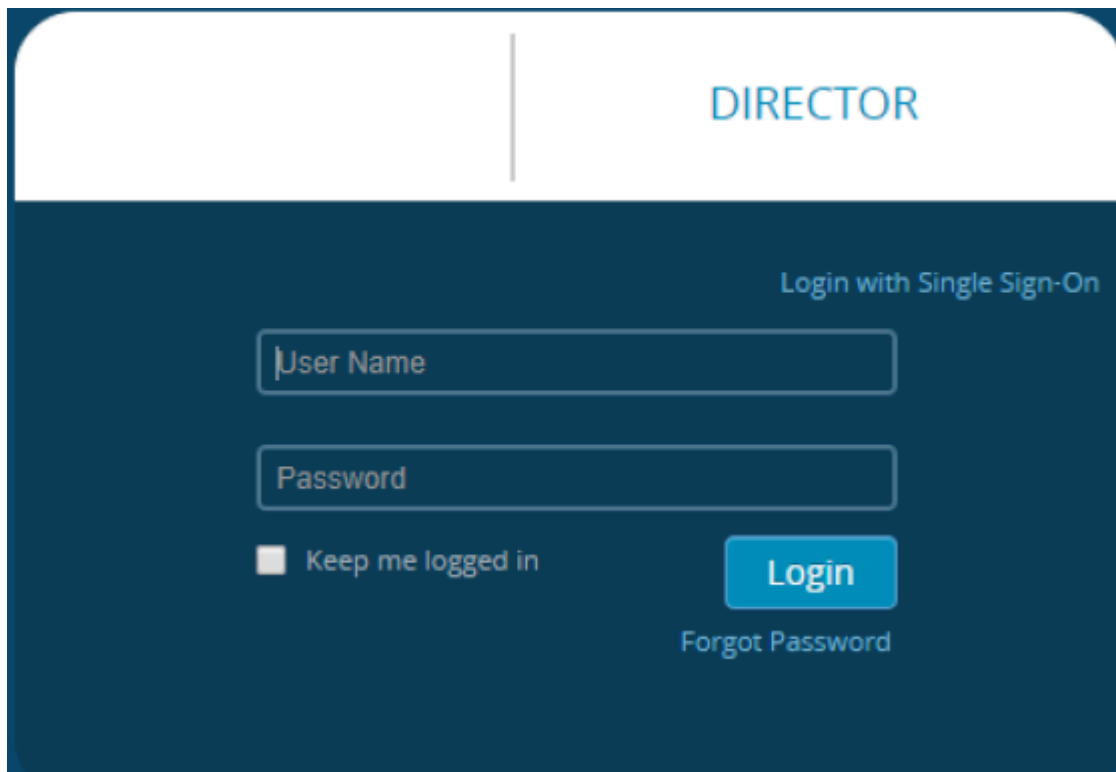
Client Secret\*

OK

Cancel

Field	Description
SSO-Initiated Type	Select IDP Initiated.
SSO Type	Select OpenID.
Authorize Endpoint	Enter your account domain's authorized endpoint.
Token Endpoint	Enter your account domain's token endpoint.
User Information Endpoint	Enter your account domain's user information endpoint.
Revoke Endpoint	Enter your account domain's revocation endpoint.
Client ID	Enter the client identifier you obtained when you created the OpenID Connect application.
Client Secret	Enter the client password you obtained when you created the OpenID Connect application.

13. Click OK.
14. Log out from the Director node, and then log in again using SSO.



---

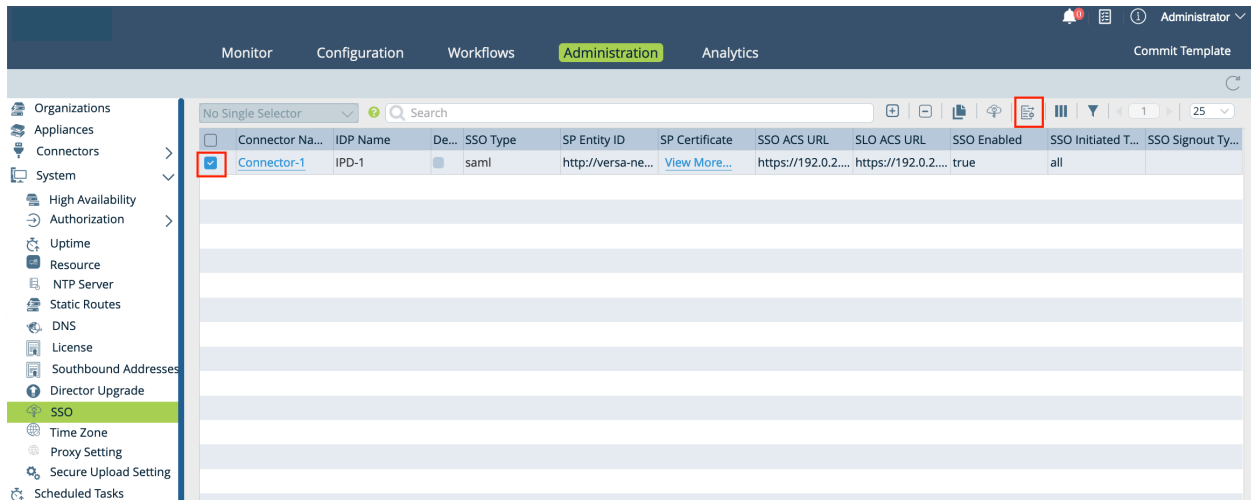
## Export SSO Configuration Metadata


*For Releases 21.1 and later.*

Some IDP providers need the SSO configuration metadata from the Versa Director so that they can configure their side of the connection. You can export the SSO metadata in XML format. If the IDP provider needs the metadata in JSON format, you can use an XML-to-JSON converter to convert the metadata.

To export the SSO configuration metadata from a Director node:

1. In Director view, select the Administration tab in the top menu bar.
2. Select System > SSO in the left menu bar.
3. In the main pane, click to select the IDP provider record.



4. Click the  Export Metadata icon.
5. Select the location to which to download the XML file.
6. Click OK.

## Limitations

The following are the limitations for configuring SSO using Director:

- A provider user who has the ProviderDataCenterSystemAdmin role and who is logged into the Director node using SSO cannot open a shell-in-a box on the Director node

## Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- Release 21.1 add support for exporting SSO configuration metadata.
- Release 22.1.2 supports additional fields in the Add SSO UI screen.

## Additional Information

[Configure Single Sign-On for Concerto](#)

[Configure Systemwide Functions](#)