
Configure Single Sign-On for Concerto

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

Single sign-on (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 Concerto, the service provider offers single sign-on as a login mechanism to different integrators and clients.

For SSO, Concerto supports:

- Security Assertion Markup Language (SAML)
- OpenID Connect SSO methods

Concerto enables identity provider (IDP)–based and local user authentication.

Concerto supports two types of SSO:

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

Concerto SSO has been tested with the ADFS, Azure, Okta, and Ping Identity IDPs.

To configure SSO on Concerto, you do the following:

1. Configure Concerto service provider–initiated or Concerto IDP-initiated SSO.
2. Access the Director node using SSO.

Configure SAML-Based SSO Using Okta

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

1. The service provider server creates an authentication request and redirects you to the IDP.

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

Note: To create an IDP-initiated SSO using Okta, configure the IDP-related field-Default RelayState. The default relay state for enabling SSO in the system user is `vd-ui::system`, and for enabling SSO in any tenant users is `vd-ui::organization-name`. To configure IDP-Initiated SSO using Okta, follow the steps in [Configure Service Provider-Initiated SSO](#), below. To log in with IDP-Initiated SSO, see [Log In with IDP-Initiated SSO](#), below.

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

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

Configure Service Provider-Initiated SSO

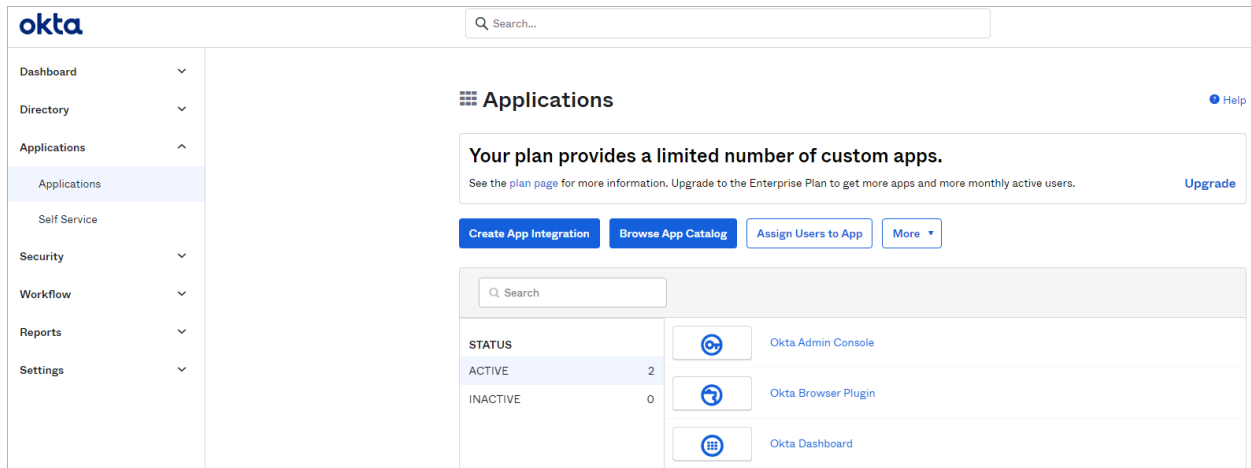
To create service provider-initiated SSO using Okta, you do the following:

- Create an application on Okta.
- Define custom attributes.
- Add users to the application.

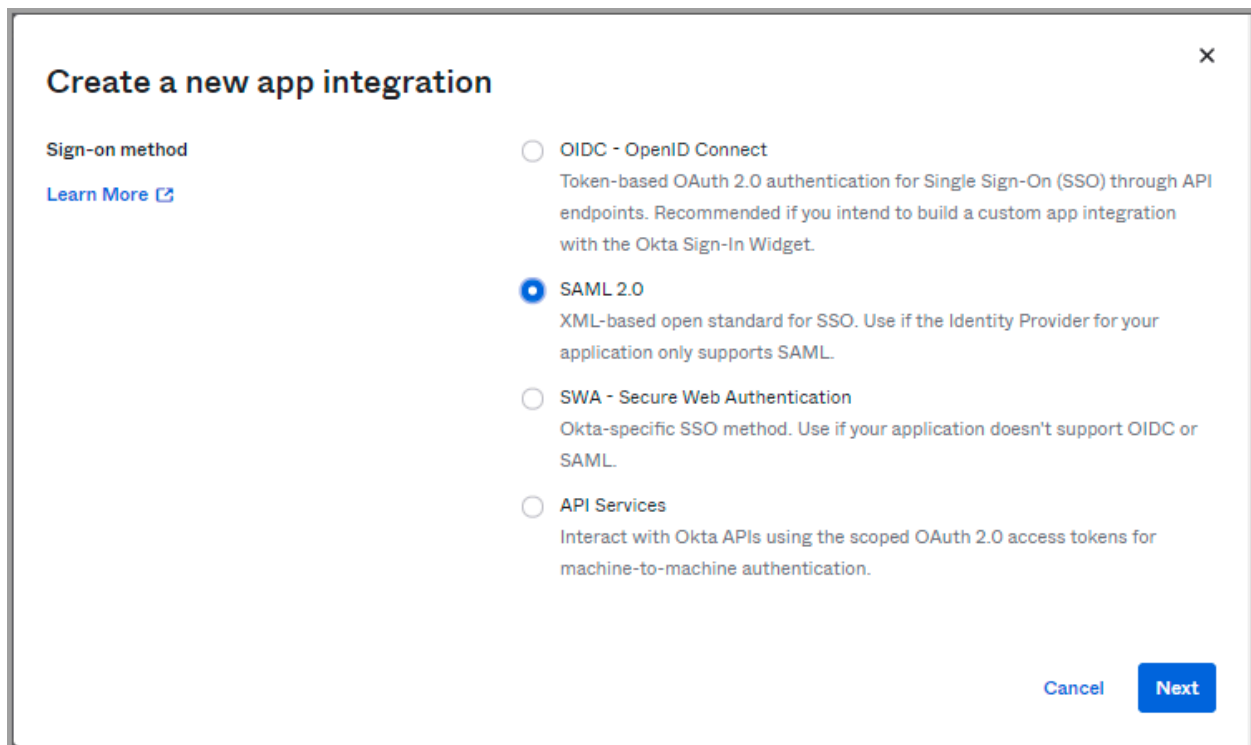
Create an Application

To create a SAML connection application:

1. Create an account in www.okta.com
2. Log in to Okta with your credentials.
3. In the left menu bar, select Applications > Applications.
4. Click Create App Integration to create a new SAML connect application.



5. In the Create a New App Integration window, click SAML 2.0, and then click Next.



6. In the General Settings > App name field, enter an Application name, and then click Next.

7. In the Configure SAML page, enter information for the indicated fields.

okta

Search...

Dashboard

Directory

Applications

Security

Workflow

Reports

Settings

Thanks for trying the Okta Starter plan. Upgrade to the Advanced plan to create more apps and get more Monthly Active Users.

Upgrade

Create SAML Integration

1 General Settings

2 Configure SAML

3 Feedback

A SAML Settings

General

Single sign on URL

https://10.xxx.xx.135/versa/sso/loginConsumer

Use this for Recipient URL and Destination URL

Allow this app to request other SSO URLs

Audience URI (SP Entity ID)

http://versa-networks.com/sp

Default RelayState

If no value is set, a blank RelayState is sent

Name ID format

Unspecified

Application username

Okta username

Hide Advanced Settings

Response

Signed

Assertion Signature

Signed

Signature Algorithm

RSA-SHA256

Digest Algorithm

SHA256

Assertion Encryption

Unencrypted

Enable Single Logout

Allow application to initiate Single Logout

Single Logout URL

https://10.xxx.xx.135/versa/sso/logoutConsumer

SP Issuer

http://versa-networks.com/sp

Signature Certificate

Browse

Upload Certificate

Assertion Inline Hook

None (disabled)

Authentication context class

PasswordProtectedTransport

Honor Force Authentication

Yes

SAML Issuer ID

http://www.okta.com/\${org.externalKey}

Attribute Statements (optional)

LEARN MORE

Name

Name format (optional)

Value

role

Unspecified

appuser.role

org

Unspecified

appuser.org

idatTimeOut

Unspecified

appuser.idatTimeOut

Unspecified

Add Another

Group Attribute Statements (optional)

Name

Name format (optional)

Filter

Unspecified

Starts with

Add Another

B Preview the SAML assertion generated from the information above

Preview the SAML Assertion

This shows you the XML that will be used in the assertion - use it to verify the info you entered above

Previous

Cancel

Next

What does this form do?

This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

Okta Certificate

Import the Okta certificate to your Identity Provider if required.

Download Okta Certificate

https://docs.versa-networks.com/Management_and_Orchestration/Versa_Concerto_Orchestrator/02_Common_Configuration/...
Updated: Wed, 23 Oct 2024 08:53:33 GMT
Copyright © 2024, Versa Networks, Inc.

5

Field	Description
Single Sign-On URL	Enter the URL to which Okta sends OAuth responses. The responses are sent in the format is <code>https://versa-director-ip-address/versa/sso/loginConsumer</code> .
Audience URI (SP Entity ID)	Enter the service provider entity ID, which is <code>http://versa-networks.com/sp</code> .
Show Advanced Settings	Click to display the advanced settings.
Delay Relay State	To create an IDP-initiated SSO using Okta, configure the IDP-related field Default RelayState . The default relay state for enabling SSO in the system user is <code>vd-ui::system</code> , and for enabling SSO in any tenant users is <code>vd-ui::organization-name</code> .
Enable Single Logout	Click to enable SAML single logout.
Single Logout URL	Enter the location to which to send the logout response.
SP Issuer	Enter the URL <code>http://versa-networks.com/sp</code> .
Attribute Statements	Enter the role, organization, and idle timeout attributes. The attribute strings are case sensitive.
Preview the SAML Assertion	<p>Click to preview the SAML assertion. Copy the metadata, and save it as an XML file. The following is an example of the SAML assertion:</p> <pre><?xml version="1.0" encoding="UTF-8"?> <saml2:Assertion ID="i....." IssueInstant="2021-05-12T09:38:33.165Z" Version="2.0" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"> <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"/> <saml2:Subject> <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified" userName="saml2:NameID"> <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"> <saml2:SubjectConfirmationData NotOnOrAfter="2021-05-12T09:43:33.359Z" Recipient="https://versa-network.com/sp/saml2:Audience"> </saml2:SubjectConfirmationData> </saml2:SubjectConfirmation> </saml2:Subject> <saml2:Conditions NotBefore="2021-05-12T09:33:33.359Z" NotOnOrAfter="2021-05-12T09:43:33.359Z"> <saml2:AudienceRestriction> <saml2:Audience>http://versa-network.com/sp/saml2:Audience</saml2:Audience> </saml2:AudienceRestriction> </saml2:Conditions> <saml2:AuthnStatement AuthnInstant="2021-05-12T09:38:33.165Z"> <saml2:AuthnContext> <saml2:AuthnContextClassRef urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml2:AuthnContextClassRef> </saml2:AuthnContext> </saml2:AuthnStatement> </saml2:Assertion></pre>

8. Click Next.
9. In the Feedback page, select Customer or Partner, and then click Finish.

okta Search...

Create SAML Integration

1 General Settings 2 Configure SAML 3 Feedback

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](#)

[Previous](#) [Finish](#)

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.

Thanks for trying the Okta Starter plan. Upgrade to the Advanced plan to create more apps and get more Monthly Active Users.

[Upgrade](#)

Define Custom Attributes

1. In the Profile Editor page, select Directory > Profile Editor > Newly Created SAML Connect > Profile in the left menu bar.

okta Search...

Profile Editor Help

Learn about Universal Directory

Universal Directory allows you to store employee, partner, and customer profiles in Okta, generating a user-based, single source of truth. Using Profile Editor, you can extend and customize user and app-specific profiles, as well as transform and map attributes between profiles. All of these features provide robust provisioning support.

[Go to Documentation](#)

[Create Okta User Type](#)

Filters	Profile
All	User (default) user Profile
Okta	User -OpenID User oidc_client Profile Mappings
Apps	User -SAML User dev2322987_sarathsaml_1 Profile Mappings
Directories	Test1-saml User dev2322987_test1saml_1 Profile Mappings
Identity Providers	

2. On the next page that opens, select Add Attribute.

okta

Q Search...

Dashboard

Directory

People

Groups

Profile Editor

Directory Integrations

Self Service

Thanks for trying the Okta Starter plan. Upgrade to the Advanced plan to create more apps and get more Monthly Active Users.

Upgrade

Profile Editor

Test1-saml User

Edit

Test1-saml

Display name

Test1-saml User

Description

Variable name

dev2322987_test1saml_1

Attributes

+ Add Attribute

Mappings

FILTERS

All

Base

Custom

Display Name	Variable Name	Data type	Attribute Type
Username	userName	string	Base

- In the Add Attribute window, add roles, organizations, and idle timeout as attributes. The attribute values are case sensitive.

Add Attribute

* Local app attributes are only stored on Okta and not created in Test1-saml. Use local attributes if you plan to add the attribute to Test1-saml or only want to store the mapped value in Okta.

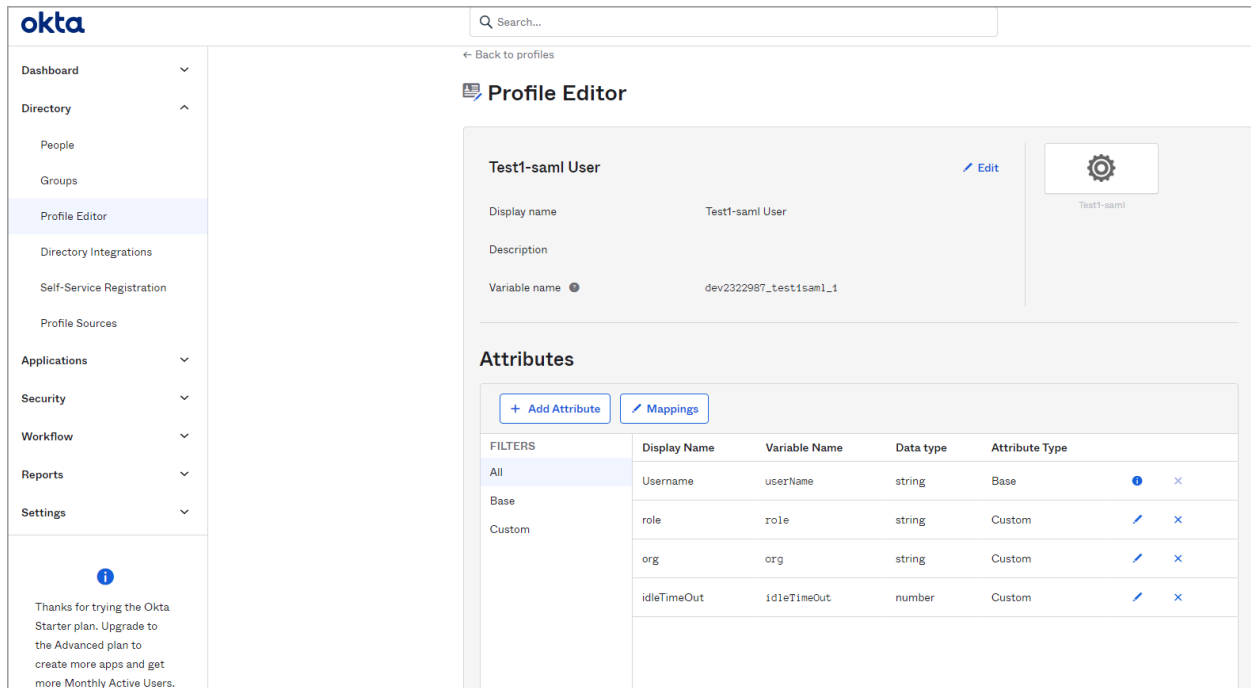
Data type	<div>string ▼</div>
Display name [?]	<div>role</div>
Variable name [?]	<div>role</div>
Description	<div></div>
Enum	<input type="checkbox"/> Define enumerated list of values
Attribute Length	<div>Between ▼</div> <div><div>min</div><div>and</div><div>max</div></div>
Attribute required	<input checked="" type="checkbox"/> Yes
Scope	<input type="checkbox"/> User personal

Save

Save and Add Another

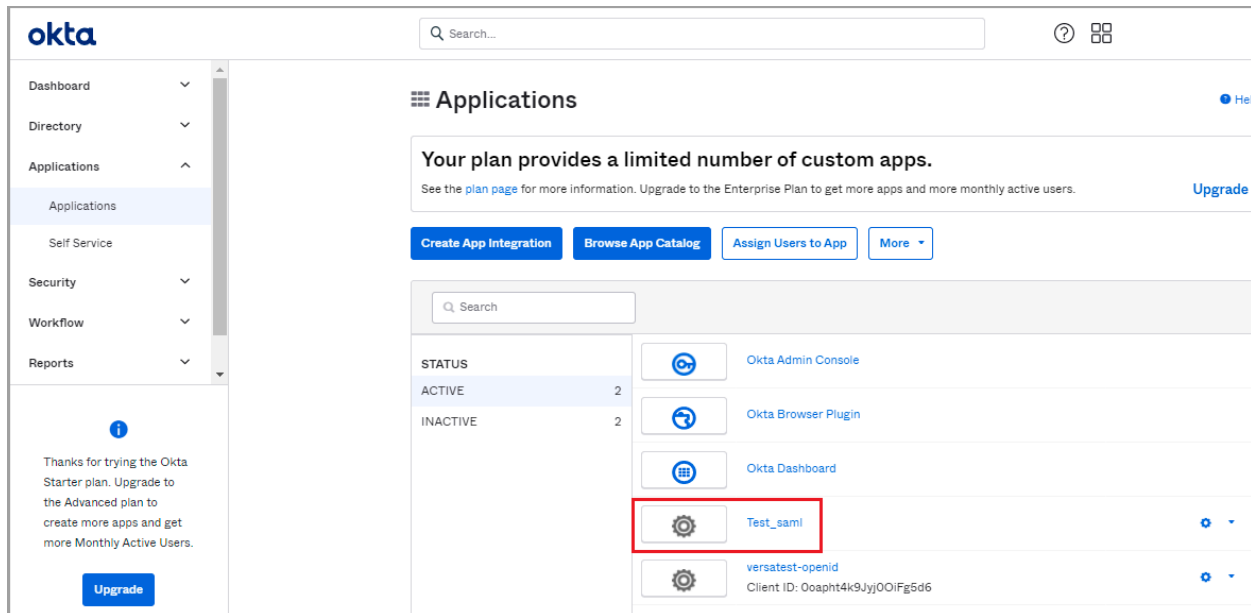
Cancel

4. These attributes display in the Attributes dashboard.



Add Users to an Application

1. To assign users to the Versa Director, select Applications > Applications in the left menu bar, and then click the newly created SAML connect.



2. In the Assignments tab, click the Assign field, and then click Assign to People.

okta

Search...

Dashboard

Directory

Applications

Applications

Self Service

Security

Thanks for trying the Okta Starter plan. Upgrade to the Advanced plan to create more apps and get more Monthly Active Users.

Upgrade

Back to Applications

Test1-saml

Active

View Logs

Monitor Imports

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

Mobile

Import

Assignments

Assign

Convert assignments

Search...

People

Assign to People

Assign to Groups

	Type
h chandra	Individual
@versa-networks.com	

REPORTS

Current Assignments

Recent Unassignments

SELF SERVICE

You need to enable self service for org managed apps

3. Select a person and then click Assign.

Assign Test1-saml to People

Tenant Super Admin

tsa@gmail.com

Assign

Done

4. Enter the role, organization, and idle timeout attribute information.

Assign Test-SAML to People

User Name

role

org



idleTimeOut

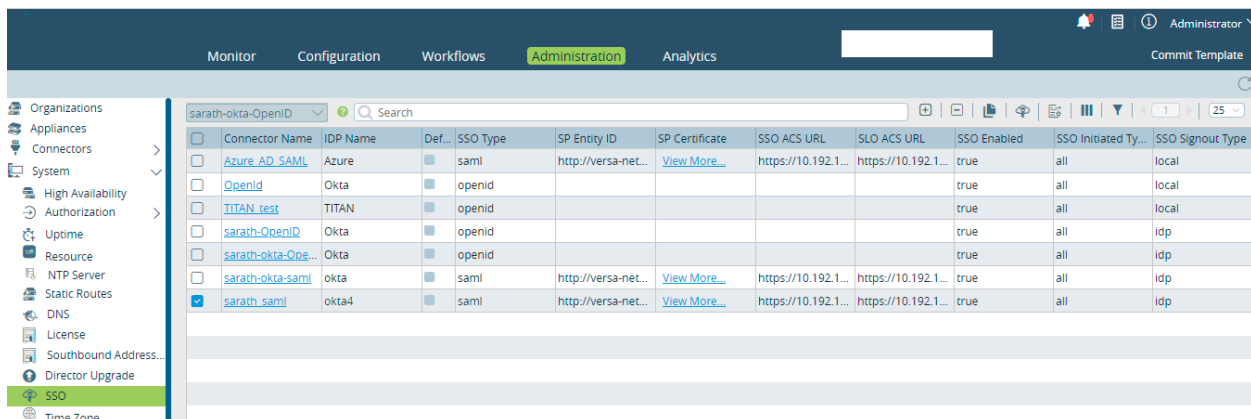
Save and Go Back

Cancel


- Click Save and Go Back.

Configure an SSO Connector in Versa Director

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



Connector Name	IDP Name	Def...	SSO Type	SP Entity ID	SP Certificate	SSO ACS URL	SLO ACS URL	SSO Enabled	SSO Initiated Ty...	SSO Signout Type
<input type="checkbox"/> Azure AD SAML	Azure	<input type="checkbox"/>	saml	http://versa-net...	View More...	https://10.192.1...	https://10.192.1...	true	all	local
<input type="checkbox"/> Openid	Okta	<input type="checkbox"/>	openid					true	all	local
<input type="checkbox"/> TITAN_test	TITAN	<input type="checkbox"/>	openid					true	all	local
<input type="checkbox"/> sarath-OpenID	Okta	<input type="checkbox"/>	openid					true	all	idp
<input type="checkbox"/> sarath-okta-Ope...	Okta	<input type="checkbox"/>	openid					true	all	idp
<input type="checkbox"/> sarath-okta-saml	okta	<input type="checkbox"/>	saml	http://versa-net...	View More...	https://10.192.1...	https://10.192.1...	true	all	idp
<input checked="" type="checkbox"/> sarath_saml	okta4	<input type="checkbox"/>	saml	http://versa-net...	View More...	https://10.192.1...	https://10.192.1...	true	all	idp

- Click  Add icon to configure SSO, and enter information for the following fields.

Add SSO

Connector Name*
tom-saml
IDP Name*
okta4
Organization
parent.org

Versa Director FQDN/IP Address*
10.123.12.123
SSO Initiated Type
IDP Initiated
SSO Type
saml
SSO Signout Type
Local

IDP Metadata XML
metadata.xml
SP Entity ID
http://versa-network.com/sp

☒ SSO Enabled
Logout Success Redirect URL

Analytics Client
SSO User Attributes
Concerto Client
Metadata

Email*
email
Organization*
org
Roles*
role

Idle Timeout*
idleTimeout

OK
Cancel

Field	Description
Connector Name (Required)	Name for the connector.
IDP Name (Required)	Name for the IDP service.
Organization	Enter the name of the organization.
Versa Director FQDN/IP Address (Required)	Enter the FQDN or IP address of Versa Director to which to connect.
SSO Initiated Type	Select the SSO initiator: <ul style="list-style-type: none"> ◦ All ◦ IDP Initiated ◦ SP Initiated
SSO Type	Select the SSO type markup language. <ul style="list-style-type: none"> ◦ OpenID—OpenID is an open-standard data format for exchanging authentication data and authorization data between an identity provider and a service provider. ◦ SAML—SAML is an XML-based, open-standard data format for exchanging authentication data and authorization data between an identity provider and a service provider.
SSO Signout Type	Select the SSO signout type: <ul style="list-style-type: none"> ◦ IDP—Both the service provider and the IDP sessions are cleared.


Field	Description
	<ul style="list-style-type: none"> Local—Only the service provider session is cleared.
IDP Metadata XML	Click Browse and then select the IDP (Okta, in this case) metadata. The metaata is generated from the IDP server.
SP Entity ID	Enter the entity ID of the service provider (that is, the VOS device).
Logout Success Redirect URL	Enter the URL to which to be redirected after successful IDP logout.
SSO Enabled	Click to enable SSO.
SSO User Attribute Tab	<p>The following attribute fields must be the same as the user configured in the IDP:</p> <ul style="list-style-type: none"> Email Idle Timeout Organization Roles

4. To configure Concerto client, click the Concerto Client tab, and enter information for the following fields.

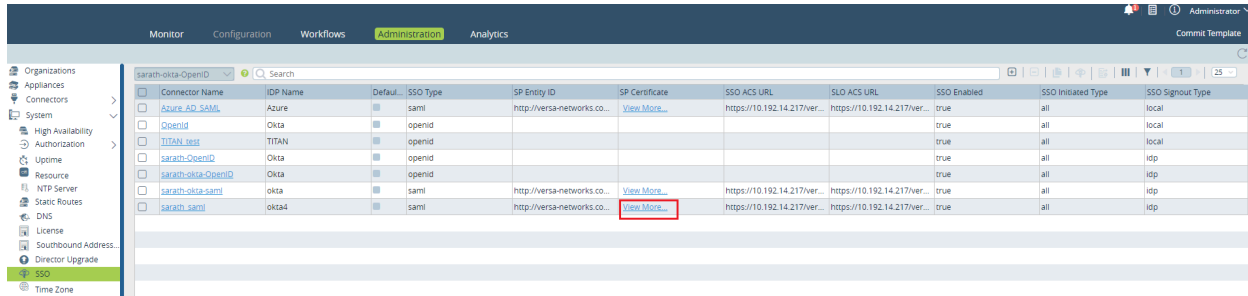
The screenshot shows the 'Add SSO' configuration window. The 'Concerto Client' tab is selected, and the 'Concerto Client' sub-tab is highlighted. The following fields are visible:

- Connector Name ***: concerto_SAML
- IDP Name ***: Okta
- Organization**: Organization
- Versa Director FQDN/IP Address ***: 10.12.13.134
- SSO Initiated Type**: All
- SSO Type**: saml
- SSO Signout Type**: IDP
- IDP Metadata XML**: (Empty field with a 'Browse' button)
- SP Entity ID**: http://versa-network.com/sp
- Logout Success Redirect URL**: (Empty field)
- SSO Enabled**: ☒
- Analytics Client**: (Empty field)
- SSO User Attributes**: (Empty field)
- Concerto Client**: (Selected tab)
- Metadata**: (Empty field)
- Concerto IP/FQDN ***: 10.21.90.123
- Concerto APP ID ***: Concerto

Buttons at the bottom: OK, Cancel.

Field	Description
Concerto IP/FQDN	Enter the FQDN or IP address of Concerto to connect.
Concerto APP ID	Enter the application ID of Concerto to connect. Click  Add icon.

5. Click OK.
6. In the main pane, click View More to view the service provider certificate.



Connector Name	IDP Name	Default	SSO Type	SP Entity ID	SP Certificate	SSO ACS URL	SLO ACS URL	SSO Enabled	SSO Initiated Type	SSO Signout Type
Azure AD SAML	Azure	<input checked="" type="checkbox"/>	saml	http://versa-networks.co...	View More...	https://10.192.14.217/ver...	https://10.192.14.217/ver...	true	all	local
DocId	Okta	<input checked="" type="checkbox"/>	openid					true	all	local
TITAN test	TITAN	<input checked="" type="checkbox"/>	openid					true	all	local
saml-Okta-OpenID	Okta	<input checked="" type="checkbox"/>	openid					true	all	idp
saml-Okta-SAML	Okta	<input checked="" type="checkbox"/>	saml	http://versa-networks.co...	View More...	https://10.192.14.217/ver...	https://10.192.14.217/ver...	true	all	idp
saml-saml	Okta4	<input checked="" type="checkbox"/>	saml	http://versa-networks.co...	View More...	https://10.192.14.217/ver...	https://10.192.14.217/ver...	true	all	idp

7. Copy and save the certificate to a notepad file with the filename extension .crt.

SP Certificate

```

-----BEGIN CERTIFICATE-----
MIICxjCCAi+gAwIBAgIJANPh4/jtt/IdMA0GCSqGSIb3DQEBCwUAMHwxETAPBgNV
BAMMCERpcmVjdG9yMRcwFQYDVQQKDA52ZXJzYS1uZXRXb3B3JrczEWMWBgA1UECwwwN
VmVyc2FEaXJlY3RvcjELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbmGmb3JuaWEx
FDASBgNVBACMC1NhbnRhlENsYXJhMB4XDTEwMDIyMDIyMDA4MDg0OVoXDTEwMDIyMDIy
MDg0OVoWfDERMA8GA1UEAwwiRGlyZWNOb3B3IxFzAVBgNVBAoMDnZlcnNhLW5ldHdv
cmVyc2FEaXJlY3RvcjELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbmGmb3JuaWEx
cmtzMRlywFAYDVQLDA1WZSJzYURpcmVjdG9yMQswCQYDVQQGEwJVVzETMBEGA1UE
CAwKQ2FsaWZvcn5pYTEUMBIgA1UEBwwLU2FudGEgQ2xhcmEwgZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBALXivmCUP6ZtklqMbfp6n/asE8nfPOOSL1iaWxnth1aG
6OuygRoqTzXid87EuntBDU+rXLm9FMqKfYsbkny9mRySorv+6KhMMHe4C4yZF9S
tpqOqQpTQvskjomEsLLs3w2XVC1y1ITXVzWxsqmpZ/yWakKHMyc1HvulwDsaue7J
AgMBAAGjUDBOMBGA1UdDgQWBBR1NKShqX7cFjTnRUR70FZYXs7WjrjAfBgNVHSME
GDAWgBR1NKShqX7cFjTnRUR70FZYXs7WjrjAMBgNVHRMEBTADAQH/MA0GCSqGSIb3
DQEBCwUAA4GBAACNHNVZ6YNRoPVxwyqoYpcShhKFXGAEubtOM+JLnAZ5MqjsctwG
qgsfkfLRHw03O+B7m/Dlnkaty+siEP1vjrj/plYqNeQ9cEspLW2qjlookne1/Guh
q6vc4V8h5OrFhtZzj485ZWKKaB2GLxxScCH+TdyLY3gmO/ckp37+9J4R
-----END CERTIFICATE-----

```

8. Log in to Okta, and then click Applications > Applications.
 - a. Select the General tab. In the SAML Settings section, click Edit and then click Next.
 - b. In the Configure SAML page, click Show Advanced Settings.

okta

Search...

Dashboard

Directory

Applications

Security

Workflow

Reports

Settings

Thanks for trying the Okta Starter plan. Upgrade to the Advanced plan to create more apps and get more Monthly Active Users.

Upgrade

1 General Settings

2 Configure SAML

A SAML Settings

General

Single sign on URL

https://10:7/versa/sso/loginConsumer

☒ Use this for Recipient URL and Destination URL
 ☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID)

http://versa-networks.com/sp

Default RelayState

vd-ui::system

If no value is set, a blank RelayState is sent

Name ID format

Unspecified

Application username

Okta username

Show Advanced Settings

c. Select Enable Single Logout. Click Browse, select the Signature Certificate file (a .crt file), and then click Upload Certificate.

https://docs.versa-networks.com/Management_and_Orchestration/Versa_Concerto_Orchestrator/02_Common_Configuration/...

Updated: Wed, 23 Oct 2024 08:53:33 GMT

Copyright © 2024, Versa Networks, Inc.

17

okta

Dashboard

Directory

Applications

Security

Workflow

Reports

Settings

Q Search...

Edit SAML Integration

1 General Settings

2 Configure SAML

A SAML Settings

General

Single sign on URL

https://10.192.14.217/versa/so/loginConsumer

Use this for Recipient URL and Destination URL

Allow this app to request other SSO URLs

Audience URI (SP Entity ID)

http://versa-networks.com/sp

Default RelayState

vd-ut:system

If no value is set, a blank RelayState is sent

Name ID format

Unspecified

Application username

Okta username

Hide Advanced Settings

Response

Signed

Assertion Signature

Signed

Signature Algorithm

RSA-SHA256

Digest Algorithm

SHA256

Assertion Encryption

Unencrypted

Enable Single Logout

Allow application to initiate Single Logout

Single Logout URL

https://10.192.14.217/versa/so/logoutConsumer

SP Issuer

http://versa-networks.com/sp

Signature Certificate

Browse

Upload Certificate

Assertion Inline Hook

None (disabled)

Authentication context class

PasswordProtectedTransport

Honor Force Authentication

Yes

SAML Issuer ID

http://www.okta.com/{org.externalKey}

Attribute Statements (optional)

LEARN MORE

Name	Name format (optional)	Value
role	Unspecified	appuser.role
org	Unspecified	appuser.org
idleTimeOut	Unspecified	appuser.idleTimeOut

Add Another

Group Attribute Statements (optional)

Name	Name format (optional)	Filter
	Unspecified	Starts with

Add Another

B Preview the SAML assertion generated from the information above

Preview the SAML Assertion

This shows you the XML that will be used in the assertion - use it to verify the info you entered above

Previous

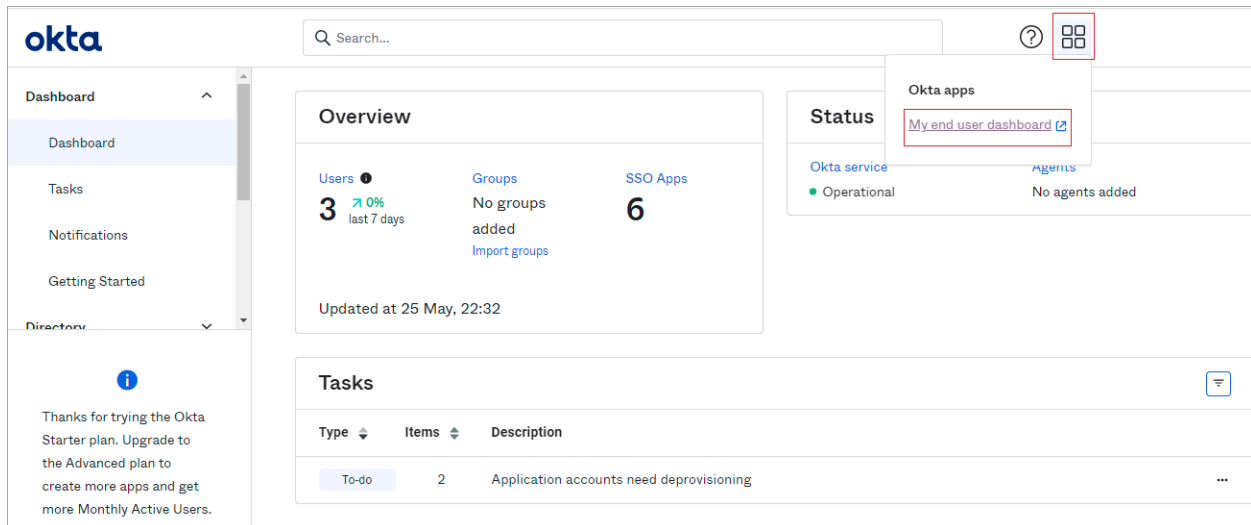
Cancel

Next

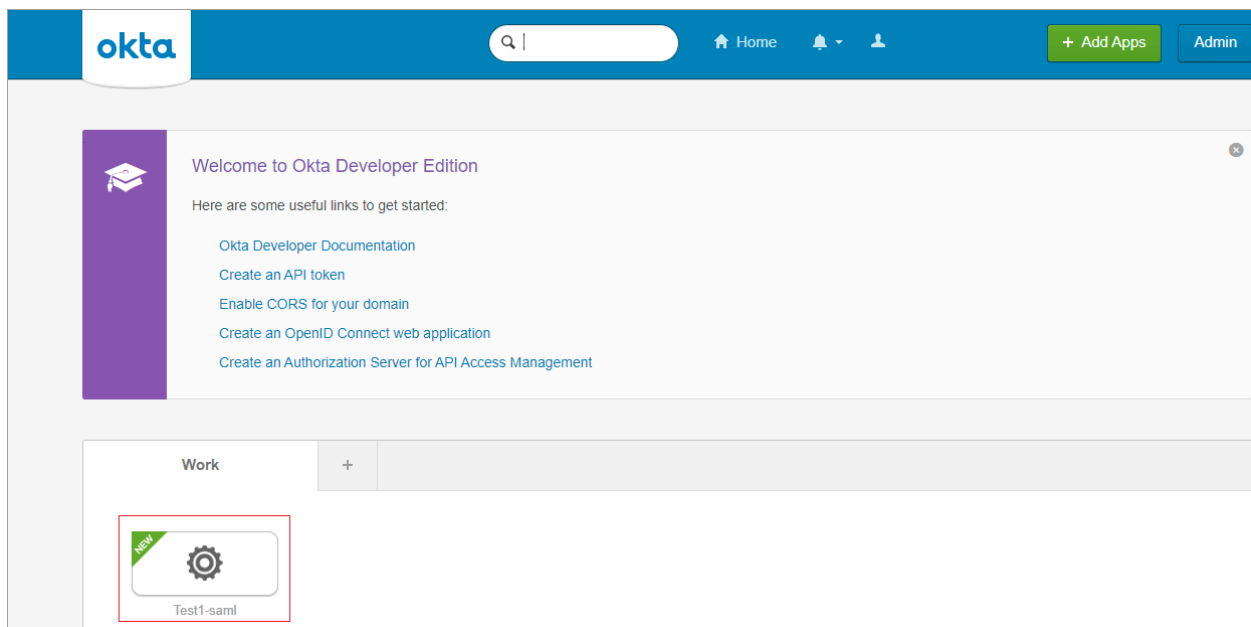
d. Click Next.

Log In with IDP-Initiated SSO

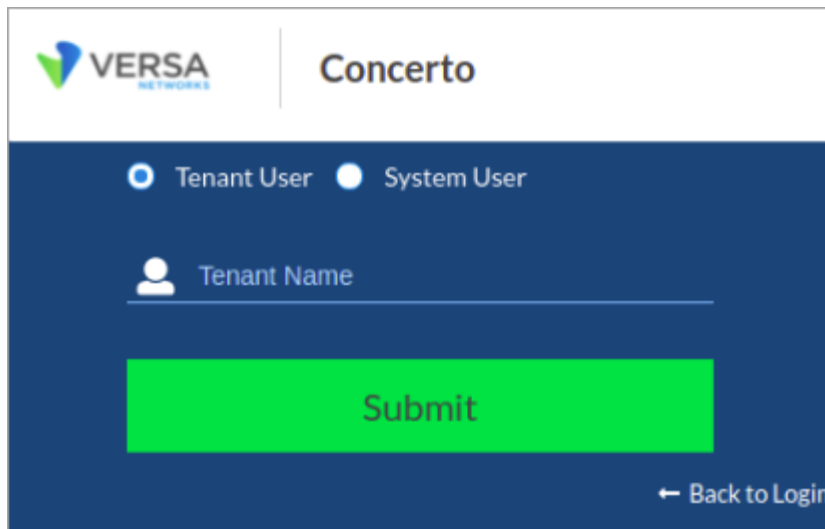
1. Log in to www.okta.com using your credentials.
2. In the left menu bar, select Dashboard > Dashboard.
3. Click the Okta Apps icon, and then click My End-User Dashboard.



4. Click the SAML connector.



The Concerto SSO login page displays.



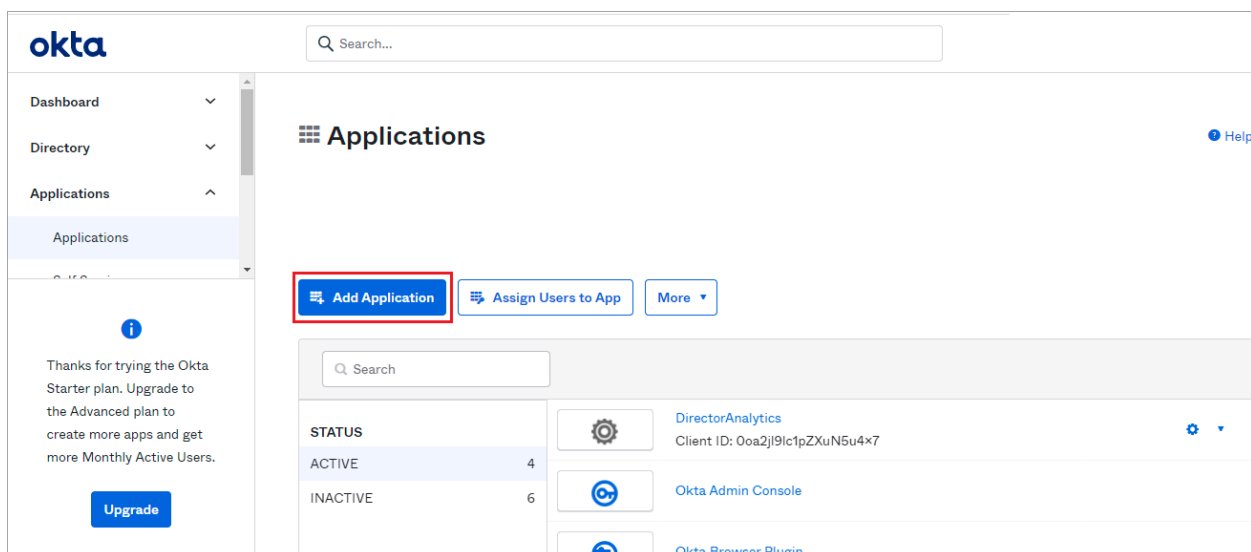
The image shows the Concerto login interface. At the top left is the Versa Networks logo, and at the top right is the word "Concerto". Below this is a dark blue header bar containing two radio buttons: "Tenant User" (selected) and "System User". Underneath is a white input field labeled "Tenant Name" with a user icon on the left. A large green "Submit" button is centered below the input field. In the bottom right corner, there is a link that says "← Back to Login".

Configure OpenID Connect SSO Using Okta

Create an Application

To create an OpenID-based single sign-on using Okta:

1. Create an account in www.okta.com
2. Log in to Okta using your credentials.
3. Select Applications in the left menu bar, and then click Add Application to create a new OpenID Connect application.

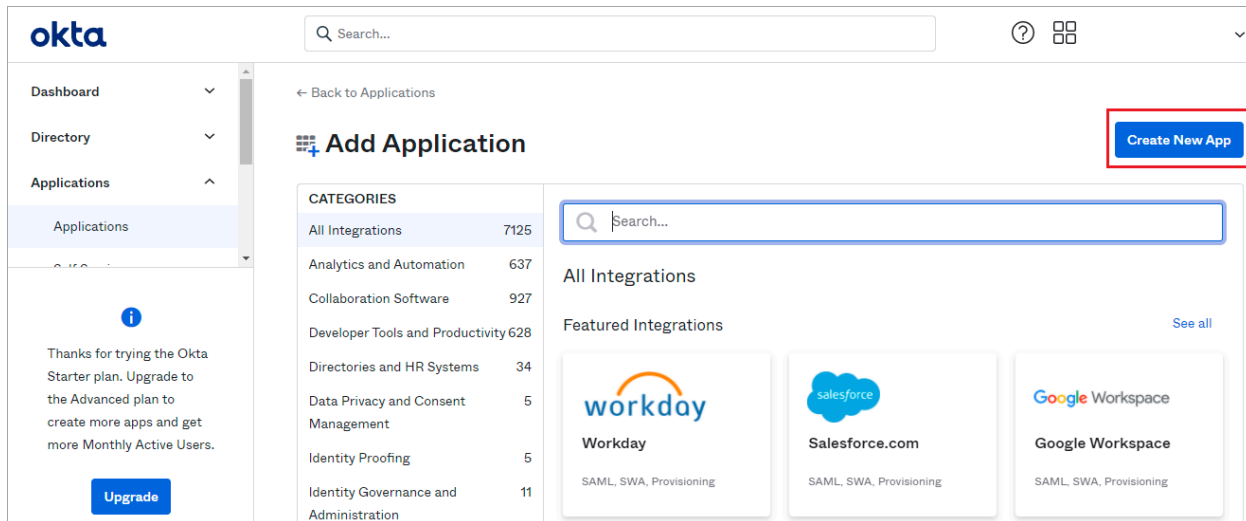


4. Click Create New App to create an OpenID application. The Create a New Application Integration screen displays.

https://docs.versa-networks.com/Management_and_Orchestration/Versa_Concerto_Orchestrator/02_Common_Configuration/...

Updated: Wed, 23 Oct 2024 08:53:33 GMT

Copyright © 2024, Versa Networks, Inc.



5. Click OIDC-OpenID Connect and Web Application, and then click Next.

Create a new app integration

Sign-on 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.

Application type

What kind of application are you trying to integrate with Okta?

Specifying an application type customizes your experience and provides the best configuration, SDK, and sample recommendations.

- ☒ **Web Application**
Server-side applications where authentication and tokens are handled on the server (for example, Go, Java, ASP.Net, Node.js, PHP)
- ☐ **Single-Page Application**
Single-page web applications that run in the browser where the client receives tokens (for example, Javascript, Angular, React, Vue)
- ☐ **Native Application**
Desktop or mobile applications that run natively on a device and redirect users to a non-HTTP callback (for example, iOS, Android, React Native)

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

https://docs.versa-networks.com/Management_and_Orchestration/Versa_Concerto_Orchestrator/02_Common_Configuration/...

Updated: Wed, 23 Oct 2024 08:53:33 GMT

Copyright © 2024, Versa Networks, Inc.

6. Enter information for the indicated fields.

okta

Search...

?

Dashboard

Directory

Applications

Security

Workflow

Reports

Thanks for trying the Okta Starter plan. Upgrade to the Advanced plan to create more apps and get more Monthly Active Users.

New Web App Integration

General Settings

App integration name

test-OpenID

Logo (Optional)

Grant type

Client acting on behalf of itself

Client Credentials

Client acting on behalf of a user

Authorization Code

Refresh Token

Implicit (Hybrid)

Sign-in redirect URIs

Okta sends the authentication response and ID token for the user's sign-in request to these URIs

https://10.230.90.135/versa/sso/openid/loginConsumer

+ Add URI

Sign-out redirect URIs (Optional)

After your application contacts Okta to close the user session, Okta redirects the user to one of these URIs.

https://10.230.90.135/versa/sso/openid/logoutConsumer|

+ Add URI

Trusted Origins

Base URIs (Optional)

Required if you plan to self-host the Okta Sign-In Widget. With a Trusted Origin set, the Sign-In Widget can make calls to the authentication API from this domain.

+ Add URI

Assignments

Controlled access

Allow everyone in your organization to access

Limit access to selected groups

Save

Cancel

Field	Description
General Setting (Group of Fields)	

https://docs.versa-networks.com/Management_and_Orchestration/Versa_Concerto_Orchestrator/02_Common_Configuration/...
Updated: Wed, 23 Oct 2024 08:53:33 GMT
Copyright © 2024, Versa Networks, Inc.

22

Field	Description
◦ Application integration name	Enter a name for the OpenID connect application.
◦ Logo	Browse and select a logo to represent the OpenID Connect.
Configure OpenID Connect (Group of Fields)	
◦ Sign-in redirect URIs	Enter the URI to which Okta sends OAuth responses. The login redirect URI format is <code>https://versa-director-ip/versa/sso/openid/loginConsumer</code> .
◦ Sign-out redirect URIs	Enter the URI to which Okta sends relying party-initiated logouts. The logout redirect URI format is <code>https://versa-director-ip/versa/sso/openid/logoutConsumer</code> .

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

okta

Q Search...

?

☰

⋮

Dashboard

Directory

Applications

Applications

Self Service

Security

Workflow

Reports

Settings

Thanks for trying the Okta Starter plan. Upgrade to the Advanced plan to create more apps and get more Monthly Active Users.

Upgrade

← Back to Applications

⚙️

-OpenID

Active

View Logs

General

Sign On

Assignments

Okta API Scopes

Client Credentials

Client ID

0oapzrmh3vt3TgHx85d6

Public identifier for the client that is required for all OAuth flows.

Client secret

.....

Secret used by the client to exchange an authorization code for a token. This must be kept confidential! Do not include it in apps which cannot keep it secret, such as those running on a client.

Ready to code

You can download a preconfigured sample app.

Download sample app

To get started using your custom app integration, see the "Sign Users In" section in the Okta Developer's guide

General Settings

Okta domain

dev-2322987.okta.com

APPLICATION

App integration name

sarath-OpenID

Application type

Web

Grant type

Client acting on behalf of itself

Client Credentials

Client acting on behalf of a user

Authorization Code

Refresh Token

Implicit (Hybrid)

USER CONSENT

User consent

Require consent

Terms of Service URI

Policy URI

Logo URI

LOGIN

Sign-in redirect URIs

https://10.192.14.217/versa/sso/openid/loginConsumer

Sign-out redirect URIs

https://10.192.14.217/versa/sso/openid/logoutConsumer

Login initiated by

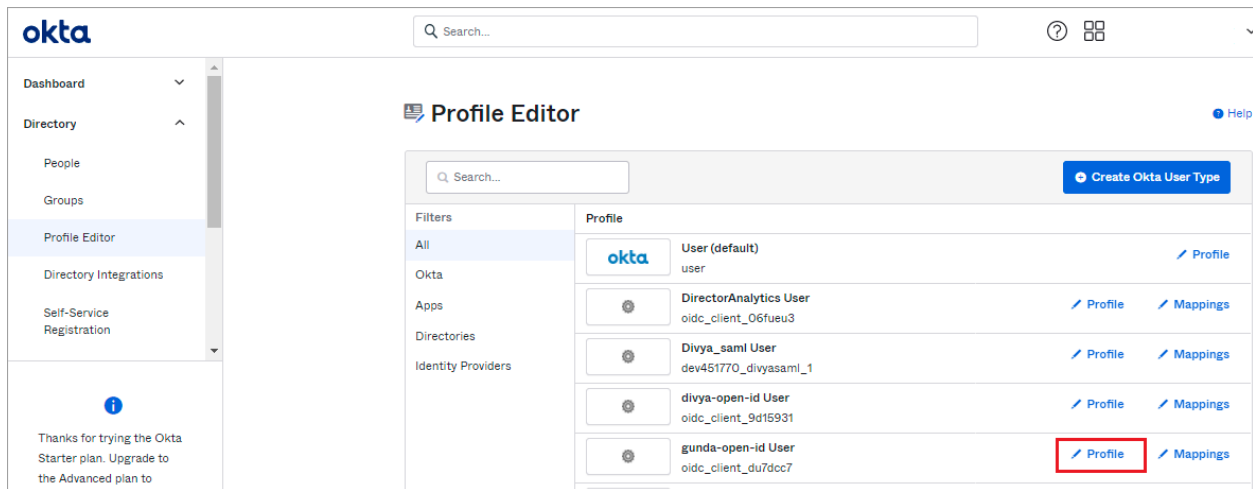
App Only

Initiate login URI

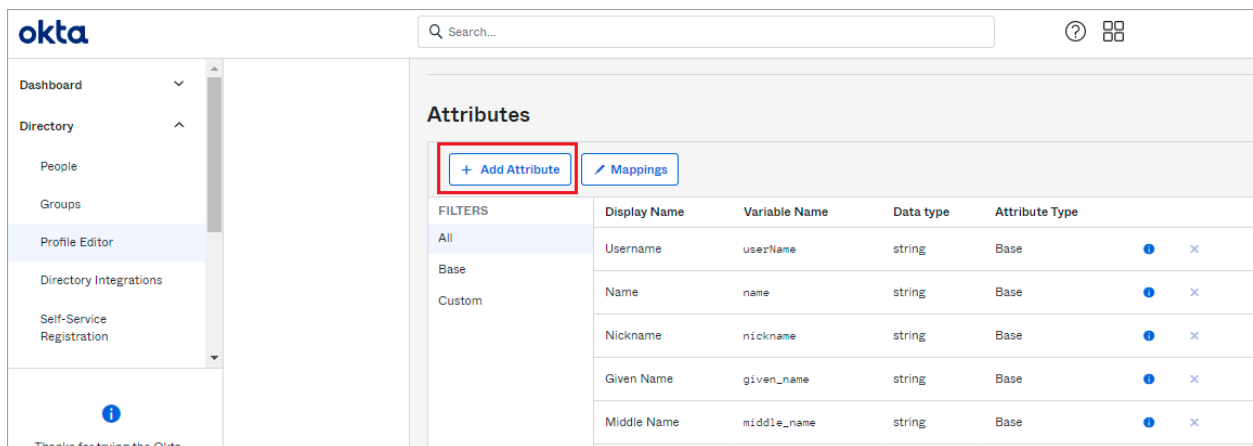
https://10.192.14.217/versa/sso/openid/loginConsumer

Create Custom Attributes

- To add custom attributes, select Directory > Profile Editor in the left menu bar and then select the newly created OpenID Connect.



2. On the next page that opens, select Add Attribute.



3. In the Add Attribute window, add roles, organization, and idle timeout as attributes. The attribute values are case sensitive.

Add Attribute

* Local app attributes are only stored on Okta and not created in versatest-openid. Use local attributes if you plan to add the attribute to versatest-openid 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

These attributes display in the attribute dashboard.

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

Add Users to an Application

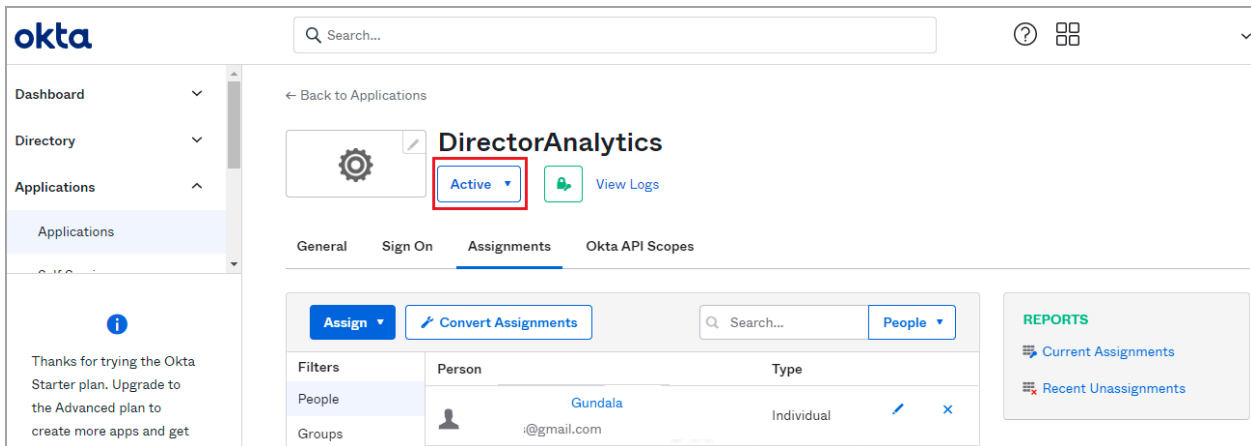
1. To assign users to the Versa Director, in the left menu bar, select Applications > Applications and click the newly

https://docs.versa-networks.com/Management_and_Orchestration/Versa_Concerto_Orchestrator/02_Common_Configuration/...

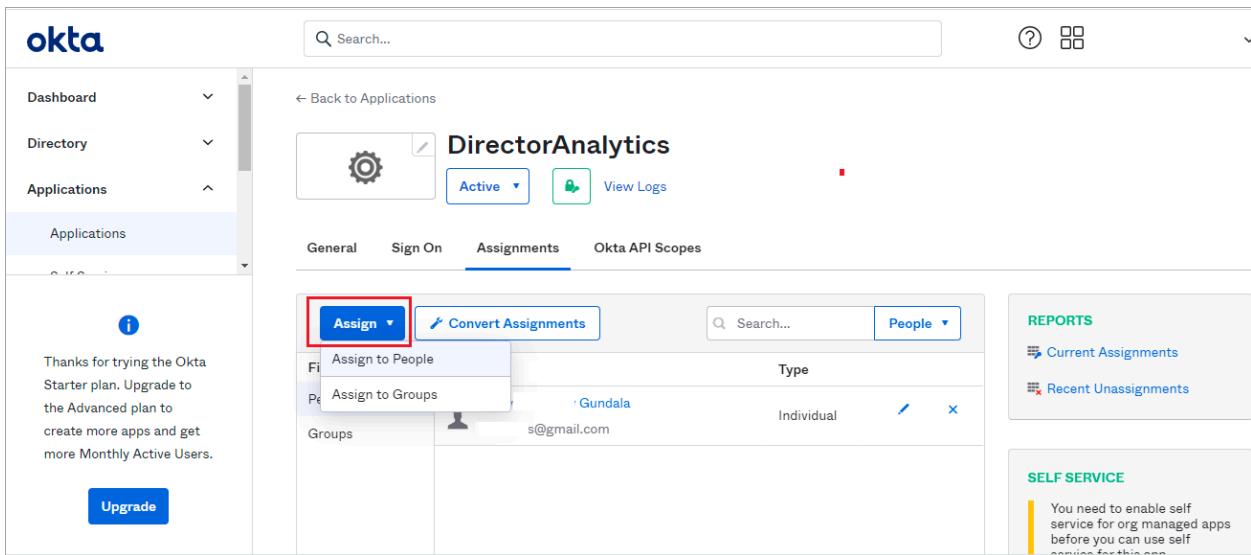
Updated: Wed, 23 Oct 2024 08:53:33 GMT

Copyright © 2024, Versa Networks, Inc.

created OpenID connect.



2. Select the Assignments tab. Click the Assign field, and then click Assign to People.



3. Select a person and then click Assign.

Assign gunda-open-id to People

Q Search...

Srinivasa mypersonal@gmail.com	Assign
sarath mypersonal@gmail.com	Assign
sarath mypersonal@gmail.com	Assign
renga mypersonalmobilea@gmail.com	Assign

4. In the preview page that opens, enter the roles, organization, and idle timeout for the user and then click Save and Go Back to complete the process.

Assign

openid to Groups

×

i

Extra info is needed to assign this app to a group.
The attributes below will apply to all people assigned to this group.

roles

provider-org

org

TenantSuperAdmin

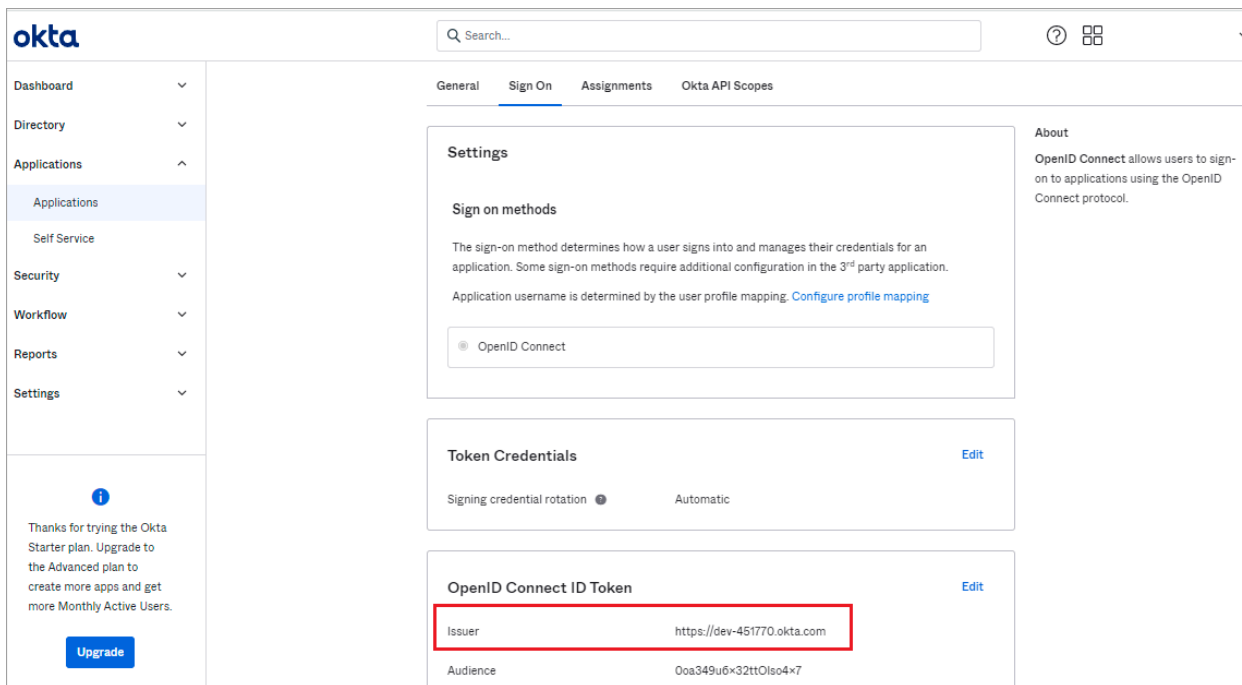
idleTimeOut

15

Save and Go Back

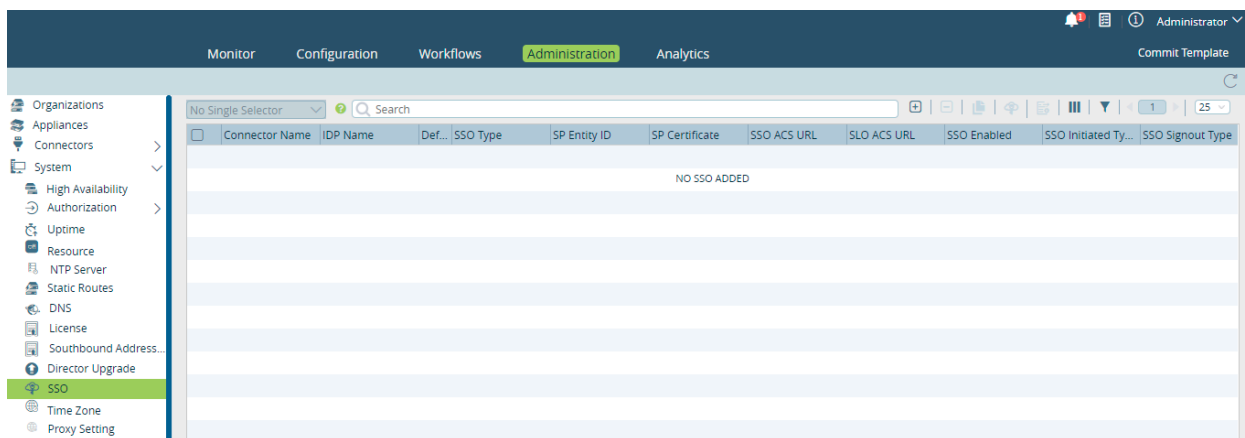
Cancel and Go Back

5. In your app, go to Application > Open, click Sign On, and then copy the Issuer to configure the connector on the Director node.



Configure an SSO Connector in Versa Director

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



3. Click the  Add icon, and in the Add SSO popup window, enter information for the following fields.

Add SSO

Connector Name*

sara-openID

IDP Name*

okta

Organization

Organization

Versa Director FQDN/IP Address*

SSO Initiated Type

All

SSO Type

openid

SSO Signout Type

Local

Logout Success Redirect URL

☒ SSO Enabled

Logout Endpoint*

https://dev-754693.oktapreview.com/oauth2/v1/logout

Authorize Endpoint*

https://dev-754693.oktapreview.com/oauth2/v1/authorize

Token Endpoint*

https://dev-754693.oktapreview.com/oauth2/v1/token

UserInfo Endpoint*

https://dev-754693.oktapreview.com/oauth2/v1/userinfo

Revoke Endpoint*

https://dev-754693.oktapreview.com/oauth2/v1/revoke

Client ID*

00kahdijfwdinikk

Client Secret*

4rhskdhaHuutgkhik

Analytics Client

OpenID User Attributes

Concerto Client

Metadata

VAN IP/FQDN*

VAN APP ID*

+

No Records to Display

OK

Cancel

Fields	Description
Connector Name (Required)	Enter the name of the connector.
IDP Name (Required)	Enter the IDP name.
Organization	Select the name of the organization.
Versa Director FQDN/IP Address (Required)	Enter the IP address of the Director node.
SSO Initiated Type	<p>Select the type of SSO initiation:</p> <ul style="list-style-type: none"> ◦ All ◦ IDP Initiated ◦ SP Initiated
SSO Type	<p>Select the SSO type:</p> <ul style="list-style-type: none"> ◦ OpenID—OpenID is an open-standard data format for exchanging authentication data and authorization data between an identity provider and a service provider. ◦ SAML—SAML is an XML-based, open-standard data format for exchanging authentication data and authorization data between an identity provider and a service provider.
SSO Signout Type	<p>Select the SSO signout type:</p> <ul style="list-style-type: none"> ◦ IDP—Both the Director and the IDP sessions are cleared. ◦ Local—Only the Director session is cleared.
Logout Success Redirect URL	Enter the URL to which to be redirected after a successful IDP logout.
SSO Enabled	Click to enable SSO.
Logout Endpoint (Required)	Enter the logout redirect URIs received from the Okta page, for example, <i>issuer/oauth2/v1/logout</i> .
Authorize Endpoint (Required)	Enter the URL that interacts with the IDP and obtains an authorization grant, for example, <i>issuer/oauth2/v1/authorize</i> .
Token Endpoint (Required)	Enter the IDP endpoint to get the access token, for example, <i>issuer/oauth2/v1/token</i> .

UserInfo Endpoint (Required)	Enter the IDP endpoint to get the user details; for example, <i>issuer/oauth2/v1/userinfo</i> .
Revoke Endpoint (Required)	Enter the IDP endpoint to revoke the access token; for example, <i>issuer/oauth2/v1/revoke</i> .
Client ID (Required)	Enter the client ID information received from the Okta page.
Client Secret (Required)	Enter the client secret information received from the Okta page.

4. Click OK.

Log In with IDP-Initiated SSO

To log in with OpenID IDP-initiated SSO, update the Okta URL to one in the following format:

`https://authorize_end_point?client_id=app_client_id&state=client_name::org_name&nonce=null&response_type=code&redirection_uri=https://ip_address:443/management/authorize/sso/openid/loginConsumer&scope=openid+profile+email`

Field	Description
<i>authorize_end_point</i>	Enter the URL that interacts with the IDP and obtain an authorization grant.
<i>app_client_id</i>	Enter the client ID information received from the Okta page.
<i>client_name</i>	Enter the name of the client: <ul style="list-style-type: none"> For Analytics, use van-ui. For Concerto, use concerto. For Director, use vd-ui.
<i>org_name</i>	Enter the name of the organization: <ul style="list-style-type: none"> For system users, use system. For tenant users, enter the tenant name.
<i>director_ip_address</i>	Enter the Director IP address.

For example:

https://docs.versa-networks.com/Management_and_Orchestration/Versa_Concerto_Orchestrator/02_Common_Configuration/...

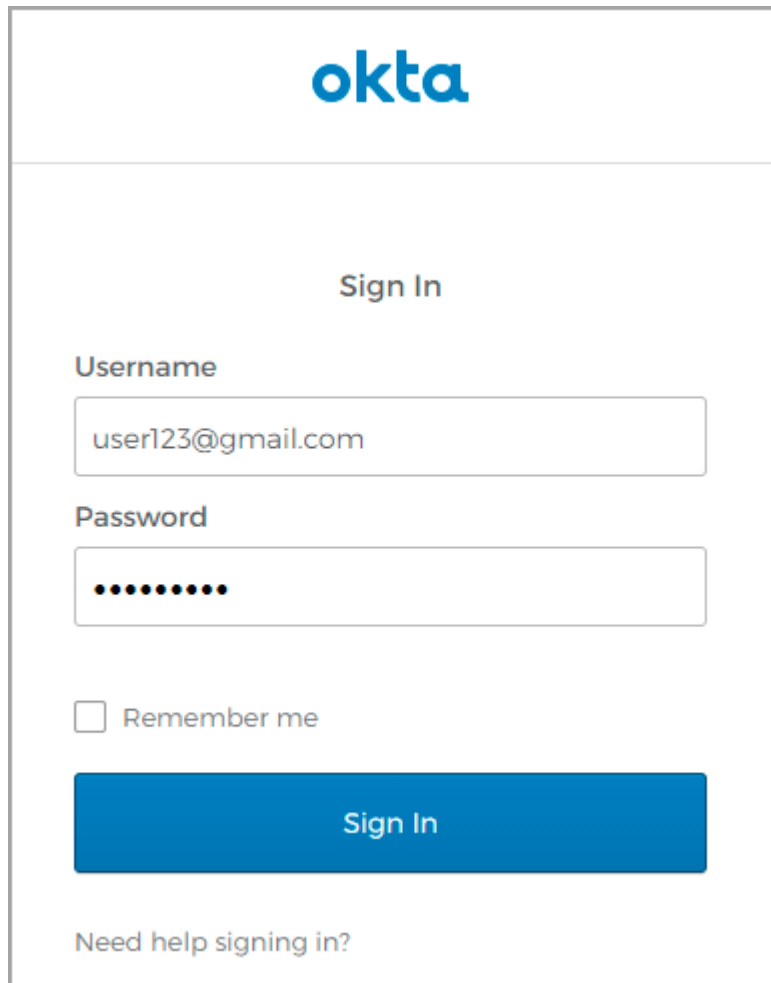
Updated: Wed, 23 Oct 2024 08:53:33 GMT

Copyright © 2024, Versa Networks, Inc.

<https://dev-754693.oktapreview.com/o...+profile+email>

Copy the link and paste it in a browser URI field. The Okta log in page displays.

Enter the Okta username and password.

The image shows the Okta Sign In page. At the top is the Okta logo. Below it is the heading "Sign In". There are two input fields: "Username" with the value "user123@gmail.com" and "Password" with masked characters. Below the password field is a checkbox labeled "Remember me". A large blue "Sign In" button is centered below the checkbox. At the bottom, there is a link that says "Need help signing in?".

okta

Sign In

Username

user123@gmail.com

Password

.....

☐ Remember me

Sign In



Need help signing in?

The Director home page displays.

Configure SSO for Tenant Users

To configure SSO for tenant users in an organization, you must update the IDP connector for the tenant's organization, and you must add supported user roles.


To configure SSO for tenant users:

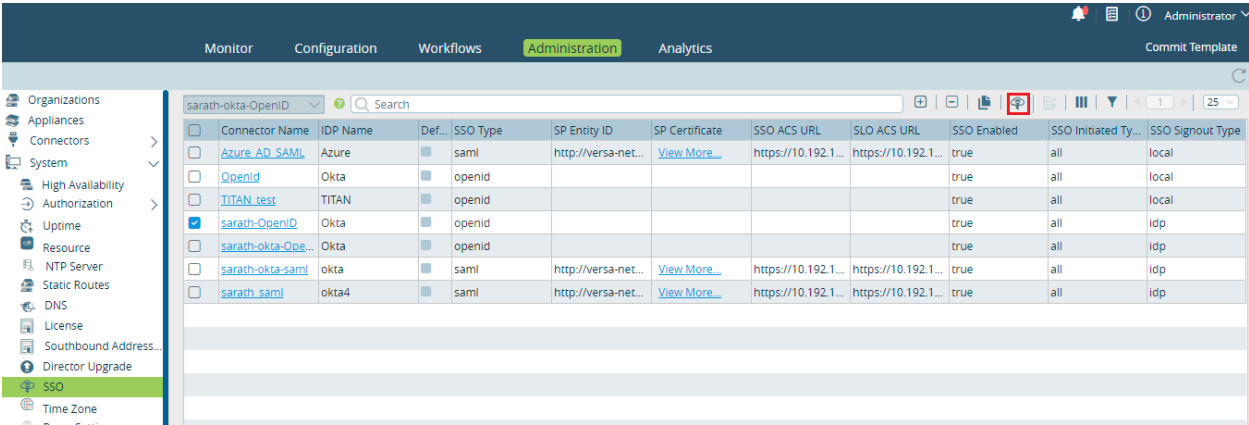
1. In Director view, select the Administration tab in the top menu bar.
2. Select System  > SSO  in the left menu bar.

https://docs.versa-networks.com/Management_and_Orchestration/Versa_Concerto_Orchestrator/02_Common_Configuration/...

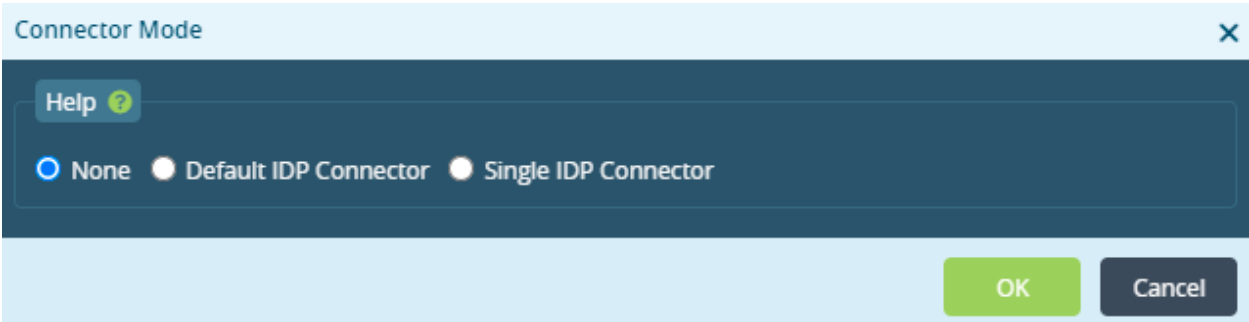
Updated: Wed, 23 Oct 2024 08:53:33 GMT

Copyright © 2024, Versa Networks, Inc.

3. Click a connector, and then click Connector Mode .




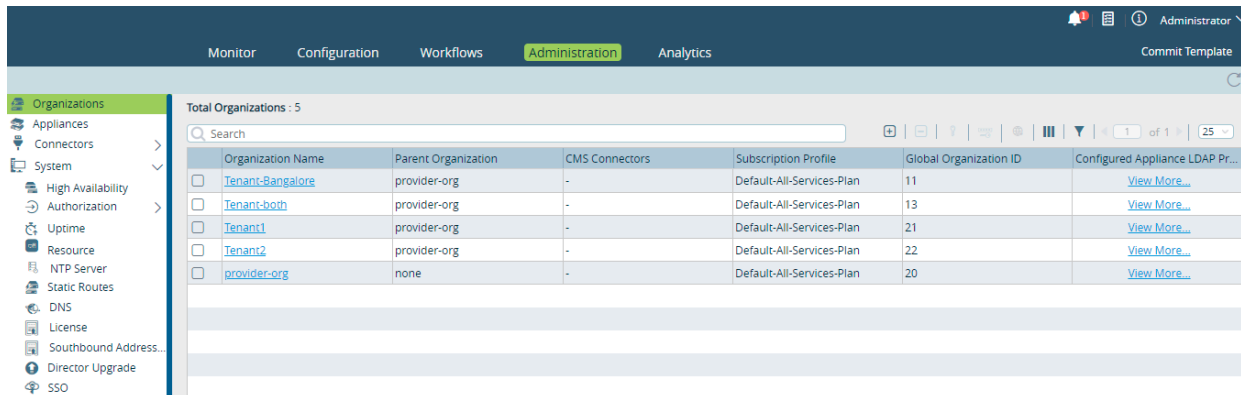
4. In the Connector Mode popup window, select the connector mode.




Field	Description
None	Click if provider users do not require connector mode. System users cannot use this connector mode to log in.
Default IDP Connector	Click for system users. Tenant users do not need to configure the IDP connector on the organization page.
Single IDP Connector	Click for all provider and tenant users. Tenant users do not need to configure the IDP connector on the organization page.

5. Click OK.

6. Select the Administration tab in the top menu bar, and then select  Organizations in the left menu bar.



7. Click an existing organization name, or click the  Add icon to add a new tenant. The Add/Edit Organization popup window displays.
8. In the IDP Connector field, select the name of IDP connector to use for Versa Director SSO.

Add Organization

Name * Description

Tags Global Organization ID * Organization Label

Parent Organization Shared Control Plane ☐ Subscription Profile * CPE Deployment Type

IDP Connector Secure Access Portal Inactivity Interval

Authentication CMS Connectors CMS Organizations Analytics Cluster Routing Instance Supported User Roles

Available Add All

Selected Remove All

TenantDashboardOperator	×
TenantSecurityAdmin	×
TenantSuperAdmin	×
TenantOperator	×

OK Cancel

9. Select the Supported User Roles tab, and select the roles for the tenant.

Add Organization

Name *
parent-org

Description

Tags

Global Organization ID *
1

Organization Label
This may be used for organization mapping

Parent Organization
provider-org

☐ Shared Control Plane

Subscription Profile *
Default-All-Services-Plan

CPE Deployment Type
SDWAN

IDP Connector
--Select--

Secure Access Portal

Inactivity Interval
48

Authentication
CMS Connectors
CMS Organizations
Analytics Cluster
Routing Instance
Supported User Roles

Available
Add All

Selected
Remove All

Search

Search

TenantDashboardOperator
x

TenantSecurityAdmin
x

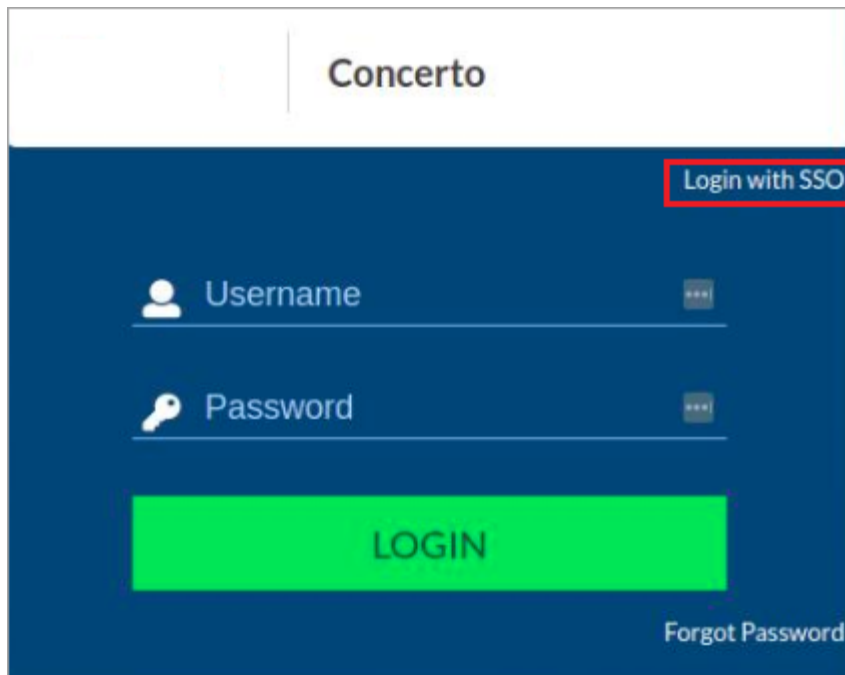
TenantSuperAdmin
x

TenantOperator
x

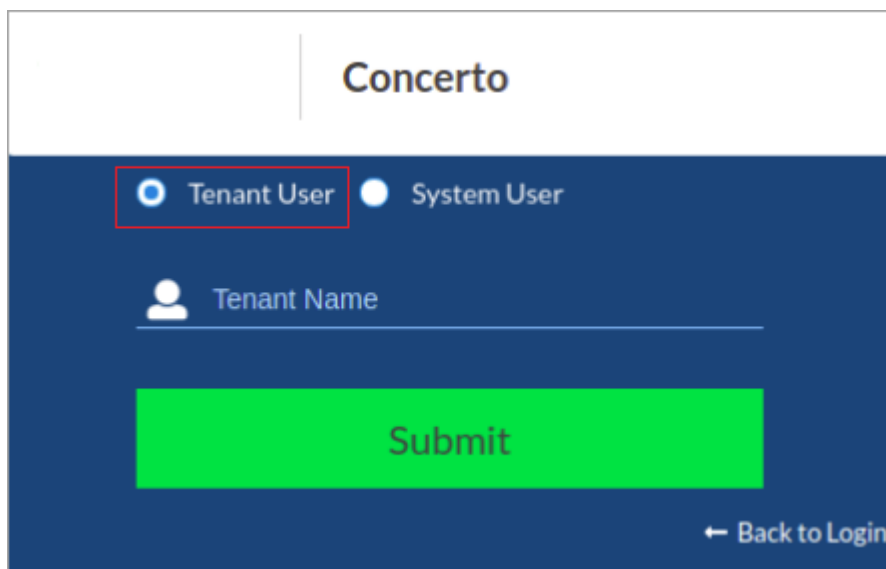
OK

Cancel

10. For information about configuring the other fields on the Add Organization popup window, see the Configure Tenants section in [Configure Multitenancy](#).
11. Click OK.
12. Log out of Versa Director.
13. In Concerto, click Login with SSO.

The image shows the Concerto login interface. At the top, the word "Concerto" is displayed in a white header. Below the header, there is a dark blue background. In the top right corner, a red box highlights the "Login with SSO" link. Below this, there are two input fields: "Username" with a person icon and "Password" with a key icon. Both fields have a small "xxx" placeholder text. Below the input fields is a large red "LOGIN" button. In the bottom right corner, there is a link that says "Forgot Password".

14. Click Tenant User, and enter the tenant name.

The image shows the Concerto tenant selection interface. At the top, the word "Concerto" is displayed in a white header. Below the header, there is a dark blue background. In the top left corner, there are two radio buttons: "Tenant User" (which is selected and highlighted with a red box) and "System User". Below the radio buttons, there is an input field labeled "Tenant Name" with a person icon. Below the input field is a large red "Submit" button. In the bottom right corner, there is a link that says "← Back to Login".

15. Click Submit.

Log In with SSO for Service Providers

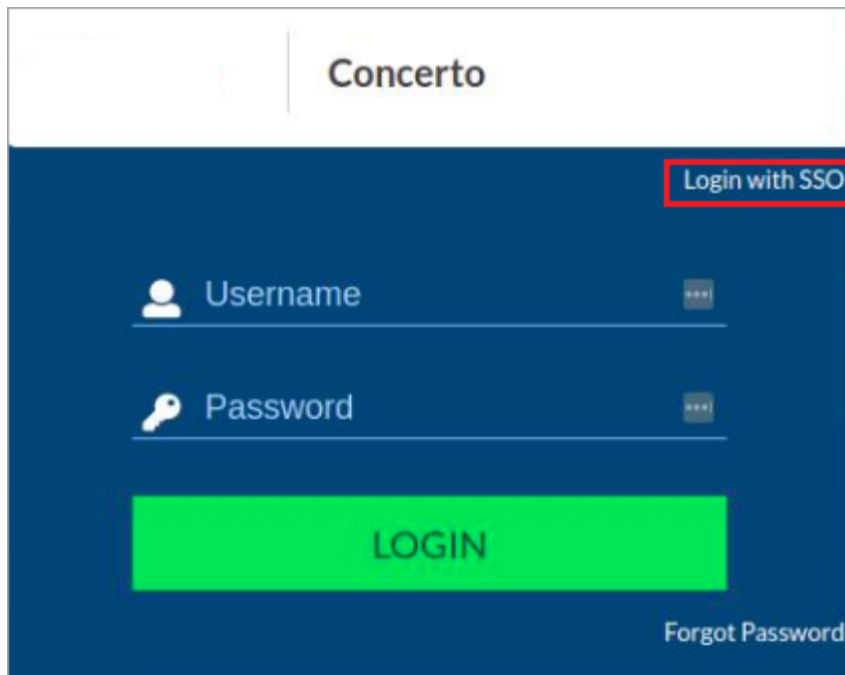
To log in with SSO for service providers:

1. In Concerto, click Login with SSO.

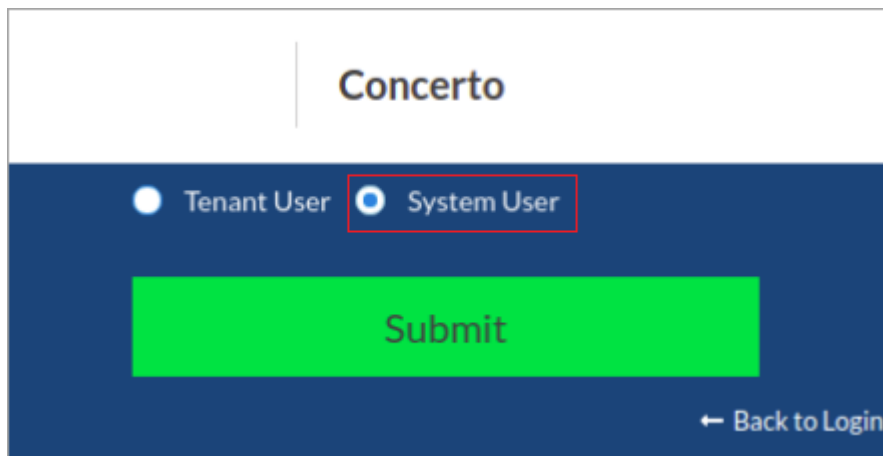
https://docs.versa-networks.com/Management_and_Orchestration/Versa_Concerto_Orchestrator/02_Common_Configuration/...

Updated: Wed, 23 Oct 2024 08:53:33 GMT

Copyright © 2024, Versa Networks, Inc.

The image shows the Concerto login interface. At the top, the word "Concerto" is displayed. Below it, there is a "Login with SSO" link highlighted with a red box. The main form has two input fields: "Username" with a user icon and "Password" with a key icon. Both fields have a red "x" icon to the right. Below the fields is a large green "LOGIN" button. At the bottom right, there is a "Forgot Password" link.

2. Click System User.

The image shows the Concerto user selection interface. At the top, the word "Concerto" is displayed. Below it, there are two radio buttons: "Tenant User" and "System User". The "System User" radio button is selected and highlighted with a red box. Below the radio buttons is a large green "Submit" button. At the bottom right, there is a "← Back to Login" link.

3. Click Submit.

Supported Software Information

Releases 10.2.1 and later support all content described in this article.

Additional Information

[Configure Single Sign-On Using Director](#)