



Rydoo Single-Sign-On

SUPPORT



Configure Rydoo Single Sign-On (SSO) with Okta

This guide walks you through setting up SAML-based Single Sign-On (SSO) between Okta and Rydoo.

In SAML terms, Okta is your Identity Provider (IdP) and Rydoo is the Service Provider (SP). You'll first configure an Okta application with Rydoo's SP details, then share Okta's Identity Provider metadata with Rydoo so we can complete the connection on our end.

Note: If you're using the Okta Developer Console, switch to the Classic UI first. Click the "< > Developer" menu in the top-left corner and select Classic UI.

1. Create the SAML application in Okta

1. Log in to your Okta organization as a user with administrator privileges. If you don't have an Okta organization yet, you can create a free Okta Developer Edition account.

2. From the Okta dashboard, click Admin.



3. Click the Add Applications shortcut.



4. Click Create New App.



5. In the dialog that opens, select the SAML 2.0 platform option, then click Create.

Create a New Application Integration

Platform

Web

Sign on method

☐ Secure Web Authentication (SWA)
Uses credentials to sign in. This integration works with most apps.

☒ SAML 2.0
Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.

☐ OpenID Connect
Uses the OpenID Connect protocol to log users into an app you've built.

Create

Cancel

6. On the General Settings screen, enter "Rydoo SAML Application" as the App name, then click Next.

1 General Settings

App name

Example SAML Application

App logo (optional) ?



Browse..

Upload Logo

App visibility

☐ Do not display application icon to users

☐ Do not display application icon in the Okta Mobile app

Cancel

Next

7. On the Configure SAML screen, in section A (SAML Settings), enter the following values:

- **Single sign on URL:** `https://accounts.rydoo.com/saml2/Acs`
- **Audience URI (SP Entity ID):** `https://accounts.rydoo.com/`
- **Name ID format:** EmailAddress
- **Application username:** Email

A SAML Settings

GENERAL

Single sign on URL ?

https://accounts.rydoo.com/saml2/Acs

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

Audience URI (SP Entity ID) ?

https://accounts.rydoo.com/

Default RelayState ?

If no value is set, a blank RelayState is sent

Name ID format ?

EmailAddress

▼

Application username ?

Email

▼

Show Advanced Settings

8. Still on the Configure SAML screen, under Attribute Statements, add the following three attributes, then click Next:

- **FirstName** → `user.firstName`
- **LastName** → `user.lastName`
- **Email** → `user.email`

ATTRIBUTE STATEMENTS (OPTIONAL)

LEARN MORE

Name	Name format (optional)	Value	
FirstName	Unspecified ▾	user.firstName ▾	×
LastName	Unspecified ▾	user.lastName ▾	×
Email	Unspecified ▾	user.email ▾	×

Add Another

9. On the Feedback screen, select “I’m an Okta customer adding an internal app” and check “This is an internal app that we have created,” then click Finish.

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

i

The optional questions below assist Okta Support in understanding your app integration.

App type ?

☒ This is an internal app that we have created
 ☐ This is an external app that we are integrating

Previous

Finish

2. Share the Identity Provider metadata with Rydoo

10. On the Sign On tab of your new Rydoo application, right-click the Identity Provider metadata link and copy its URL. Keep this tab open — you'll come back to it later.

Settings Edit

SIGN ON METHODS

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

SAML 2.0

Default Relay State



SAML 2.0 is not configured until you complete the setup instructions.

View Setup Instructions

[Identity Provider metadata](#) is available if this application supports dynamic configuration.

CREDENTIALS DETAILS

Application username formatOkta username

Password reveal☐ Allow users to securely see their password (Recommended)

11. Send this metadata link to Rydoo. We'll use it to establish the trust connection between Okta and Rydoo.

3. Assign users to the application

12. Open the Assignments tab of your Rydoo application (open it in a new tab so you can return to the Sign On tab afterward).

13. Click Assign, then select Assign to People.

General Sign On Import Assignments

Assign 

 Convert Assignments

Assign to People

Assign to Groups

Groups

14. Search for the person who should have access, then click Assign next to their name.

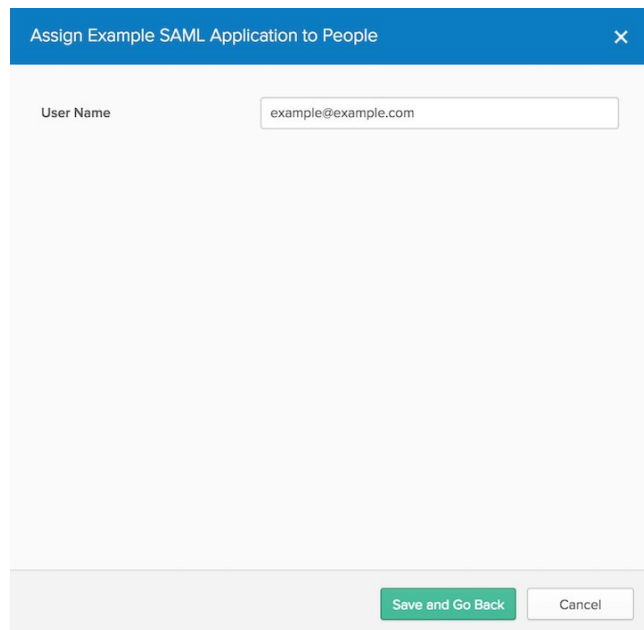
Assign Example SAML Application to People ×

Q Search...

Example User
example@example.com

Assign

15. Review the user's attributes, then click Save and Go Back.



Assign Example SAML Application to People

User Name

example@example.com

Save and Go Back Cancel

16. Click Done to close the assignment wizard.

Once you've completed these steps and shared the Identity Provider metadata with us, we'll finish setting up the connection on the Rydoo side. After that, anyone assigned to the application can sign in to Rydoo directly through Okta.