

Single sign-on: Okta as Identity Provider

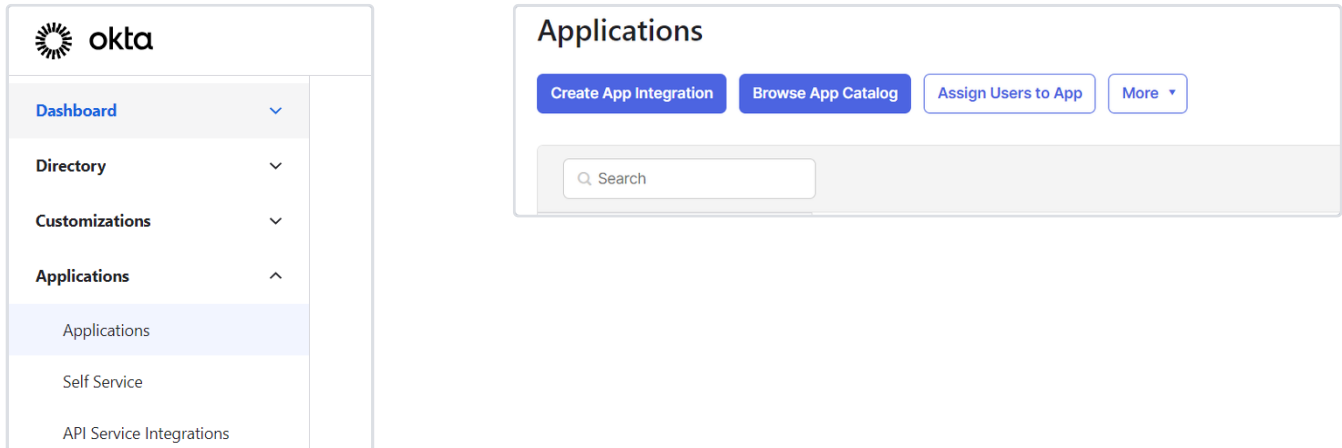
Introduction

This is an example of setting up SAML-based Single sign-on (SSO) with an Okta Workforce account as your Identity Provider.

Instructions

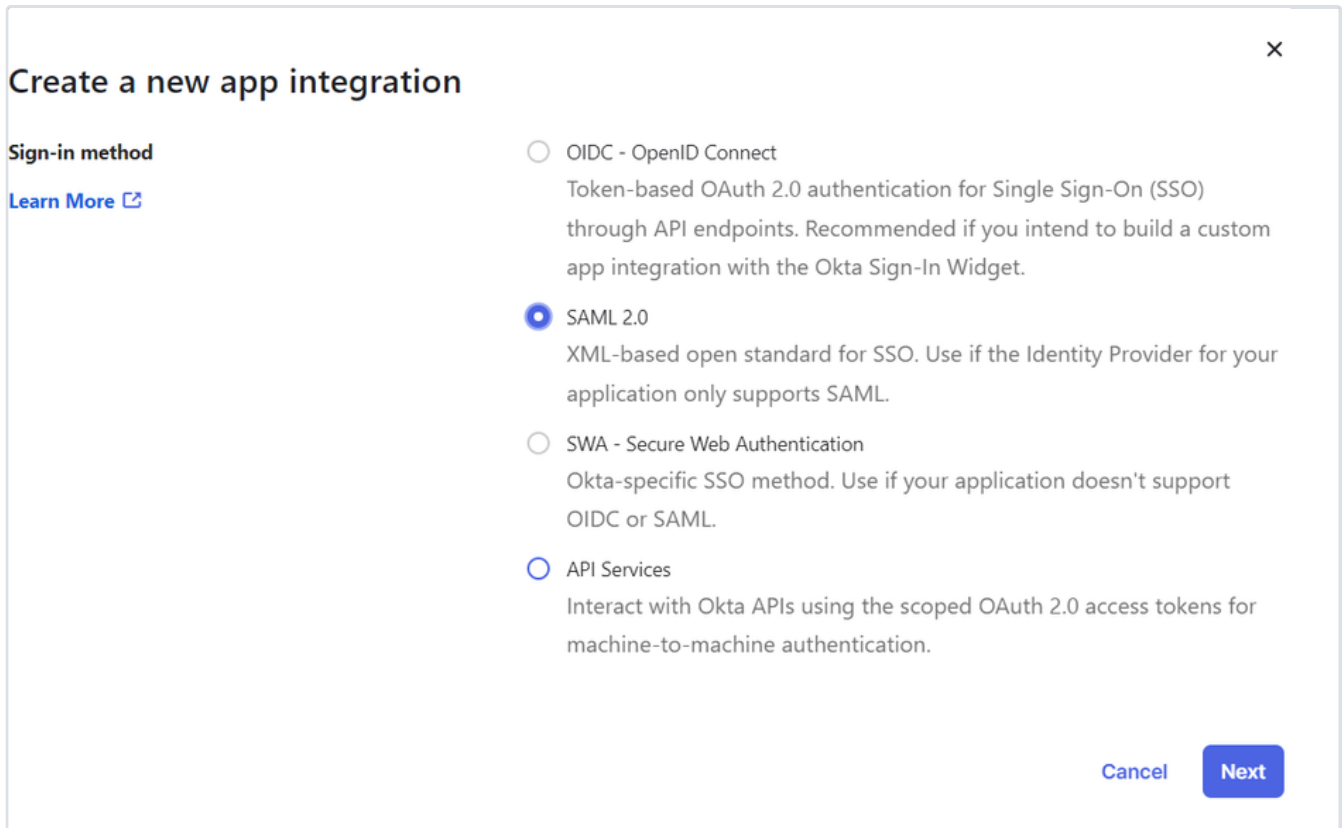
Create a new Application Integration

1. Go to applications and click on 'Create App integration'



The screenshot shows the Okta dashboard on the left with a sidebar menu containing 'Dashboard', 'Directory', 'Customizations', 'Applications', 'Applications', 'Self Service', and 'API Service Integrations'. The 'Applications' menu item is highlighted. On the right, the 'Applications' page is shown with buttons for 'Create App Integration', 'Browse App Catalog', 'Assign Users to App', and 'More'. A search bar is also visible.

2. Select SAML 2.0 as the Sign-in method



The screenshot shows a dialog box titled 'Create a new app integration' with a close button (X) in the top right corner. Under the 'Sign-in method' section, there is a 'Learn More' link and four radio button options: 'OIDC - OpenID Connect', 'SAML 2.0', 'SWA - Secure Web Authentication', and 'API Services'. The 'SAML 2.0' option is selected. At the bottom right, there are 'Cancel' and 'Next' buttons.

3. Set App name as **Barco** and click on Next.

Create SAML Integration


1 General Settings

2 Configure SAML

3 Feedback

1 General Settings

App name

App logo (optional) 

App visibility Do not display application icon to users

[Cancel](#)

[Next](#)

Configure SAML settings

1. Under **General**, set the values as given below:

A SAML Settings

General

Single sign-on URL

Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID)

Default RelayState

If no value is set, a blank RelayState is sent

Name ID format

Application username

Update application username on

Single sign-on URL (ACS URL)	https://auth.barco.com/barcociam.onmicrosoft.com/B2C_1A_Common/samlp/sso/assertionconsumer
Audience URI (SP Entity ID)	https://auth.barco.com/barcociam.onmicrosoft.com/B2C_1A_Common

2. Under **Attribute Statements** add the following two claims, and then click Next:

Attribute Statements (optional) [LEARN MORE](#)

Name	Name format (optional)	Value
<input type="text" value="http://schemas.xmlso"/>	<input style="border: none; background-color: #f0f0f0; padding: 2px 5px;" type="text" value="Unspecified"/>	<input style="border: none; background-color: #f0f0f0; padding: 2px 5px;" type="text" value="user.firstName"/>
<input type="text" value="http://schemas.xmlso"/>	<input style="border: none; background-color: #f0f0f0; padding: 2px 5px;" type="text" value="Unspecified"/>	<input style="border: none; background-color: #f0f0f0; padding: 2px 5px;" type="text" value="user.lastName"/> ×

[Add Another](#)

Group Attribute Statements (optional)

Name	Name format (optional)	Filter
<input type="text"/>	<input style="border: none; background-color: #f0f0f0; padding: 2px 5px;" type="text" value="Unspecified"/>	<input style="border: none; background-color: #f0f0f0; padding: 2px 5px;" type="text" value="Starts with"/>

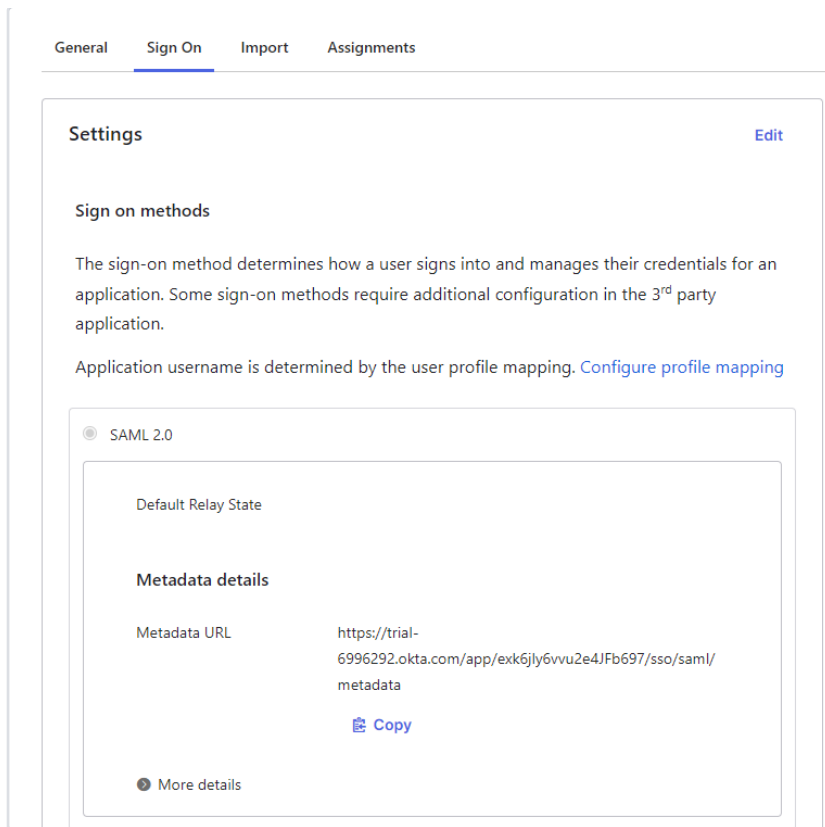
[Add Another](#)

Name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.firstName
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.lastName

3. Complete the **Feedback** and click on Finish.

Save your App integration metadata

1. From the Sign On section, copy the **Metadata URL** and open it in a new tab.



2. Once you have opened it, you need to Save this as (.xml) file. You can do so by right clicking anywhere on the page → Save.

Configure in BMS

1. Sign-in to <https://msuite.barco.com> and navigate to Single sign-on.
2. For the domain you are currently configuring SSO, go to options → Configure Single sign-on
3. From the Protocol dropdown, select SAML v2.0.
4. Under 'Your metadata' select and upload the (.xml) file that you saved in the previous step.
5. Select the Signing algorithm as SHA-256.
6. Click on Save.
7. Enable the Single sign-on configuration.

Related articles

[Application Integration Wizard SAML field reference | Okta](#)

[SAML Signed Requests failing with error code 400 \(SP initiated SSO flow\) \(okta.com\)](#)