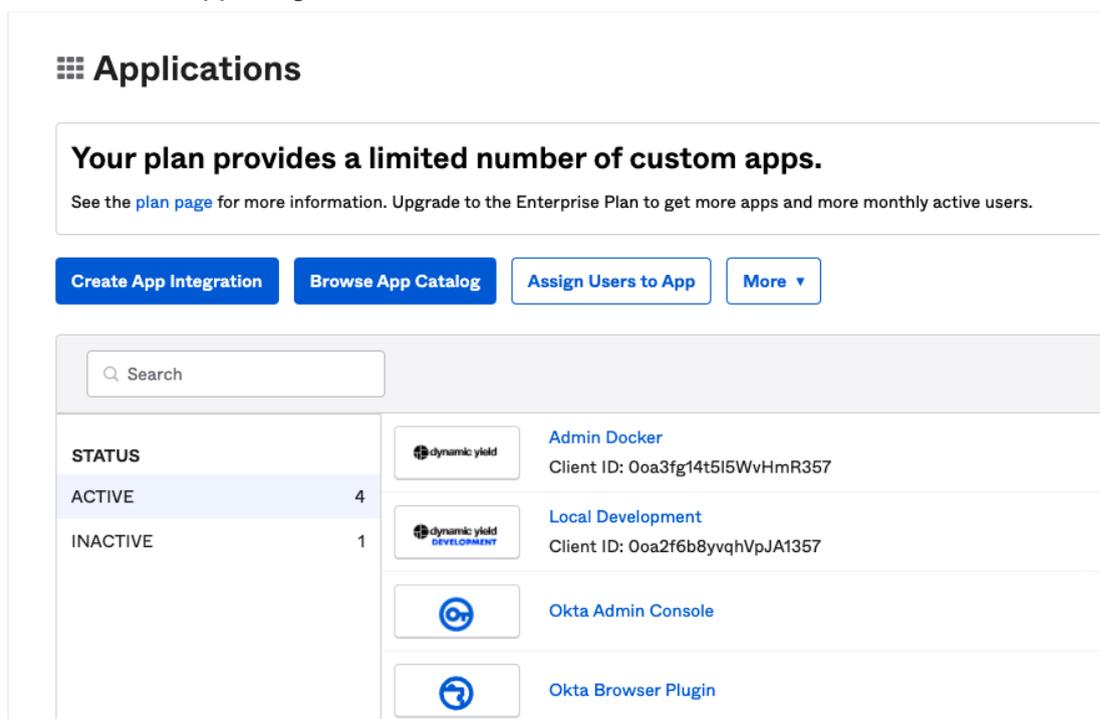


Setting up Dynamic Yield on Okta (SAML 2.0)

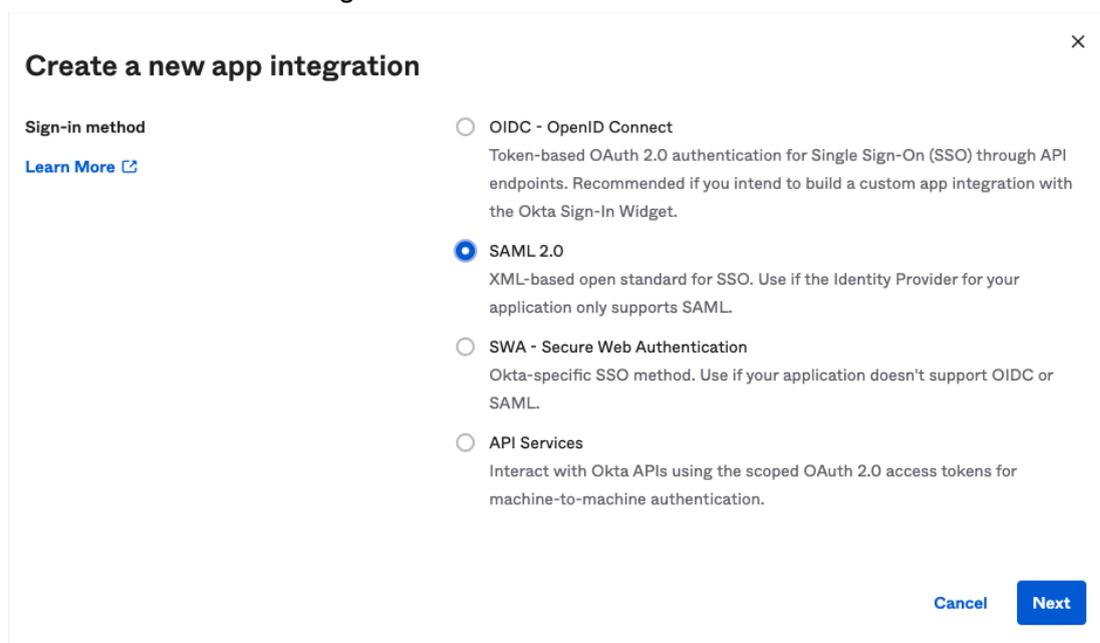
[Single sign-on on the knowledge base](#)

1. Create a new app integration on Okta



The screenshot shows the 'Applications' page in Okta. At the top, there is a notification: 'Your plan provides a limited number of custom apps. See the [plan page](#) for more information. Upgrade to the Enterprise Plan to get more apps and more monthly active users.' Below this are four buttons: 'Create App Integration', 'Browse App Catalog', 'Assign Users to App', and 'More'. A search bar is present above a table of applications. The table has two columns: 'STATUS' and a list of applications. The 'ACTIVE' status has a count of 4, and 'INACTIVE' has a count of 1. The applications listed are: 'Admin Docker' (Client ID: Ooa3fg14t5I5WvHmR357), 'Local Development' (Client ID: Ooa2f6b8yvqhVpJA1357), 'Okta Admin Console', and 'Okta Browser Plugin'.

2. Select SAML 2.0 as the sign in method



The screenshot shows the 'Create a new app integration' dialog box. It has a close button (X) in the top right corner. The 'Sign-in method' section is active, with a 'Learn More' link. There are four radio button options: 'OIDC - OpenID Connect' (described as token-based OAuth 2.0 authentication), 'SAML 2.0' (selected, described as XML-based open standard for SSO), 'SWA - Secure Web Authentication' (Okta-specific SSO method), and 'API Services' (interact with Okta APIs using OAuth 2.0 access tokens). At the bottom right, there are 'Cancel' and 'Next' buttons.

3. On the general setting tab name the app and check both App visibility checkboxes:

The screenshot shows the 'General Settings' tab for an application named 'Dynamic Yield'. The 'App name' field is filled with 'Dynamic Yield'. The 'App logo (optional)' field contains a gear icon, with 'upload' and 'delete' buttons. Under 'App visibility', both checkboxes are checked: 'Do not display application icon to users' and 'Do not display application icon in the Okta Mobile app'. 'Cancel' and 'Next' buttons are at the bottom.

4. In the SAML Settings for “Single Sign-on URL” use:
.com:
[https://ssobroker.dynamicyield.com/auth/realms/admin/broker/\[accountID\]/endpoint](https://ssobroker.dynamicyield.com/auth/realms/admin/broker/[accountID]/endpoint)
.eu:
[https://ssobroker.dynamicyield.eu/auth/realms/admin/broker/\[accountID\]/endpoint](https://ssobroker.dynamicyield.eu/auth/realms/admin/broker/[accountID]/endpoint)
5. for “Audience URI” use:
.com:
<https://ssobroker.dynamicyield.com/auth/realms/admin>
.eu:
<https://ssobroker.dynamicyield.eu/auth/realms/admin>
6. Name ID format should be EmailAddress

7. Application username should be Email

The screenshot shows the 'SAML Settings' configuration page for an application. Under the 'General' section, the following fields are visible:

- Single sign on URL:** A text input field containing the URL `https://ssobroker.dynamicyield.com/auth/realms/admin/`. Below it, there are two checkboxes: 'Use this for Recipient URL and Destination URL' and 'Allow this app to request other SSO URLs'.
- Audience URI (SP Entity ID):** A text input field containing the URL `https://ssobroker.dynamicyield.com/auth/realms/admin`.
- Default RelayState:** An empty text input field. Below it, a note states: 'If no value is set, a blank RelayState is sent'.
- Name ID format:** A dropdown menu currently set to 'EmailAddress'.
- Application username:** A dropdown menu currently set to 'Email'.

A blue link labeled 'Show Advanced Settings' is located at the bottom right of the configuration area.

8. Provide your TAM with the app identity provider metadata URL

The screenshot shows the 'SAML 2.0' configuration page. At the top, there is a radio button selected for 'SAML 2.0'. Below it is a text input field for 'Default Relay State'. A prominent orange warning banner contains the following text:

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

Below the warning is a blue button labeled 'View Setup Instructions'. Underneath the button, it says: 'Identity Provider metadata is available if this application supports dynamic configuration.'

At the bottom of the page, under the heading 'Credentials Details', there is a table with one row:

Application username format	Email
-----------------------------	-------

9. Make sure to assign the relevant users to the app. These users should be invited to the Dynamic Yield platform as well to be able to sign in.

10. Create a test user in your Okta account and assign it to the DY account. Provide your TAM with the test user credentials.

If there is any other data missing you may find it on our metadata file:

.com:

[SAML 2.0 Identity Provider Metadata](#)

.eu:

[SAML 2.0 Identity Provider Metadata](#)