

Create an Okta App Integration

Create the app integration in Okta

1. Create a new app integration

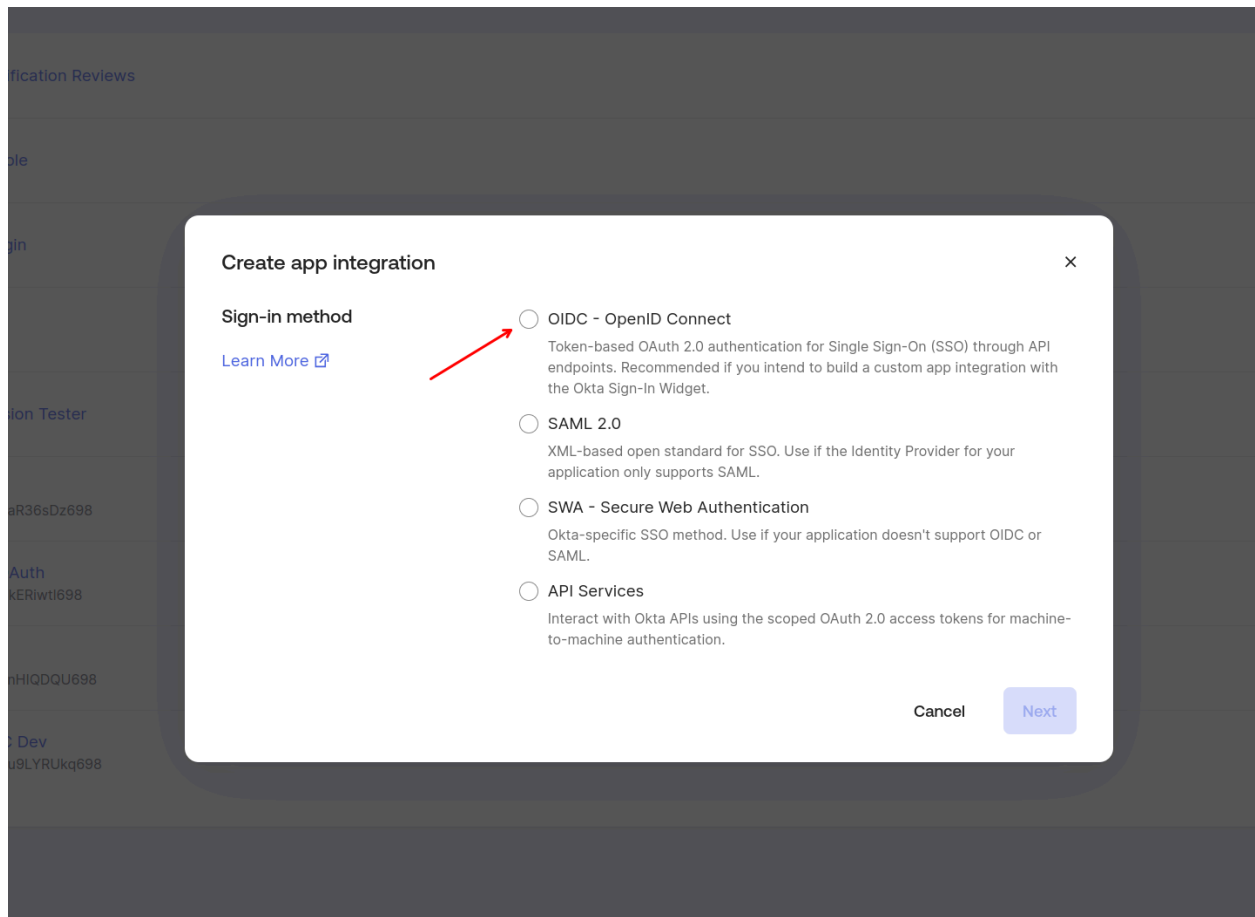
Login to the Okta admin console and navigate to **Applications and Resources** → **Applications** from the menu on the left, then click the **Create App Integration** button.

The screenshot displays the Okta Admin Console interface. On the left, the 'okta' logo is at the top, followed by the 'Admin Console' section. Under 'Applications and Resources', the 'Applications' link is highlighted with a red arrow. The main content area is titled 'Applications' and features a search bar at the top. Below the search bar, there are three buttons: 'Create App Integration' (highlighted with a red arrow), 'Browse App Catalog', and 'Assign Users to App'. A 'More' dropdown menu is also present. Below these buttons, there is a table with two columns: 'STATUS' and 'NAME'. The 'STATUS' column has two rows: 'Active' with a count of 3, and 'Inactive' with a count of 0. The 'NAME' column lists several applications, each with an icon and a name: 'Okta Access Certification Reviews', 'Okta Admin Console', 'Okta Browser Plugin', 'Okta Dashboard', 'Okta OIN Submission Tester', and 'Okta Workflows' (with a 'Client ID: 00a13if88kaR36sDz698' listed below it).

STATUS	COUNT	NAME
Active	3	Okta Access Certification Reviews
Inactive	0	Okta Admin Console
		Okta Browser Plugin
		Okta Dashboard
		Okta OIN Submission Tester
		Okta Workflows Client ID: 00a13if88kaR36sDz698

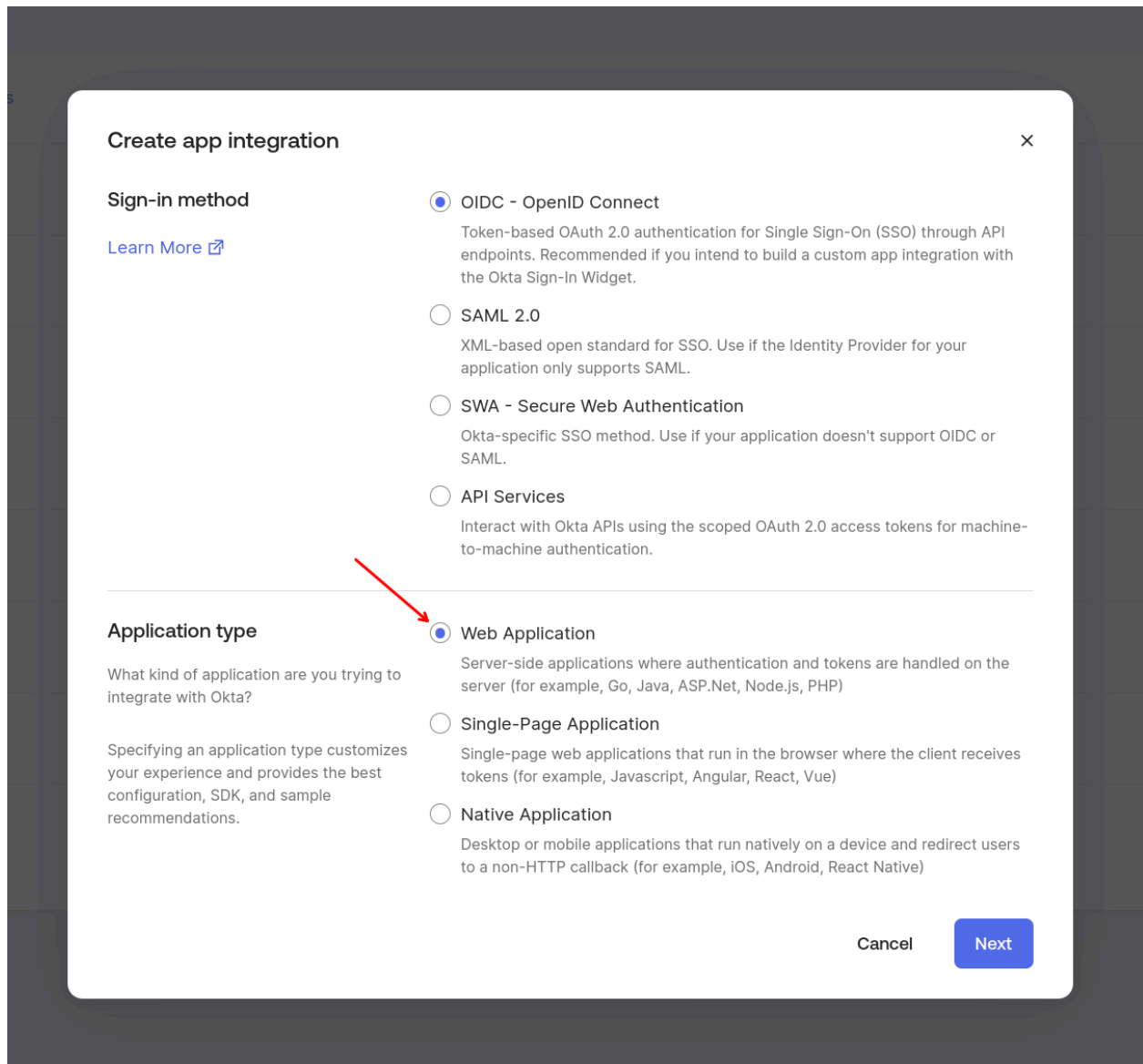
2. Choose OIDC

A modal dialog will open asking you to select a **Sign-in method**. Select **OIDC - OpenID Connect**.



3. Choose Web Application

The dialog will then be extended and you will be asked to select an **Application type**. Select **Web Application** and click the **Next** button.



Create app integration ×

Sign-in 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**

4. Configure the new web app

You will be directed to the **New Web App Integration** form, where you will need to enter the following settings:

App integration name: Ready Room

Grant Type: Authorization Code

Sign-in redirect URIs: <https://app.readyroom.net/auth/okta/callback>

Assignments: Skip group assignment for now. *If you have already created a Ready Room group, you can select "Limit access to selected groups" instead.*

New Web App Integration

General Settings

App integration name → Ready Room

Proof of possession
☐ Require Demonstrating Proof of Possession (DPoP) header in token requests

Grant type
Client acting on behalf of itself
☐ Client Credentials
Core grants
→ ☒ Authorization Code
☐ Refresh Token
Advanced >

Sign-in redirect URIs
☐ Allow wildcard * in sign-in URI redirect.
Okta sends the authentication response and ID token for the user's sign-in request to these URIs
[Learn More](#)
https://app.readyroom.net/auth/okta/callback
+ 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.
[Learn More](#)
http://localhost:8080
+ 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.
[Learn More](#)
+ Add URI

Assignments
Controlled access
Select whether to assign the app integration to everyone in your org, only selected group(s), or skip assignment until after app creation.
☐ Allow everyone in your organization to access
☐ Limit access to selected groups
→ ☒ Skip group assignment for now

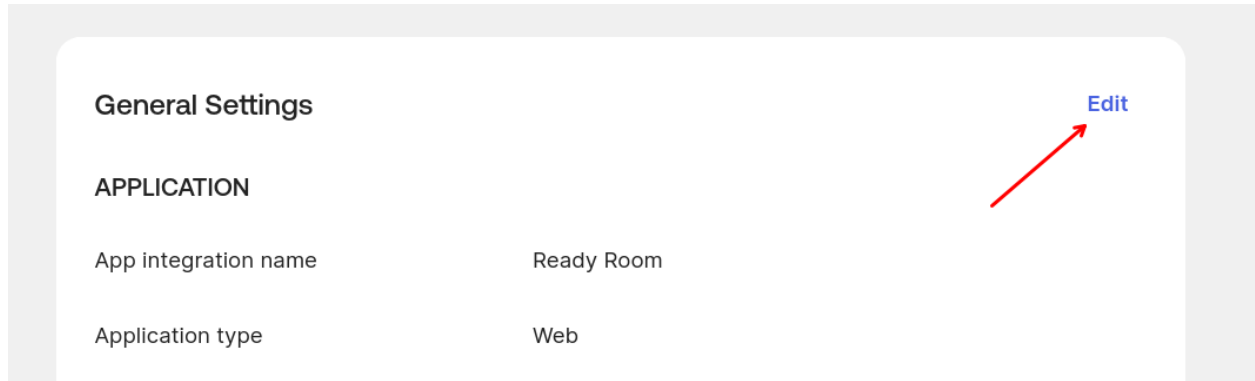
Save Cancel

After verifying the changes, click **Save**.

5. **Edit the general settings**

The Okta App **Web Application** has now been created, and you are redirected to a summary screen. However, there is one more step.

Make sure you are on the **General** tab, then scroll down until you see the **General Settings** section, and click **Edit**.



6. **Enable IdP-initiated login**

The **General Settings** content will become editable and you will need to enter the following information:

Logo URI: <https://ok14static.oktacdn.com/fs/bco/4/fs049qnqmkL7O2vw5697>

Login initiated by: Either Okta or App

Application Visibility: Display application icon to users

Login Flow: Redirect to app to initiate login (OIDC Compliant)

Initiate login URI: <https://app.readyroom.net/auth/okta>

(See screenshot next page)

USER CONSENT

User consent ?

☒ Require consent

Terms of Service URI ?

Policy URI ?

Logo URI ?



https://ok14static.oktacdn.com/fs/bco/4/fs049qnqmkL;

LOGIN

Sign-in redirect URIs ?

☐ Allow wildcard * in login URI redirect.



https://app.readyroom.net/auth/okta/callback



+ Add URI

Sign-out redirect URIs ?



+ Add URI

Login initiated by



Either Okta or App



Application visibility



☒ Display application icon to users

Login flow



☒ Redirect to app to initiate login (OIDC Compliant)
☐ Send ID Token directly to app (Okta Simplified)

Initiate login URI ?



https://app.readyroom.net/auth/okta

EMAIL VERIFICATION EXPERIENCE

Callback URI ?

Save

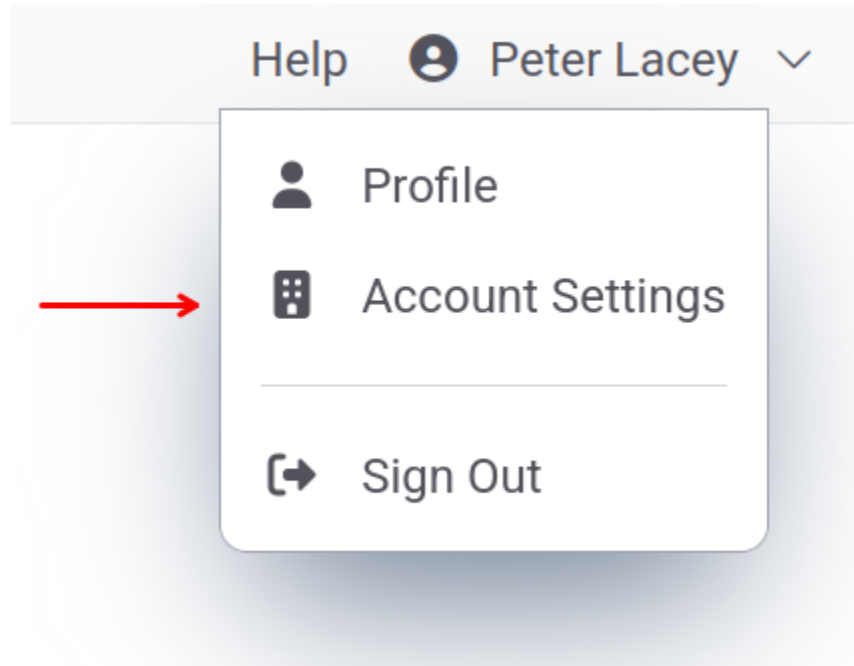
Cancel

Your Okta App Integration is now complete. Now you need to tell Ready Room about it.

Connect Okta to Ready Room

1. Open Account Settings

Leave the Okta admin console open and in a new tab or window login to Ready Room as an administrator. Click your name in the upper right hand corner and select **Account Settings** from the dropdown.



2. Enter your Okta details

From the menu on the left select **Single Sign-on**

Select **Okta** as an **Identity Provider**

Enter your Okta issuer (domain), Client ID, and Client Secret. These can all be found on the **General** tab of the Okta application you created in the previous steps. See image below.

Click **Save**

Important: When entering the domain, add *only* the domain. Do not prepend a scheme (e.g. "https://") or add any additional path components. In the image below, the domain is [example.okta.com](#)

Synclinical

READY ROOM

Help Peter Lacey

All Accounts > Synclinical > Single Sign-On

- Customers are *strongly encouraged* to enable SSO to secure their accounts.
- The settings below are meant to be configured by your IT department.

Select an Identity Provider

Okta

Detailed instructions for configuring SSO with Okta are available [here](#).

Issuer *

Client ID *

Client Secret *

Save

