

# How to connect Okta to Upflow

This guide comes in addition to our [dedicated article](#) on SSO Authentication.

## Let's begin!

1 - Sign in to Okta's Administration console and select the Applications panel in the Applications section in the main menu.

The screenshot displays the Okta Administration console interface. On the left is a navigation sidebar with the following items: Dashboard (with an expand/collapse arrow), Dashboard (highlighted), Tasks, Agents, Notifications, Getting Started, Directory (with a collapse arrow), Customizations (with a collapse arrow), Applications (with an expand/collapse arrow), Applications (highlighted), and Self Service. The main content area on the right features a search bar at the top right. Below it, the 'Overview' section shows 'Users' with a count of '2' and a '100%' increase over the 'last 7 days'. The 'Tasks' section is currently empty. The 'Org change' section shows an 'Update policy' notification dated '5 Oct, 14:05'.

## 2 - Create a new App Integration, then select:

- Sign-in method: OIDC
- Application type: Web Application

### Create a new 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](#)

## 3 - Input the following settings in the New Web App Integration panel:

- App integration name: input **Upflow SSO**
- Grant type: **Authorization Code**
- Sign-in redirect URIs: input **https://auth.upflow.io/\_\_/auth/handler**
- Sign-out redirect URIs: **https://app.upflow.io/**

### New Web App Integration

#### General Settings

**App integration name**

**Logo (Optional)**

**Grant type** [Learn More](#)

Client acting on behalf of itself

- Client Credentials

Client acting on behalf of a user

- Authorization Code
- Interaction Code
- Refresh Token
- Implicit (hybrid)

---

**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

[×](#)

[+ 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.

[×](#)

[+ Add URI](#)

[Learn More](#)

4 - Assignments (optional): if you wish to have fine-grained access control over which users can access the Upflow application, you can select **Controlled access** and identify authorized **group(s)**. As an alternative, groups, and users can also be authorized individually later on the application settings page. **Note that users will still have to be invited to your organization to be able to enter the Upflow application.**

**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

**Selected group(s)**

Finance

Save Cancel

5 - After hitting Save, the following application settings window displays the parameters that need to be securely transmitted to Upflow:

- o the `client_id` (Client ID)
- o the `client_secret` (Secret)
- o the **issuer** can be found in the top right corner of the window, right below your email address

General Sign On Assignments Okta API Scopes

**Client Credentials** Edit

Client ID: Ooa2m59wwwWOU1s41697

Client authentication:  Client secret

Proof Key for Code Exchange (PKCE):  Require PKCE as additional verification

**CLIENT SECRETS**

Creation date	Secret	Status
Oct 6, 2022	.....	Active

6 - Transmit the **client\_id**, **client\_secret**, and **issuer** to Upflow through a secure channel, such as [secrets.upflow.io](https://secrets.upflow.io).

If you have any additional questions, [contact us!](#)