

OpenID Authorization

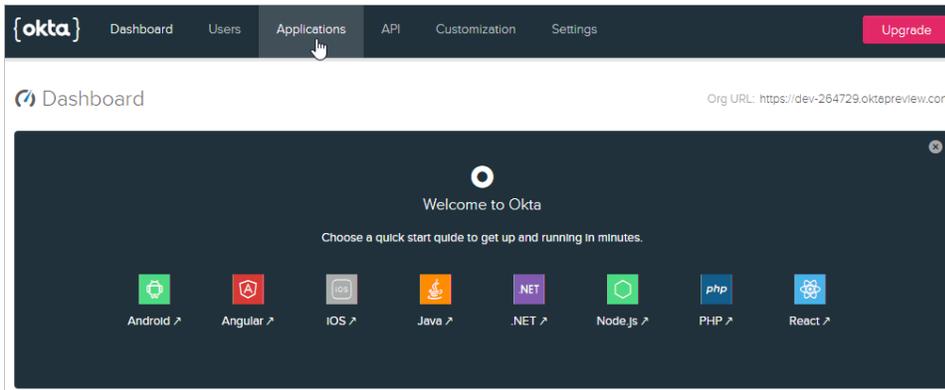
OpenID is a popular single sign-on technology that allows access to all company web-resources with the same credentials. In iSpring Learn, OpenID Connect protocol works with the Okta identity provider - an authorization server that authenticates users and transmits info about a successful authorization to LMS.

✔ Authorization with OpenID and Okta works in the mobile application.

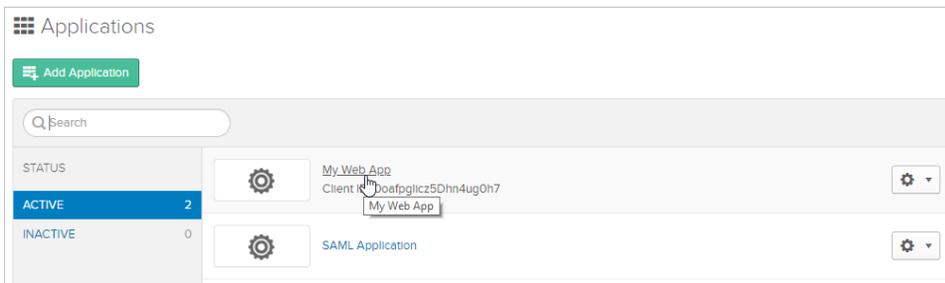
- [Okta Authorization Server Configuration](#)
- [Adding Users to iSpring Learn](#)
- [Authorization without OpenID](#)

Okta Authorization Server Configuration

1. Log in to your Okta account and open the **Applications** section in the top menu.

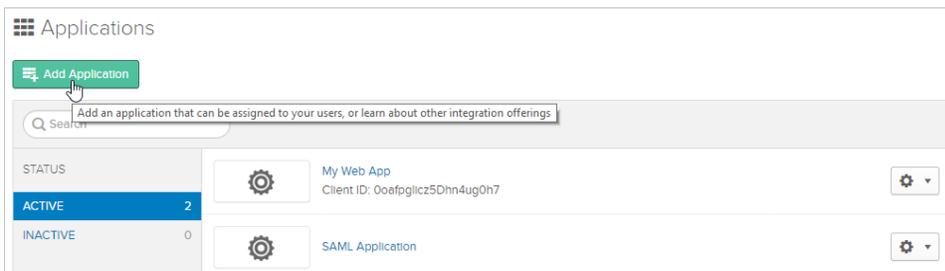


2. Then, start editing the application.



In case you haven't created an application yet, add it now.

1. In the **Applications** section, click the **Add Application** button.



2. At the second step, select **Web** and click **Next**.

Create New Application

1 Platform — 2 Settings

An application in Okta represents an integration with the software you're building. Choose your platform, and we'll recommend settings on the next step.



Native
iOS, Android



Single-Page App
Angular, React, etc.



Web
.NET, Java, etc.



Service
Machine-to-Machine

Previous Cancel Next

3. After that, start configuring the application. Add **Base URIs** and **Login redirect URIs** — these can be taken from your iSpring Learn account. Also, in the **Grant type allowed** section, check **Refresh Token** and **Implicit (Hybrid)**. Finally, click **Done**.

APPLICATION SETTINGS

Name: My Web App

Base URIs (Optional): https://mycompany.ispringonline.ru/ ✕
 + Add URI

The domains where your application runs. Trusted Origins will be created for these URIs, and will be the only domains Okta accepts API calls from. [Docs](#)

Login redirect URIs: https://mycompany.ispringonline.ru/sso/login/oidc ✕
 + Add URI

Okta will send OAuth authorization response to these URIs. Add your application's callback endpoint. [Docs](#)

Group assignments (Optional): Everyone ✕

Users can only sign in to apps that they are assigned to. Group assignments are easier to manage than individual users.

Grant type allowed

Client acting on behalf of itself
 Client Credentials

Client acting on behalf of a user
 Authorization Code
 Refresh Token
 Implicit (Hybrid)

Okta can authorize your native app's requests with these OAuth 2.0 grant types. Limit the allowed grant types to minimize security risks. [Docs](#)

Previous Cancel Done

3. Then, scroll down to the bottom of the page — here you can copy **Client Id** and **Client secret**.

Client Credentials
Edit

Client ID

Public identifier for the client that is required for all OAuth flows.

Client secret

Secret used by the client to exchange an authorization code for a token. This must be kept confidential! Do not include it in apps which cannot keep it secret, such as those running on a client.

4. Add **Return Url** — the web-page address where a non-authenticated user will be redirected.

LOGIN

Login redirect URIs

<https://test@version.springonline.ru/sso/login/oidc>
<http://test@version.springonline.ru/sso/login/oidc>

To make the authorization in the mobile application work, add a modified Return Url to the authorization server. Swap the **https** scheme with **islearn**: for example, change <https://auth.dev.mycompany.com/sso/login/oidc> to <islearn://auth.dev.mycompany.com/sso/login/oidc>

Configuring iSpring Learn

1. Sign in with your iSpring Learn account and put the following link into the browser: <https://yourcompany.ispringlearn.ru/settings/sso/oidc>
2. Fill out the fields of the form.

Automatically add new users via OpenID	Check this option to enable non-registered users to get added to iSpring Learn when attempting to login.
Response Type	The response type which is issued by the authorization server.
Return Url	The web-address of the page where non-authenticated users are redirected to.
Issuer	The security token issuer. This value can be retrieved on the authorization server — it is the URL of your Okta account.
Client Id	The client identifier which can be copied on the authorization server.
Client Secret	This parameter is used to authenticate the application when it is asking to get access to a user's account. It's created on the authorization server.

Connection Settings

Automatically add new users via OpenID

Response Type:

Return URL:

Issuer:

Client Id:

Client Secret:

3. If needed, [match fields](#) in iSpring Learn and your SSO service.

Matching fields of iSpring Learn with the external OpenID attributes

The data will be automatically synced when users sign in for any of the fields listed below.

Email	email	
Last Name	family_name	
First Name	given_name	
Login	preferred_username	
Login	sub	

[+ Add a field](#)

4. Finally, click **Enable**.

← OpenID integration settings  

Use this page to manage OpenID settings.

Enable 

Adding Users to iSpring Learn

Even if users are not present in the iSpring Learn database yet, they will be automatically added to the users list. The only thing that can prevent a new user from adding can be your subscription plan limitation.

To create users when signing in with OpenID, we use the following parameters received from the authorization server:

Claim	Profile Field in iSpring Learn
preferred_username	Login
email	Email
family_name	Last Name
given_name	First Name

Authorization without OpenID

If you have enabled OpenID in your iSpring Learn account and for some reasons can't login using single sign-on, type the following web address: https://yourcompany.ispringlearn.com/login?no_sso.

Now you will sign in with the account as usual, using your login and password.