

×

OKTA Configurations

1. While creating a new application, you must have the sign-in method as "OIDC" and the application type as Web Application.

Create a new app integration

Sign-in method

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)

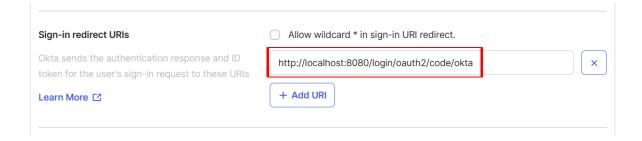
Single-Page Application

Single-page web applications that run in the browser where the client receives tokens (for example, Javascript, Angular, React, Vue)

Native Application

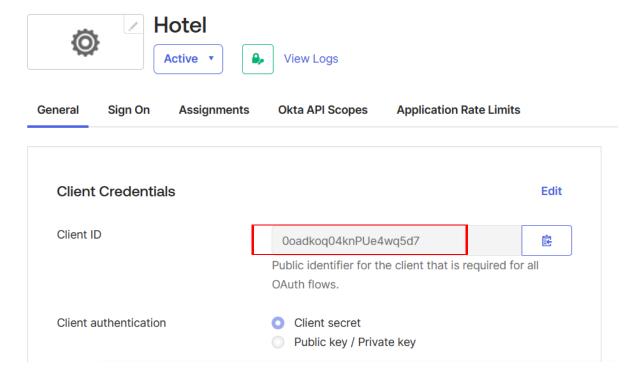
Desktop or mobile applications that run natively on a device and redirect

2. The Sign-in redirect URL should be in the format given below.





- 3. You need two things to configure your spring boot application with Okta
 - a. Client ID
 - b. Client Secret
 - c. Issuer URI



CLIENT SECRETS



