

OKTA Single Sign-On configuration (Basic configuration)

Introduction

This document will help you register a new application in OKTA, so you will be able to connect your users with Certainty Software applications.

General information

Once all the steps are completed, you will have to share some information with the Certainty Software team.

To connect Okta as an external provider within Certainty Software, we will need:

- The Client ID (can be found in the general tab of your application)
- The Client Secret (can be found in the general tab of your application)
- Your OKTA domain name (this is created when you create a new account in OKTA)



Register a new application

In this section, you'll have to register the Certainty authorization server within your OKTA account.

First, go to the administration section in OKTA admin.

Open "Applications" in the left menu and click the "Applications" submenu.

okta



Click the "Create App Integration" button.

Create App Integration	Browse A	App Catalog	Assign Users to App More 🔻	
Q Search				
STATUS		©	Okta Admin Console	
ACTIVE	0	0	Okta Browser Plugin	
			Okta Dashboard	

Select "OIDC - OpenID Connect" in the "Sign-in method"

 SAML 2.0 XML-based open standard for SSO. Use if the Identity Provider f application only supports SAML. SWA - Secure Web Authentication Okta-specific SSO method. Use if your application doesn't support SAML. API Services 	gle Sign-On (SSO) through API d a custom app integration with	
 SWA - Secure Web Authentication Okta-specific SSO method. Use if your application doesn't support SAML. API Services 	ldentity Provider for your	0
O API Services	tion doesn't support OIDC or	0
Interact with Okta APIs using the scoped OAuth 2.0 access toke machine-to-machine authentication.	th 2.0 access tokens for	0

In the "Application type", select "Web Application" and click the "Next" button.

Application type

Web Application

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.

Single-Page Application Single-page web applications that run in the browser where the client receives

Server-side applications where authentication and tokens are handled on the

tokens (for example, Javascript, Angular, React, Vue)

server (for example, Go, Java, ASP.Net, Node.js, PHP)

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

You will then be redirected to a new page, where you will have to specify all the settings to register the new app.

In general settings, specify the app integration name and the grant types. You can add an optional logo.

General Settings		
App integration name	Certainty Software	
Logo (Optional)	C	
Grant type	Client acting on behalf of itself	
Learn More	✓ Client Credentials	
	Client acting on behalf of a user	
	Authorization Code	
	Refresh Token	
	Implicit (hybrid)	

In the "Sign-in redirect URIs" section, please enter the URL below:

• <u>https://connect.certaintysoftware.com/[CLIENT_INSTANCE]/signin-oidc</u> where the CLIENT_INSTANCE is the subdomain used to access your certainty software app.



In the "Sign-out redirect URIs" section, please enter the URIs below:

- <u>https://connect.certaintysoftware.com</u>
- <u>https://[CLIENT_INSTANCE].certaintysoftware.com</u>
- <u>https://[CLIENT_INSTANCE].certaintysoftware.mobi</u>

Under "Assignments", select the controlled access based on your requirements.

If you plan to allow access to all users, select the first option, "Allow everyone in your organization to access".

If you want to limit access to certain users in production or test environments, you can select the "Limit access to selected groups" option. You will then have to select existent groups.

 Allow everyone in your organization to access Limit access to selected groups Skip group assignment for now
Enable immediate access with Federation Broker Mode
• To ensure optimal app performance at scale, Okta End User Dashboard and provisioning features are disabled. Learn more about Federation Broker Mode ^[2] .

Click the "Save" button to validate your changes.

From the 'General' tab of your newly created application, take note of the 'Client ID' and 'Client Secret' as you will need to share them with the Certainty Software team.

ior ar	Sign On	Assignments	Okta API Scopes	Application Rate Limits	
Clien	t Creden	tials			Edit
Client I	D		Ooa97bpcjuPhKBX	1C5d7	Ê
			Public identifier fo OAuth flows.	r the client that is require	d for al
Client authentication		 Client secret Public key / Priva 	ate key		
Proof Key for Code Exchange (PKCE)		Require PKCE as	additional verification		
CLIEN	NT SECRE	тѕ			
				Generate new sec	ret
	tion date	Secret		Status	
Crea	and a date				

****Important**** Note that whenever the client secret is updated, you will have to share it with the Certainty Software team.