Single-Sign-On and API Access Management with OpenID Connect and OAuth

okta Edu

Course overview

You successfully use Okta today to securely manage employee identity and access to internal applications using SAML. Are you ready take advantage of modern techniques for securing your business to consumer (B2C) apps and web APIs?

In this course, you will learn about OAuth actors and flows, how JSON Web Tokens work, and OpenID Connect and its use as an identity framework for both Social Auth and Single Sign-On (SSO). You will also learn how to add social log in to your custom applications.

Beginning with an architectural introduction, we will discuss common access scenarios supported by each standard to give you the ability to make the right authentication and authorization decision for your application.

Students use the Okta identity Cloud platform to implement SSO with OIDC, API Authorization with OAuth, and Social Authentication to a custom-built B2C loyalty platform through completion of extensive Javascript coding labs. Best practices are covered, as well as testing and troubleshooting techniques.

This course is perfect for Architects and Developers who are familiar with using Okta REST APIs, Widgets, and SDKs to customize B2B identity management scenarios and want to expand their knowledge around B2C use cases.

Who should attend

- Developers
- Technical Architects

Prerequisites

- Familiarity with Okta REST APIs and widgets.
- Experience with front-end development, using HTML, JavaScript, and CSS.

Format

- Instructor-led with hands-on labs
- Duration: 2 days
- Delivery: Virtual (public or private); Onsite (private)

Setup requirements

- Students use their own computers.
- Okta provides access to an Okta tenant + virtual machine to complete the labs.

Learn how to:

- Take the use of OAuth, OpenID Connect (OIDC), and JSON Web Tokens (JWT) from theory to practice.
- Develop SSO to a custom application using Okta and OpenID Connect.
- Securely protect custom REST APIs with Okta API Access Management and OAuth.
- Understand OAuth actors and flows and when to use them.
- Implement Social Authentication in your custom application.
- Use Proof Key for Code Exchange (PKCE) to secure hybrid flows for mobile apps.
- Understand best practices and troubleshoot common problems.

Single-Sign-On and API Access Management with OpenID Connect and OAuth

okta Edu

Course outline

1: Introduction to OAuth, JWT, and OpenID Connect

Define the SSO and Authorization requirements for Modern Applications.
Describe OAuth, JWT, and OpenID Connect.

2: Okta SSO with OpenID Connect

Describe how Okta SSO implements OAuth and OpenID Connect.
Implement Okta SSO with OAuth and OpenID Connect.
Explore Okta differentials on top of the Standard implementation.

3: Authorization with Okta API Access Management

Describe Okta API Access Management.
Compare API Access Management and Okta SSO.
Protect APIs with Okta API Access Management.

4: Social Authentication

Describe how to Use Social Authentication.
Configure Social Authentication in your App.