

WSO2 Identity Server 7.3 Developer Fundamentals

OEM: WSO2 • Code: IS73DF

COURSE DESCRIPTION

WSO2 Identity Server Fundamentals is a course aimed at training Identity Server administrators on the features of the product as well as the underlying concepts and standards. The scope of this course will be limited to using commonly used features of the WSO2 Identity Server to provide a solution related to identity management without having to extend the product. Training Type: WSO2 product training and hands-on session. Complexity: Beginner/Intermediate.

AUDIENCE PROFILE

- System Administrators and Identity Administrators

PREREQUISITES

- Open Standards

Having a knowledge of the following standards will be useful when following this course:

- SAML2
- OAuth 2.0
- OpenID Connect
- SCIM 2.0

COURSE OBJECTIVES

By the end of this course, participants will be able to:

- This section doesn't contain any content.

COURSE OUTLINE

Module 1: Session 1

Introduction to Identity and Access Management

- Traditional Access Management
- Identity and Access Management Concepts
- Introduction to WSO2 Identity Server

User Management

- Introduction to User Management
 - User Account Management
 - Users, Roles, and Groups
 - Role-Based Access Control
 - User Stores
- Lab: User Management via Management Console
 - Lab: User Self-Registration via My Account

Module 2: Session 2

User Account Management

- User Registration
 - Password Management
 - Account Recovery
 - Account Locking and Disabling
- Lab: Password Recovery
 - Lab: Username Recovery
 - Lab: Account Locking
 - Lab: Password Policies

Agentic AI

- Introduction to AI Agents
 - Why Agents can't be trusted
 - The Pillars of Agent Identity to address AI Agent Challenges
 - Agent Registration and Management
 - MCP Servers
- Lab: Agent registration and management via Console

Access Delegation with OAuth 2.0

- Access delegation
 - OAuth 2.0 Concepts
 - OAuth 2.0 in Action
 - Tokens and Grants
 - Token Types
 - Grant Types
- Lab: Access Delegation with OAuth 2.0

Module 3: Session 3

Single Sign-on SSO

- Introduction to SSO

- Benefits of SSO
- SSO Standards

SSO with OpenID Connect

- Requirement of OpenID connect
 - ID token and OIDC Identity Layer
 - OpenID Connect Overview
- Lab: SSO with OpenID Connect

SSO with SAML

- Introduction to SAML
 - SAML2 participants and Authorization Flow
 - SAML Specifications
- Lab: Single Sign-On - SAML

Module 4: Session 4

Identity Federation

- Requirement of Identity Federation
 - Identity Federation Concepts
 - Benefits of Identity Federation
- Lab: Identity Federation

Strong Authentication with Multi-Factor Authentication MFA

- Authentication
 - Multi-Factor Authentication
 - Benefits of Multi-Factor Authentication
- Lab: Strong Authentication - MFA

Strong Authentication with Adaptive Authentication

- Authentication
 - Adaptive Authentication
 - Adaptive Authentication Scenarios
- Lab: Strong Authentication - Adaptive Authentication

Strong Authentication with Passwordless Authentication

- FIDO2 security key/biometrics login
 - Magic Link Login
- Lab: Strong Authentication - Passwordless Authentication

Module 5: Session 5

User Provisioning

- User Provisioning
- Benefits of User Provisioning
- User Provisioning Standards
- User Provisioning Methods
- Provisioning Capabilities in WSO2 IS
- Lab: Inbound Provisioning with SCIM
- Lab: Outbound Provisioning with Salesforce

Module 6: Session 6

B2B CIAM

- Overview of B2B CIAM
- Organization Management
- Key Workflows in a B2B Business
- B2B Applications
- Lab: Sub organization creation and application

API Authorization

- Benefits of securing APIs
- Types of API authorization
- Role Based Access Control RBAC
- Lab: API Authorization

Flows

- The limitations of static identity journeys
- How Flows adapt to evolving business and security requirements
- Flow elements
- How to design a flow
- Lab: Implementing Authentication Flows

DELIVERY NOTE

- Hardware Requirement: During the lab session attendees are required to deploy the created samples in multiple middleware products. Participants are required to have a workstation with at least 6GB of memory to run the samples smoothly.
- Software Requirement: If you are using the product installer to install the product, by default, WSO2 Identity Server is installed with OpenJDK, which allows you to run the product as soon as it is installed.
- Software Requirement: Apache Tomcat 8
- Software Requirement: MySQL 8.0 or 8.4
- Software Requirement: Corresponding MySQL JDBC Connector
- Software Requirement: Oracle/OpenJDK 21 or Oracle/Open JDK 25
- WSO2 Product: WSO2 Identity Server 7.3