**WSO2**

**WSO2 Identity Server:**

[WSO2 Identity Server](https://wso2.com/identity-and-access-management/) can be used to simplify identity and access management (IAM) related activities.

WSO2 Identity Server comes with seamless, easy to use integration capabilities that help connect applications, user stores, directories and identity management systems.

WSO2 Identity Server is responsible for providing the below features:

* User stores and directories
* Authentication of users (OAuth type is included)
* Authorization of users
* Single sign-on
* Provisioning
* Access delegation
* Password reset
* Self-registration
* Account locking

**Single Sign-On with WSO2 features:**

* OpenID connect support is available
* Single logout
* SSO between on-premise applications and cloud applications
* Simple service provider and identity provider ecosystem management

**What Is Service provider in WSO2?**

A Service Provider (SP) is an entity that provides Web services.

The WSO2 Identity Server allows to add service providers and specify various details which helps to link the service provider to the identity server.

* Adding a Service Provider
* Managing Service Providers
* Configuring a Resident Service Provider

Link : https://docs.wso2.com/display/IS500/Working+with+the+Service+Provider

**What Is Identity provider in WSO2?**

An identity provider (IdP) is a service that stores and manages digital identities.

An IdP workflow typically involves:

* A **request**. The user can enter credentials from another login (such as Google or Facebook or Twitter).
* **Verification**. The IdP checks with a company's IT to determine if the user has access and what work that person is allowed to do.
* **Unlocking**. The user gains access to the specified resources, and the visit is logged.

The WSO2 Identity Server allows you to add identity providers and specify various details which help to link the identity provider to the Identity Server

* Adding an Identity Provider
* Managing Identity Providers
* Configuring a Resident Identity Provider

Configuring OAuth2-OpenID Connect Single-Sign-On

To enable OAuth support for your client application, we must first register our application

Further details can be referred from this below link:

https://is.docs.wso2.com/en/latest/learn/configuring-oauth2-openid-connect-single-sign-on/

**OAuth/OpenID Connect**: OAuth 2.0 has three main phases. They are; requesting an Authorization Grant, exchanging the Authorization Grant for an Access Token and accessing the resources using this Access Token. OpenID Connect is another identity layer on top of OAuth 2.0. OAuth applications can get authentication event information over the ID token and can get the extra claims of the authenticated user from the OpenID Connect UserInfo endpoint. WSO2 IS supports Oauth 1.0 and 2.0.

**WSO2 API Manager:**

WSO2 API Manager is responsible for below features:

* Creating and publishing an API via the Publisher Portal of WSO2 API- Manager.
* Deploy the API in a Gateway environment.
* Publish the API in the Developer Portal.
* Subscribing to the API via the Developer Portal of WSO2 API- Manager and generating keys.
* Invoking the API with the generated keys.