

# Single Sign-On (SSO) - OIDC

## Introduction:

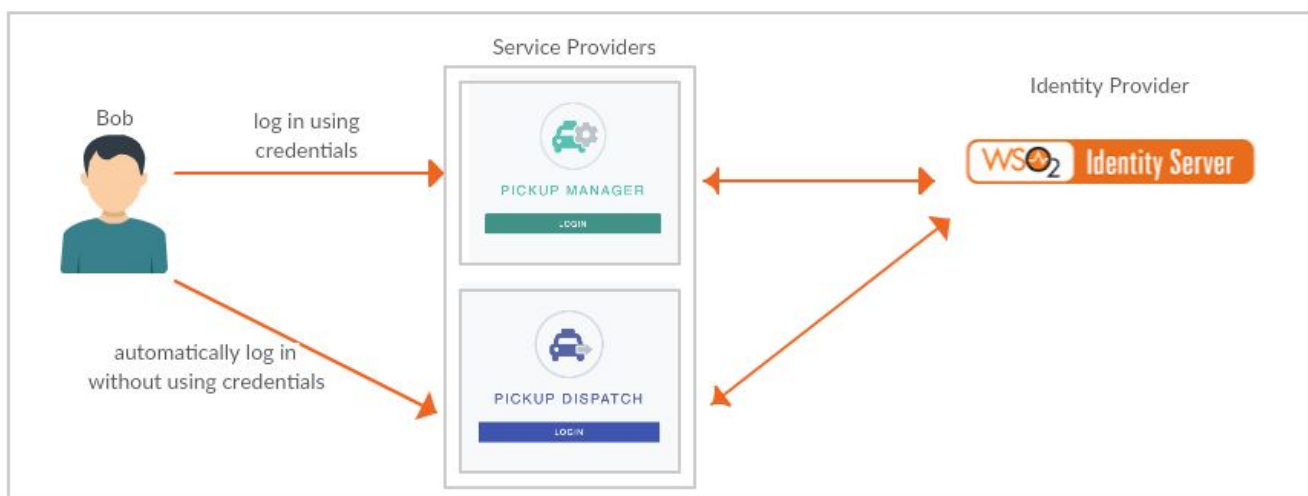
**Pickup** is a cab company that has many employees and different internal enterprise applications. Following are two such applications:

- **Pickup Dispatch:** This application helps manage the overall operations at Pickup.
- **Pickup Manager:** This application helps allocate vehicles to drivers.

Pickup is using **WSO2 Identity Server** as the identity provider for their applications.

Bob is a Pickup employee who usually forgets application passwords. As a result, Bob uses the same credentials for all the Pickup applications. However, due to busy schedules, Bob does not like entering the credentials at every login. So, WSO2 Identity Server team suggested Bob to use Single Sign-On (SSO).

With SSO, Bob only needs to provide the login credentials to one Pickup application and automatically be logged in to other Pickup applications.



# Setting up:

Let's learn how to configure OIDC-based SSO in WSO2 Identity Server:

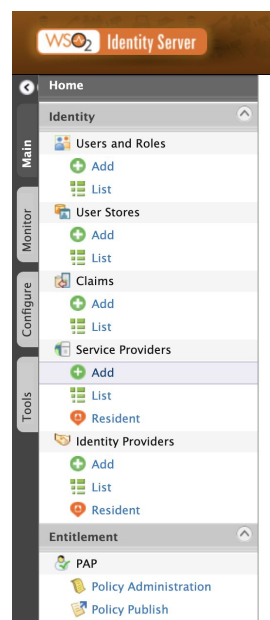
## Before you begin

1. Download the latest version of WSO2 Identity Server from [the web site](#).
2. Navigate to <IS\_HOME>/bin and start the server by executing either of the following, **./wso2server.sh** or **./wso2server.bat** run
3. [Download](#) and [install](#) Apache Tomcat version < tomcat8\*> or above.
4. Open the /etc/hosts file (**c:\Windows\System32\Drivers\etc\hosts** in windows) and add the following entry.

127.0.0.1 localhost.com

5. Access the WSO2 Identity Server Management Console at <https://localhost.com:9443/carbon> and login with admin:admin credentials.
6. To create a service provider for the Pickup Dispatch application:

- a. On the **Main** tab, click **Identity > Service Providers > Add**



- b. Enter the Service Provider Name as dispatch.

Home > Identity > Service Providers > Add

## Add New Service Provider

**Select Mode**


☒ Manual Configuration

☐ File Configuration


**Basic Information**

Service Provider Name:\*

dispatch

 A unique name for the service provider

Description:

 A meaningful description about the service provider

- c. Click **Register**.
- d. In the **Inbound Authentication** section, click **OAuth/OpenID Connect Configuration**.


☒ Claim Configuration

☒ Role/Permission Configuration

☒ Inbound Authentication Configuration

☒ SAML2 Web SSO Configuration

☒ OAuth/OpenID Connect Configuration

 Configure

☒ OpenID Configuration

☒ WS-Federation (Passive) Configuration

☒ WS-Trust Security Token Service Configuration

☒ Kerberos KDC

☒ Local & Outbound Authentication Configuration

☒ Inbound Provisioning Configuration

☒ Outbound Provisioning Configuration

- e. Enter the **Callback URL** as  
<http://localhost.com:8080/pickup-dispatch/oauth2client>.

[Home](#) > [Register New Application](#)

## Register New Application

New Application

OAuth Version\*

☐ 1.0a ☒ 2.0

☒ Code

☒ Implicit

☒ Password

☒ Client Credential

Allowed Grant Types

☒ Refresh Token


☒ SAML2

☒ IWA-NTLM

☒ urn:ietf:params:oauth:grant-type:jwt-bearer

Callback Url\*

☐ PKCE Mandatory

 Only allow applications that bear PKCE Code Challenge with them.

- ▼

Claim Configuration

▼

Role/Permission Configuration

▼

Inbound Authentication Configuration

▼

SAML2 Web SSO Configuration

▼

OAuth/OpenID Connect Configuration

OAuth Client Key	OAuth Client Secret	Actions
M_kq3pqGiW02B8QfqPhtbcpK_zla	..... <div>Show</div>	<div>Edit</div> <div>Revoke</div>

▼

OpenID Configuration

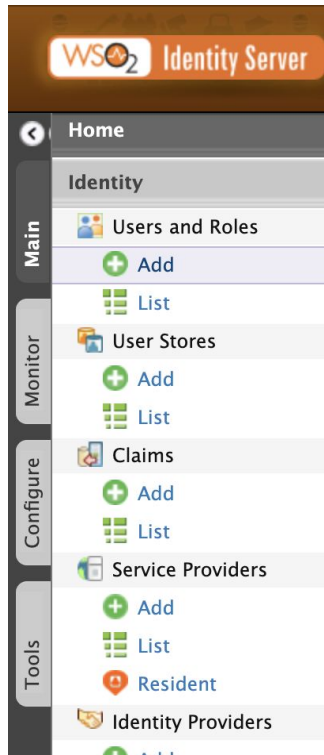
▼

WS-Federation (Passive) Configuration

- **Service Provider Name:** manager
- **Callback URL:**  
http://localhost.com:8080/pickup-manager/oauth2client

8. To create the application user:

- On the **Main** tab, click **Identity > Users and Roles > Add**.



- Click **Add New User**.

---

[Home](#) > [Identity](#) > [Users and Roles](#) > [Add](#)

## Add Users and Roles

---



- Enter the account details as follows.

- **Domain:** Select the user store in which you want to create the user.
- **Username:** bob
- **Password:** bob123

[Home](#) > Add User

## Add New User

### Step 1: Enter Username and Password

Enter username

Domain

PRIMARY ▾

Username\*

bob

Password\*

.....

Confirm Password\*

.....

Next >

Finish

Cancel

- Click **Next**.
- Select Application/dispatch and Application/manager user roles.

## Add New User

### Step 2: Select Roles of the User

Enter Role Name Pattern (\* for all)

Search Roles

#### Users of Role

[Select all on this page](#) | [Unselect all on this page](#)

- ☐ admin
- ☒ Application/dispatch
- ☒ Application/manager
- ☒ Internal/everyone
- ☐ Internal/system

Finish

Cancel

Click **Finish**.

9. Get the two war files [pickup-dispatch.war](#) and [pickup-manager.war](#) from the repo and deploy them in the tomcat.

10. Edit the dispatch.properties file in (pickup-dispatch -> WEB-INF -> classes) with the copied client\_id and secret in step 6 above.

11. Similarly edit the manager.properties file in (pickup-manager -> WEB\_INF -> classes) with the copied client\_id and secret in Step 7 above.

12. Restart the tomcat server.

## Try It:

Follow the steps below to try out the sample applications:

1. To access the Pickup Dispatch application, go to the following URL:  
http://<TOMCAT\_HOST>:<TOMCAT\_PORT>/pickup-dispatch, e.g.,  
<http://localhost.com:8080/pickup-dispatch> and sign in using Bob's credentials.
2. To access the Pickup Manager application, go to the following URL:  
http://<TOMCAT\_HOST>:<TOMCAT\_PORT>/pickup-manager, e.g.,  
<http://localhost.com:8080/pickup-manager>. Note that Bob is automatically logged in to the Pickup Manager application.

You have successfully configured OIDC-based SSO using WSO2 Identity Server as the identity provider.