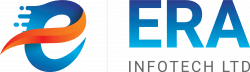
**“SSO (Single Sign On) with WSO2 Identity Server”**

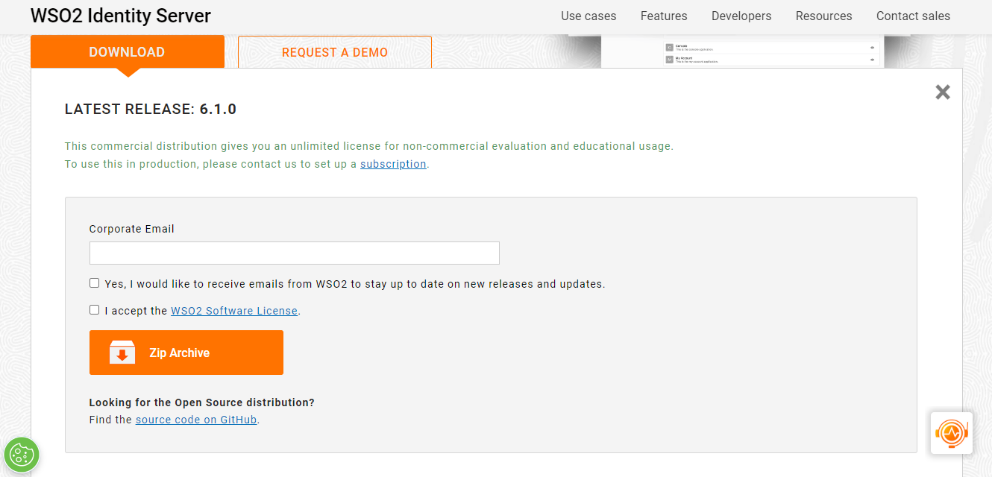
****

By



* Required tools and technology:
* WSO2 Identity Server.
* ELK (Optional)
* System Requirements:
* CPU: 4vCPUs(x86\_64 Architecture)
* Memory: 4 GB RAM
* Disk: ~ 10 GB disk space, excluding space allocated for log files and databases.
* JDK Version: Oracle JDK 11 or 17
* Configuration:
* WSO2 Identity Server:

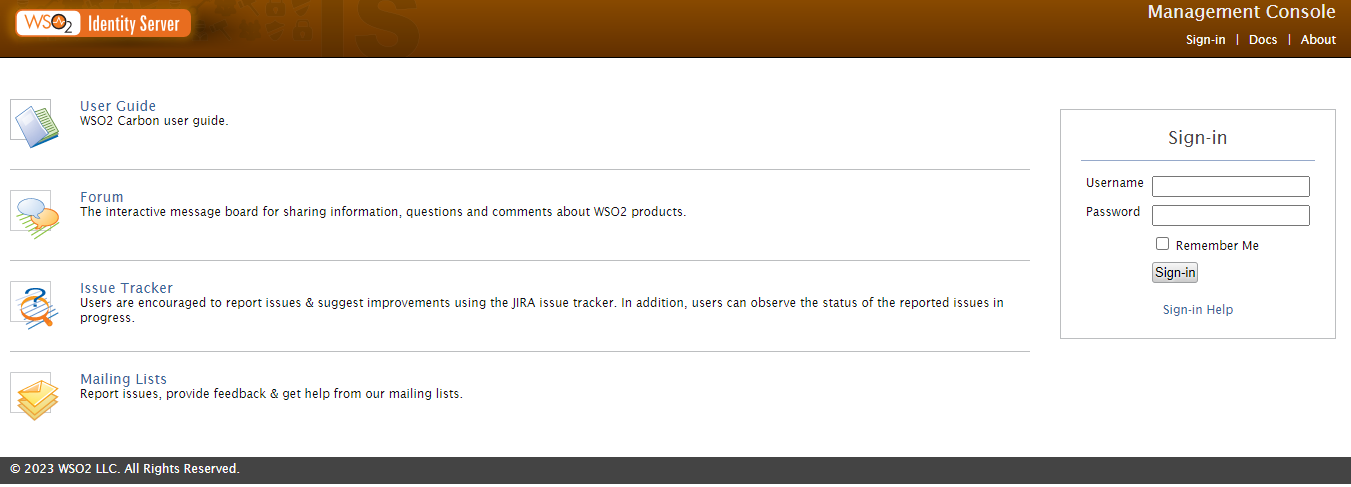
1. Download Identity Server from Identity server official site (<https://wso2.com/identity-server/>)



1. All the Installation related information is given in this link (https://is.docs.wso2.com/en/latest/deploy/get-started/install/)
2. Download JDK-11 and set System variable named JAVA\_HOME = <JDK path> (ex. C:\Program Files\Java\jdk-11.0.16)
3. Run Identity Server:

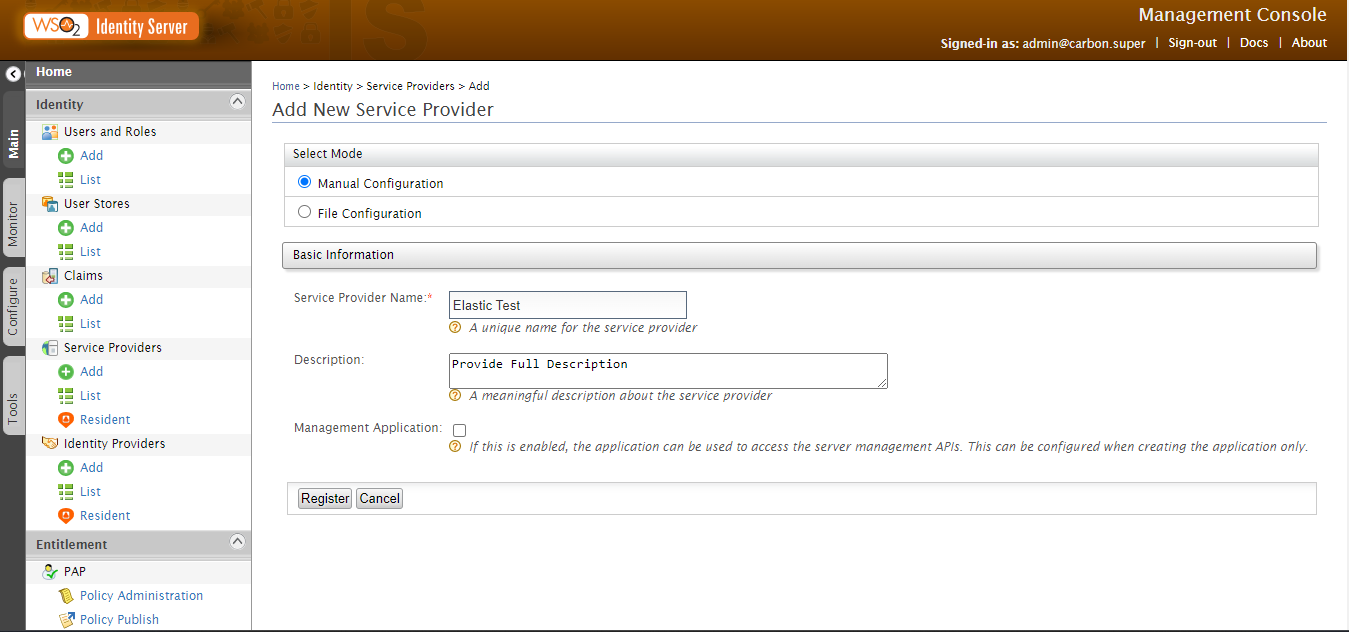
C:\Program Files\WSO2\Identity Server\6.0.0\bin> wso2server.bat (wso2server.sh for Linux)

1. Go to the browser and enter this url: (user: admin/pass: admin) <https://10.11.200.117:9443/carbon>

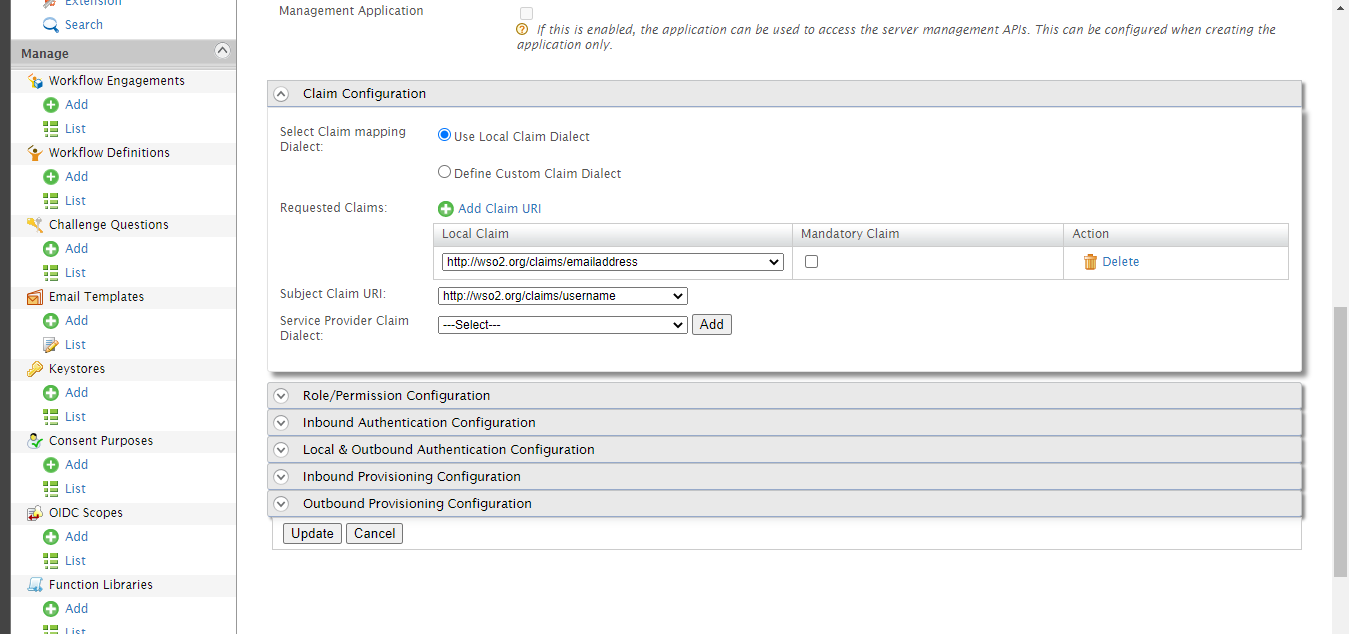


* User and Role Creation: Create a User and Role for identification by selecting User and Roles in Identity Server.
* Create Service Provider: Create a Service Provider by selecting Service Provider Option.

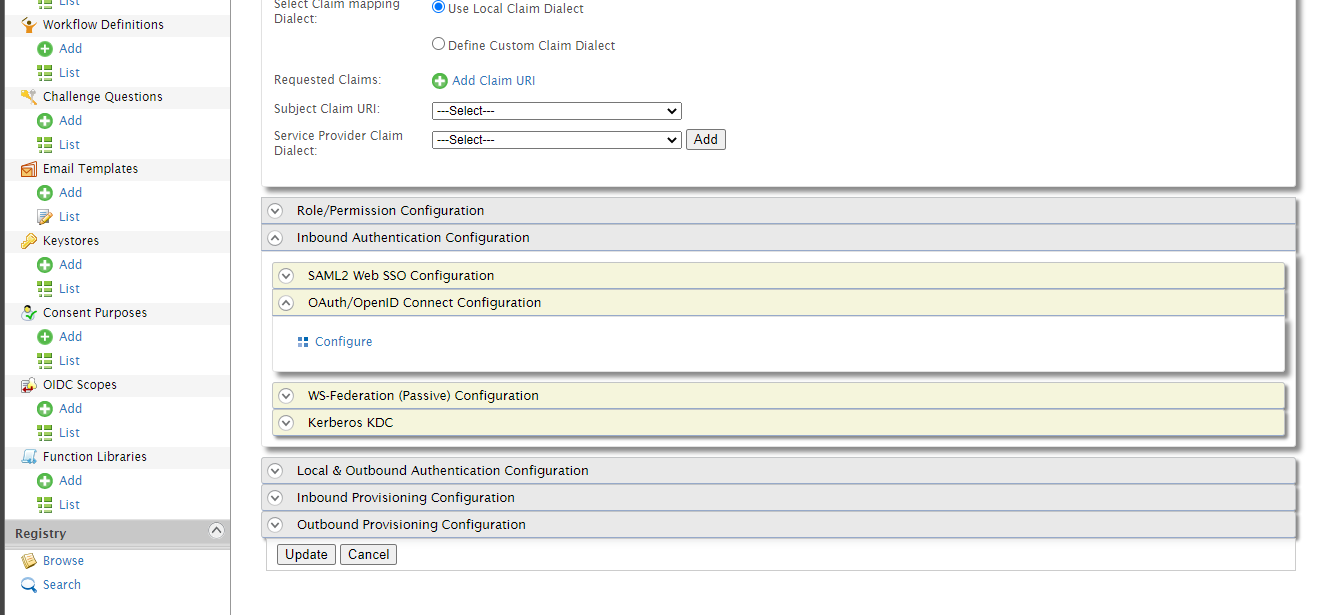
1. Click Add Button and Provide some Information –

**

1. Click Register Button and Provide Claim Configuration info.

**

1. Select Inbound Authentication Configuration>OAuth/OpenID Connect Configuration>Configure

**

1. Now Provide Callback Url\* (regexp=(<http://10.11.200.117:5601/api/security/oidc/callback|http://10.11.200.117:5601/security/logged_out)>) based on your kibana config.

Everything remain same.

* Elasticsearch Configuration: Open elasticsearch.yml file and do some change add below configuration.

xpack.security.authc.token.enabled: true

xpack.security.authc.realms.oidc.oidc1:

  order: 2

  rp.client\_id: "b2ttVQkmLbk72X2YvKKR1UbNlkEa"

  rp.response\_type: code

  rp.redirect\_uri: "http://10.11.200.117:5601/api/security/oidc/callback"

  op.issuer: "https://localhost:9443/oauth2/token"

  op.authorization\_endpoint: "https://localhost:9443/oauth2/authorize"

  op.token\_endpoint: "https://localhost:9443/oauth2/token"

  op.jwkset\_path: "https://localhost:9443/oauth2/jwks"

  op.endsession\_endpoint: "https://localhost:9443/oidc/logout"

  op.userinfo\_endpoint: "https://localhost:9443/oauth2/userinfo"

  rp.post\_logout\_redirect\_uri: "http://10.11.200.117:5601/security/logged\_out"

  #ssl.certificate\_authorities: ["oidc/amincer.cer"]

  #rp.requested\_scopes: ["profile","email","usergroups"]

  ssl.verification\_mode: none

  claims.principal: sub

  claims.groups: groups

  claims.name: name

  claims.mail: email

* Kibana Configuration: Open kibana.yml file and do some change add below configuration.

xpack.security.authc.providers:

  oidc.oidc1:

    order: 2

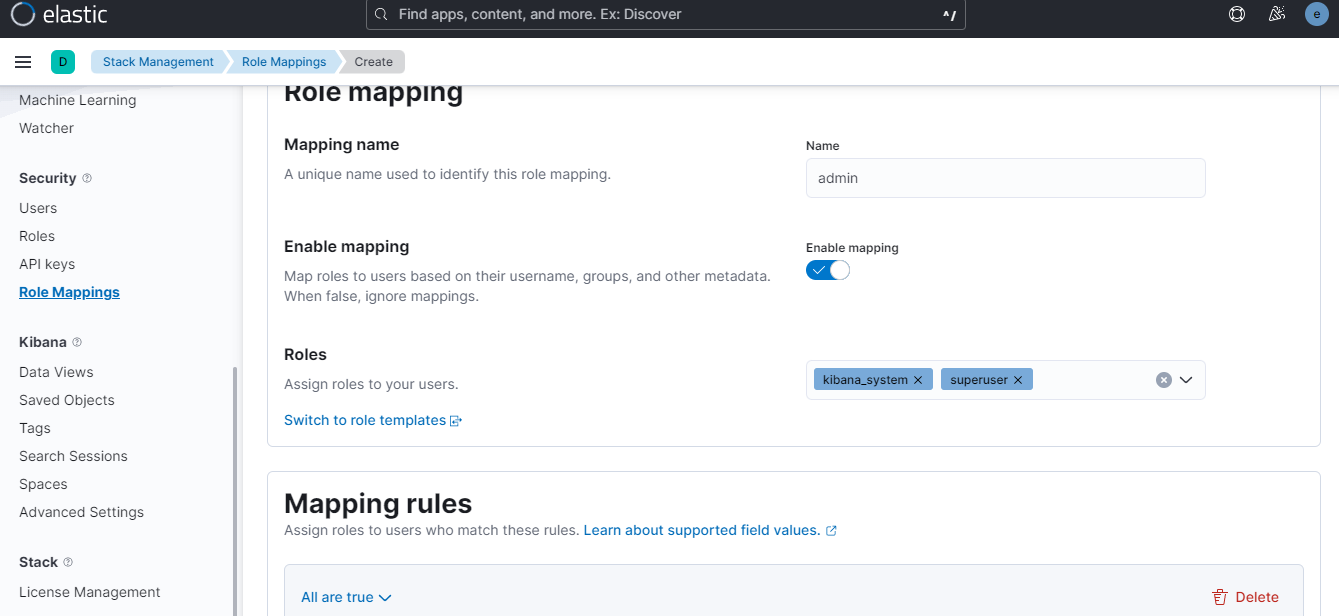
    realm: "oidc1"

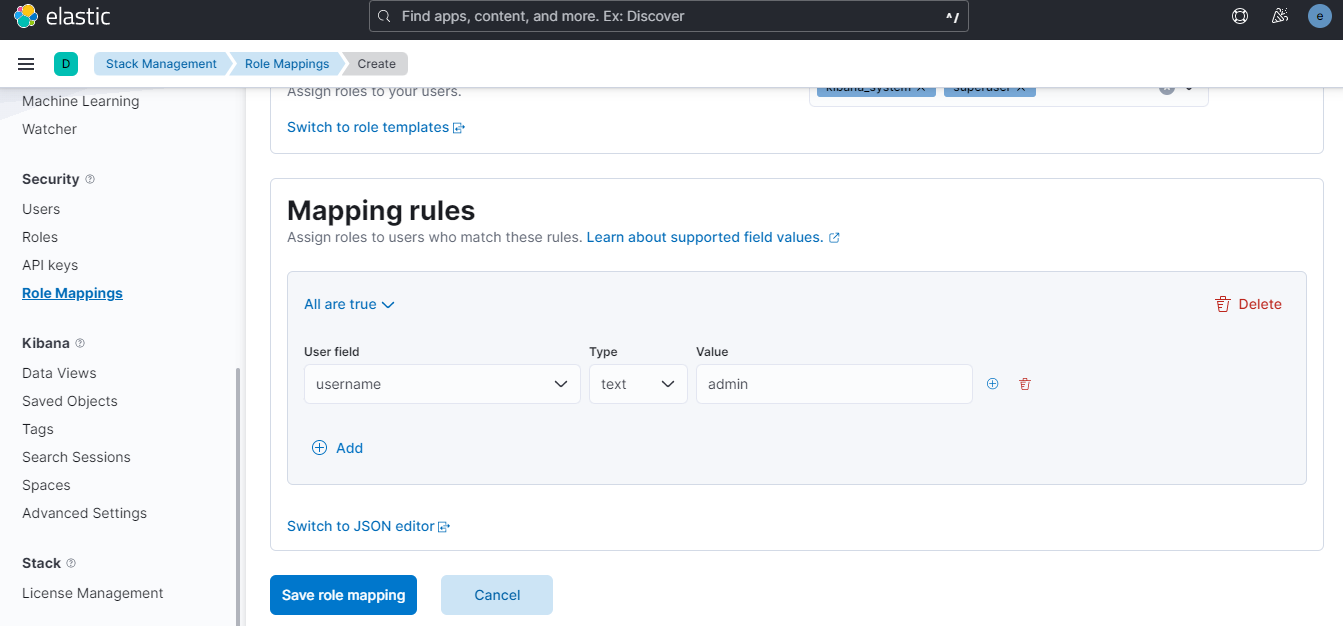
    description: "Log in with WSO2"

  basic.basic1:

    order: 1

* Kibana Role Mapping: Open Kibana Dashboard then go to Stack management > Stack > License Management menu and activate license. After activation you will find a menu (Security > Role Mappings) click on it and complete the setup.

**

**

* Wso2 Identity server API Document:

Url: <https://is.docs.wso2.com/en/latest/apis/overview/>