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

By

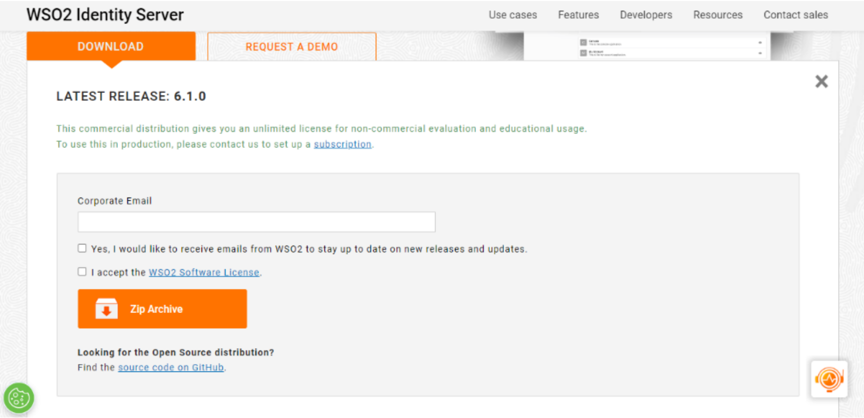
ERA INFOTECH LTD

Md. Ashiqul Islam Shajal (ASC)

- 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/)



LATEST RELEASE: 6.1.0

This commercial distribution gives you an unlimited license for non-commercial evaluation and educational usage.
To use this in production, please contact us to set up a subscription.

Corporate Email

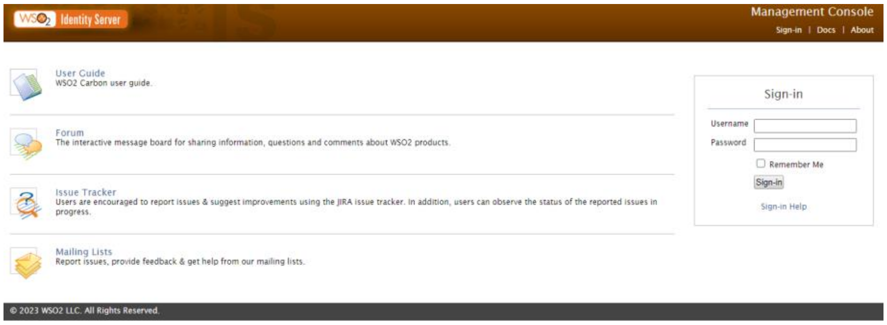
□ Yes, I would like to receive emails from WSO2 to stay up to date on new releases and updates.

□ I accept the WSO2 Software License.

Looking for the Open Source distribution?
Find the source code on GitHub.

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

       C:\Program Files\WSO2\Identity Server\6.0.0\bin>
       wso2server.bat (wso2server.sh for Linux)
    5) Go to the browser and enter this url: (user: admin/pass: admin) https://10.11.200.117:9443/carbon



User Guide
WSO2 Carbon user guide.

Forum
The interactive message board for sharing information, questions and comments about WSO2 products.

Issue Tracker
Users are encouraged to report issues & suggest improvements using the JIRA issue tracker. In addition, users can observe the status of the reported issues in progress.

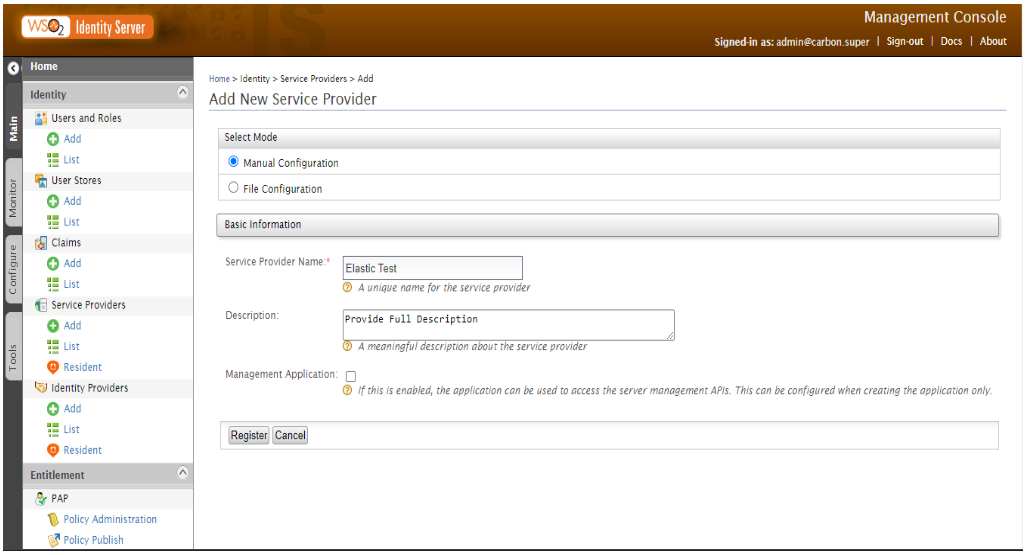
Mailing Lists
Report issues, provide feedback & get help from our mailing lists.

Username
Password
□ Remember Me

© 2023 WSO2 LLC. All Rights Reserved.

- 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 –



Add New Service Provider

Select Mode

● Manual Configuration

○ File Configuration

Basic Information

Service Provider Name:* Elastic Test

A unique name for the service provider

Description: Provide Full Description

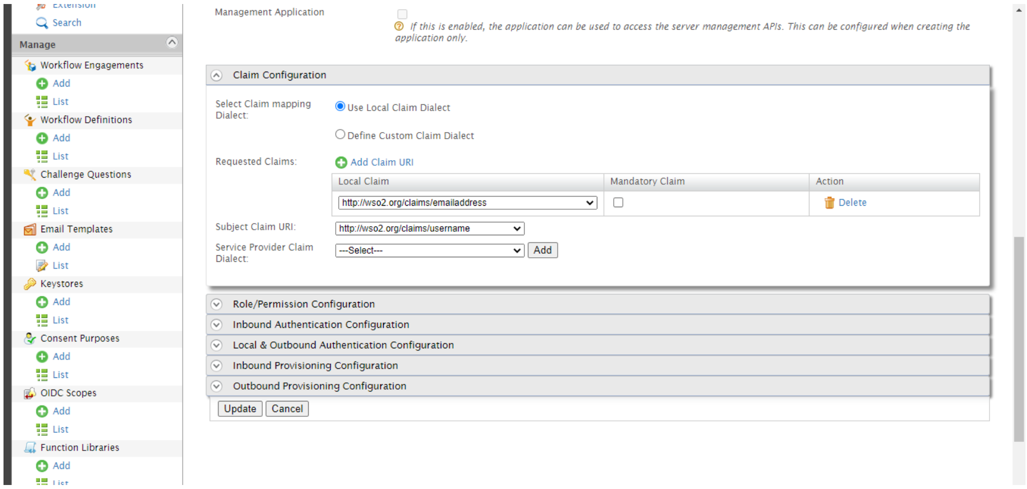
A meaningful description about the service provider

Management Application: □

If this is enabled, the application can be used to access the server management APIs. This can be configured when creating the application only.

Register Cancel

2) Click Register Button and Provide Claim Configuration info.



Management Application □

If this is enabled, the application can be used to access the server management APIs. This can be configured when creating the application only.

Claim Configuration

Select Claim mapping Dialect: ● Use Local Claim Dialect

○ Define Custom Claim Dialect

Requested Claims: Add Claim URI

Local Claim	Mandatory Claim	Action
http://wso2.org/claims/emailaddress	□	Delete

Subject Claim URI: http://wso2.org/claims/username

Service Provider Claim Dialect: ---Select--- Add

Role/Permission Configuration

Inbound Authentication Configuration

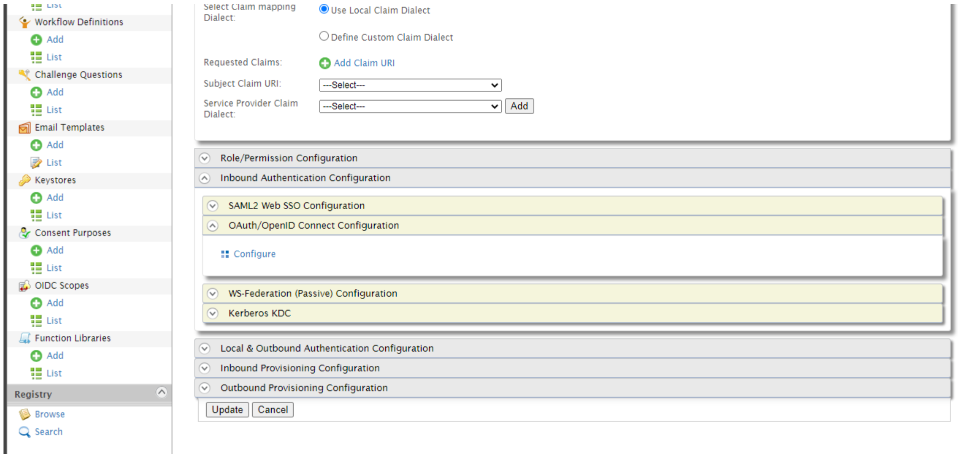
Local & Outbound Authentication Configuration

Inbound Provisioning Configuration

Outbound Provisioning Configuration

Update Cancel

3) Select Inbound Authentication Configuration>OAuth/OpenID Connect Configuration>Configure


List
Workflow Definitions
Add
List
Challenge Questions
Add
List
Email Templates
Add
List
Keystores
Add
List
Consent Purposes
Add
List
OIDC Scopes
Add
List
Function Libraries
Add
List
Registry
Browse
Search

Select Claim mapping Dialect: ● Use Local Claim Dialect ○ Define Custom Claim Dialect

Requested Claims: Add Claim URI

Subject Claim URI: ---Select---

Service Provider Claim Dialect: ---Select--- Add

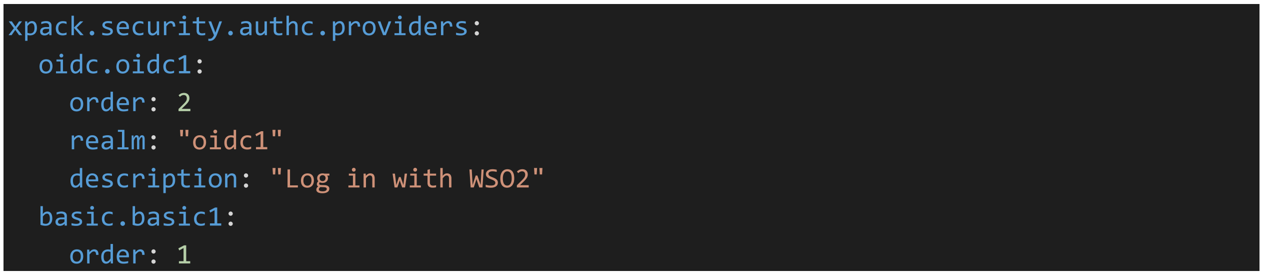
Role/Permission Configuration
Inbound Authentication Configuration
SAML2 Web SSO Configuration
OAuth/OpenID Connect Configuration
Configure
WS-Federation (Passive) Configuration
Kerberos KDC
Local & Outbound Authentication Configuration
Inbound Provisioning Configuration
Outbound Provisioning Configuration
Update
Cancel

4) 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.

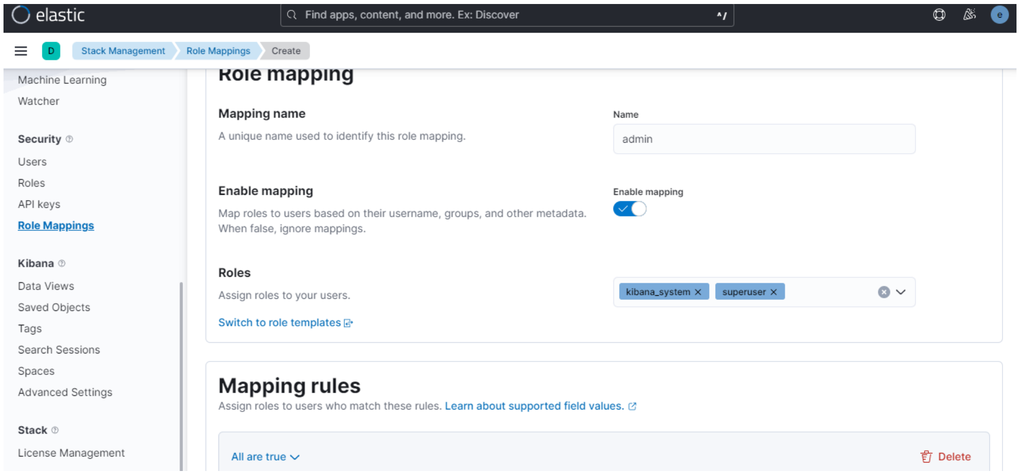
```
xpack.security.authc.token.enabled: true
xpack.security.authc.realms.oidc.oidc1:
  order: 2
  rp.client_id: "b2ttVQkmLbk72X2YvKKR1UbNlkEa"
  rp.response_type: code
  rp.redirect_uri: "http://10.11.200.117:5601/api/security/oidc/callback"
  op.issuer: "https://localhost:9443/oauth2/token"
  op.authorization_endpoint: "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.



Role mapping

Mapping name
A unique name used to identify this role mapping.

Name: admin

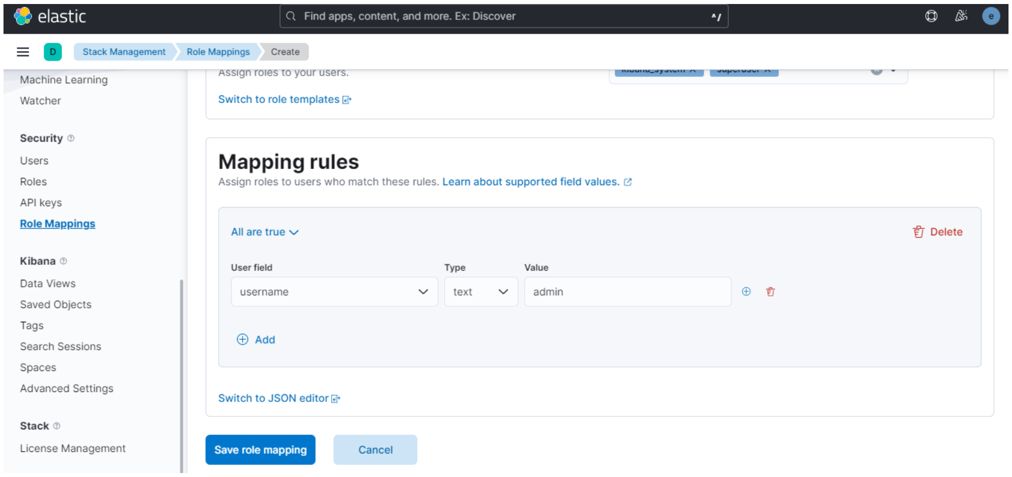
Enable mapping
Map roles to users based on their username, groups, and other metadata. When false, ignore mappings.

Enable mapping: ☑

Roles
Assign roles to your users.

kibana_system ✕ superuser ✕

Mapping rules
Assign roles to users who match these rules. Learn about supported field values.



Mapping rules

Assign roles to users who match these rules. Learn about supported field values.

User field: username
Type: text
Value: admin

- Wso2 Identity server API Document:

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