# WSO2 Integration

* [Install WSO2 Server](#WSO2Integration-InstallWSO2Server)
* [Configure SAML Provider](#WSO2Integration-ConfigureSAMLProvider)
* [Configure Incorta SSO](#WSO2Integration-ConfigureIncortaSSO)

## Install WSO2 Server

1- If you don’t have a **WSO2 server**,you can download it from <https://wso2.com/identity-server/>

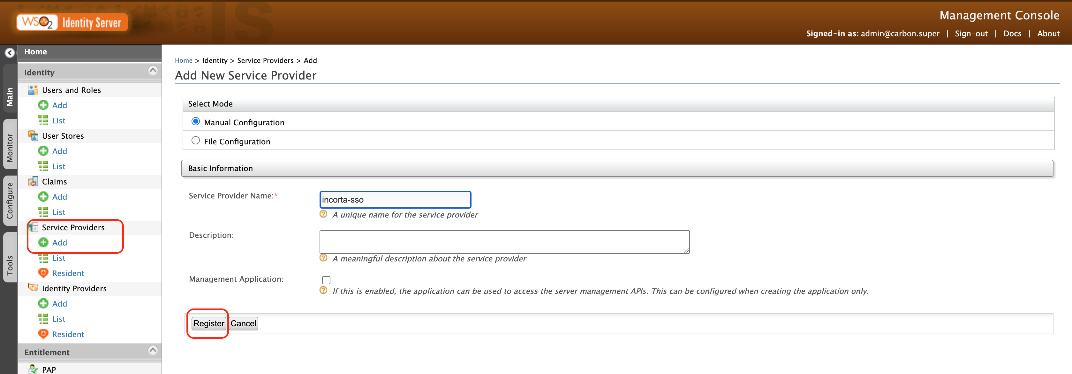
2- Follow these steps to install and setup it <https://is.docs.wso2.com/en/latest/get-started/sample-use-cases/set-up/>

## Configure SAML Provider

1- Log in to the Management Console (https://<WSO2-server-url>/carbon)

2- Navigate to **Main** > **Identity** > **Service Providers** and click **Add**.

3- Enter the **Service Provider Name** text box, for example, incorta-sso, and click **Register**.



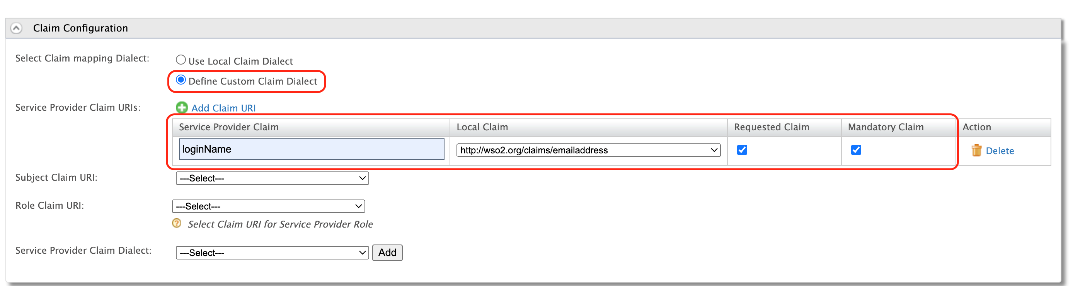
4- In the **Claim Configuration** section, click **Define Custom Claim Dialect**, then click **Add Claim URI**

a- Set **Service Provider Claim:** loginName  
b- Set **Local Claim:** a unique user identifier (should match the login name field for the Incorta user), for example, HTTP://wso2.org/claims/emailaddress

c- Select the following checkboxes:

- Requested Claim

- Mandatory Claim



5- In the **Inbound Authentication Configuration** section, click **Configure** under the **SAML2 Web SSO Configuration** section.

Now set the configuration as follows:

a- **Issuer**: incorta-sso.com

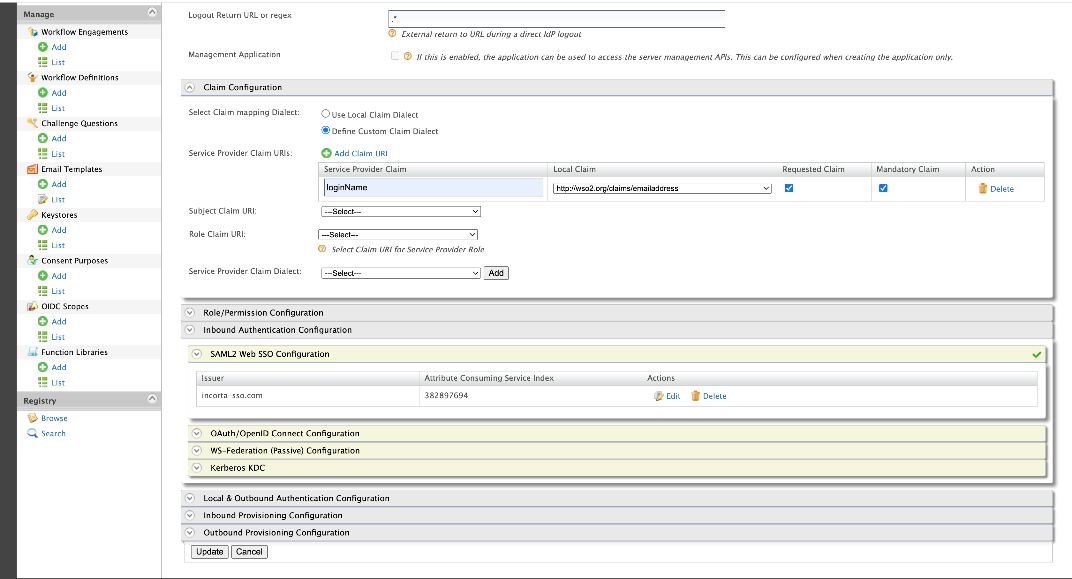
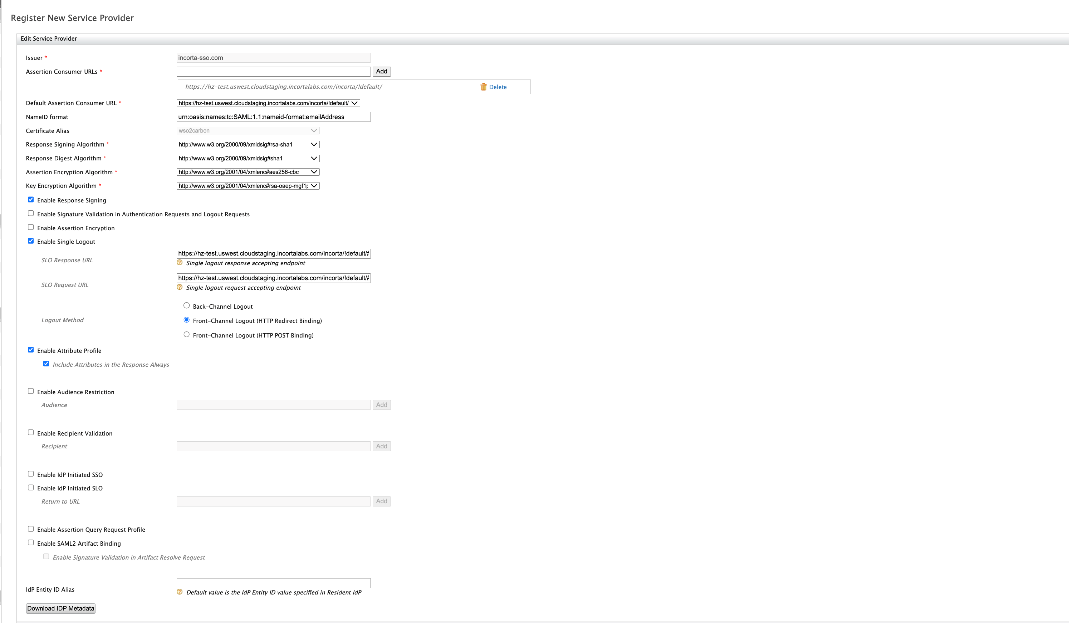
b- **Assertion Consumer URL**: https://IncortaUrl/!<tenantName>, then click **Add**  
**ex**: https://hz-test.uswest.cloudstaging.incortalabs.com/incorta/!default/

c- Select **Enable Response Signing** checkbox

d-Select **Enable Single Logout**, Then set the Incorta logout URL   
like https://hz-test.uswest.cloudstaging.incortalabs.com/incorta/!default/#/logout.jsp  
and select the **logout method** Front-Channel Logout (HTTP Redirect Binding)  
e- Select **Enable Attribute Profile**, and ***Include Attributes in the Response Always***

6- Then Click **Download IDP Metadata**, to download the metadata XML

7- Click **Register** to save the changes, Then click **Update.**



## Configure Incorta SSO

1- In CMC, Navigate to your tenant configuration > **Security**   
2- Set **Authentication Type** SSO  
3- Set **Provider type** SAML2  
4- From the metadata XML, prepare the following configs

onelogin.saml2.strict = false

onelogin.saml2.debug = true

onelogin.saml2.sp.entityid = <Issuer value>

onelogin.saml2.sp.assertion\_consumer\_service.url = <the configured assertion consumer URL>

onelogin.saml2.sp.assertion\_consumer\_service.binding = urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST

onelogin.saml2.sp.single\_logout\_service.url = <incorta-Logout-url>

onelogin.saml2.sp.single\_logout\_service.binding = urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect

onelogin.saml2.sp.nameidformat = urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

onelogin.saml2.idp.entityid = <Issuer value>

onelogin.saml2.idp.single\_sign\_on\_service.url = <login URL in SingleSignOnService tag in xml>

onelogin.saml2.idp.single\_sign\_on\_service.binding = urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect

onelogin.saml2.idp.single\_logout\_service.url = <logout URL in SingleLogoutService tag in xml>

onelogin.saml2.idp.single\_logout\_service.response.url = <logout URL in SingleLogoutService tag in xml>

onelogin.saml2.idp.single\_logout\_service.binding = urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect

onelogin.saml2.idp.x509cert= <the value of the X509Certificate tag in xml>

onelogin.saml2.security.nameid\_encrypted = false

onelogin.saml2.security.authnrequest\_signed = false

onelogin.saml2.security.logoutrequest\_signed = false

onelogin.saml2.security.logoutresponse\_signed = false

onelogin.saml2.security.want\_messages\_signed =

onelogin.saml2.security.want\_assertions\_signed = false

onelogin.saml2.security.want\_assertions\_encrypted = false

onelogin.saml2.security.want\_nameid\_encrypted = false

onelogin.saml2.security.requested\_authncontext = urn:oasis:names:tc:SAML:2.0:ac:classes:urn:oasis:names:tc:SAML:2.0:ac:classes:Password

onelogin.saml2.security.onelogin.saml2.security.requested\_authncontextcomparison = exact

onelogin.saml2.security.want\_xml\_validation = true

onelogin.saml2.security.signature\_algorithm = http://www.w3.org/2000/09/xmldsig#rsa-sha1

* The following is a sample configuration
* onelogin.saml2.strict = false
* onelogin.saml2.debug = true
* onelogin.saml2.sp.entityid = incorta-sso.com
* onelogin.saml2.sp.assertion\_consumer\_service.url = https://hz-test.uswest.cloudstaging.incortalabs.com/incorta/!default/
* onelogin.saml2.sp.assertion\_consumer\_service.binding = urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST
* onelogin.saml2.sp.single\_logout\_service.url = https://hz-test.uswest.cloudstaging.incortalabs.com/incorta/!default/#/logout.jsp
* onelogin.saml2.sp.single\_logout\_service.binding = urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect
* onelogin.saml2.sp.nameidformat = urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
* onelogin.saml2.idp.entityid = incorta-sso.com
* onelogin.saml2.idp.single\_sign\_on\_service.url = https://localhost.com:9443/samlsso
* onelogin.saml2.idp.single\_sign\_on\_service.binding = urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect
* onelogin.saml2.idp.single\_logout\_service.url = https://localhost.com:9443/samlsso
* onelogin.saml2.idp.single\_logout\_service.response.url = https://localhost.com:9443/samlsso
* onelogin.saml2.idp.single\_logout\_service.binding = urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect
* onelogin.saml2.idp.x509cert=
* onelogin.saml2.security.nameid\_encrypted = false
* onelogin.saml2.security.authnrequest\_signed = false
* onelogin.saml2.security.logoutrequest\_signed = false
* onelogin.saml2.security.logoutresponse\_signed = false
* onelogin.saml2.security.want\_messages\_signed =
* onelogin.saml2.security.want\_assertions\_signed = false
* onelogin.saml2.security.want\_assertions\_encrypted = false
* onelogin.saml2.security.want\_nameid\_encrypted = false
* onelogin.saml2.security.requested\_authncontext = urn:oasis:names:tc:SAML:2.0:ac:classes:urn:oasis:names:tc:SAML:2.0:ac:classes:Password
* onelogin.saml2.security.onelogin.saml2.security.requested\_authncontextcomparison = exact
* onelogin.saml2.security.want\_xml\_validation = true

onelogin.saml2.security.signature\_algorithm = http://www.w3.org/2000/09/xmldsig#rsa-sha1

5- Click **Save.**