# SAML-2.0 Single Sign-On Configuration Guide

**Products:**

* wso2is-5.0.0 (Identity Provider)
* wso2am-1.7.0
* wso2bps-3.2.0
* wso2bam-2.4.1

**Pr-Requisites:**

* The user store configuration of all carbon JVMs should point to the same datasource.

**Configure API Manager Jaggery Applications as SSO Service Providers**

Following configurations are used to register the jaggery applications as SSO service providers. The AM server needs to be restarted after the configuration changes.

|  |  |
| --- | --- |
| **Entry** | **Description** |
| ssoConfiguration | JSON block containing the SSO configurations for the jaggery module. |
| enabled | To enable SSO for the application, set the value to “true”. To disable SSO, set the value to “false”. |
| issuer | The issuer identifier for the application. This value is used by the identity provider to distinguish between different service providers. |
| identityProviderURL | The redirecting SSO url of the identity provider. Configure to point to the running wso2is instance.  **Syntax:** [https://<identity\_provider\_ip>:<port>/samlsso](https://localhost:9444/samlsso)  **E.g.:** https://localhost:9444/samlsso |
| keyStoreName | The keystore of the running identity provider.  To use a remote instance of WSO2 IS here, you can import the public certificate of the IS keystore to the APIM and then point to the APIM keystore.  The default keystore of the APIM: <APIM\_HOME>/repository/resources/security/wso2carbon.jks |
| keyStorePassword | Password of the keystore. |
| identityAlias | Set the value as “wso2carbon”. |
| responseSigningEnabled | Set the value to “true”. |

Followings are examples for each jaggery application configuration available in API Manager;

***API Publisher:***

**File:**

<AM\_HOME>/repository/deployment/server/jaggeryapps/publisher/site/conf/site.json

**Configuration:**

"ssoConfiguration" : {

"enabled" : "true",

"issuer" : "API\_PUBLISHER",

"identityProviderURL" : "https://localhost:9444/samlsso",

"keyStorePassword" : "wso2carbon",

"identityAlias" : "wso2carbon",

"responseSigningEnabled":"true",

"keyStoreName" :"repository/resources/security/wso2carbon.jks"

}

***API Store:***

**File:**

<AM\_HOME>/repository/deployment/server/jaggeryapps/store/site/conf/site.json

**Configuration:**

"ssoConfiguration" : {

"enabled" : "true",

"issuer" : "API\_STORE",

"identityProviderURL" : "https://localhost:9444/samlsso",

"keyStorePassword" : "wso2carbon",

"identityAlias" : "wso2carbon",

"responseSigningEnabled":"true",

"keyStoreName" :"repository/resources/security/wso2carbon.jks"

}

***API Manage:***

**File:**

<AM\_HOME>/repository/deployment/server/jaggeryapps/manage/site/conf/site.json

**Configuration:**

"ssoConfiguration" : {

"enabled" : "true",

"issuer" : "API\_MANAGE",

"identityProviderURL" : "https://localhost:9444/samlsso",

"keyStorePassword" : "wso2carbon",

"identityAlias" : "wso2carbon",

"responseSigningEnabled":"true",

"keyStoreName" :"repository/resources/security/wso2carbon.jks"

}

***API Sandbox:***

**File:**

<AM\_HOME>/repository/deployment/server/jaggeryapps/sandbox/site/conf/site.json

**Configuration:**

"ssoConfiguration" : {

"enabled" : "true",

"issuer" : "API\_SANDBOX",

"identityProviderURL" : "https://localhost:9444/samlsso",

"keyStorePassword" : "wso2carbon",

"identityAlias" : "wso2carbon",

"responseSigningEnabled":"true",

"keyStoreName" :"repository/resources/security/wso2carbon.jks"

}

#### **Configure SSO for Carbon Server Management Consoles**

As the first step, the SAML2 relying party(SAML2SSOAuthenticator) feature needs to be installed in below carbon servers;

* wso2am-1.7.0
* wso2bps-3.2.0
* wso2bam-2.4.1

Steps are as follows;

1. Log in to Carbon Server Management Console of the server.
2. Configure → Features
3. Under “Feature Management”, go to “Available Features” tab.
4. Add WSO2 online P2 repository as a new repository. Usually the P2 repository is available under below URL;

**Syntax:**

<http://dist.wso2.org/p2/carbon/releases/><Carbon-Release-Version>

**E.g.:**

<http://dist.wso2.org/p2/carbon/releases/4.2.0>

1. Uncheck “Group features by category” option. Type “authenticator” in “Filter by feature name” textbox and click on “Find Features”.
2. Install the feature “SAML2 based Single Sign-On authenticator”.

The following configurations enable SSO for each carbon server management console. The server needs to be restarted after the configuration changes;

|  |  |
| --- | --- |
| **Entry** | **Description** |
| Authenticator → name | Set the value as “SAML2SSOAuthenticator”. |
| Authenticator → disabled | To enable SSO for management console, set the value to “false”. To disable, set the value to “true”. |
| Priority | The priority level of the authenticator. |
| LoginPage | The default login page URL of Carbon. All requests coming to this page will be intercepted for authentication. It is not necessary to change this value from the value given in the sample configuration. |
| ServiceProviderID | The unique identifier for the Carbon Server in an SSO setup. This value should be used as the value of the issuer in the Identity Server configuration. |
| IdentityProviderSSOServiceURL | The Identity Provider URL to which the users will be redirected for authentication.  **Syntax:** [https://<identity\_provider\_ip>:<port>/samlsso](https://localhost:9444/samlsso)  **E.g.:** https://localhost:9444/samlsso |
| NameIDPolicyFormat | This specifies the name identifier format that the Carbon server wants to receive in the subject of an assertion from a particular identity provider. Leave the default configuration as it is. |

Followings are examples of SSO enabling configurations for carbon server management consoles;

***WSO2 AM:***

**File:**

<AM\_HOME>/repository/conf/security/authenticators.xml

**Configuration:**

<Authenticator name="SAML2SSOAuthenticator" disabled="false">

<Priority>0</Priority>

<Config>

<Parameter name="LoginPage">/carbon/admin/login.jsp</Parameter>

<Parameter name="ServiceProviderID">WSO2AM</Parameter>

<Parameter name="IdentityProviderSSOServiceURL"> <https://localhost:9444/samlsso>

</Parameter>

<Parameter name="NameIDPolicyFormat">

urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified </Parameter>

</Config>

</Authenticator>

***WSO2 IS:***

**File:**

<IS\_HOME>/repository/conf/security/authenticators.xml

**Configuration:**

<Authenticator name="SAML2SSOAuthenticator" disabled="false">

<Priority>10</Priority>

<Config>

<Parameter name="LoginPage">/carbon/admin/login.jsp</Parameter>

<Parameter name="ServiceProviderID">WSO2IS</Parameter>

<Parameter name="IdentityProviderSSOServiceURL"> <https://localhost:9444/samlsso>

</Parameter>

<Parameter name="NameIDPolicyFormat">

urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified </Parameter>

</Config>

</Authenticator>

***WSO2 BPS:***

**File:**

<BPS\_HOME>/repository/conf/security/authenticators.xml

**Configuration:**

<Authenticator name="SAML2SSOAuthenticator" disabled="false">

<Priority>10</Priority>

<Config>

<Parameter name="LoginPage">/carbon/admin/login.jsp</Parameter>

<Parameter name="ServiceProviderID">WSO2BPS</Parameter>

<Parameter name="IdentityProviderSSOServiceURL"> <https://localhost:9444/samlsso>

</Parameter>

<Parameter name="NameIDPolicyFormat">

urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified </Parameter>

</Config>

</Authenticator>

***WSO2 BAM:***

**File:**

<BAM\_HOME>/repository/conf/security/authenticators.xml

**Configuration:**

<Authenticator name="SAML2SSOAuthenticator" disabled="false">

<Priority>10</Priority>

<Config>

<Parameter name="LoginPage">/carbon/admin/login.jsp</Parameter>

<Parameter name="ServiceProviderID">WSO2BAM</Parameter>

<Parameter name="IdentityProviderSSOServiceURL"> <https://localhost:9444/samlsso>

</Parameter>

<Parameter name="NameIDPolicyFormat">

urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified </Parameter>

</Config>

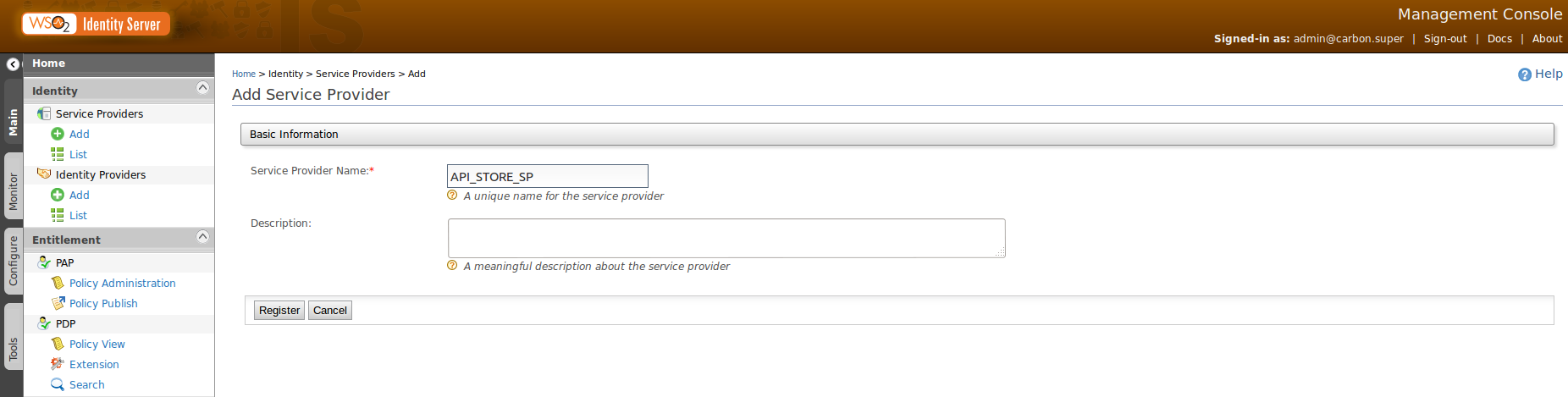
</Authenticator>

#### **Configuring WSO2 Identity Server as SAML 2.0 SSO Identity Provider**

1. Start wso2is and login to Carbon Management Console as administrator.
2. Navigate to “Add Service Provider“.

Main → Identity → Service Providers → Add

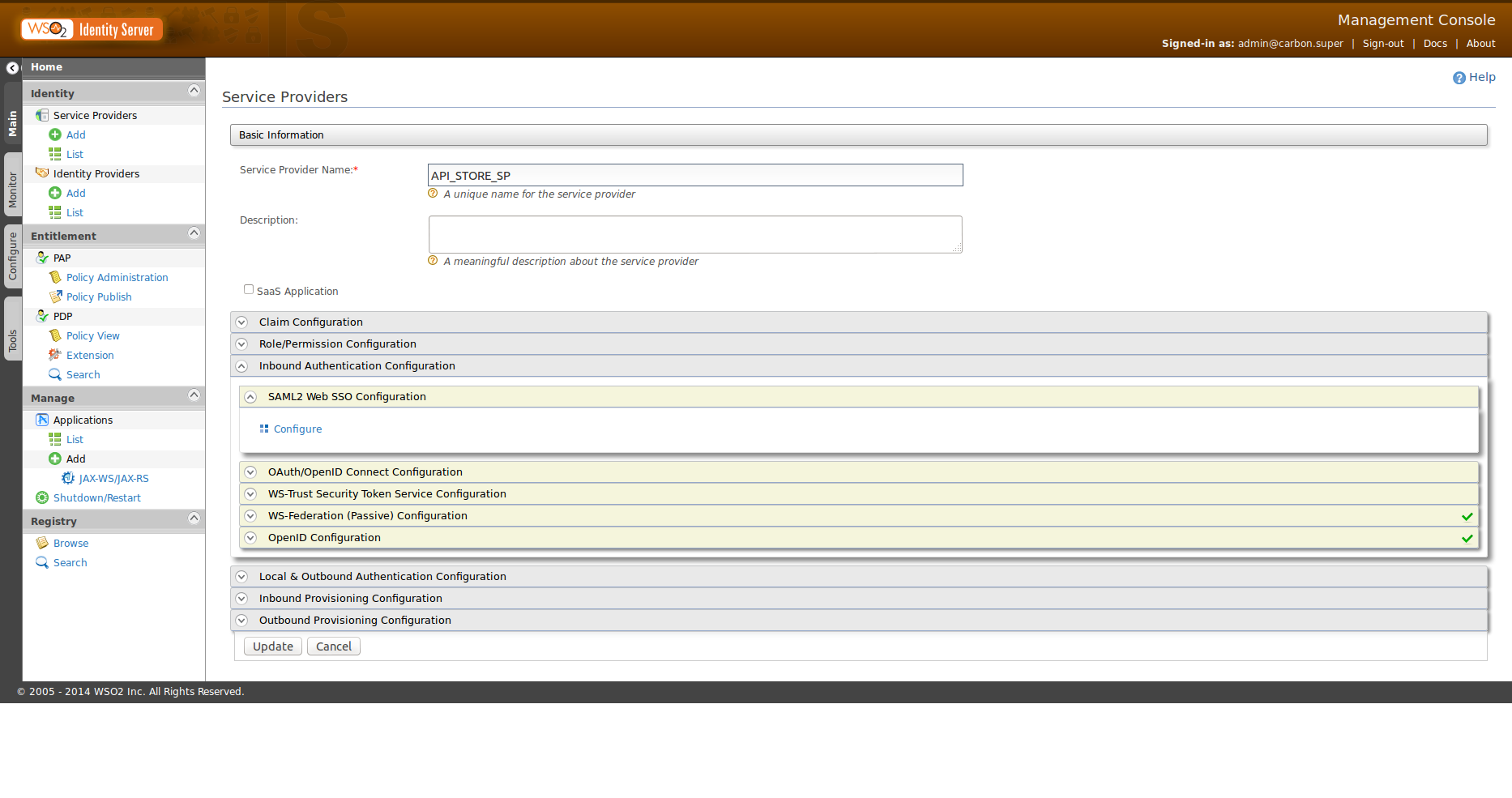
1. Give a service provider name and click “Register”.



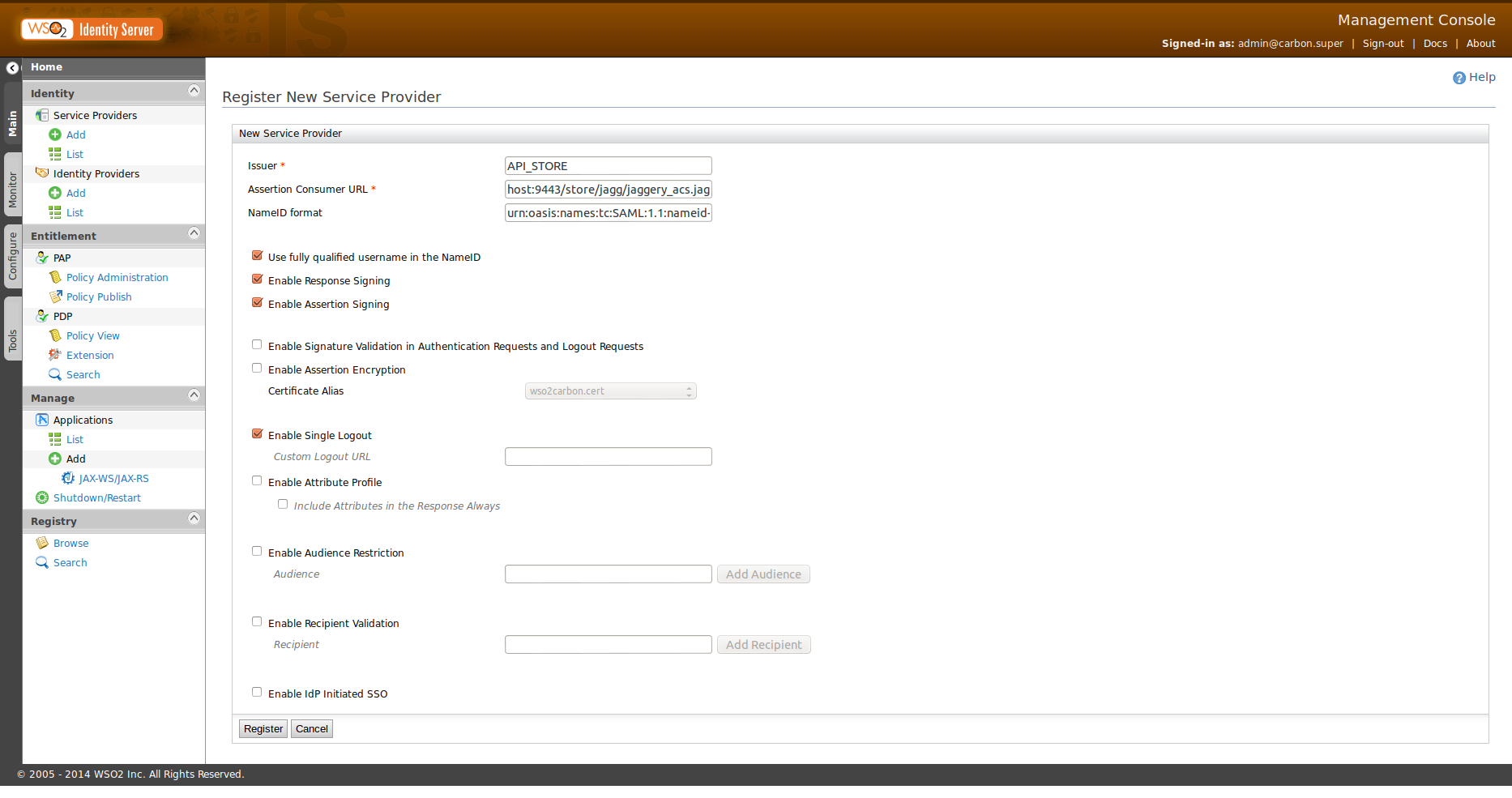
1. You are navigated to “Service Providers” detailed configuration page.
2. Navigate to;

Inbound Authentication Configuration→ [SAML2 Web SSO Configuration](https://localhost:9444/carbon/application/configure-service-provider.jsp)

→ Configure



1. You are navigated to “Register New Service Provider” page.
2. Perform below configurations for each APIM jaggery application and Carbon server to register as a service provider in IS.



1. Click “Register” → “Update” to complete the SP setup.

***API\_STORE\_SP:***

Service Provider Name: API\_STORE\_SP

Issuer: API\_STORE

Assertions Consumer URL:

*Syntax:*

https://<apim\_ip>:<port>/store/jagg/jaggery\_acs.jag

*E.g.:*

<https://localhost:9443/store/jagg/jaggery_acs.jag>

Select the following options:

* Use fully qualified username in the NameID
* Enable Response Signing
* Enable Assertion Signing
* Enable Single Logout

***API\_PUBLISHER\_SP:***

Service Provider Name: API\_PUBLISHER\_SP

Issuer: API\_PUBLISHER

Assertions Consumer URL:

*Syntax:*

https://<apim\_ip>:<port>/publisher/jagg/jaggery\_acs.jag

*E.g.:*

[https://localhost:9443/publisher/jagg/jaggery\_acs.jag](https://localhost:9443/store/jagg/jaggery_acs.jag)

Select the following options:

* Use fully qualified username in the NameID
* Enable Response Signing
* Enable Assertion Signing
* Enable Single Logout

***API\_MANAGE\_SP:***

Service Provider Name: API\_MANAGE\_SP

Issuer: API\_MANAGE

Assertions Consumer URL:

*Syntax:*

https://<apim\_ip>:<port>/manage/jagg/jaggery\_acs.jag

*E.g.:*

[https://localhost:9443/manage/jagg/jaggery\_acs.jag](https://localhost:9443/store/jagg/jaggery_acs.jag)

Select the following options:

* Use fully qualified username in the NameID
* Enable Response Signing
* Enable Assertion Signing
* Enable Single Logout
* Enable Audience Restriction

- Add “WSO2BPS” as an audience.

***API\_SANDBOX\_SP:***

Service Provider Name: API\_SANDBOX\_SP

Issuer: API\_SANDBOX

Assertions Consumer URL:

*Syntax:*

https://<apim\_ip>:<port>/sandbox/jagg/jaggery\_acs.jag

*E.g.:*

[https://localhost:9443/sandbox/jagg/jaggery\_acs.jag](https://localhost:9443/store/jagg/jaggery_acs.jag)

Select the following options:

* Use fully qualified username in the NameID
* Enable Response Signing
* Enable Assertion Signing
* Enable Single Logout

***WSO2AM\_SP:***

Service Provider Name: WSO2AM\_SP

Issuer: WSO2AM

Assertions Consumer URL:

*Syntax:*

https://<apim\_ip>:<port>/acs

*E.g.:*

https://localhost:9443/acs

Select the following options:

* Use fully qualified username in the NameID
* Enable Response Signing
* Enable Assertion Signing
* Enable Single Logout

***WSO2IS\_SP:***

Service Provider Name: WSO2IS\_SP

Issuer: WSO2IS

Assertions Consumer URL:

*Syntax:*

https://<is\_ip>:<port>/acs

*E.g.:*

https://localhost:9444/acs

Select the following options:

* Use fully qualified username in the NameID
* Enable Response Signing
* Enable Assertion Signing
* Enable Single Logout

***WSO2BPS\_SP:***

Service Provider Name: WSO2BPS\_SP

Issuer: WSO2BPS

Assertions Consumer URL:

*Syntax:*

https://<bps\_ip>:<port>/acs

*E.g.:*

https://localhost:9445/acs

Select the following options:

* Use fully qualified username in the NameID
* Enable Response Signing
* Enable Assertion Signing
* Enable Single Logout

***WSO2BAM\_SP:***

Service Provider Name: WSO2BAM\_SP

Issuer: WSO2BAM

Assertions Consumer URL:

*Syntax:*

https://<bam\_ip>:<port>/acs

*E.g.:*

https://localhost:9446/acs

Select the following options:

* Use fully qualified username in the NameID
* Enable Response Signing
* Enable Assertion Signing
* Enable Single Logout