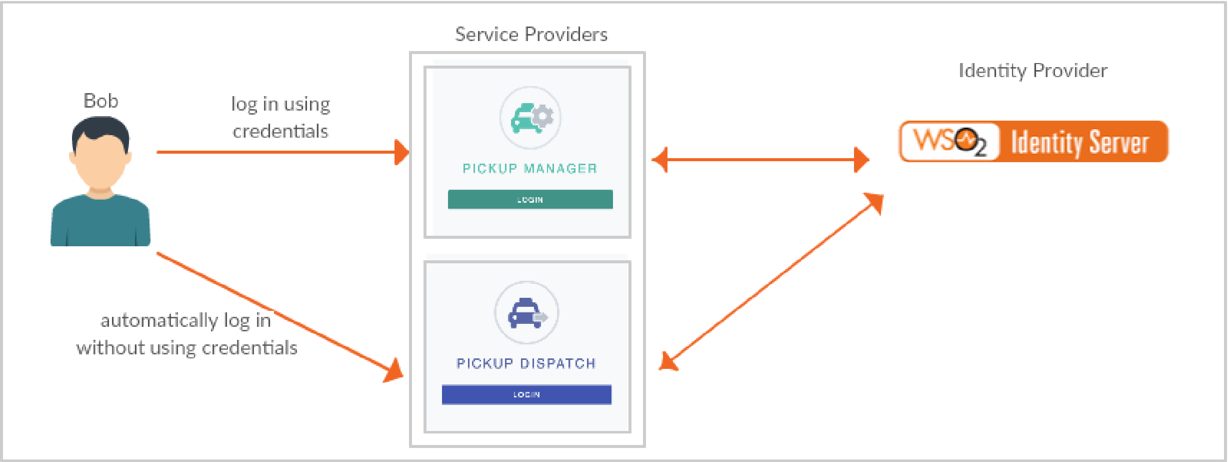
Single Sign On (SSO) - SAML

Introduction:

This tutorial will allow you to have hands-on experience on how to configure SSO with WSO2 Identity Server using SAML protocol.

To demonstrate the scenario in this tutorial, we are going to use two sample web applications called **pickup-dispatch** and **pickup-manager**. Both will be using **WSO2 IS** as the identity provider. When both these applications are configured for SSO at WSO2 IS, a user is only required to provide his credentials to a first application and he will be automatically logged in to the second application.

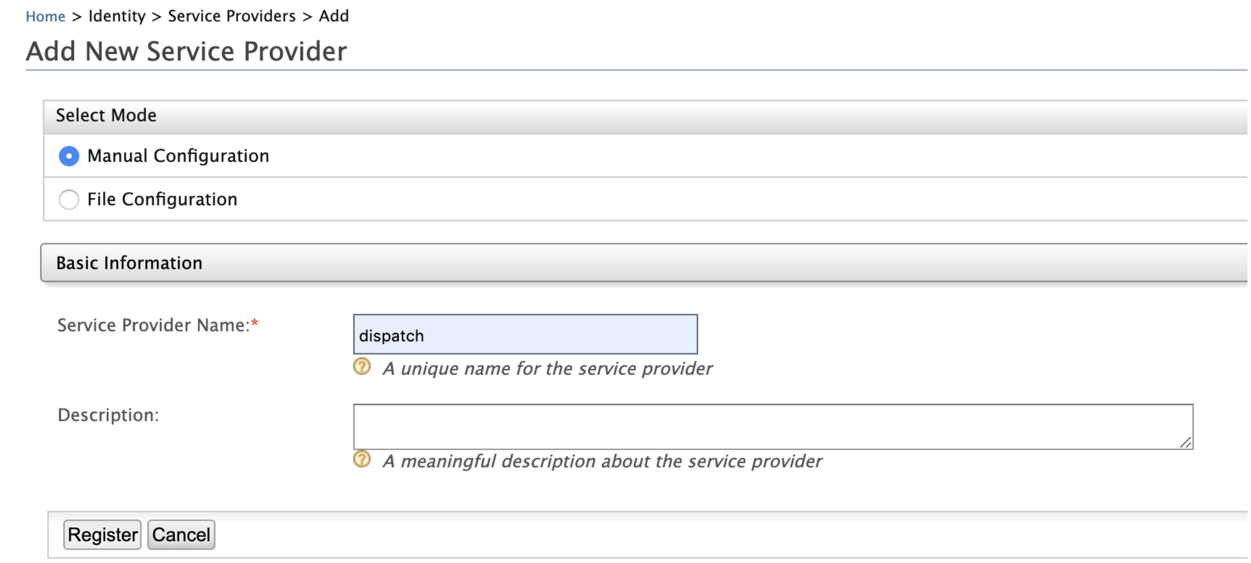


Setting up:

1. Download a tomcat server above tomcat8, run the server on port 8080
2. Download the saml2-web-app-pickup-dispatch.war and saml2-web-app-pickup-manager.war from here and deploy them in tomcat.

Configure web application pickup-dispatch and pickup-manager as Service Providers

1. Sign in to the WSO2 Identity Server Management Console at https://<Server Host>:9443/carbon using your username and password (e.g. admin:admin).
2. Navigate to the **Service Provider** section under **Main > Identity** menu-item and Click **Add**.
3. Type the name “dispatch” and register the Service Provider.

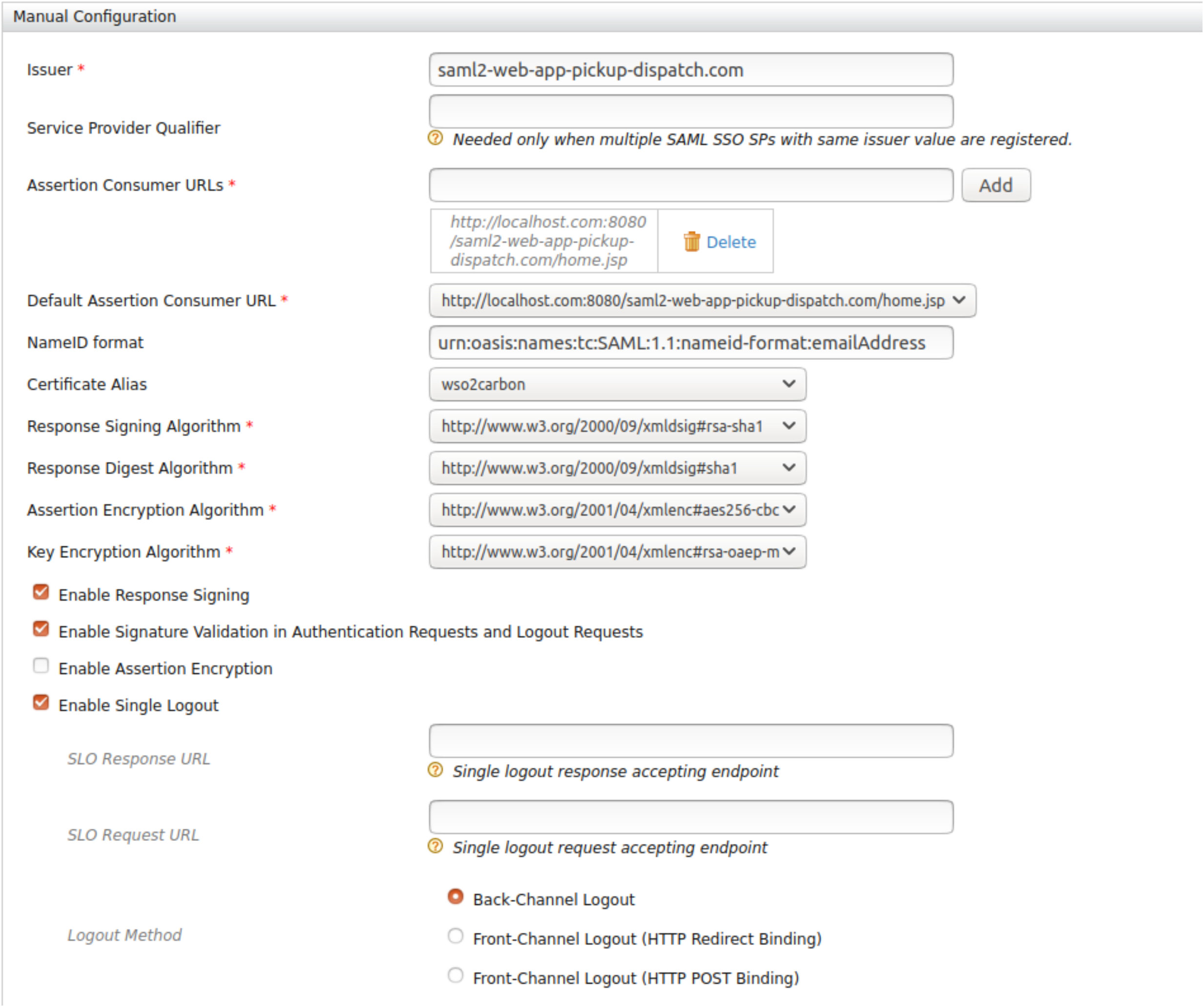


● Manual Configuration
○ File Configuration

Service Provider Name:* dispatch
A unique name for the service provider

Description:
A meaningful description about the service provider

4. Next, go to **SAML2 Web SSO Configuration** in the **Inbound Authentication Configuration**
5. Update the configuration as below by giving **issuer** as **saml2-web-app-pickup-dispatch.com** the **Assertion Consumer URL** as “http://localhost.com:8080/saml2-web-app-pickup-dispatch.com/home.jsp” and click add.
6. Enable **Response Signing** and **Signature validation in authentication and logout requests.**



Manual Configuration

Issuer *	saml2-web-app-pickup-dispatch.com
Service Provider Qualifier	Needed only when multiple SAML SSO SPs with same issuer value are registered.
Assertion Consumer URLs *	http://localhost.com:8080/saml2-web-app-pickup-dispatch.com/home.jsp
Default Assertion Consumer URL *	http://localhost.com:8080/saml2-web-app-pickup-dispatch.com/home.jsp
NameID format	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
Certificate Alias	wso2carbon
Response Signing Algorithm *	http://www.w3.org/2000/09/xmldsig#rsa-sha1
Response Digest Algorithm *	http://www.w3.org/2000/09/xmldsig#sha1
Assertion Encryption Algorithm *	http://www.w3.org/2001/04/xmlenc#aes256-cbc
Key Encryption Algorithm *	http://www.w3.org/2001/04/xmlenc#rsa-oaep-m

☑ Enable Response Signing

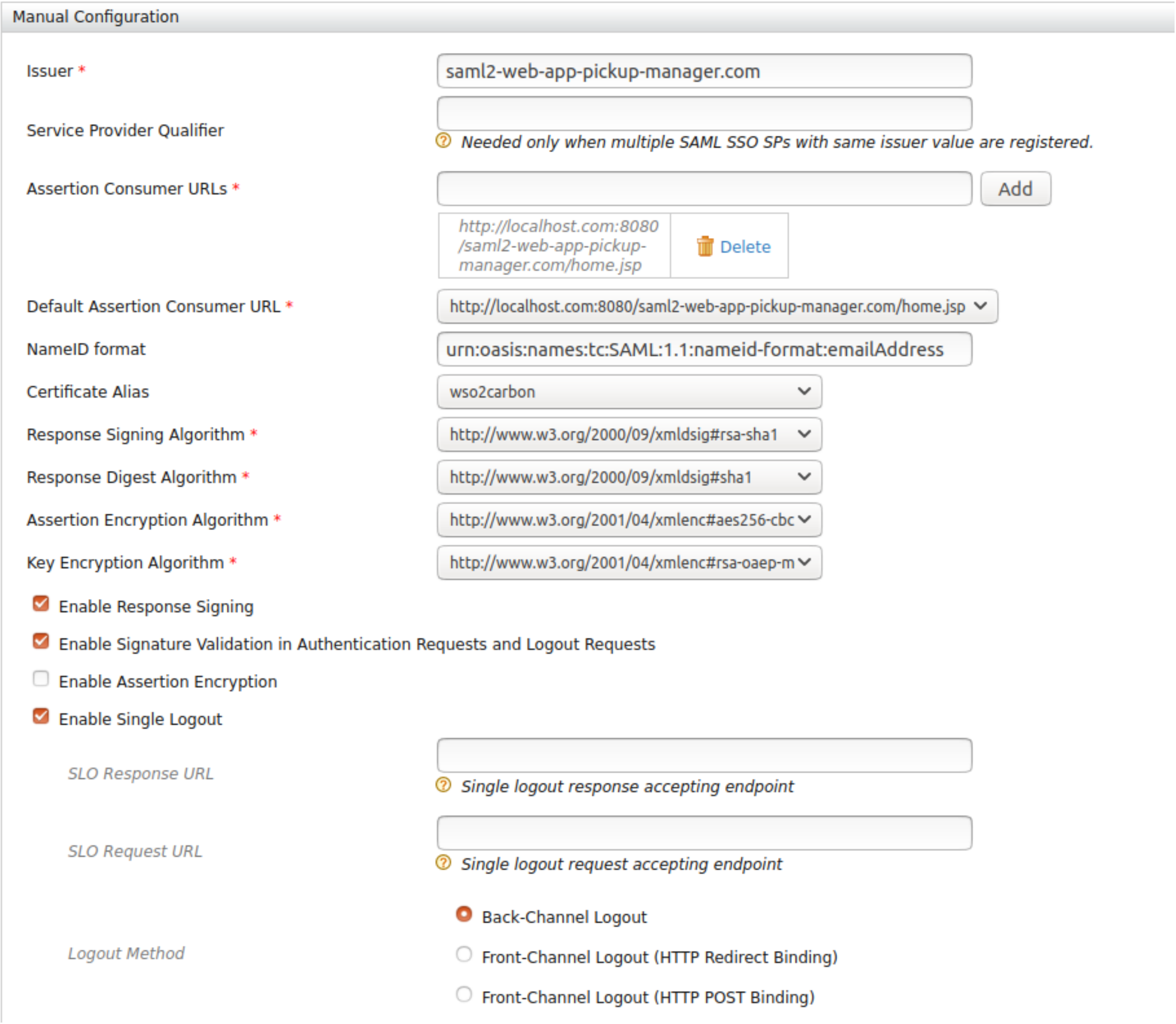
☑ Enable Signature Validation in Authentication Requests and Logout Requests

☐ Enable Assertion Encryption

☑ Enable Single Logout

SLO Response URL	Single logout response accepting endpoint
SLO Request URL	Single logout request accepting endpoint
Logout Method	● Back-Channel Logout ○ Front-Channel Logout (HTTP Redirect Binding) ○ Front-Channel Logout (HTTP POST Binding)

7. Click on update to save service provider configurations.
8. Next, repeat the same steps 3,4 to create a new service provider for pickup-manager application. For this service provider, the name should be registered as "manager", **issuer** should be **saml2-web-app-pickup-manager.com** and **Assertion Consumer URL** should be "http://localhost.com:8080/saml2-web-app-pickup-manager.com/home.jsp"
9. Enable **Response Signing** and **Signature validation in authentication and logout requests.**



Manual Configuration

Issuer *	saml2-web-app-pickup-manager.com
Service Provider Qualifier	 Needed only when multiple SAML SSO SPs with same issuer value are registered.
Assertion Consumer URLs *	Add *http://localhost.com:8080/saml2-web-app-pickup-manager.com/home.jsp* Delete
Default Assertion Consumer URL *	http://localhost.com:8080/saml2-web-app-pickup-manager.com/home.jsp
NameID format	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
Certificate Alias	wso2carbon
Response Signing Algorithm *	http://www.w3.org/2000/09/xmldsig#rsa-sha1
Response Digest Algorithm *	http://www.w3.org/2000/09/xmldsig#sha1
Assertion Encryption Algorithm *	http://www.w3.org/2001/04/xmlenc#aes256-cbc
Key Encryption Algorithm *	http://www.w3.org/2001/04/xmlenc#rsa-oaep-m

☑ Enable Response Signing

☑ Enable Signature Validation in Authentication Requests and Logout Requests

□ Enable Assertion Encryption

☑ Enable Single Logout

SLO Response URL	 *Single logout response accepting endpoint*
SLO Request URL	 *Single logout request accepting endpoint*
Logout Method	● Back-Channel Logout ○ Front-Channel Logout (HTTP Redirect Binding) ○ Front-Channel Logout (HTTP POST Binding)

10. Click update.
11. Now you are ready to try out the sample with SAML SSO.

Navigate to the deployment.toml file in the <IS_HOME>/repository/conf directory.Make sure the following CORS Configurations are in place.

```
[cors]
allow_generic_http_requests = true
allow_any_origin = true
allow_subdomains = true
supported_methods = [
"GET",
"POST",
"HEAD",
"OPTIONS"
]
support_any_header = true
supported_headers = []
exposed_headers = []
supports_credentials = true
max_age = 3600
tag_requests = false
```

Restart the WSO2 Identity Server.

Try It:

1. Go to http://localhost.com:8080/saml2-web-app-pickup-dispatch.com and click on the login button.
2. You will be redirected to the login page of the WSO2 Identity Server. Log in using your Identity Server credentials. You will be redirected to saml2-web-app-pickup-dispatch.com application home page.
3. Now if you go to http://localhost.com:8080/saml2-web-app-pickup-manager.com, you can see that the user has automatically logged in to this application.