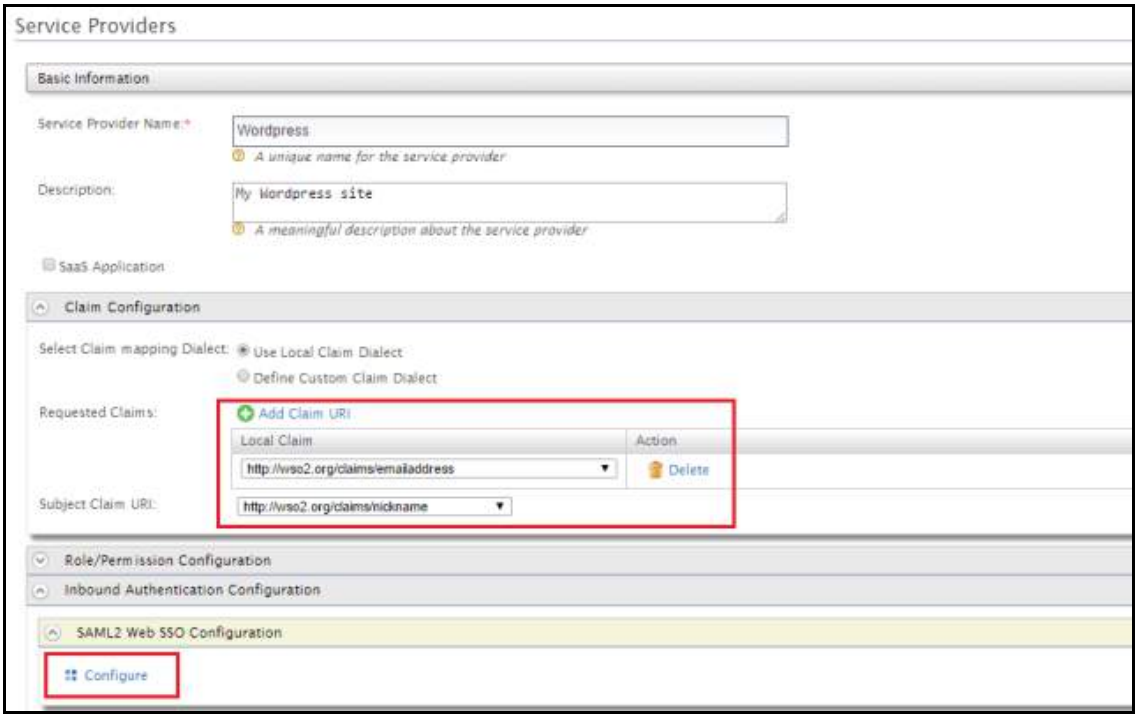
SETUP GUIDE WSO2 AS IdP

STEP 1:

- Login to your WSO2 admin console.
- Select **Add** under **Service Provider** tab.
- Enter the Service Provider Name. Eg. WordPress
- Click on **Register.**
- Under Basic Information**,** check **SaaS Application.**
- Under Claim Configuration, select **Use Local Claim Dialect.**
- For Requested Claims, add **http://wso2.org/claims/emailaddress** claim URI.
- Set Subject Claim URI to **http://wso2.org/claims/nickname**
- Under **Inbound Authentication Configuration** > **SAML2 Web SSO Configuration**, click **Configure**.

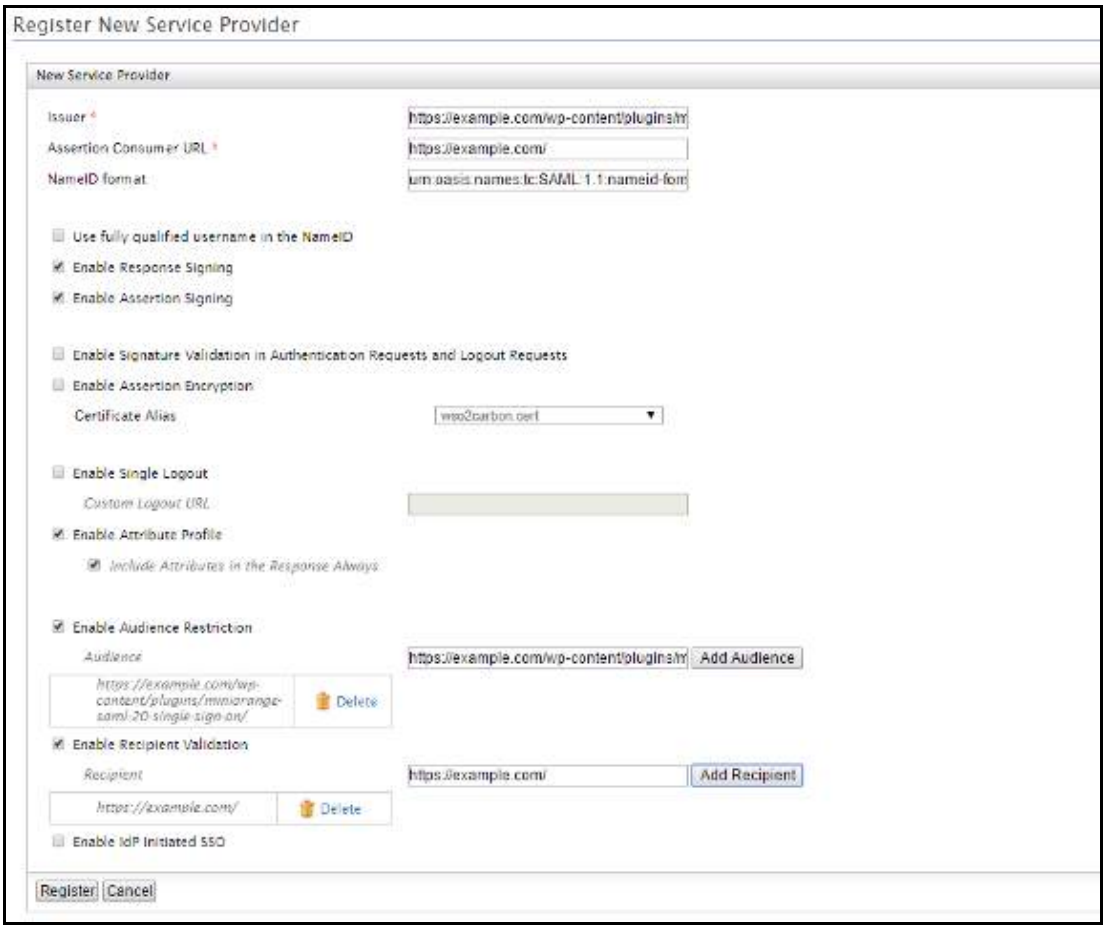


- Enter **Issuer** as **SP-EntityID** value provided in the Step 1 of the plugin under Identity Provider tab. Eg. *https://example.com/wp-content/plugins/miniorange-saml-20-single-sign-on/*

- Enter **Assertion Consumer URL** as provided in the Step 1 of the plugin under Identity Provider tab. Eg. *https://example.com/*

- Check **Enable Response Signing**
- Check **Enable Assertion Signing**
- Check the **Enable Attribute Profile** and **Include Attributes in the Response Always.**
- Check the **Enable Audience Restriction.** Enter the Audience URL value, provided in the Step 1 of the plugin under Identity Provider tab, in the textbox and click **Add Audience.** Eg. *https://example.com/wp-content/plugins/miniorange-saml-20-single-sign-on/*

- Check the **Enable Recipient Validation.** Enter the Audience URL value, provided in the Step 1 of the plugin under Identity Provider tab, in the textbox and click **Add Recipient.** Eg. *https://example.com/*
- Click on **Register** to save the configuration.



- Click on **Update** on Service Providers to save the configuration.
- Select **List** under **Identity Providers** tab from the menu.
- Click on **Resident Identity Provider** link.

- Enter Home Realm Identifier value that you want (usually your WSO2 server address). Eg. *https://wso2.example.com*
- Click on **Update.**

STEP 2:

- Go to **Service provider** Tab in **miniOrange SAML Plugin** and enter the following details:

Identity Provider Name	WSO2
SAML Login URL	https://<YOUR_WSO2_DOMAIN>/samlsso

IdP Entity ID or Issuer	The **Home Realm Identifier** value that you updated in the previous step.
X.509 Certificate*	Provide the certificate from the Keystore that you have configured in your WSO2.
Response Signed	Checked
Assertion Signed	Unchecked

* By default WSO2 is shipped with the following certificate:

```
-----BEGIN CERTIFICATE-----
MIICNTCCAZ6gAwIBAgIES343gjANBgkqhkiG9w0BAQUFADBVMQswCQYDVQQGEwJV
UzELMAkGA1UECAwCQ0ExFjAUBgNVBAcMDU1vdW50YWluIFZpZXcxDTALBgNVBAoM
BFdTTzIxEjAQBgNVBAMMCWxvY2FsaG9zdDAeFw0xMDAyMTkwNzAyMjZaFw0zNTAy
MTMwNzAyMjZaMFUxCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJDQTEWMBQGA1UEBwwN
TW91bnRhaW4gVmlldzENMAsGA1UECgwEV1NPMjESMBAGA1UEAwwJbG9jYWxob3N0
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCUp/oV1vWc8/TkQSiAvTousMzO
M4asB2iltr2QKozni5aVFu818MpOLZIr8LMnTzWllJvvaA5RAAdpbECb+48FjbBe
0hseUdN5HpwvnH/DW8ZccGvk53I6Orq7hLCv1ZHtuOCokghz/ATrhyPq+QktMfXn
RS4HrKGJTzxaCcU7OQIDAQABoxIwEDAOBgNVHQ8BAf8EBAMCBPAwDQYJKoZIhvcN
AQEFBQADgYEAW5wPR7cr1LAdq+IrR44iQlRG5ITCZXY9hI0PygLP2rHANh+PYfTm
xbuOnykNGyhM6FjFLbW2uZHQTY1jMrPprjOrmyK5sjJRO4d1DeGHT/YnIjs9JogR
Kv4XHECwLtIVdAbIdWHEtVZJyMSktcyysFcvuhPQK8Qc/E/Wq8uHSCo=
-----END CERTIFICATE-----
```

If you have changed the Keystore for your server then you can use these links to get the X.509 Signing certificate:

http://soasecurity.org/2013/12/24/how-to-saml-generating-saml-metadata-for-saml2-sso-idp/

http://soasecurity.org/2013/11/30/how-to-certificate-retrieve-x509-certificate-as-data/