

### STEP 1:

- Login to your WSO2 admin console.
- Select **Add** under **Service Provider** tab.
- Enter the Service Provider Name. Eg. Confluence
- 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**.

The screenshot shows the 'Service Providers' management interface in the WSO2 Admin Console. The 'Basic Information' section is expanded, showing the 'Service Provider Name' as 'Confluence' and the 'SaaS Application' checkbox checked. The 'Claim Configuration' section is also expanded, showing the 'Select Claim mapping Dialect' set to 'Use Local Claim Dialect'. Under 'Requested Claims', a table lists a claim with URI 'http://wso2.org/claims/emailaddress' and a 'Delete' button. The 'Subject Claim URI' is set to 'http://wso2.org/claims/nickname'. At the bottom, the 'SAML2 Web SSO Configuration' section is expanded, showing a 'Configure' button highlighted with a red box.

- Enter **Issuer** as **SP-Entity ID** value provided in the Step 1 of the plugin under Configure IDP tab. Eg. <https://wso2.example.com/plugins/>
- Enter **Assertion Consumer URL** as provided in the Step 1 of the plugin under Configure IDP tab. Eg. <https://wso2.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 Configure IDP tab, in the textbox and click **Add Audience**. Eg. <https://wso2.example.com>

- Check the **Enable Recipient Validation**. Enter the Audience URL value, provided in the Step 1 of the plugin under Configure IDP tab, in the textbox and click **Add Recipient**. Eg. <https://wso2.example.com/>
- Click on **Register** to save the configuration.

Register New Service Provider

New Service Provider

Issuer

Assertion Consumer URL

NameID format

☐ Use fully qualified username in the NameID

☒ Enable Response Signing

☒ Enable Assertion Signing

☐ Enable Signature Validation in Authentication Requests and Logout Requests

☐ Enable Assertion Encryption

Certificate Alias

☐ Enable Single Logout

Custom Logout URL

☒ Enable Attribute Profile

☒ Include Attributes in the Response Always

☒ Enable Audience Restriction

Audience

☒ Enable Recipient Validation

Recipient

☐ Enable IdP Initiated SSO

- Click on **Update** on Service Providers to save the configuration.
- Select **List** under **Identity Provider** 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 **Configure SP** Tab in **miniOrange SAML Plugin** and enter the following details:

IDP Entity ID	The <b>Home Realm Identifier</b> value that you updated in the previous step.
Single Sign On URL	https://<YOUR_WSO2_DOMAIN>/samlso
Single Logout URL	<b>gout URL</b> from Identity Provider Info in your wso2 SAML APP.
X.509 Certificate*	Provide the certificate from the Keystore that you have configured in your WSO2.

\* By default WSO2 is shipped with the following certificate:

```
-----BEGIN CERTIFICATE-----
MIICNTCCAZ6gAwIBAgIES343gjANBgkqhkiG9w0BAQUFADBVMQswCQYDVQQGEwJV
UzELMAkGA1UECAwCQ0ExFjAUBgNVBACMDU1vdW50YWluIFZpZxcxDTALBgNVBAoM
BFdTTzIxZjAQBgNVBAMMCWxvY2FsaG9zdDAeFw0xMDAyMTkwNzAyMjZaFw0zNTAy
MTMwNzAyMjZaMFUxCzAJBgNVBAYTA1VTMQswCQYDVQQIDAJDQTEWMBQGA1UEBwwN
TW91bnRhaW4gVm1ldzENMAsGA1UECgwEV1NPMjESMBAGA1UEAwwJbG9jYWxob3N0
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCUp/oV1vWc8/TkQSiAvTousMzO
M4asB2iltr2QKozni5aVFu818MpOLZIr8LMnTzW1lJvvaA5RAAdpbECb+48FjbBe
0hseUdN5HpwnH/DW8ZccGvk53I6Orq7hLCv1ZHtuOCokghz/ATrhyPq+QktMfXn
RS4HrKGJTzxaCcU7OQIDAQABoxIwEDAObgNVHQ8BAf8EBAMCBPAwDQYJKoZIhvcN
AQEFBQADgYEAW5wPR7cr1LAdq+IrR44iQ1RG5ITCZXY9hI0PygLP2rHANh+PYfTm
xbuOnykNGyhM6FjFLbW2uZHQTyljMrPprjOrmyK5sjJRO4d1DeGHT/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/>

## STEP 3:

In miniOrange SAML plugin, go to **Attribute Mapping** tab. Enter the following values:

- Username:** Name of the username attribute from IDP (Keep NameID by default)
- Email:** Name of the email attribute from IDP (Keep NameID by default)
- FirstName:** Name of the firstname attribute from IDP
- LastName:** Name of the lastname attribute from IDP

[Account](#)[Configure IDP](#)[Configure SP](#)[Attribute Mapping](#)[Role Mapping](#)[Sign In Settings](#)[Certificates](#)[Support](#)

## Attribute Mapping

Username: \*

Enter the Attribute Name that contains Confluence Username. Use *NameID* if Username is in Subject element.

Email: \*

Enter the Attribute Name that contains Email. Use *NameID* if Email is in Subject element.

Full Name Attribute:

Enter the Attribute Name that contains Full Name.

Separate Name  
Attributes:☐

(Select this if your IDP is sending First name and Last name as separate attributes.)

First Name:

Enter the Attribute Name that contains First Name.

Last Name:

Enter the Attribute Name that contains Last Name.

### **STEP 4:**

Go to **Role Mapping** tab. Enter the following values:

- **Role Mapping:** Name of the Role attribute from IDP

You can check the **Test Configuration Results** to get a better idea as to which values to map here.

Under the Role Mapping Section configure which GROUP value coming in the SAML response needs to be mapped to which role. The Group value coming in the SAML response will be mapped to the Role assigned here and the user will be assigned that role.

## Role Mapping

Role Attribute:

Enter the Attribute Name that contains Roles of the User.

Create Users: ☐ If checked, Users will be created only if roles are mapped.

Default Group:

Select Default Group to assign to new Users.

confluence-administrators:

confluence-users:

**Note:** Enter semi-colon separated list of role values in the textbox.

Save

## STEP 5:

Go to **Sign In Settings** tab. Enable auto-redirect to IDP using **Disable Confluence login** option.

## Sign In Settings

Login Button Text:

Disable Confluence login: ☒

Enable backdoor: ☒ Use `http://localhost:8091/login.action?saml_sso=false`  
For administrative tasks use `http://localhost:8091/authenticate.action?saml_sso=false`

Save