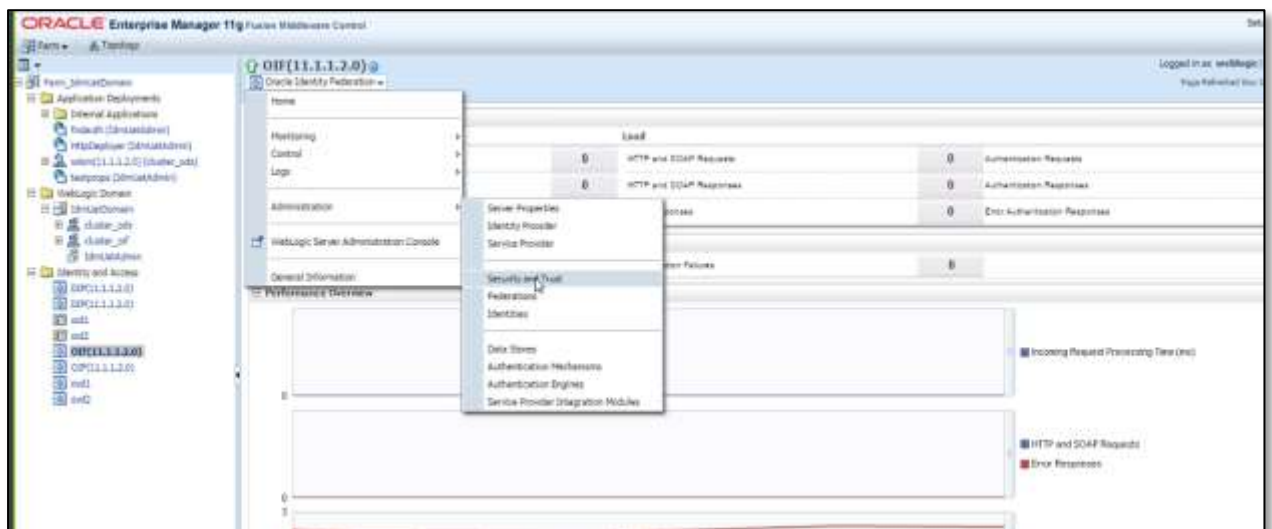


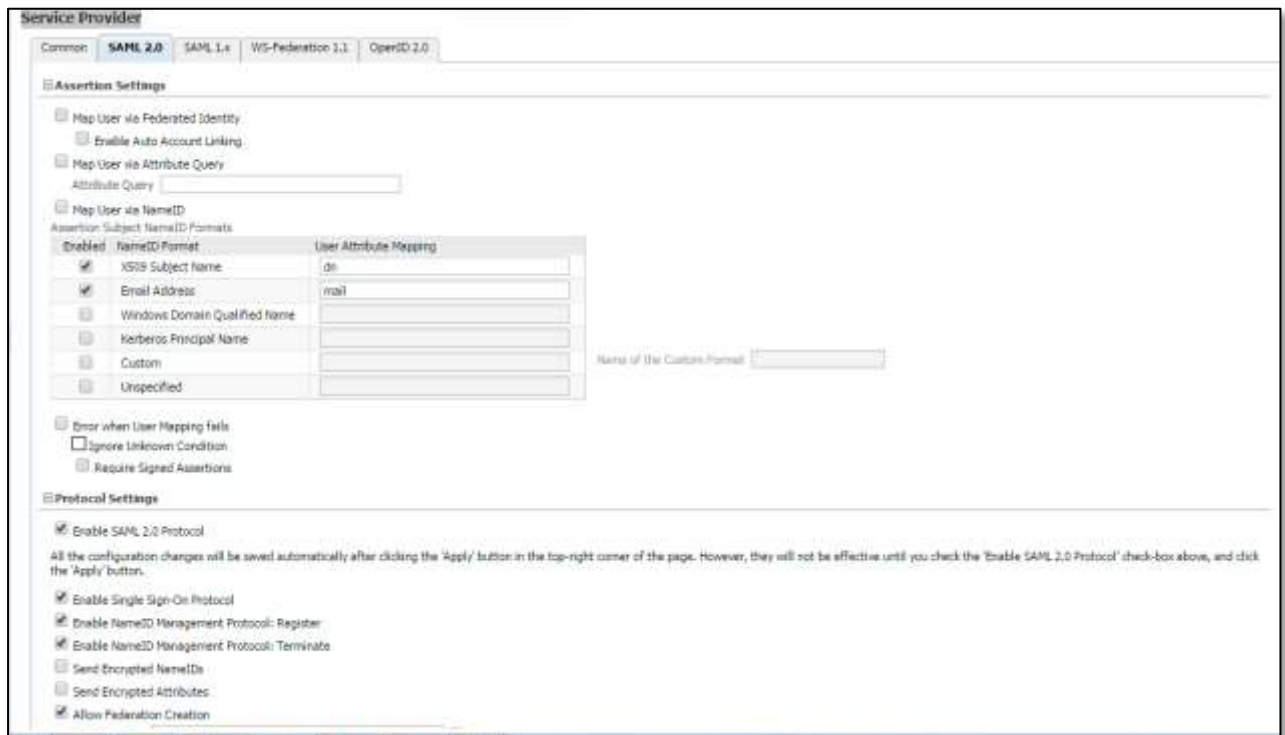
Setup Guide for Oracle As Idp

STEP 1: Configure Confluence site as SAML Service Provider in Oracle Enterprise Manager

- Login to your Oracle Enterprise Manager (OEM) Console. From Side Menu Go to Identity and Access -> Oracle Identity Federation (OIF).
- Now Select the Oracle Identity Federation dropdown from top. Go to Administration -> Service Provider.



- In Service Provider Section, Select SAML 2.0 Tab.



1. Check Map User via NameID.
2. Under Protocol Settings, check Enable SAML 2.0 Protocol

The screenshot shows the 'Protocol Settings' tab for SAML 2.0. The 'Enable Protocol Bindings' dropdown is set to 'All'. The 'Default Binding' is 'HTTP Redirect'. The 'Default SSO Request Binding' is 'HTTP Redirect'. The 'Default SSO Response Binding' is 'HTTP POST'. The 'Default Authentication Request NameID Format' is 'Email Address'. The 'Request Authentication Context Mechanism' is 'None'. The 'Request Authentication Context Comparison' is 'None'.

Message	Send Signed	Require Signed
Request - SOAP	<input type="checkbox"/>	<input type="checkbox"/>
Response - HTTP Redirect	<input type="checkbox"/>	<input type="checkbox"/>
Response - HTTP POST	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Response - SOAP	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Request - HTTP POST	<input type="checkbox"/>	<input type="checkbox"/>
Response with Assertion - SOAP	n/a	<input type="checkbox"/>
Request - HTTP Redirect	<input type="checkbox"/>	<input type="checkbox"/>
Response with Assertion - HTTP POST	n/a	<input type="checkbox"/>
AuthnRequest	<input type="checkbox"/>	n/a

STEP 2: Download IDP Metadata from Oracle Enterprise Manager –

- Again Select the Oracle Identity Federation dropdown from top. Go to Administration - >Security and Trust.
- Select Provider Metadata Tab.

The screenshot shows the 'Security and Trust' page in Oracle Enterprise Manager 11g. The 'Provider Metadata' tab is selected. The 'Metadata Settings' section has 'Require Signed Metadata' and 'Sign Metadata' checked. The 'Validity Period (hours)' is set to 24. The 'Generate Metadata' section has a 'Generate' button. The 'Provider Type' is set to 'Service Provider' and the 'Protocol' is set to 'SAML 2.0'.



- Select **Identity Provider** in Provider Type dropdown and click generate button to download Idp metadata.

STEP 3: Go to Configure SP tab in miniOrange SAML plugin. Then enter the following details:

IDP Entity ID	https://<your domain>/fed/idp
Single Sign On URL	https://<your domain>/fed/idp/initiatesso?providerid=<sp_entity_id>
Single Logout URL	Identity Provider Logout URL from Identity Provider Info in your Centrify SAML APP.
X.509 Certificate	The public key certificate of your IdP

STEP 4: 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 5:

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.

Account	Configure IDP	Configure SP	Attribute Mapping	Role Mapping	Sign In Settings	Certificates	Support
---------	---------------	--------------	-------------------	--------------	------------------	--------------	---------

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 6:

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

Account	Configure IDP	Configure SP	Attribute Mapping	Role Mapping	Sign In Settings	Certificates	Support
---------	---------------	--------------	-------------------	--------------	------------------	--------------	---------

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