



SETUP GUIDE FOR SHIBBOLETH AS IdP

STEP 1:

- In **conf/idp.properties**, uncomment and set 'idp.encryption.optional' to true.Eg.

```
idp.encryption.optional = true
```

- In **conf/metadata-providers.xml**, configure Confluence as an SP like this

```
<MetadataProvider id="Confluence"
xsi:type="FileBackedHTTPMetadataProvider"
backingFile="%{idp.home}/metadata/wp-metadata.xml"
metadataURL="http://<YOUR_WP_DOMAIN>/ plugins/servlet/saml/metadata
```

- In **conf/saml-nameid.properties**, uncomment and set default NameID as EmailAddress like this

```
idp.nameid.saml2.default=urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
```

- In **conf/saml-nameid.xml**, search for *shibboleth.SAML2NameIDGenerators*.
Uncomment the *shibboleth.SAML2AttributeSourcedGenerator* bean and comment all other ref beans.Eg.

```
<!-- SAML 2 NameID Generation -->
<util:list id="shibboleth.SAML2NameIDGenerators">
    <!--<ref bean="shibboleth.SAML2TransientGenerator" /> -->
    <!--<ref bean="shibboleth.SAML2PersistentGenerator" /> -->
    <bean parent="shibboleth.SAML2AttributeSourcedGenerator"
        p:format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
        p:attributeSourceIds="#{ {'email'} }" />
</util:list>
```

- Make sure you have defined Attribute Definition in **conf/attribute-resolver.xml**.Eg.

```
<!-- Note: AttributeDefinitionid must be same as what you provided in
attributeSourceIds in conf/saml-nameid.xml -->
<resolver:AttributeDefinitionxsi:type="ad:Simple" id="email" sourceAttributeID="mail">
    <resolver:Dependency ref="ldapConnector" />
    <resolver:AttributeEncoderxsi:type="enc:SAML2String" name="email"
        friendlyName="email" />
</resolver:AttributeDefinition>

<resolver:DataConnector id="ldapConnector" xsi:type="dc:LDAPDirectory"
    ldapURL="%{idp.authn.LDAP.ldapURL}"
    baseDN="%{idp.authn.LDAP.baseDN}"
    principal="%{idp.authn.LDAP.bindDN}"
```



```
principalCredential="%{idp.authn.LDAP.bindDNCredential}">
<dc:FilterTemplate>
<!-- Define you User Search Filter here -->
    <![CDATA[
        (&(objectclass=*)(cn=$requestContext.principalName))
    ]]>
</dc:FilterTemplate>
<dc:ReturnAttributes>*</dc:ReturnAttributes>
</resolver:DataConnector>
```

- Make sure you have AttributeFilterPolicy defined in **conf/attribute-filter.xml**. Eg.

```
<afp:AttributeFilterPolicy id="ldapAttributes">
    <afp:PolicyRequirementRule xsi:type="basic:ANY" />
    <afp:AttributeRule attributeID="email">
        <afp:PermitValueRule xsi:type="basic:ANY" />
    </afp:AttributeRule>
</afp:AttributeFilterPolicy>
```

- Restart the Shibboleth Server.

STEP 2:

- Go to **Configure SP** Tab in **miniOrange SAML Plugin** and enter the following details:

IDP Entity ID	https://<your_domain>/idp/shibboleth
Single Login URL	https://<your_domain>/idp/profile/SAML2/Redirect/SSO
Single Logout URL	https://<your_domain>/idp/profile/SAML2/Redirect/Logout
X.509 Certificate	The public key certificate of your IdP

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