



## SETUP GUIDE FOR SHIBBOLETH AS IdP

### STEP 1:

- In conf/relying-party.xml, configure Confluence as an SP like this

```
<MetadataProvider xsi:type="InlineMetadataProvider" xmlns="urn:mace:shibboleth:2.0:metadata"
id="MyInlineMetadata">
    <EntitiesDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
        <md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="<ENTITY_ID_FROM_PLUGIN>">
            <md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
                <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress</md:NameIDFormat>
                <md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="<ACS_URL_FROM_PLUGIN>"
index="1"/>
            </md:SPSSODescriptor>
        </md:EntityDescriptor>
    </EntitiesDescriptor>
</MetadataProvider>
```

- Make sure your Shibboleth server is sending **Email Address** of the user in **Name ID**. In attribute-resolver.xml, get the email attribute as Name ID:

```
<resolver:AttributeDefinition xsi:type="ad:Simple" id="email" sourceAttributeID="mail">
    <resolver:Dependency ref="ldapConnector" />
    <resolver:AttributeEncoder xsi:type="enc:SAML2StringNameID"
nameFormat="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"/>
</resolver:AttributeDefinition>
```

- In attribute-filter.xml, release the email attribute:

```
<afp:AttributeFilterPolicy id="releaseTransientIdToAnyone">
<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 Sign On URL	https://<your_domain>/idp/profile/SAML2/Redirect/SSO



Single Logout URL	Single Logout URL from identity provider info in your SAML APP
X.509 Certificate	The public key certificate of your Shibboleth server

### 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: \*

username

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

Email: \*

NameID

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.

Save

### 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