



SETUP GUIDE FOR SIMPLESAML AS IdP

STEP 1:

In **config/config.php**, make sure that **'enable.saml20-idp'** is **true**. Example:

```
'enable.saml20-idp' => true
```

STEP 2:

In **metadata/saml20-idp-hosted.php**, configure SimpleSAML as an Identity Provider like this:

```
$metadata['__DYNAMIC:1__'] = array(
    'host' => '__DEFAULT__',

    /*
    * X.509 key and certificate. Relative to the cert directory.
    */
    'privatekey' => '<YOUR_PRIVATE_KEY_FILE_NAME>', //eg.RSA_Private_Key.pem
    'certificate' => '<YOUR_PUBLIC_KEY_FILE_NAME>', //eg. RSA_Public_Key.cer

    /*
    * Authentication source to use. Configured in 'config/authsources.php'.
    */
    'auth' => '<YOUR_AUTH_SOURCE_NAME>',
);
```

STEP 3:

In **metadata/saml20-sp-remote.php**, register your Service Provider like this:

```
/* Replace example.com with your wordpress domain name. */
$metadata['https://example.com/wp-content/plugins/miniorange-saml-20-single-sign-on/']
= array(
    'AssertionConsumerService' => 'https://example.com/',
    'SingleLogoutService' => 'https://example.com/',
    'NameIDFormat' => 'urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress',
    'simplesaml.nameidattribute' => 'mail',
    'simplesaml.attributes' => true,
    'attributes' => array('mail', 'givenname', 'sn', 'memberOf'),
);
```

STEP 4:

Also in the miniOrange SAML plugin, configure your IDP as:

- **Single Sign On URL:** https://<YOUR_DOMAIN>/simplesaml/saml2/idp/SSOService.php
- **Single Logout URL:** https://<YOUR_DOMAIN>/simplesaml/saml2/idp/SingleLogoutService.php
- **IDP Entity ID:** https://<YOUR_DOMAIN>/simplesaml/saml2/idp/metadata.php
- **X.509 Certificate:** Your public key certificate that you configured in metadata/saml20-idp-hosted.php file.



STEP 5:

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

First Name:
Enter the Attribute Name that contains First Name.

Last Name:
Enter the Attribute Name that contains Last Name.

STEP 6:

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 7:

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