miniOrange

SETUP GUIDE 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 Servider 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:

- **SAML Login URL:**   https://<YOUR_DOMAIN>/simplesaml/saml2/idp/SSOService.php
- **SAML Logout URL:**   https://<YOUR_DOMAIN>/simplesaml/saml2/idp/SingleLogoutService.php
- **IdPEnittityID:**   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.
- **Response Signed:**   Checked
- **Assertion Signed:**   Checked