

simpleSAMLphp installation

Using these instructions, you should be able to install the simpleSAMLphp service provider into a specific directory on a web server running PHP 5.2 or newer.

Prerequisites: PHP 5.2>= with

- Hashing function
- zlib
- openssl
- SimpleXML
- XML DOM
- Regex support

Quick Installation

You can clone a version of simplesamlphp configured for Cornell Shibboleth (basically most of the work documented below is already done for you) [here](#). I can't promise that this will be kept up to date, but you should be able to drop it into /var/ on a RHEL/CentOS box, make a few edits and be on your way.

Full Installation

Follow the instructions for installing simpleSAMLphp:

- <http://simplesamlphp.org/docs/stable/>

Cornell Configuration

Configure for remote SP

Follow the directions for Service Provider QuickStart

- <http://simplesamlphp.org/docs/stable/simplesamlphp-sp>

Generating metadata

You'll need to populate saml20-idp-remote.php with the contents of [This Cornell specific info \(XML file\)](#). This can be done by going to the "Federation" tab, clicking the "XML to simpleSAMLphp metadata converter" link, and pasting the XML from the link above. Paste the contents of the generated file into \$INSTALLATION_DIR/metadata/saml20-idp-remote.php, making sure to add "<?php" and ">" to the beginning / end of the file.

Testing Configuration

Go to the "Authentication" tab and click on "Test configured authentication services" and "default-sp". If it is all working you should see output. You'll probably want to set the default-sp to avoid the intermediary screen: http://simplesamlphp.org/docs/stable/simplesamlphp-sp#section_3. For Cornell, change:

```
// The entity ID of the IdP this should SP should contact.
// Can be NULL/unset, in which case the user will be shown a list of available IdPs.
'idp' => NULL,
```

To:

```
// The entity ID of the IdP this should SP should contact.
// Can be NULL/unset, in which case the user will be shown a list of available IdPs.
'idp' => 'https://shibidp.cit.cornell.edu/idp/shibboleth',
```

Known Issues

Attribute mapping: By default, attributes map to the OID string and not something friendly like EduPersonName, etc. To use friendly attribute names, edit your <simplesaml_installdir>/config/config.php and change:

```
'authproc.sp' => array(
    /*
    10 => array(
        'class' => 'core:AttributeMap', 'removeurnprefix'
    ),
    */
```

To:

```
'authproc.sp' => array(  
  10 => array(  
    'class' => 'core:AttributeMap', 'oid2name'  
  ),  

```

See comments here for more context: <http://drupal.org/node/1931394>

Datastore: The simpleSAMLphp Drupal module requires using a datastore other than the default phpsession. Other options are memcache and SQL - below is a sample config for using sqlite3 on a *nix machine (using no username/password):

```

/*
 * Configure the datastore for simpleSAMLphp.
 *
 * - 'phpsession': Limited datastore, which uses the PHP session.
 * - 'memcache': Key-value datastore, based on memcache.
 * - 'sql': SQL datastore, using PDO.
 *
 * The default datastore is 'phpsession'.
 *
 * (This option replaces the old 'session.handler'-option.)
*/

'store.type' => 'sql',
/*
 * The DSN the sql datastore should connect to.
 *
 * See http://www.php.net/manual/en/pdo.drivers.php for the various
 * syntaxes.
*/
'store.sql.dsn' => 'sqlite:/tmp/saml.db',
/*
 * The username and password to use when connecting to the database.
*/
'store.sql.username' => NULL,
'store.sql.password' => NULL,
/*
 * The prefix we should use on our tables.
*/
'store.sql.prefix' => 'simpleSAMLphp',

```