

Shibboleth Apache Multiple Virtual Host Configuration (using Moodle as an example)

About

Below are steps to configure a shibboleth SP to work with multiple Apache virtual hosts using a single entityID and an Assertion Consumer Service (ACS) and shibboleth's `NativeSPApplicationOverride`. More information can be found here regarding [NativeSPApplicationOverride](#).

The notations are old, but it is backwards compatible with the current version of SAML. If you find documentation that supports the newer notation, please help and update this article.

You will need to do this if you are running more than one virtual named host and each virtual host is running it's own Moodle instance.

In this example, we will use the server names <http://www.moodle1.ucla.edu> and <http://www.moodle2.ucla.edu> with an entityID of <http://www.moodle1.ucla.edu>.

Note: You will need shibboleth installed and 2 instances of Moodle installed. You will also have needed to request attribute releases for the entityID and the ACS where <http://www.moodle1.ucla.edu> is the entityID and <http://www.moodle2.ucla.edu> is the ACS that is associated with the <http://www.moodle1.ucla.edu> entityID.

shibboleth2.xml file configuration

Below are the changes I needed to make in the default configuration file. All other settings were left as default from the shibboleth 2.1 installation.

Modifying the host name for the 2 virtual host web servers

```
<RequestMapper type="Native" >
```

```
<RequestMap applicationId="default" >
```

```
<Host name="www.moodle1.ucla.edu" >
```

```
<Path name="default" authType="shibboleth" requireSession="true" />
```

```
</Host>
```

```
<Host name="www.moodle2.ucla.edu" applicationId="moodle2" authType="shibboleth" requireSession="true" />
```

```
</RequestMap>
```

```
</RequestMapper>
```

Entering entityID

```
<ApplicationDefaults id="default" policyId="default"
```

```
entityID="http://www.moodle1.ucla.edu"
```

```
REMOTE_USER="Shib-eduPersonPrincipalName"
```

```
signing="false" encryption="false"
```

```
>
```

Point to Production AIS IdP

```
<SessionInitiator type="Chaining" Location="/Login" isDefault="true" id="default"
```

```
relayState="cookie" entityID="urn:mace:incommon:ucla.edu">
```

h3.Pulling the MetadataProvider ID Information

```
<MetadataProvider id="incommon" type="XML"
xmlns="urn:mace:shibboleth:2.0:metadata"
url="http://wayf.incommonfederation.org/InCommon/InCommon-metadata.xml"
backingFilePath="/etc/shibboleth/InCommon-metadata.xml"
reloadInterval="28800">
</MetadataProvider>
```

Setup the ApplicationOverride

```
<ApplicationOverride id="moodle2" entityID="http://www.moodle1.cdh.ucla.edu"/>
```

Save and close the file. Check the shibboleth configuration file for errors: shibd -t and restart the shibboleth service: service shibd restart

Apache Virtual Host Configuration

Note: The Moodle root for www.moodle1.ucla.edu is at /var/www/html/moodle1 and the Moodle root for www.moodle2.ucla.edu is at /var/www/html/moodle2.

At the bottom of the httpd.conf file there should be a Virtual Hosts section. You will need to uncomment and add the following lines in your httpd.conf file.

```
# Use name-based virtual hosting.
NameVirtualHost *:80
```

```
<VirtualHost *:80>
ServerAdmin webmaster@Tucla.edu
DocumentRoot /var/www/html/moodle1
ServerName www.moodle1.ucla.edu
```

This section allows for the use of .htaccess files to enable Shibboleth on directories

```
<Directory "/var/www/html/moodle1">
Options All
AllowOverride All
Order allow,deny
Allow from all
</Directory>
```

This section is required by Moodle to use Shibboleth authentication along with local authentication by only restricting the index.php file to shib auth.

```
<Directory /var/www/html/moodle1/auth/shibboleth/index.php>
AuthType shibboleth
ShibRequireSession On
require valid-user
```

```
</Directory>
</VirtualHost>
```

```
<VirtualHost *:80>
ServerAdmin webmaster@ucla.edu
DocumentRoot /var/www/html/moodle2
ServerName www.moodle2.ucla.edu
```

This section allows for the use of .htaccess files to enable Shibboleth on directories

```
<Directory "/var/www/html/moodle2">
Options All
AllowOverride All
Order allow,deny
Allow from all
</Directory>
```

This section is required by Moodle to use Shibboleth authentication along with local authentication by only restricting the index.php file to shib auth.

```
<Directory /var/www/html/moodle2/auth/shibboleth/index.php>
AuthType shibboleth
ShibRequireSession On
require valid-user
</Directory>
</VirtualHost>
```

Save and close the file and check the apache configuration: **httpd -t** Then restart apache. **sudo /sbin/service httpd restart**

Configure Moodle to use Shibboleth authentication and local login.

For this to work you need to have the require shibboleth directives only restricting the index.php file in the auth/shibboleth/ directory. You can then put a link to auth/shibboleth/index.php page in the login page and should be able to login with both local and shibboleth accounts.

#1. As Moodle admin, under Site Administrator, browse to Users → Authentication → Shibboleth.

#2. Fill in the fields of the form. The fields 'Username', 'First Name', 'Surname', etc. should contain the name of the environment variables of the Shibboleth attributes that you want to map onto the corresponding Moodle variable. For Shibboleth 2.1, these are set in the attribute-map.xml file.

#####

Shibboleth Attributes needed by Moodle:

For Moodle to work properly Shibboleth should at least provide the attribute

that is used as username in Moodle. It has to be unique for all Shibboleth
Be aware that Moodle converts the username to lowercase. So, the overall
behaviour of the username will be case-insensitive.

All attributes used for moodle must obey a certain length, otherwise Moodle
cuts off the ends. Consult the Moodle documentation for further information
on the maximum lengths for each field in the user profile.

#####

#3. Save the changes you made on the Shibboleth page.

#4. Browse to Users → Authentication → Manage Authentication to Enable and Disable Shibboleth
login. You can control the priority of the failthrough here if you would like as well.

#5. Save the changes.

CLE UCLAlogin.php page

If you are going to use CLE UCLAlogin.php page you will need to edit the httpswwwroot variable
and hard code the server name.

Example for www.moodle1.ucla.edu

Comment this line:

```
//$CFG->httpswwwroot = str_replace("http://", "https://", $CFG->httpswwwroot);
```

Enter this instead:

```
$CFG->httpswwwroot = "http://www.moodle1.ucla.edu";
```

Revision #13

Created Wed, Apr 14, 2010 10:50 PM by Lopez, Denise

Updated Fri, May 26, 2017 5:56 PM by Kong, Caroline