Shibboleth

- Why does Shibboleth sometimes return different names for students than class roster?
- Will Shibboleth say this is a UCLA person, so that we can limit some content to just UCLA?
- Shibboleth Apache Multiple Virtual Host Configuration (using Moodle as an example)
- Campus Resources for Registrar Data, ISIS, Shibboleth
- IAMUCLA Shibboleth Set-Up Guides
- Is it possible to set up a survey using Shibboleth logins?
- Shibboleth
- Can Shibboleth log all attributes retrieved?

Why does Shibboleth sometimes return different names for students than class roster?

The legacy UCLA Single Sign On solution ISIS, now replaced by Shibboleth, used to prioritize data in payroll record from QDB over student record from SRDB if a student works at UCLA and their payroll record shows a different name. After the Enterprise Directory (ED) rolled out in production in November 2006, ISIS (now Shibboleth) switched its backend to ED which pulls a person's name information based on a different logic. This ED name logic favors the name recorded in student system when different names are found in both student and payroll system for the same UID, if the person is a current student with UCLA. Therefore ISIS (now Shibboleth) no longer returns the name in payroll system as long as the person is a current student. The only case that payroll name is returned instead of student record name is that the person is a current UCLA employee but not a current UCLA student.

Exception: Students who have full-on FERPA restriction flag turned on in student system are not recognized in the Enterprise Directory because their information including names in student system are restricted for release. In such case, if they are UCLA employee at the same time, ED will recognize them as current UCLA employee but not current UCLA student, and thus return the names in payroll system.

Here's the current name resolution logic implemented in ED:

a. If a person currently has student affiliation (meaning UID exists in V610), select the name in the order below no matter what other affiliation this person has:

1. SR0 name

2. SI0 name
3. PP0 name
4. UNX name

Note: If the name selected is found with APP_USAGE_STATUS <> ‘A’, an error message will be logged but the name still goes in ED.

b. Else, if a person currently has employee affiliation (meaning UID in payroll system with a emp_status<> ‘S’ – ‘not seperated’), select the name in the order below:

1. PP0 name
2. SR0 name
3. SI0 name
4. UNX name

Note: If the name selected is found with APP_USAGE_STATUS <> ‘A’ an error message will be logged but the name still goes in ED.

c. Else, meaning a person does not have either student of employee affiliation, go with the same order of step a.

Will Shibboleth say this is a UCLA person, so that we can limit some content to just UCLA?

Shibboleth has a very flexible attribute release mechanism, and can in theory tell an application whether a person is a UCLA person.

However, the defintion of “UCLA person” varies depending on the cotext. You can find a list of attributes Shibboleth potentially offers at:

https://spaces.ais.ucla.edu/display/iamucla/AvailableShibAttributes

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 webmasterATucla.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 webmasterATucla.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.

CCLE UCLAlogin.php page

If you are going to use CCLE UCLAlogin.php page you will need to edit the htpswwwroot 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";
```

Campus Resources for Registrar Data, ISIS, Shibboleth

I am looking to develop an application and would like to have access to data such as class roster information, student info, etc. How can I obtain this data and who do I need to contact to get access to this data?

Campus Authentication using ISIS and Shibboleth

What kind of info can be retrieved using campus authentication?

That is yet to be decided but it’s worth discussing your needs with the personnel in charge of ISIS and Shibboleth.

What is ISIS?

Integrated Security Information Services (ISIS) is UCLA’s de facto common web authentication service. It provides a common interface for UCLA web applications to authenticate users using Bruin Online ID/password, UID/PIN, AIS mainframe logon ID password, or QDB logon ID/password. Furthermore, ISIS enables single user sign-on to participating campus web applications.

For general information regarding ISIS, please contact Albert Wu.

Why should I use ISIS?

Don’t think of it as using ISIS but instead as using the UCLA Login System. This allows your users

to login with their UCLA Login the way they do for My.UCLA, the Library and other applications, instead of having to have a special login just for your system.
https://kb.ucla.edu/link/32

Useful Links

- Getting Started with ISIS
  http://www.sscnet.ucla.edu/consortium/index.pl?GettingStartedWithIsis

What is Shibboleth?

Shibboleth is an Internet2 sponsored way for schools to federate their login systems for cross-campus courses. See https://kb.ucla.edu/link/298 for links to more info.

Should I start developing applications using ISIS or Shibboleth?

ISIS is proprietary to UCLA. Shibboleth is an Internet2 standard. Therefore, you have more future potential programming to Shibboleth. And if you are using an Open Source app it may already work with Shibboleth, and that can save you adapting it to UCLA's ISIS. Moodle and Plone, among others, have Shibboleth modules.

For additional info on ISIS and Shibboleth

http://mi6.ais.ucla.edu

Registrar Data – Accessing Student Data

I am looking to develop an application that would be able to access class roster information, student data, etc.

Registrar's Service Request

Provides consulting on data selection, business approaches, and support of Student Records data via a wide array of delivery methods. You can contact, Martin Bjel or Valerie Romero for more

details.

https://saweb.uclanet.ucla.edu/

Use the Registrar’s Service Request (RSR) application to request any of the following services:

- Mass e-mail to students
- Student addresses for bulk mailing
- SRS reports
- Access to student data from any source
- Access to Registrar’s Office web application

What is SRS number?

SRS stands for Student Record Systems and every UCLA course has a 9 digit SRS#. Combined with Term, this provides a unique key for every course offered.

To get the SRS number for a given course:

Go to the Schedule of Classes available at https://sa.ucla.edu/ro/public/soc/.

IAMUCLA Shibboleth Set-Up Guides

Please visit our official [IAMUCLA Shibboleth site]. Our site contains detailed information on shibboleth installation and configuration.

https://spaces.ais.ucla.edu/display/iamucla/Shibboleth

There you will find links to the following :

Shibboleth Planning Guide For Both Ver.1.3 & 2.x

Shibboleth 1.3 Installation and Configuration

Shibboleth 2.x Installation and Configuration Beta Guide

Available Shibboleth Attributes

Shibboleth KnowledgeBase

Is it possible to set up a survey using Shibboleth logins?

Q: Hi, our department is looking for a way to allow voting on various topics… is there a way set up so that we can do this using people's BOL logins? – *posted by David Schiller*

A: (or at least the start of one) Here are some options:

1. Contact the folks at MyUCLA because they have hosted many student elections, and presumably the same process could be used for surveys.
2. Moodle used http://ccle.ucla.edu and http://classes.sscnet.ucla.edu has a Questionnaire Tool and uses Shibboleth.
3. Set up simple voting app in a web scripting language running Shibboleth, or if you don't want to run it yourself, see if any of the many depts. programming with Shibboleth on campus could help. For UCLA Shibboleth docs, see IAMUCLA
4. Check if this fellow at Duke managed to get Shibboleth working with SurveyMonkey: Shibboleth conversations with BlogSpot or SurveyMonkey?

Shibboleth

“Shibboleth is the standard federated authentication and attribute query service protocol in the higher education. It was designed from the ground up to support the pseudo-anonymous login scenarios required by the libraries.

Shibboleth has strong support from the Internet2. It is also on a converging path with similar commercial efforts (Liberty Alliance)."

— Taken from EDIMIassumptions.doc found on AIS website

Shibboleth Resource

- Shibboleth Set Up Guide on the UCLA IAMUCLA site
- ISIS to Shibboleth Migration Help Center
- The Official Internet2 Shibboleth Site
- Internet2 Shibboleth Support

Deprecated Pages

- Shibboleth Target Deployment Guide for v1.2.1

Presentations Related to Shibboleth

- Slides from the January 30, 2007 ISIS/Shibboleth Technical Information Session
- Slides from the September 18, 2007 Campus Web Publishers presentation
- A very cool series of demos of how Shibboleth works
  Produced by SWITCH, this is probably the best set of online demonstration/explanation of how Shibboleth works

---

More information about Shibboleth and ISIS, taken from a post by Albert Wu to the ISISdev mailing list:

1. What is Shibboleth?
2. Why haven’t you rolled out Shibboleth to a broader group?

3. Which is better for me, ISIS or Shibboleth?

4. What about authorization? How will that be handled?

5. How might I use data returned from Shibboleth to perform authorization?

6. What does a user see when he/she logs into a Shibboleth enabled application? What will my Shibboleth-enabled application be able to see about that user?

1. What is Shibboleth?

-————————————-

Shibboleth (http://shibboleth.internet2.edu/) is standards-based, open source middleware software which provides Web Single SignOn (SSO) across or within organizational boundaries. It is open source and is developed and support by the Internet2 Middleware Group.

Shibboleht IS the next version of ISIS.

We have in the past two years, been preparing to evolve ISIS to a standards-based protocol. Shibboleth is the right fit. Shibboleth has been adopted by many institutions throughout the world as their web single sign-on service of choice. It has been adopted by UC as its federated Single Sign-on solution.

We are in fact operating a fully functioning Shibboleth Identity Provider (that would be the “server” side of the service) parallel to the curent ISIS 5 interface. The two are integrated. Applications can choose to use either API and get single sign-on across applications using either.

At this time, we are working with several early adopters on deploying Shibboleth. They include CCLE, Paul’s Plone site, MyEvents.ucla.edu, UCLA GRID, and our own sites.

2. Why haven’t you rolled out Shibboleth to a broader group?

-————————————————————————————————

There are several considerations.

First, we are ourselves learning how to deploy a Shibboleth-enabled

application. Since we didn't write the sofware, there is a fair amount of learning to do.

Second, Shibboleth does not offer the exact same set of features ISIS does. In particular, it has a different concept of session management. We need to better understand how that impacts the applicaitons.

Third, transitioning from the current ISIS API to Shibboleth will require a fair amount of work. We want to minimize that work as much as possible for you all. To do that, we are using the pilot program to develop a series of support materials and to try streamline the set up process as much as possible before we make everyone jump through unnecessary hoops.

The good news is that we are just about there. Stay tuned. :-)

3. What are the differences between ISIS and Shibboleth, and Which is better for me?

———————————————————————————————————————

These are the key differences between ISIS and Shibboleth:

- ISIS is a home grown system with a proprietary API. Shibboleth is developed based on SAML (http://en.wikipedia.org/wiki/SAML)
- ISIS is only used within UCLA. Shibboleth is used at a significant number of institutions. More significantly, Shibboleth enables member of one instution to use his/her credential to log in to services at another institution. Imagine using your UCLA Logon ID to log into a UCOP, or UC Berkeley application. It's happening. :-)

- To use ISIS, you need to write code to call the ISIS Web Serivce. Internet2 provides standard “client” (called Service Provider) modules for Apache and IIS. These SP modules handle all communications between your server and the Shibboleth Identity Provider. Any information returned is presented to your application in the HTTP headers. So all your application needs to be able to do is to read HTTP headers. On top of that, if you only have static pages, the Shibboleth SP modules have enough logic built-in that it can controll access to static documents by simply editing configuration files.

- ISIS can only provide a fixed set of user attributes. Shibboleth is designed to be able to flexible return any arbitrary number of attributes, AND be able to control the release of those attributes in a very granular fashion.

Which one is better? Generally speaking, if you are launching a new application, I’d seriously consider using Shibboleth. After all, eventually, we will phase the current ISIS API out in favor of Shibboleth. That won’t happen for a couple of years, but if your new application will be around for at least 2 years, now may be the time to move onto Shibboleth. We are still a couple of months away from fully ramped up to support a large number of adopters, but if you are interested and have an active project, we want to work with you.

Besides, while there is significant set up (at least for the first time), there is far less coding involved on your part. It may just shorten your deployment window.

Reason for not going to Shibboleth now:

a. You already have a set of working ISIS applications, and you have no immediate plans to launch new projects/rewrite your applications.

You have very specific session management requirements, and you can’t change those requirements in the short term. Shibboleth works differently. It may require some rethinking how session management is done

c. You want to wait till the full set of support material is available. :-)

4. What about authorization? How will that be handled?

-

————————————————————————————

At least for web applications, we expect authorization data will come through the Shibboleth attribute response packets. As a user logs into your application and runs through the shibboleth authentication sequence, the shibboleth SP module eventually fires attribute requests against the IdP. The IdP in turn returns any attribute the SP requests AND has the authorization to see.

The technical framework for this service is available now. Our main problem is the availability of data, and lining up proper support for managing the release of attributes. Keep in mind that AIS does not have the authority to arbitrarily release data. The business offices (e.g., Registrar's Office for student data, CHR/Payroll for employee data) need to be involved in the process.

Our main challenge now is to come up with a scalable mechanism for the offices to efficiently manage the release of sensitive data. That process is ongoing. We have a significant permission management system proposed in the UTIPP2 funding cycle. Whether we get the funding to proceed there will significantly determine the types of services we can offer moving forward.

5. How might I use data returned from Shibboleth to perform authorization?

————————————————————————————-

Shibboelth attributes returned to your application are presented as name/value pairs in the HTTP header. You simply read the headers and parse out the data you are looking for. Specifically for authorization data, they are returned in the form or affiliation values or entitlement values.

For example, if we had the proper data, we may assert me as:

eduPersonScopedAffiliation = affiliate@ucla.edu,employee@ucla.edu, staff@ucla.edu,alum@ucla.edu

Note that attributes can contain multiple values. Also note that the "@ucla.edu" part is the scope of the value. so "employee@ucla.edu" means "employee of UCLA".

As I mentioned in 4., whether we receive funding significantly impacts how much we expand this moving forward. In theory, we can assert any amount of details about a person that we have data for. In fact, paired with a permission management tool for the security administrators, we can assert any custom authorization attributes the administrators might set…

6. What does a user see when he/she logs into a Shibboleth enabled application? What will my Shibboleth-enabled application be able to see about that user?

-——-

The best way to explain this is for you to log in to a live Shibboleth-enabled application.

If you want to see what the application sees in the header, try this little diagnostic application:

https://whoa.mi.ais.ucla.edu

7. How can I contact AIS if Shibboleth appears to be problematic?

-——-

“AIS help desk does not check emails over the weekend. A different group answers the help desk phone during evenings and on weekends. They route calls to the appropriate party for production outage issues. The AIS help desk extension is x66951.” (Albert Wu 09/30/2007)

Can Shibboleth log all attributes retrieved?

Please answer this question and change the tags.

In debugging Moodle login problems it would be extremely helpfulv if we could log the attributes Shibboleth delivers for each person on login.

The reason this is useful is that some Extension Students have uclaLogonID but not uclaBOLEmail and may or may not have uclaOfficialEmail or uclaUniversityID. Finding this out would help in solving login problems.

Related KB entries:

- https://kb.ucla.edu/link/298
- https://kb.ucla.edu/link/834

Moodle does not have the code to do the actual logging, although it does not look hard to add the code ourselves. Basically it should use Moodle's add_to_log() function to write all "HTTP_SHIB_*" server variables to the log.

The Shibboleth Service Provider module also logs transactional details. You may consider looking into those logs:

https://spaces.internet2.edu/display/SHIB/LogFiles