Shibboleth Knowledge / Commonly Asked Questions from Application Administrators

Intended for application / system administrators on either apache-linux and windows-iis who are interested in working with the Shibboleth SP.

Original MI KB

Post a question, get an answer.

- Intended for application / system administrators on either apache-linux and windows-iis who are interested in working with the Shibboleth SP.
- Q: How do I get started?
- Q: I would like to know if Shibboleth for IIS will support ASP pages or just ASP.NET pages or both?
- Q: How do I get permission to use student data?
- Q: How do I test my newly installed SP in the Test Environment?
- Q: We are planning on getting a SSL certificate for our internal web server. Does it matter if the SSL certificate is standard or premium?
- Q: We are planning on getting a SSL certificate for our internal web server. Does it matter if the SSL certificate is standard or premium?
- Q: I thought I was logging into application X. What is this "UCLA Web Single Sign-On"?
- Q: What is a UCLA Logon ID?
- Q: I'm affiliated with another institution, how do I get back to its login page instead of UCLAs?
- Q: What browsers Are supported
- Q: Do I need to enable Javascript?
- Q: Do I need to accept browser cookies?
- Q: Why might my MacOS Safari continually loop when signing into Shibboleth?
- Q: Why does my logon id not work when i try to test against testshib?
- Q: I noticed that Shibboleth only support UCLA logon ID. Is there a plan in the near future to provide support for OASIS and QDB logons?
- Q: What do I need to know about setting up a Test Account with uclaAISMainframeID?

Q: How do I get started?

A: Visit the IAMUCLA Shibboleth Support Central

Fill out the application info and send it to us.

Q: I would like to know if Shibboleth for IIS will support ASP pages or just ASP.NET pages or both?

A: Shibboleth will work for either ASP or ASP.NET.

FYI, The Shibboleth module is an ISAPI filter. It converts information returned from the IDP (the "server" side of Shibboleth) into a bunch of HTTP headers. As long as you are using a scripting language that can read HTTP headers, Shib will work.

Q: How do I get permission to use student data?

A: If you need access to employee data, contact us for help. If you need access to student data, use this link http://www.registrar.ucla.edu/rsr/ to submit a request with the Registrar's office.

Q: How do I test my newly installed SP in the Test Environment?

A: Contact us for an existing test account.

Q: We are planning on getting a SSL certificate for our internal web server. Does it matter if the SSL certificate is standard or premium?
A: Where do you plan on using this - within Shibboleth or on the web server for browser traffic (https://)?

Within Shibboleth: If you are using SP 2.1 or above the cert generated at the time of installation works just fine. You can always use a commercial cert here too.

Web server: Either standard or premium will do. You just have to compare and see whether premium is worth paying for (Encryption level, Verification process etc.). Make sure the CA is recognized by major browsers.

Q: I thought I was logging into application X. What is this "UCLA Web Single Sign-On"?

A: The UCLA Web Single Sign-On is UCLA's standard web authentication and single sign-on service. You have been redirected here because the application you are visiting uses this service to authenticate users.

UCLA Web Single Sign-On provides a common user interface for user authentication. It also enables single sign-on among participating applications. There are currently over 200 web applications across the UCLA campus using this service. In addition we are rolling out expanded functionality to allow for collaboration between the UC and national universities.

Q: What is a UCLA Logon ID?

A: The [UCLA Logon ID](https://logon.ucla.edu) is a campus wide digital identifier formerly known as the Bruin Online ID. You can create, modify, or edit an account directly at [https://logon.ucla.edu](https://logon.ucla.edu).

Q: I'm affiliated with another institution, how do I get back to its login page instead of UCLAs?

A: You will need to restart your browser - furthermore if you selected "this week" instead of "this session" at the WAYF (where are you from page) you will need to clear out your browser cookies (or else you won't be able to choose your proper institution from the WAYF page).

Q: What federations is UCLA Web Single Sign-On a part of?

A: UCLA Web Single Sign-On is a member of the [UCTrust](http://uctrust.com) and InCommon Federations.

Q: What browsers Are supported

A: We have tested against Internet Explorer 6+, Firefox 1.5+, Safari 2-3, and Opera 8-9 - browsers using the same webkit or gecko engines should also function properly. While we strive to assure an accessible experience, some older browsers may in the future be blacklisted due to unacceptable security flaws within them.

Q: Do I need to enable Javascript?

A: Yes. UCLA Web Single Sign-On uses Javascript to perform a number of functions. Please enable javascript in your browser when using this authentication service.

Q: Do I need to accept browser cookies?

A: Yes. UCLA Web Single Sign-On writes temporary cookies to your browser in order to provide single sign-on service. For most browsers, these cookies are never written to disk. They are erased when you close your browser. Please accept browser cookies from ucla.edu in your browser when using this authentication service.

**Additional questions**

- How do I configure mod_shib to look for the TCPLlistener on another box? What mod_shib directive?
- What about the acl field of TCPLlistener? Can that use wildcards or x.x.x.x/mask notation? Is blank equivalent to “Allow All”?
- What port is recommended for the TCPLlistener?
  - Answers: I was successful in pointing Apache/mod_shib at the configuration file with the ShibConfig directive. This seemed to work, but I had to install the shibboleth2.xml config on each webserver even though technical shibd is not running on any of the webservers anymore, as I set up a dedicated box for shibd, per the "cluster" instructions on the Shibboleth wiki.
  - A: I just used port 1600 as it appeared in several examples and nothing else was running on it.
  - A: I didn't have success with a blank acl="" field so I put in all 8 webserver IP addresses and it seemed to work. (IMO this is a configuration/maintenance hassle as adding webservers to the
cluster will require us tweaking this config on the shib box)

Unanswered questions

- Why does mod_shib show up as mod_apache.cpp? (just curious, really)
- How do I add another IdP? Specifically,
  - Where in the context of <ApplicationDefaults> does another IdP fit?
  - As another <SessionInitiator>?

Q: Why might my MacOS Safari continually loop when signing into Shibboleth?

A: I just discovered an issue with the SP and the most recent Mac versions of Safari that cause the browser to refuse to set the session cookie after you login, and results in a loop or whatever happens in a particular app's setup.

The cause appears to be using a cookieProps setting that ends in a semicolon, which causes two semicolons to appear together in some of the Set-Cookie response headers, which in turn causes the next Set-Cookie it sees to be ignored. No, not kidding.

Anyway, I'll add code to check for this, but for now, if it happens, that's probably why. Normally you want to leave it unset entirely except for SSL use, where you'd use "; path=/; secure". The problem value we found was "; path=/;"

-Contributed by Scott Cantor

Q: Why does my logon id not work when i try to test against testshib?

A: The test system does not mirror the production system. It does not contain your user data. We can give you test logon ids for attribute testing purposes. Contact us for further help.

Q: I noticed that Shibboleth only support UCLA logon ID. Is there a plan in the near future to provide support for OASIS and QDB logons?

A: Shibboleth will not be supporting log in using OASIS or QDB logon ID’s.

We will, however, continue to support managing access control through DACSS functions. I understand that External Affairs’ applications manage authorization via DACSS. We have a way to make that mapping work so that your users can sign in using UCLA logon ID and still be managed by DACSS.

We are also working on replacing DACSS, thus eliminating the need to have an OASIS logon ID altogether if the user only needs to access web applications.

Q: What do I need to know about setting up a Test Account with uclaAISMainframeID?

A: We have pre-existing test accounts that you can use to verify that shibboleth is delivering mainframe id. Email us for them