Shibboleth at Cornell Page

Introduction

This wiki site is offered to assist Cornell web site administrators who are interested in using Shibboleth authentication and authorization technology for access to their website, or to a vendor's website. The Shibboleth Service Provider can usually be used as a replacement for CUWebAuth. The advantage of using Shibboleth is that you can enable access to your site to users from other institutions that are members of the InCommon Federation.

See the InCommon website for more information and a list of Colleges and Universities that are members.

Shibboleth will not enable people from all colleges and universities to have access to your site, only those that are members of the InCommon Federation. In addition, you can restrict your site to only certain members of InCommon, and only if those members have certain attributes (such as student, faculty, staff, etc.)

Shibboleth is also a popular method for enabling cloud vendor sites to authenticate and authorize Cornell users.

Integrators outside of InCommon who would like to make use of Cornell's Identity Provider may point to the test IDP first and work through any initial issues. When you are ready to move your integration into production, please submit a request at https://shibrequest.cit.cornell.edu to start the process.

Please join Cornell Shibboleth admins mailing list by sending an email to cornell-shib-users-L-request@cornell.edu with the word join as the subject line. Leave the body of the message blank.

> In the follow up to a critical security advisory that Shibboleth Consortium released on Feb 27 2018, Identity Provider should begin to insist on the use of XML Encryption going forward. From now on, **all the new service provider must provide a certificate for encryption in the metadata**.

Cornell IDP Info

Generally, vendors will have the following questions. You can send them a link to this page to get started

Prod IDP: https://shibidp.cit.cornell.edu/idp/shibboleth

Test IDP: https://shibidp-test.cit.cornell.edu/idp/shibboleth
Cornell is the member of InCommon. Cornell's metadata is included in InCommon's metadata. Get Cornell's metadata from InCommon:

http://md.incommon.org/InCommon/InCommon-metadata-idp-only.xml

If you just need the content of Cornell IDP metadata, get it from:

https://shibidp.cit.cornell.edu/idp/shibboleth

If you are integrating test instance of your application, please point it to Cornell IDP test instance. Test IDP's metadata can be accessed from https://shibidp-test.cit.cornell.edu/idp/shibboleth
Download Prod IDP certificate

Download Test IDP certificate
Prod IDP login URL(POST binding): https://shibidp.cit.cornell.edu/idp/profile/SAML2/POST/SSO

Prod IDP login URL(Redirect binding): https://shibidp.cit.cornell.edu/idp/profile/SAML2/Redirect/SSO

Test IDP login URL (POST binding): https://shibidp-test.cit.cornell.edu/idp/profile/SAML2/POST/SSO

Test IDP login URL(Redirect binding): https://shibidp-test.cit.cornell.edu/idp/profile/SAML2/Redirect/SSO
No. Our IdP doesn't support logout because our credentials stick around until you close your browser. We usually recommend that you give the user instructions to quit the browser if they want to log out. Recently one of our vendors hooked up their logout button to a page that gives instructions – see example.
No. Weill Medical school has its own Identity Provider. If your application service provider supports multiple Identity Providers, we can publish your SP's metadata with InCommon. Then your application is able to use Weill Medical Identity provider.
Yes, GuestID login need to be enabled for your site in IDP if your site support it. On the last page of Shibboleth Integration request form, there is a question about if your site support GuestID login. Please check "Yes" if your site need to support it.
Yes, the Identity Provider is behind the load balancer which provides load balancing and failover.
Currently we release the following public attributes. Other attributes are available but must be configured - please send email to idmgmt@cornell.edu if you don't see the attribute you are looking for.

Majority of Service Providers use Attribute Name In SAML Assertion(value in second column) to map to the attribute in their system, but some service providers use Friendly name in SAML Assertion.

AttributeNameInEnterpriseDirectory	Attribute Name In SAML Assertion
edupersonprimaryaffiliation	urn:oid:1.3.6.1.4.1.5923.1.1.1.5
cn(commonName)	urn:oid:2.5.4.3

eduPersonPrincipalName (netid@cornell.edu)	urn:oid:1.3.6.1.4.1.5923.1.1.1.6
givenName (first name)	urn:oid:2.5.4.42
sn(last name)	urn:oid:2.5.4.4
displayName	urn:oid:2.16.840.1.113730.3.1.241
uid (netid)	urn:oid:0.9.2342.19200300.100.1.1
eduPersonOrgDN	urn:oid:1.3.6.1.4.1.5923.1.1.1.3
mail	urn:oid:0.9.2342.19200300.100.1.3
eduPersonAffiliation	urn:oid:1.3.6.1.4.1.5923.1.1.1.1
eduPersonScopedAffiliation	urn:oid:1.3.6.1.4.1.5923.1.1.1.9
eduPersonEntitlement	urn:oid:1.3.6.1.4.1.5923.1.1.1.7

TransientId is the default NameID.
If you don't already have a Cornell NetID, you might be able to obtain an exception with sponsor NetID. Please talk to the person who is your contact at Cornell, or email idmgmt@cornell.edu.

Service Provider Installation

There are many Service Provider products, for example Shibboleth, SimpleSAMLphp, passport-saml, etc. You should choose one that fit your hosting environment. We have installation instructions for Shibboleth Service Provider. For other Service Providers please refer to its own product documentation.

How to install Shibboleth Service Provider on Windows

How to Install Shibboleth Service Provider on Linux

Simplesamlphp