Install Shibboleth Service Provider on Linux

This document describes the procedure used to install Shibboleth Service Provider (SP) software on Centos, RedHat and to configure it to work with the Cornell Shibboleth Identity Provider (IdP).

If you are moving shib protected domain to a new serve, please use instruction here: Move Shibboleth Service Provider to a Different Server

Prerequisites

- Apache must be installed and your website have an SSL certificate installed and SSL enabled. To request a SSL certificate: https://it.cornell.edu/ssl/renew-or-request-ssl-certificate.
- Shibboleth doesn't support http access. If http access is supported on your site, define a redirect rule in Apache configuration that route http traffic to https.
- Make sure your server time is accurate.
- **Your server has user shibd available.**
- **We do not recommend the use of the old prefork MPM and strongly encourage the worker MPM. The prefork option will fail under load in a variety of cases, with some limited workarounds possible.**

Installation

If you are on a CIT Managed Server, please check this document: https://sysdocs.cit.cornell.edu/Documentation/LinuxShibbolethRepository

Otherwise, Install using RPM: https://wiki.shibboleth.net/confluence/display/SP3/RPMInstall

1. Visit https://shibboleth.net/downloads/service-provider/RPMS/, choose your platform, then click Generate
2. Copy generated content to /etc/yum.repos.d/shibboleth.repo
3. sudo yum install `shibboleth.x86_64` (64 bit OS)
   `sudo yum install shibboleth (32 bit OS )`

Make sure you are running Ubuntu version 20.04 or above. Otherwise you may have SP 2 instead of SP 3 installed. SP 2 is no longer supported.

sudo apt-get update

sudo apt-get install libapache2-mod-shib2

sudo a2enmod shib

Configuration - Shibboleth SP

After installation Shibboleth configuration files are placed at **/etc/shibboleth/**. Necessary Apache configuration in */etc/httpd/conf.d/shib.conf(Centos /Redhat), /etc/apache2/conf-available/shib.conf (Ubuntu).* Make sure shib.conf is included in your Apache configuration file. **If you are converting CUWebAuth to Shibboleth on a production server, make sure you set "ShibCompatValidUser" to "On" in shib.conf to avoid interruption to your website's CUWebAuth authentication.** Set it back to "Off" after you finish the conversion.

Download our **sample attribute-map.xml** and replace your /etc/shibboleth/attribute-map.xml with downloaded file. Our attribute-map.xml defines all commonly used attributes.

All attributes except groups defined in attribute-map.xml are released by default to all SP. Attribute "groups" is released on demand. Please specify your group names in Shibboleth Integration Request form. Shibboleth IDP doesn't support nested groups(for example group B is a member of group A, user C is a member of group B, IDP doesn't know user C is a member of group A) . If you have to use nested group, you need to convert nested group to dynamic group.
Download our **sample shibboleth2.xml** and replace your /etc/shibboleth/shibboleth2.xml with downloaded file. Open shibboleth2.xml in a text editor.

- Update SP entityID:

  Search <ApplicationDefaults entityID="https://mysite.cit.cornell.edu/shibboleth"... >. EntityID is the Unique identifier for your SP. Cornell Shibboleth Identity Provider(IDP) provides service to many applications. This entityID will help Cornell IDP to identify your SP. We recommend you follow shibboleth convention named it "https://xxx/shibboleth". It's better not include space or special characters in it(/ and : are fine). One SP can server multiple sites in your Apache so it does **not** necessarily equate to the hostname(s) at which your service runs.

- Update SP session:
  Search <Sessions lifetime="28800" timeout="3600" ...>

  --- lifetime is the maximum duration in `seconds` that a session maintained by the SP will be valid.The settings shown in the example will set your Shibboleth session lifetime to 28800 (8 hours). The maximum session lifetime you can set is 36000 (10 hours).

  --- timeout is the maximum inactivity allowed between requests in a session maintained by the SP. The settings shown in the example will set your Shibboleth session timeout to 3600 (1 hour).

Force authentication

When session expire or timeout, user will be redirected back to Identity Provider(IDP). If user still has active IDP session, user will NOT be prompted for login screen. They will just be redirected back to your website. If you would like to force user re-login when SP session expire /timeout, please configure Force Re-Authentication in SP:Configure a Service Provider to Force Re-Authentication

--- postData="ss:mem" postTemplate="postTemplate.html" postLimit="1048576"

Add it to <Sessions ..> if your website hosts web form(with Content-Type application/x-www-form-urlencoded). Web form POST data with Content-Type application/x-www-form-urlencoded will be saved in the Shibboleth memory cache rather than discarded when a user requires authentication after filling out a web form. "postTemplate.html" is located in /etc/shibboleth directory. Modify it to meet your website's style. "postLimit" is the maximum number of bytes to allow when saving off POST data. Over this limit, a warning in the log will appear, but the data will not be saved. When not defined it uses the default which is 1048576 bytes(1024k).

More information: https://wiki.shibboleth.net/confluence/display/SP3/Sessions

- Update the support contact:

Search < *Errors supportContact ="root@localhost" helpLocation ="/about.html" styleSheet ="/shibboleth-sp/main.css" />* . Change the email address to your application's support email address. Change the helpLocation to your application's help page.

- Update redirectLimit if needed

If Shibboleth is installed via RPM, signing/encryption key and certificate files are generated automatically. Check if you have sp-signing-cert.pem, sp-signing-key.pem, sp-encrypt-key.pem, sp-encrypt-cert.pem in /etc/shibboleth directory. If they are not there, generate them.

```
./keygen -u shibd -g shibd -n sp-signing -h yourServername -y 10 (your servername will be the CN of the certificate)
./keygen -u shibd -g shibd -n sp-encrypt -h yourServername -y 10

After you run the commands, four files are created: sp-encrypt-cert.pem, sp-encrypt-key.pem, sp-signing-cert.pem, sp-signing-key.pem. These files should be owned by shibd.

NOTE: Signing and encryption certificates are included in your SP's metadata. You should preserve these four files and put them back when you do a fresh SP rebuild using Docker or other container software.
```

If your website is behind a Load Balancer

Please make sure that the real client's IP address (e.g. "x-forwarded-for") is being passed to the SP, instead of the load-balancer's IP address. Please see this page for details: Pass the real client IP to the Shibboleth SP when your site is behind a load balancer

Shibboleth Configuration Check

In the command line, execute the following command to see whether the Shibboleth Service Provider can load the default configuration:

```
sudo LD_LIBRARY_PATH=/opt/shibboleth/lib64 /sbin/shibd -t
```

The last line of the output should read:

```
overall configuration is loadable, check console for non-fatal problems
```

If there are any **ERROR** log entries, we strongly recommend you resolve these. Messages with log level **WARN** are generally not problematic but you should understand the causes of these warning messages and run the configuration check again when you are finished with your setup.

Logs for Shibboleth SP are located at /var/log/shibboleth/. Take a look at /var/log/shibboleth/shibd_warn.log and make sure there is no error in there. You need to fix error if there is any and restart shibd and httpd.

Start Shibboleth Service Provider and Apache

shibd is installed to /usr/sbin and may be managed using service and chkconfig (on System V platforms) or with systemctl (on systemd platforms, some additional information available).

On Centos 7, you can start shibd and apache by running

```
sudo systemctl start shibd

sudo systemctl start httpd
```

After you run the command, make sure shibd and httpd are running.

Register Service Provider with Cornell IDP

Navigate to *https://yoursiteDomain/Shibboleth.sso/Metadata* and download it. Open your downloaded file with text editor. **Some browser doesn't show metadata correctly in the browser. DO NOT copy the content in the browser.** Make sure the entityID is the same as your defined in shibboleth2.xml. If there are multiple sites in Apache require Shibboleth authentication, you can get SP's metadata by navigating to one of the site, then manually add assertion consumer service HTTP-POST bindings for each of the other sites in your SP's metadata. You may see other AssertionConsumerService bindings, 'SingleLogoutService', 'ArtifactResolutionService' etc in your downloaded metadata. Those are not being used. You don't need to add those for other sites.

Example

```
In our example, SP's metadata can be obtained from https://shibtest.cit.cornell.edu/Shibboleth.sso/Metadata. In
the metadata there should be a line:
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="
https://shibtest.cit.cornell.edu/Shibboleth.sso/SAML2/POST" index="1"/>

There is another site mytest.cit.cornell.edu hosted in the same Apache. Another AssertionConsumerService url
for mytest.cit.cornell.edu need to be manually added in the metadata:
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://mytest.
cit.cornell.edu/Shibboleth.sso/SAML2/POST" index="2"/>
```

Submit your shibboleth integration request from https://shibrequest.cit.cornell.edu. On the second page of the request form, select 'No' for question "Has the application service provider's metadata been published with InCommon?". Use text editor open your SP's metadata, copy the content of the metadata and paste it in the "Service Provider's metadata field. Once the form is submitted, Identity Management team get a Remedy case. We'll configure your SP in IDP in 1 - 2 business day. We'll notify you when the configuration is complete.

Configuration - Apache Access control

After you are notified that your metadata has been integrated in Cornell IDP, you can continue your configuration. If you are converting CUWebAuth to Shibboleth SP, you may refer to Converting CUWebAuth to Shibboleth.

Open /etc/httpd/conf.d/shib.conf in a text editor. If you are Not using default Apache installation, make sure this file is included in your Apache config. All the authorization rules should be defined in this file.

Require authentication for entire site

```
<Location />
AuthType shibboleth
ShibRequestSetting requireSession 1
Require valid-user
</Location>
```

Authorization by affiliation

```
<Location /studentOnly>
  AuthType shibboleth
  ShibRequestSetting requireSession 1
  Require shib-attr eduPersonPrimaryAffiliation student
</Location>

<Location /secure>
  AuthType shibboleth
  ShibRequestSetting requireSession 1
  Require shib-attr eduPersonAffiliations staff
</Location>

*eduPersonPrimaryAffiliation is single value attribute while eduPersonAffiliations is multi-values attribute.
For example, a staff who also taking courses at Cornell has staff as the value of eduPersonPrimaryAffiliation,
has staff and student as the value of eduPersonAffiliations.
All the possible value of affiliations can be found at https://confluence.cornell.edu/display/IDM
/edupersonprimaryaffiliation+and+edupersonaffiliation+details
```

Authorization by group/permit

```
<Location /secure>
AuthType shibboleth
ShibRequestSetting requireSession 1
Require shib-attr groups myGroup1 myGroup2
</Location>

*Group Name is CASE SENSITIVE
```

Authorization by NetID

```
<Location /secure>
AuthType shibboleth
ShibRequestSetting requireSession 1
Require shib-attr uid hjy789 jpq2020
</Location>
```

Require Two-Factor for Everyone

```
https://confluence.cornell.edu/display/SHIBBOLETH/Configure+Website+for+Two-Factor+Authentication+in+Apache
```

Addition configuration information can be found at https://wiki.shibboleth.net/confluence/display/SP3/Apache

After you finish the configuration, restart Apache.

Test SP integration with IdP

Confirm you are able to log in with your netID and user's attributes are properly released. To verify attribute release, in shibboleth2.xml, you need to set showAttributeValues to true and restart shibd, httpd.

<Handler type="Session" Location="/Session" showAttributeValues="true"/>

1. Using a web browser, visit the **/secure** directory (or other protected location) of your SP.
2. If you are prompted to log in, that means that your SP is properly integrated with Cornell IdP.
3. After you log in, open a new tab of the same browser and point your web browser to https://<your dns name>/Shibboleth.sso/Session. Your browser should return a status page that show you all the attributes and values released to your SP.

Auto start shibd after server reboot

sudo systemctl enable shibd

Retrieve Shibboleth Attributes in Application

By default, Shibboleth attributes that released to your shibboleth SP are available to your application as environment variables, not available in HTTP headers. In your application, you should get authenticated user's netID from server variable REMOTE_USER.

Detail and examples about attribute access.

https://wiki.shibboleth.net/confluence/display/SP3/AttributeAccess

If you have tomcat in your environment and REMOTE_USER is not working, you can try add `attributePrefix="AJP_"` to the `<ApplicationDefaults>` element in your configuration:

`<ApplicationDefaults id="default" entityID="xxx" REMOTE_USER="uid" attributePrefix="AJP_">`

Need Help?

contact idmgmt@cornell.edu