Configuring DSpace and Shibboleth

As of DSpace 3.x, this page is outdated. Look at the official documentation instead: Authentication Plugins#ShibbolethAuthentication

Ensure that you are running Apache Tomcat (the web application server) behind Apache HTTPD (the web server). This is required as the Shibboleth authentication is performed in Apache HTTPD, while DSpace runs within Apache Tomcat. There are two ways how to do that - using **mod_proxy_ajp** or **mod_jk** - both are described on https://wiki.duraspace.org/display/DSPACE/DspaceOnStandardPorts

Follow the standard instructions for installing a Shibboleth Service Provider (SP) in Apache HTTPD. Instructions are available from https://wiki.shibboleth.net/confluence/display/SHIB2/Installation

Configure the service provider to protect the following URL:

1. If running DSpace in the ROOT context: http://dspace.example.com/shibboleth-login
2. If running DSpace in a different context: http://dspace.example.com/xmlui/shibboleth-login (adjust xmlui as appropriate)

If you're running DSpace in the ROOT context and you're using ProxyPass directives as described in Running DSpace on Standard Ports, you will most likely have to add

```
    ProxyPass /Shibboleth.sso !
```

to prevent DSpace from taking over these URLs.

Edit config/modules/authentication.cfg to set the authentication method (in older DSpace versions, this is in dspace.cfg):

```
plugin.sequence.org.dspace.authenticate.AuthenticationMethod = org.dspace.authenticate.ShibAuthentication
```

In config/modules/authentication-shibboleth.cfg, edit the rest of the Shibboleth settings. You will need to ask your Shibboleth administrator for some of these:

```
#### Shibboleth Authentication Configuration Settings ####
# Check https://mams.melcoe.mq.edu.au/zope/mams/pubs/Installation/dspace15/view
# for installation detail.
#
# DSpace requires email as user's credential. There are 2 ways of providing
# email to DSpace:
# 1) by explicitly specifying to the user which attribute (header)
#    carries the email address.
# 2) by turning on the user-email-using-tomcat=true which means
#    the software will try to acquire the user's email from Tomcat
# The first option takes PRECEDENCE when specified. Both options can
# be enabled to allow fallback.


# this option below specifies that the email comes from the mentioned header.
# The value is CASE-Sensitive.
authentication.shib.email-header = MAIL


# optional. Specify the header that carries user's first name
# this is going to be used for creation of new-user
authentication.shib.firstname-header = SHIB-EP-GIVENNAME


# optional. Specify the header that carries user's last name
# this is used for creation of new user
authentication.shib.lastname-header = SHIB-EP-SURNAME


# this option below forces the software to acquire the email from Tomcat.
authentication.shib.email-use-tomcat-remote-user = true


# should we allow new users to be registered automtically
# if the IdP provides sufficient info (and user not exists in DSpace)
authentication.shib.autoregister = true
```

```
# these two header here specify which attribute that is responsible
# for providing user's roles to DSpace and unscope the attributes if needed.
# When not specified, it is defaulted to 'Shib-EP-UnscopedAffiliation', and
# ignore-scope is defaulted to 'false'.
# The value is specified in AAP.xml (Shib 1.3.x) or
# attribute-filter.xml (Shib 2.x). The value is CASE-Sensitive.
# The values provided in this header are separated by semi-colon or comma.
# If your sp only provides scoped role header, you need to set
# authentication.shib.role-header.ignore-Scope as true.
# for example if you only get Shib-EP-ScopedAffiliation instead of Shib-EP-ScopedAffiliation,
# you have to  make your setting as:
# authentication.shib.role-header = Shib-EP-ScopedAffiliation
# authentication.shib.role-header.ignore-scope = true


# authentication.shib.role-header = Shib-EP-UnscopedAffiliation
authentication.shib.role-header.ignore-scope = false


# when user is fully authN on IdP but would not like to release
# his/her roles to DSpace (for privacy reason?), what should be
# the default roles be given to such users?
# The values are separated by semi-colon or comma
# authentication.shib.default-roles = Staff, Walk-ins


# The following mappings specify role mapping between IdP and Dspace.
# the left side of the entry is IdP's role (prefixed with
# "authentication.shib.role.") which will be mapped to
# the right entry from DSpace. DSpace's group as indicated on the
# right entry has to EXIST in DSpace, otherwise user will be identified
# as 'anonymous'. Multiple values on the right entry should be separated
# by comma. The values are CASE-Sensitive. Heuristic one-to-one mapping
# will be done when the IdP groups entry are not listed below (i.e.
# if "X" group in IdP is not specified here, then it will be mapped
# to "X" group in DSpace if it exists, otherwise it will be mapped
# to simply 'anonymous')
#
# Given sufficient demand, future release could support regex for the mapping
# special characters need to be escaped by \
authentication.shib.role.Senior\ Researcher = Researcher, Staff
authentication.shib.role.Librarian = Administrator
```

Restart tomcat, and test by logging in.