Shibboleth example

Almost all of the configuration described on this page is not unique to VIVO and will likely vary by your own institution's Shibboleth configuration. That said, an example configuration is provided to hopefully help implementers move their own setup in the right direction.

Install the Shibboleth module for Apache

Installation of the Shibboleth service provider module will depend on your OS distribution. Some documentation on installation is available here: https://shibboleth.atlassian.net/wiki/spaces/SP3/pages/2065335547/LinuxInstall.

Edit Shibboleth Application Defaults

Edit defaults. Example location is /etc/shibboleth/shibboleth2.xml. Add in your site's URL as the entityID, the attribute name Shibboleth will provide the user ID in, and set attributePrefix so Apache's AJP will pass the attributes through. The attribute name in this example is 'eppn' but may be different depending on your Shibboleth configuration.

shibboleth2.xml

```
    <!-- The ApplicationDefaults element is where most of Shibboleth's SAML bits are defined. -->
    <ApplicationDefaults entityID="https://vivo.school.edu/shibboleth" REMOTE_USER="eppn" attributePrefix="AJP_"
>
```

Secure VIVO's 'special page' at /loginExternalAuthReturn

Somewhere in your Apache configuration, load the Shibboleth module and secure the pages.

httpd.conf

```
LoadModule mod_shib /usr/lib64/shibboleth/mod_shib_24.so

<Location /Shibboleth.sso>
  AuthType None
  Require all granted
</Location>

<Location /loginExternalAuthReturn>
  AuthType shibboleth
  ShibRequestSetting requireSession 1
  require shib-session
</Location>
```

Allow Shibboleth's pages to be served by Apache

Exempt Shibboleth's pages from the Tomcat/VIVO proxy. Example Virtualhost:

ssl.conf

```
<VirtualHost _default_:443>
  ServerName vivo.school.edu
  ProxyPass /Shibboleth.sso/* !
  ProxyPassMatch "/Shibboleth.sso/.*/" !
  ProxyPass / ajp://localhost:8009/ retry=15 secret=your_tomcat_secret timeout=600
</VirtualHost>
```

Allow Shibboleth attributes to be passed through to Tomcat

As a security feature, Tomcat does not pass through request attributes to applications unless they meet a specific pattern. You can specify the allowed attributes in regex by adding 'allowedRequestAttributesPattern' to your AJP connector definition.

Example AJP connector config in Tomcat's server.xml.

server.xml

```
    <!-- Define an AJP 1.3 Connector on port 8009 -->
    <Connector protocol="AJP/1.3"
               address="::1"
               port="8009"
               redirectPort="8443"
               secretRequired="true"
               secret="your_tomcat_secret"
               URIEncoding="UTF-8"
               tomcatAuthentication="false"
               allowedRequestAttributesPattern="^(Shib-.*|eppn)$"
               />
```

Edit runtime.properties

Add the header or attribute name Shibboleth will use to provide VIVO the user's ID.

runtime.properties

```
externalAuth.netIdHeaderName = eppn
```

Specifying externalAuth.netIdHeaderName will activate the external authentication in VIVO. Restart Shibboleth, Apache, Tomcat, and VIVO to allow your changes to take effect.