DSpace 7 Shibboleth Configuration

- Problem
- Solution
- Separate REST and Angular hostname
- Related resources

Problem

Based on the work done on https://github.com/DSpace/dspace-angular/pull/568 and https://github.com/DSpace/DSpace/pull/2651, it isn’t been possible for all to accomplish authentication using shibboleth. We agree to share workable configurations.

Solution

In DSpace configuration, local.cfg file, ensure these lines are uncommented:

```properties
# Shibboleth authentication/authorization. See authentication-shibboleth.cfg for default configuration.
plugin.sequence.org.dspace.authenticate.AuthenticationMethod = org.dspace.authenticate.ShibAuthentication

# Enabled by default in authentication.cfg
plugin.sequence.org.dspace.authenticate.AuthenticationMethod = org.dspace.authenticate.PasswordAuthentication
```

we also use default attributes that are mapped in my Shibboleth (version 3.0.4) attribute map (this may differ accordingly with the IdP).

In my local setup (Paulo Graça), I’m using Apache/2.4.6 (CentOS) with Proxypass with this settings. This is also tested (Ben Bosman) with Apache/2.4.41 (Amazon Linux 2):
The AJP proxy only works ([Ben Bosman](https://github.com/bosman)) if shibboleth2.xml doesn't contain the attribute `attributePrefix="AJP_"` in the ApplicationDefaults.

I'm ([Paulo Graça](https://github.com/paulograça)) also using Tomcat v9 (apache-tomcat-9.0.30) and java-11-openjdk.x86_64, with a almost default tomcat server.xml file. Ben Bosman has created the setup with apache-tomcat-9.0.31 and OpenJDK Runtime Environment Corretto-11.0.6.10.1:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<Server port="8005" shutdown="SHUTDOWN">
  <!-- (...) -->
  <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
  <Engine name="Catalina" defaultHost="localhost">
    <!-- (...) -->
    <Host name="localhost" appBase="/dspace/webapps" unpackWARs="true" autoDeploy="true" xmlNamespaceAware="false" xmlValidation="false">
      <Context allowLinking="true" path="" docBase="server" />
      <Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs" prefix="access_log" suffix=".log" pattern="%h %l %u %t "%r" %>s %b" />
    </Host>
  </Engine>
  <!-- (...) -->
</Server>
```
Separate REST and Angular hostname

When using separate hostnames for REST and Angular, more configuration is required on the REST Apache to make sure you allow requests from the given hostname. The configuration below allows access from localhost:3000 and dspace7-demo.atmire.com (tested by Ben Bosman)

**Apache config**

```
SetEnvIf Origin "^http(s)?://(www\.|)(dspace7\-demo\.|atmire\.|localhost\:3000|127\.|0\.|0\.|1\:3000)$"
AccessControlAllowOrigin="0"
    Header set Access-Control-Allow-Origin $0 env=AccessControlAllowOrigin
    Header set Access-Control-Allow-Credentials true env=AccessControlAllowOrigin
    Header set Access-Control-Expose-Headers: "Authorization, expires, Location, Content-Disposition, WWW-
    Authenticate, Set-Cookie, X-Requested-With"
    Header merge Vary Origin
```

Also make sure you don't have a Proxy for http://localhost:3000/ if you're testing from http://localhost:3000/

This setup currently causes warnings:

A cookie associated with a cross-site resource at http://dspace7-rest.atmire.com/ was set without the `SameSite` attribute. A future release of Chrome will only deliver cookies with cross-site requests if they are set with `SameSite=None` and `Secure`. You can review cookies in developer tools under Application>Storage>Cookies and see more details at [https://www.chromestatus.com/feature/5088147346030592](https://www.chromestatus.com/feature/5088147346030592) and [https://www.chromestatus.com/feature/56335216221686032](https://www.chromestatus.com/feature/56335216221686032).

**Related resources**

- DSpace 7 Shibboleth Configuration