

# SHRINE 4.0.0 Appendix A.2 - Quick Configuration

The following instructions are meant to get you going as quickly as possible. If you want a better understanding of what's going on, go to the "More Details" sections of this document.

## Configuration Directories

In summary, the directories containing configuration files which need to be modified are:

```
/opt/shrine/tomcat/conf/ Tomcat configuration files

/opt/shrine/tomcat/lib/ Shrine config files

/etc/shibboleth/ Shibboleth configuration files

/etc/httpd/** Apache configuration files

/var/www/html/ Apache static content as set in, for instance, /etc/httpd/conf/httpd.conf
```

## Configuration files to create from scratch or to import

	Location on SP	Description
key pair	<code>/etc/shibboleth/sp-key.pem</code>  <code>/etc/shibboleth/sp-cert.pem</code>	If the Shibboleth installer has not already done so, create a key pair; include the content of the public key certificate ( <b>sp-cert.pem</b> ) in <b>sp-metadata.xml</b> (see below), and the paths of the <b>key</b> and <b>certificate</b> as xml attributes of the <b>&lt;CredentialResolver&gt;</b> element of <b>shibboleth2.xml</b> (see below)  To create a key pair, use <code>/etc/shibboleth/keygen.sh</code> ; as per <a href="https://shibboleth.atlassian.net/wiki/spaces/SP3/pages/2067398706/keygen">https://shibboleth.atlassian.net/wiki/spaces/SP3/pages/2067398706/keygen</a> and also <a href="https://docs.shib.ncsu.edu/docs/configure/index.html">https://docs.shib.ncsu.edu/docs/configure/index.html</a> .  You don't need to create separate key pairs for signing and for encryption.
idp-metadata.xml	<code>/etc/shibboleth/idp-metadata.xml</code>	A copy of your idP's metadata. You'll need to ask the admin(s) of your idP for a copy of it, most likely over a secure channel. Rename it to <b>idp-metadata.xml</b> and put it in <code>/etc/shibboleth</code>

## Configuration files based on samples in Git

Sample configuration files can be found in the nightly shrine-setup zip file located at <https://repo.open.catalyst.harvard.edu/nexus/content/groups/public/net/shrine/shrine-setup/4.0.0/shrine-setup-4.0.0-dist.zip>

- `sso/apache/sp.conf-sample`
- `sso/apache/sp-metadata.xml-sample`
- `sso/shibboleth/attribute-map.xml-sample`
- `sso/shibboleth/shibboleth2.xml-sample`
- `sso/tomcat/server.xml-sample`
- `sso/shrine/shrine.conf-sample`
- `sso/shrine/override.conf-sample`

Copy these files to the location on the SP (i.e. your server) indicated in the table below. Remove the "-sample" from the file names. Overwrite the existing config files.

Then search for the marker: '**ADJUST\_FOR\_YOUR\_SITE**' in each of these files for indications of what / where you need to edit them.

Location in zip file	Location on SP	Description
<code>sso/apache/sp-metadata.xml-sample</code>	<code>/var/www/html/sp-metadata.xml</code>  – as long as your Apache configuration sets <code>DocumentRoot</code> to <code>/var/www/html</code> (for instance in <code>/etc/httpd/conf/httpd.conf</code> )	To be shared dynamically with your site's IdP (i.e. make it available as a document at the document root and share that URL with your IdP's maintainers/admins); or omit from the SP's (i.e. your) web server, and instead share it securely with the IdP admins whenever it changes (if it does)  In either case, populate the <b>entityID</b> , public key <b>certificate</b> , and consumer service <b>location</b> with yours.

sso /shibboleth /shibboleth2.xml-sample	/etc/shibboleth /shibboleth2.xml	<p>Populate the <b>entityID</b> attribute in <b>&lt;ApplicationDefaults&gt;</b> to match your <b>entityID</b> in <b>sp-metadata.xml</b>.</p> <p>Populate the <b>entityID</b> attribute in <b>&lt;SSO&gt;</b> to match the idP's <b>entityID</b> in <b>idp-metadata.xml</b>.</p> <p>Populate the <b>supportContact</b> attribute of the <b>&lt;Errors&gt;</b> element with an email address.</p> <p>The <b>&lt;CredentialResolver&gt;</b> element specifies the private+public key to use for encryption and signing while communicating with the idP. If you put the keys in the location specified above and the private key is not password-protected, then there is no need to modify this element. Otherwise edit this file to reflect the location of the keys and optionally the private key password.</p> <p>The private key should be stored in a "safe" location. If it is password-protected, that should be reflected in the <b>&lt;CredentialResolver&gt;</b>'s <b>password</b> attribute.</p>
sso /shibboleth /attribute-map.xml-sample	/etc/shibboleth /attribute-map.xml	Populate the idP's attribute name for the user; to be mapped to the attribute id <b>"userId"</b>
sso /apache /sp.conf-sample	/etc/httpd/conf.d/sp.conf	Populate the <b>ServerName</b> , <b>ProxyPass</b> and <b>Header set Access-Control-Allow-Origin</b> directives with your hostname.
sso /tomcat /server.xml-sample	/opt/shrine/tomcat/conf /server.xml	<p>Most likely the following 3 attributes of <b>&lt;Connector port="6443"... /&gt;</b> are already populated, but if not then populate <b>certificateKeystoreFile</b>, <b>certificateKeystorePassword</b>, <b>certificateKeyAlias</b>.</p> <p>You will need to populate <b>proxyName</b> in the <b>AjpNio2Protocol</b> connector.</p> <p>Once done, <b>Merge</b> the contents of <b>server.xml-sample</b> into the existing <b>/opt/shrine/tomcat/conf/server.xml</b>.</p>
sso /shrine /shrine.conf-sample or sso /shrine /override.conf-sample	/opt/shrine/tomcat/lib /shrine.conf or /opt/shrine/tomcat/lib /override.conf	<p>Set Shrine configuration options for using SSO for login/logout.</p> <p>In <b>override.conf</b> it would look like:</p> <ul style="list-style-type: none"> <li>Specify that we are using SSO: <b>shrine.queryEntryPoint.authenticationType = "sso"</b></li> <li>Specify the logout URL (<b>shrine.webclient.ssoLogoutUrl</b>) = (see override.conf-sample)</li> <li>Specify Shrine's session timeout as such: <b>shrine.webclient.sessionTimeout = "30 minutes"</b>.</li> </ul> <p>You should use either file and <b>merge it</b> into the existing <b>shrine.conf</b> or <b>override.conf</b> in <b>/opt/shrine/tomcat/lib</b></p>

## Next Steps:

Fast forward to [SHRINE 4.0.0 Appendix A.8 - Starting and Stopping the Software](#)

or

Read the "More Details" pages that follow, starting with [SHRINE 4.0.0 Appendix A.3 - More Details : Shibboleth Configuration](#)