Timeouts

In shibboleth2.xml, <Sessions> element controls how the SSO process is managed by the SP. Following child elements inside Sessions control timeouts:

Name	Type	Default	Description
`timeout`	seconds	3600 (1 hour)	Maximum inactivity allowed between requests in a session maintained by the SP. This inactivity applies only to requests to this SP and is not aware of activity between the browser and other web sites .
`lifetime`	seconds	28800 (8 hours)	Maximum duration in `seconds` that a session maintained by the SP will be valid.

Shibboleth IDP uses CUWebLogin for primary authentication. The valid SSO session lasts for 10 hours. If you would like to prompt user for netID /password when they access your site even if user already have valid SSO session in CUWebLogin, forceAuthn="true" should be added in <Host> element.

If you would like to have a different timeout for some locations of your site, you can use <ApplicationOverride>. You can also add forceAuthn="true" to <Path> element to force authentication.

Example of Path-Based Application Override (shibboleth2.xml)

```
 <RequestMap applicationId="default">

    <Host name="www.example.org">
        <Path name="myappfolder" applicationId="myappname"/>
    </Host>
</RequestMap>
...
<ApplicationDefaults ...>
...
    <ApplicationOverride id="myappname">
        <Sessions lifetime="3600" timeout="600" checkAddress="false" handlerURL="/myappfolder/Shibboleth.
sso" />
    </ApplicationOverride>
</ApplicationDefaults>
```

Make sure that the metadata you provide for the SP includes the necessary endpoints of this handler. In this example, metadata should have AssertionConsumerServiceURL:

<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://www.example.org/myappfolder /Shibboleth.sso/SAML2/POST" index="5" />

More info about ApplicationOverride.