Converting CUWebAuth to Shibboleth (Apache)

Before you start to convert CUWebAuth to Shibboleth, review your CUWebauth configurations and compare them to this instruction. If you are using any CUWebAuth feature that is no longer available in Shibboleth, you need to modify your application to replace it with other method before you convert.

Features that are not supported in Shibboleth:

- CUWebAuth Portal Permit: <Location /CUWAPortal/Permit>
  - Suggestion: Your application need to query Active Directory to get group membership.
- CUWebAuth Portal Proxy: <Location /CUWAPortal/Proxy>
- CUWebAuth DavLogin: SetHandler cuwa_davlogin

When you are ready to covert, follow the instruction to install/configure Shibboleth Service Provider first. Shibboleth Service Provider is one of the products that implement SAML protocol. You may choose other SAML service provider product that work best with your application. For example, you may want to use simpleSAMLphp if you have a PHP application.

CUWebAuth Directive to Shibboleth mapping

<table>
<thead>
<tr>
<th>CUWebAuth</th>
<th>Shibboleth (shib.conf)</th>
<th>Shibboleth (shibboleth2.xml)</th>
</tr>
</thead>
</table>
| AuthType all                  | AuthType shibboleth                                                                   | ShibRequestSetting authnContextClassRef https://refeds.org/profile/mfa
<RequireAll>
  - Require shib-session
</RequireAll> |
| Require valid-user            | Require valid-user                                                                     | ShibRequirement authnContextClassRef "https://refeds.org/profile/mfa"
Apache 2.2
  - ShibRequestSetting authnContextClassRef https://refeds.org/profile/mfa
  - ShibRequireAll on
  - ShibCompatWith24 on
  - Require shib-session
  - Require authnContextClassRef "https://refeds.org/profile/mfa"
| Require netid netid1 netid2   | Require shib-attr uid netid1 netid2                                                   | ShibRequestSetting authnContextClassRef "https://refeds.org/profile/mfa"
| Require permit myPermit       | Require shib-attr groups myPermit                                                     |
  - "Group membership is not released by default. Please specify group name in shibboleth integration form"
| Require noprompt              | Not supported                                                                           | ShibRequestSetting authnContextClassRef "https://refeds.org/profile/mfa"
| CUWA2FARequire all            | Apache 2.4                                                                             |
  - ShibRequestSetting authnContextClassRef https://refeds.org/profile/mfa
<RequireAll>
  - Require shib-session
</RequireAll> |
| CUWA2FARequire permit-name1 permit-name2 | Not supported in Shibboleth SP. But can be supported in Shibboleth IDP. Please specify your requirement in shibboleth integration request form |
| CUWACredentialAge             |                                                                                       | ShibRequestSetting forceAuthn true
Configure a Service Provider to Force Re-Authentication |
| CUWACredentialAge 0 or low value (the purpose is forcing user to re-login) |                                                                                       | ShibRequestSetting authnContextClassRef "https://refeds.org/profile/mfa"
| CUWAINactivityTimeout         |                                                                                       | ShibRequestSetting authnContextClassRef "https://refeds.org/profile/mfa"
<Sessions lifetime=...>       |
| Combination of CUWACredentialAge and CUWAINactivityTimeout for the purpose of forcing user re-login |                                                                                       | ShibRequestSetting authnContextClassRef "https://refeds.org/profile/mfa"
<Sessions lifetime=...>       |

https://confluence.cornell.edu/display/SHIBBOLETH/Configure+a+Service+Provider+to+Force+Re-Authentication
<table>
<thead>
<tr>
<th>CUWAwake2Name</th>
<th>If your site supports GuestID login, there is no special configuration needed on your end. You just need to indicate that in Shibboleth integration request form. If your site supports Weill Medicine CWID login, please read: Login with Cornell NetID and Weill Cornell CWID</th>
</tr>
</thead>
<tbody>
<tr>
<td>CUWAwakeK0Realms</td>
<td>When CUWAInquire is defined in CUWebAuth, your application probably retrieve user's group from server variable CUWA_GROUPS. When you convert it to shib, let us know the group names your application need to know in Shibboleth integration request form. Then your application can retrieve user's group from server variable &quot;groups&quot;</td>
</tr>
</tbody>
</table>

Following directives can be simply deleted:

- AuthName Cornell
- CUWAKerberosPrincipal
- CUWAWebLoginURL
- CUWAKeytab
- CUWAsessionFilePath