Implementing no-PDS Authentication

Nathan Mealey, Portland State
Summer Meeting 2016
PDS vs. no-PDS

- **Patron Directory Services** - separate layer from Primo that handles patron authentication
- no-PDS removes this supplemental layer, and Primo handles authentication itself
What method does no-PDS support?

- Shibboleth (SAML)
- LDAP
- Alma
- CAS is planned for May 2017 implementation
Key no-PDS features

- Parallel authentication profiles
  - Patrons can choose one of two authentication options
- Cascading authentication profiles
  - Only works for Alma and LDAP methods
- Silent login (demo), i.e. auto-login
Why implement no-PDS?

- Resolves known issue with quoted searches (the dreaded white screen)
- Gives you local control over sign-in page and configuration of your sign-in options
- Removes a point of failure
- Integrates well with the new Primo UI
Implementation steps

Note that authentication setup affects all views for the instance (production vs. sandbox).

1. Confirm whether you need multiple profiles or just one
   a. Do you need to authenticate both campus and community patrons?
2. Create a new profile
   a. Config wizards > User authentication wizard
3. Select the authentication method
   a. Alma is very simple and may be good for just getting the ball rolling
4. Set configuration for the new profile and save
Implementation steps (2)

5. Set which profile is the main and which is secondary
6. Save settings
7. Deploy authentication
8. Change PDS setting in Alma
   a. General Configuration > General Configuration > Other Settings
Implementation steps (3)

9. Change labels for authentication options
   a. Advanced > Code tables > Front end > User login
      i. Default.parallel.login.link1
      ii. Default.parallel.login.link2
Implementation steps (4)

10. Other labels to update
   a. Advanced > Code tables > Front end > User login
      i. Default.login.dual.title
      ii. Default.login.title (if not using two auth methods)
      iii. Default.login.error.message
      iv. Default.login.login (text for login submit button)
      v. Default.login.cancel (text for login cancel button)
     vi. Default.login.userid (label used for Alma username field)
     vii. Default.login.password (label used for Alma password field)
## Implementing Shibboleth/SAML

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDP_LOGIN_URL</td>
<td><a href="https://sso.pdx.edu/idp/profile/SAML2/Redirect/SSO">https://sso.pdx.edu/idp/profile/SAML2/Redirect/SSO</a></td>
</tr>
<tr>
<td>IDP_ISSUER</td>
<td><a href="https://sso.pdx.edu/idp/shibboleth">https://sso.pdx.edu/idp/shibboleth</a></td>
</tr>
<tr>
<td>USER_ID_ATTR_NAME</td>
<td>uid</td>
</tr>
<tr>
<td>IDP_LOGOUT_URL</td>
<td><a href="https://sso.pdx.edu/idp/profile/Logout">https://sso.pdx.edu/idp/profile/Logout</a></td>
</tr>
<tr>
<td>SILENT_LOGIN_ENABLE</td>
<td>True</td>
</tr>
<tr>
<td>EMAIL_OVERRIDE</td>
<td>False</td>
</tr>
<tr>
<td>AUTH_BASE_URL</td>
<td></td>
</tr>
<tr>
<td>Certificate File</td>
<td></td>
</tr>
<tr>
<td>Select User Information Method:</td>
<td>ALMA</td>
</tr>
<tr>
<td>USER_INFO_URL</td>
<td><a href="http://na01">http://na01</a>. Alma.exlibrisgroup.com</td>
</tr>
</tbody>
</table>
Implementing Shibboleth/SAML (2)

1. Update settings
   a. Note about auth_base_url setting
2. Upload certificate file for your Shib server (steps at end of slides)
3. Download metadata
4. Upload metadata to your Shib server (IdP)
   a. Note about Incommon participation
5. Test!
Steps for downloading shib cert

1. Navigate to the sign-in page for your shib server.
2. Click the padlock icon in the FF url bar.
3. Click the right-hand arrow to get into the details.
4. Click More Information
5. Click View Certificate
6. Click the Details tab
7. Click the Export... button
8. Save the .pem file to your local drive.
9. When you open it up, it should be a LONG string of characters and numbers starting with -----BEGIN CERTIFICATE----- and ending with -----END CERTIFICATE-----.. For instance, mine was 48 lines in total.