Logout Config

Overview

This page discusses options for logging a user out of your application and out of the MyAccess Shibboleth Single Sign-On service, and how to configure them on the Service Provider side.

Options

There are a few options for logging a user out of a Shibboleth Service Provider (SP), and out of the MyAccess Single Sign-On service itself. Before we discuss too much detail, it is important to understand that Shibboleth does not implement the concept of "global sign out", meaning, there is no way to log out of all applications to which you have signed onto during your Single Sign-On session. Well, actually there is **one** way: to quit your browser. Since quitting your browser is not usually a feasible option given how most users use tabs and have multiple pages open at once, we will discuss ways to log a user out of your application and out of the Single Sign-On service.

Local, Service Provider Logout

Most applications have a concept of logout/signout. Logging out of an application accomplishes two thing:

- Cleaning up the session (and thereby freeing up memory for the application)
- Preventing the user (or someone else) from entering the application again (using the same browser) without having to log in again

If you wish to accomplish either of these things, you should continue to provide a logout link on your application once it has been Shibbolized.

Along with logging the user out of your application, you also need to log the user out of the Shibboleth Service Provider. If you are using `shibd` for either Linux or Windows, the way to accomplish this is to send the user the following URI on your

```
host:/Shibboleth.sso/Logout
```

By doing this you are instructing the `shibd` process to end the local Shibboleth session for the user. At this point, the user is now logged out of your application and out of the Shibboleth Service Provider (`shibd`).

IdP Logout

The MyAccess Single Sign-On service also provides a means for logging the user out of the Single Sign-On service itself. To do this, after you have logged the user out of the application and the Shibboleth Service Provider, you should send the user to the IdP logout page. The best way to do this is to add the SingleLogoutService code below to the in the MyAccess metadata file (put it in the IDPSSODescriptor section, just before the end of that section) which you configured for your SP. For production this line looks like this (for test/stage, change dp.ucsf.edu to idp-stage.ucsf.edu):

```
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
    Location="https://dp.ucsf.edu/idp/pre_logout.jsp"/>
```

Once this code is added, whenever a user is sent to /Shibboleth.sso/Logout, the user will be redirected to the "Location" listed. The MyAccess IdP pre logout and logout pages also accept a url= parameter, so if you wish to provide a link to the user that they can use to return to your application, you can do so. For instance:

```
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
    Location="https://dp.ucsf.edu/idp/pre_logout.jsp?url=https://wiki.ucsf.edu/"/>
```

The above "Location" directive provides a link back to the Library Wiki. Below is an image of what this looks like to the user.

If you download the IdP Metadata from the links on the main MyAccess page, the above sections are already provided for you, and you just need to uncomment the one of your choice.

Pre-logout

If you notice in the code samples above, the page to which you redirect the user is a pre-logout page. This page gives the user the following options:

Go to MyAccess application list
Log out of MyAccess
Do nothing

This pre-logout page was developed to give users the opportunity to just log out of their application, and not log out of Single Sign-On service altogether.

A screenshot of the pre-logout

Logout

Once a user either clicks on "Log out of MyAccess" or leaves the page alone for 3 minutes, the user is redirected to the actual logout page. The two screenshots below show what the user will see if the application did not provide a return URL link, and if the application did provide a return URL link.

Without Return URL

A screenshot of logout page without return URL logout without url

With Return URL

A screenshot of logout page with return URL logout with url