iOS Single Sign-on and custom page workflow:

The custom login page allows clients to implement their own authentication process via a jsp. The jsp can use the client’s existing authentication process as long as it returns a Yellowfin web service token which is then used by the Yellowfin iOS app to sign in.

The workflow is as follows:

The client must firstly create or modify an existing JSP to handle the authentication.

If modifying an existing JSP the client can check for requests specific to the iOS app by checking that the mobileSSO parameter is not null and is set to true.

This can be done using:

if (request.getParameter("mobileSSO") != null) {

//is mobile SSO

}

The mobile app will also pass the mobileUsername, mobilePassword and mobileOrg

parameters to the JSP which are the username, password and org ref from the connection profile in the iOS app.

This custom JSP can present the user with an interface, two factor authentication, client org selection or other client created process.

The JSP can also load other URLs if needed.

Once the client’s sign-in process is completed and the user is authenticated, they can be signed into Yellowfin using the webservice call to “LOGINUSER” or “LOGINUSERNOPASSWORD”  which returns a Yellowfin webservice token.

To then return this webservice token to the Yellowfin server, call the URL

yfj2o://yftoken=token where token is the webservice token.

The best way to do this is to call a javascript bridge with an iFrame that loads the URL

<script type="text/javascript">

   function callJavascriptBridge(token) {

       var iframe = document.createElement("IFRAME");

       iframe.setAttribute("src", "yfj2o://yftoken=" + token);

       iframe.setAttribute("height", "1px");

       iframe.setAttribute("width", "1px");

       document.documentElement.appendChild(iframe);

       iframe.parentNode.removeChild(iframe);

       iframe = null;

   };

</script>

The client can also display errors on the custom JSP or if they want to return the user to the main section of the app with an error they can call yfj2o://yferror= with url encoded text such as There%20was%20an%20error

Once the iOS app has the webservice token it will then use this to sign into the Yellowfin server.

If the user’s connection times out or they chose the login option they will then be redirected back to the custom JSP to once again sign in.

Then to activate to custom SSO process the client must then insert a row pointing to their own custom JSP in their Yellowfin configuration table using the following sql command:

INSERT INTO Configuration (IpOrg, ConfigTypeCode, ConfigCode, ConfigData) values (1, 'SYSTEM', 'MOBILE\_SSO\_LOCATION', '[http://my.yellowfininstnace.com/customMobileSSO.jsp](http://10.10.0.10:8080/yellowfin71/mobileSSO/mobileSSOExample.jsp)')

I have created two different JSP examples to show this process which can be found in development/examples/mobileSSO