APS Sample App

**Description:**

Simple .JSP application that may help POC the APS side of PingOne, demonstrates both login and the admin SSO setup widget.

Consists of four pages:

Index.jsp

Sample landing page. Picture this as the existing login page for the application. Users have options to either login manually or use SSO to login.

Manually login just uses the querystring to send over a user. SSO launches the SSO process through PingOne.

Admin.jsp

Sample administration page. Provides the widget to enable admin’s to auto-configure SSO without the app provider having to do a thing.

Login.jsp

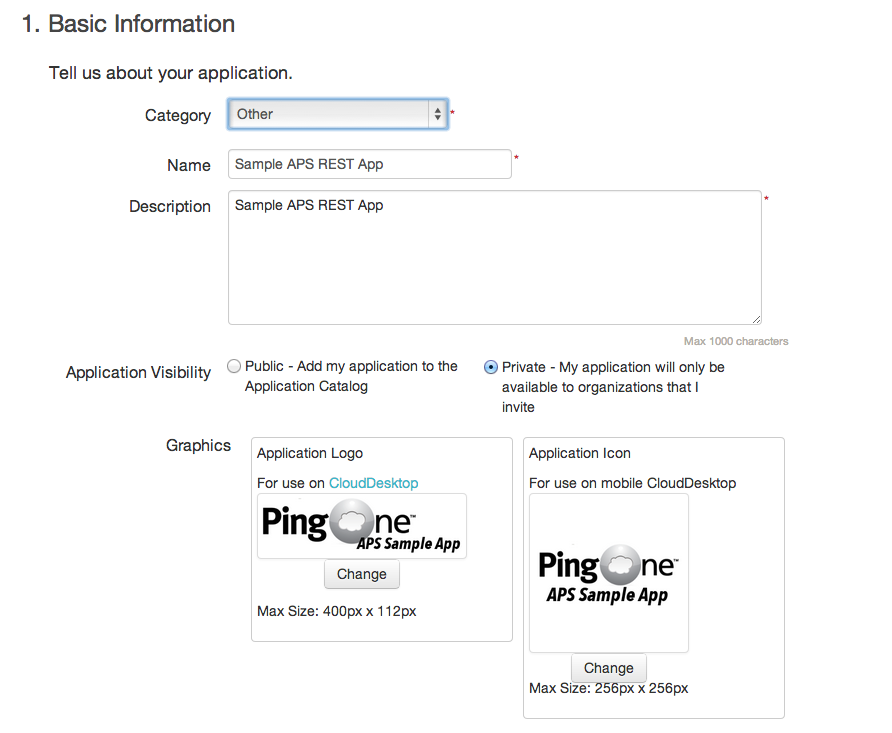
Sample post-authentication page. Will dump all the attributes received from the SSO token.

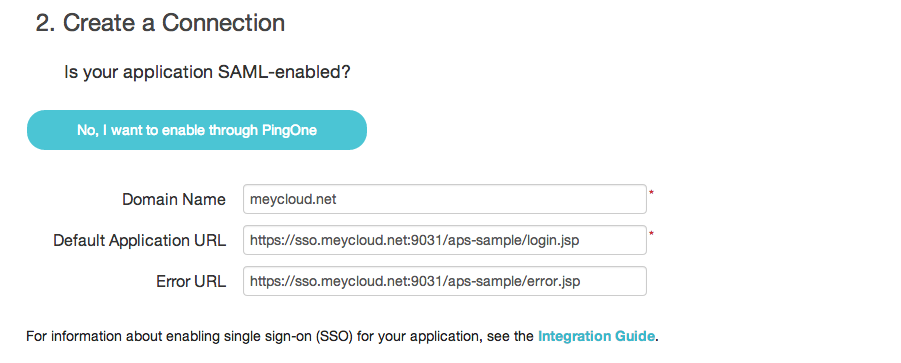
Error.jsp

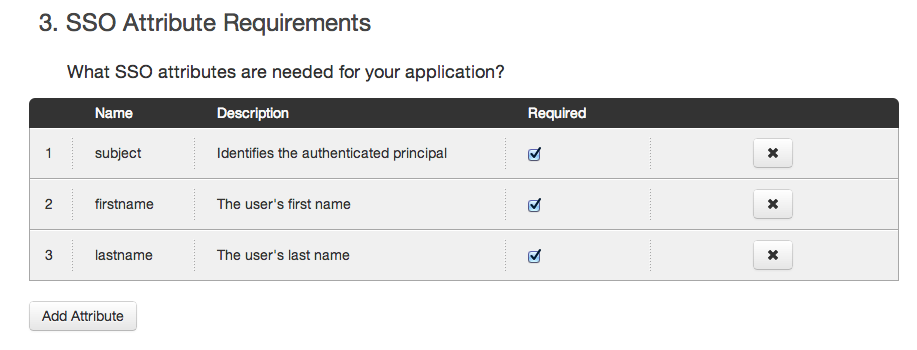
Displays any errors that occur during the process.

**Installation:**

1. Unzip the aps-sample.zip to your PingFederate server’s default/deploy folder.
2. Create a new Application in your PingOne APS instance







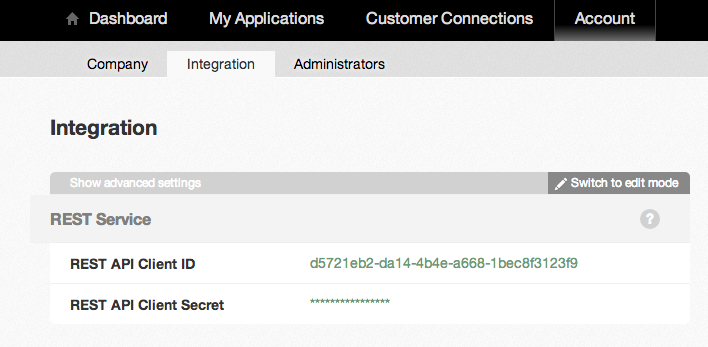


1. Copy the SaaS ID from the application name:



For this example, the SaaS ID is: c95b5a2a-ebef-4be3-b70a-8a10d925470a

1. Take note of your PingOne APS REST Username and Password:



1. Create a customer connection to a PingOne CAS customer. Review the https://admin.pingone.com/web-portal/connections/integrate url for directions for performing this step.

If sending an Email, note the idpid you assign to the customer.

If using the self-service widget, modify the admin.jsp page to specify a customer id.

1. Modify the .JSP files with the appropriate values:

Index.jsp

Look for the line:

<p>Click the <a href="https://sso.connect.pingidentity.com/sso/sp/initsso?saasid=c95b5a2a-ebef-4be3-b70a-8a10d925470a&idpid=pm-test-sso">SSO Initiation link</a> to begin an SSO transaction</p>

Change the saasid parameter to your saasid gathered in step 3 above.

Change the idpid parameter to your sample customer connection idpid created in step 5 above.

Login.jsp

Change the following lines:

final String REST\_USERNAME = "d5721eb2-da14-4b4e-a668-1bec8f3123f9";

final String REST\_API\_KEY = "REST\_API\_KEY";

To match your REST Username/Password (Step 4 above).

Admin.jsp

Look for the lines:

// Replace me! See the sample code README in your download

openToken : '<%=writeToken("pm-test-sso", "pmeyer+cas@pingidentity.com")%>',

saasId : 'c95b5a2a-ebef-4be3-b70a-8a10d925470a',

accountId : '450c9d23-6b97-4edb-b969-1346f3a46c71',

Update with the values appropriate for your instance. You can find the saasid and accountid from this page: https://admin.pingone.com/web-portal/connections/integrate/javascript

1. Test. Hit https://<server>/aps-sample then click the “SSO Initiation link” option. This will redirect you through PingOne to your CAS connection, then back to the login.jsp with the authenticated users details.