Leverage OpenID Connect and Inbound Federation for Custom Branding Requirements

Okta Inc.
301 Brannan Street
San Francisco, CA 94107

Vishal Rohilla
Sr. Solutions Architect

Background:

Various Okta customers have been leveraging OpenID Connect capabilities from Okta for application integration and single sign on. The customer requirements are brand specific and focused on seamless user experience. Various customers have applications are across various departments, and business units accessed by employees, partners and customers. The common requirement is to leverage OpenID Connect and have a single point of entry for authentication. The requirements span from having a single login page across the organization for all the applications, to multiple login pages either per application or per customer.

The following article explains the mechanics of how to set up Okta to accomplish both Single login page and multiple login pages in a tenant.

Objectives:

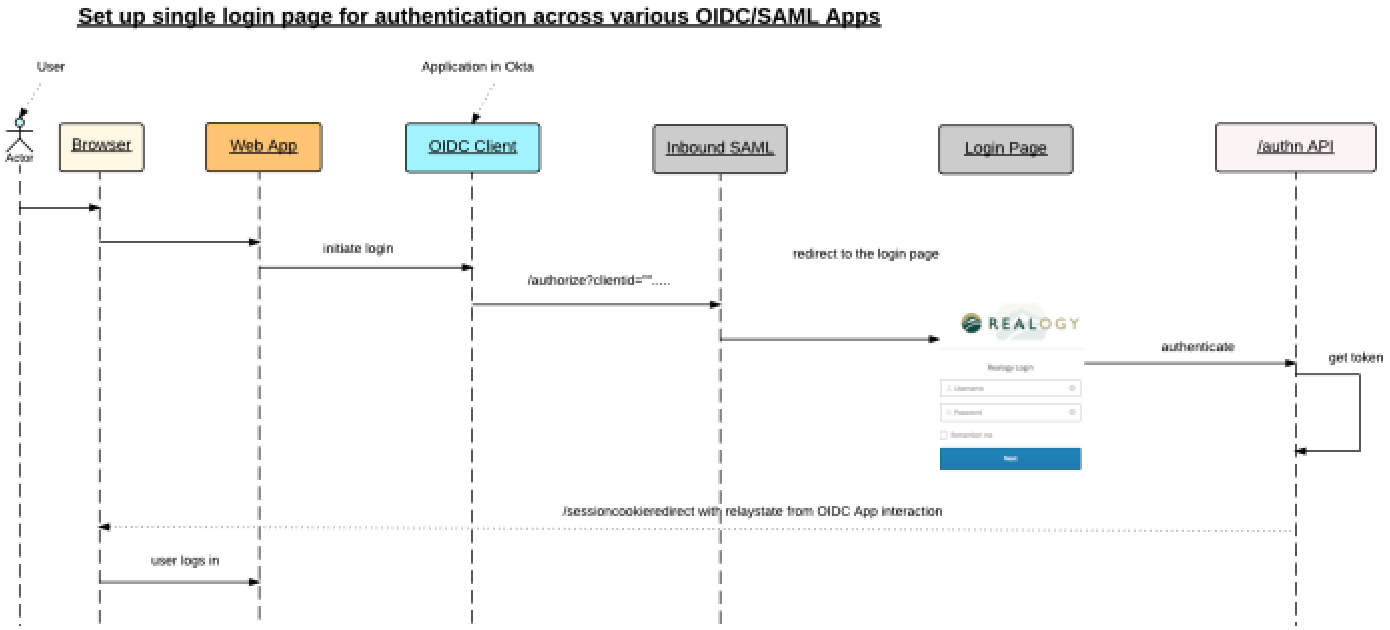
This document outlines steps on how to set up Okta to redirect the request from various OIDC clients to a various login pages for various applications out of an Okta Tenant.

Set up Okta to redirect to a custom login page for all the apps in the current Okta Tenant.

Common requirements:

1. Need for many web apps in place to authenticate users from Okta.
2. The web apps leverage OIDC/SAML protocols for authentication.
3. The requirement is to have a single front door (login entry/page) for the users.
4. Each of the application will initiate login process and the user needs to fall on the same login page.
5. Authenticate and gets redirected back to the app specific landing page.

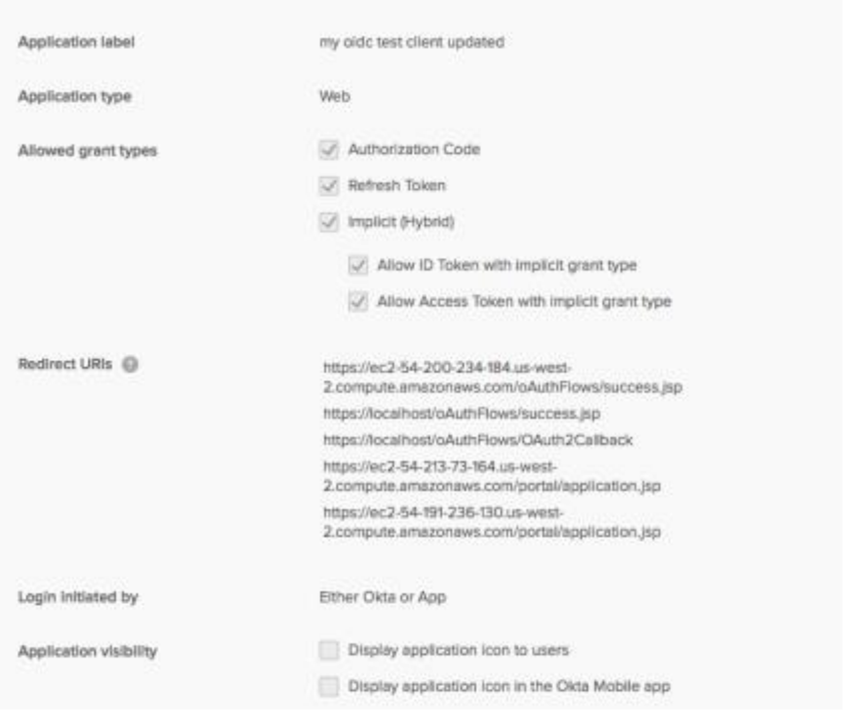
Flow Diagram –



Set up single login page for authentication across various OIDC/SAML Apps

Steps to be taken in Okta: -

1. Set up an OIDC Client. The following link has the details on how to setup and OIDC Client https://support.okta.com/help/Documentation/Knowledge_Article/Using-OpenID-Connect
2. The client gives you the client specific client_id.
3. Also, the client supports various redirect URIs (app specific). Please see the picture.

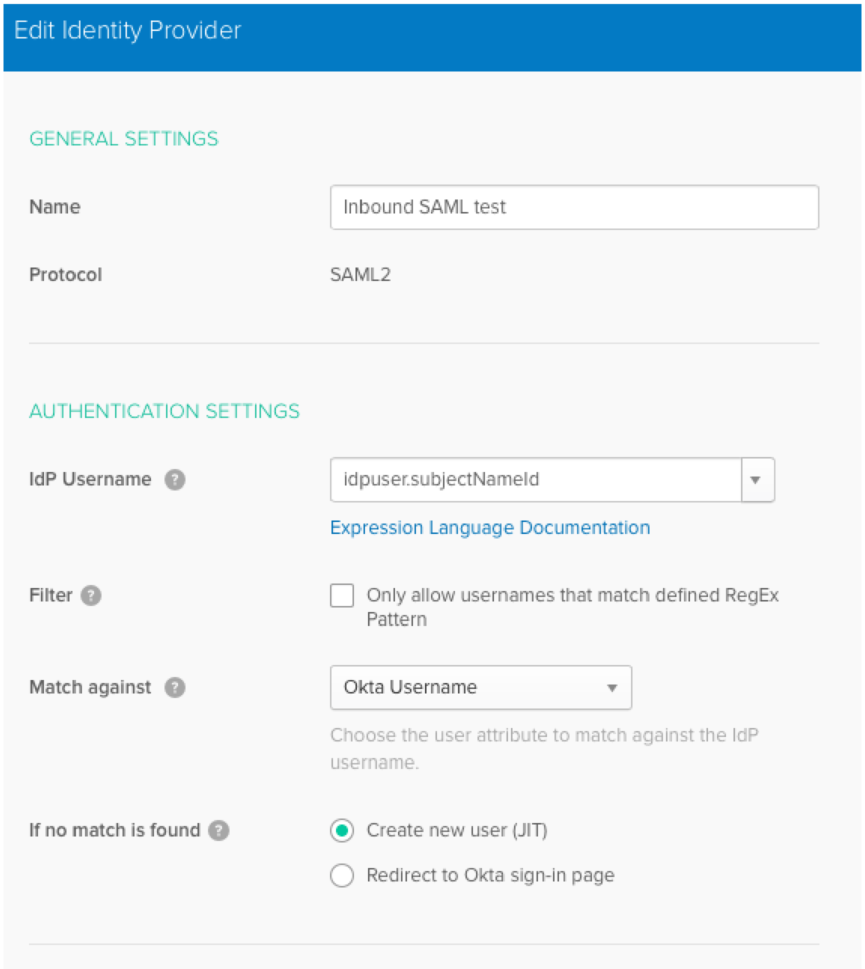


Application label	my oidc test client updated
Application type	Web
Allowed grant types	☑ Authorization Code ☑ Refresh Token ☑ Implicit (Hybrid) ☑ Allow ID Token with implicit grant type ☑ Allow Access Token with implicit grant type
Redirect URIs	https://ec2-54-200-234-184.us-west-2.compute.amazonaws.com/oAuthFlows/success.jsp https://localhost/oAuthFlows/success.jsp https://localhost/oAuthFlows/OAuth2Callback https://ec2-54-213-73-164.us-west-2.compute.amazonaws.com/portal/application.jsp https://ec2-54-191-236-130.us-west-2.compute.amazonaws.com/portal/application.jsp
Login initiated by	Either Okta or App
Application visibility	□ Display application icon to users □ Display application icon in the Okta Mobile app

4. Set up Inbound SAML in Okta to redirect the user to the custom login page. This is needed for Okta to redirect the user to the default login page irrespective of the application that initiates the login.

   Add Identity Provider from Security → Identity Providers. (screenshots attached)

5. Following is the sample configuration of the identity provider, it is suggested to keep various values as is.



Edit Identity Provider

GENERAL SETTINGS

Name: Inbound SAML test

Protocol: SAML2

AUTHENTICATION SETTINGS

IdP Username: idpuser.subjectNameId

Expression Language Documentation

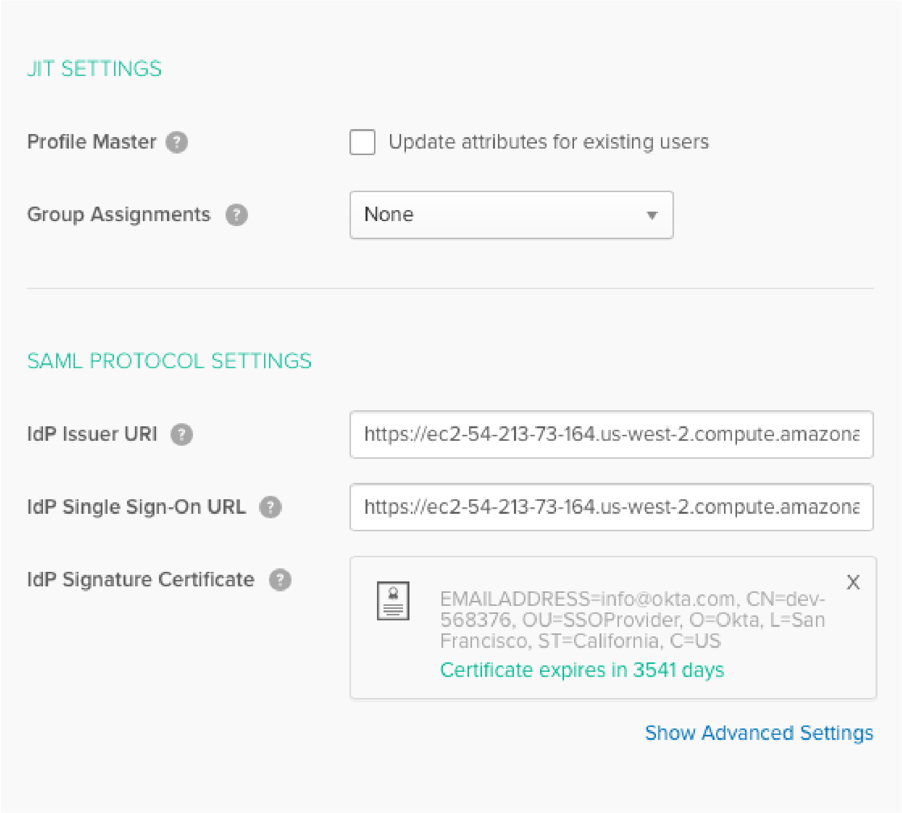
Filter: □ Only allow usernames that match defined RegEx Pattern

Match against: Okta Username

Choose the user attribute to match against the IdP username.

If no match is found: ● Create new user (JIT) ○ Redirect to Okta sign-in page

6. The following steps are key, enter the url of the hosted login page in both Issuer URI and the Single-Sign On URL (this could be Okta sign in widget hosted on the web server in your infrastructure). Also upload the cert, this could be an Okta cert downloaded from any SAML app config on your Okta environment. (The cert is needed to save the configs)



JIT SETTINGS

Profile Master ? □ Update attributes for existing users

Group Assignments ? None ▾

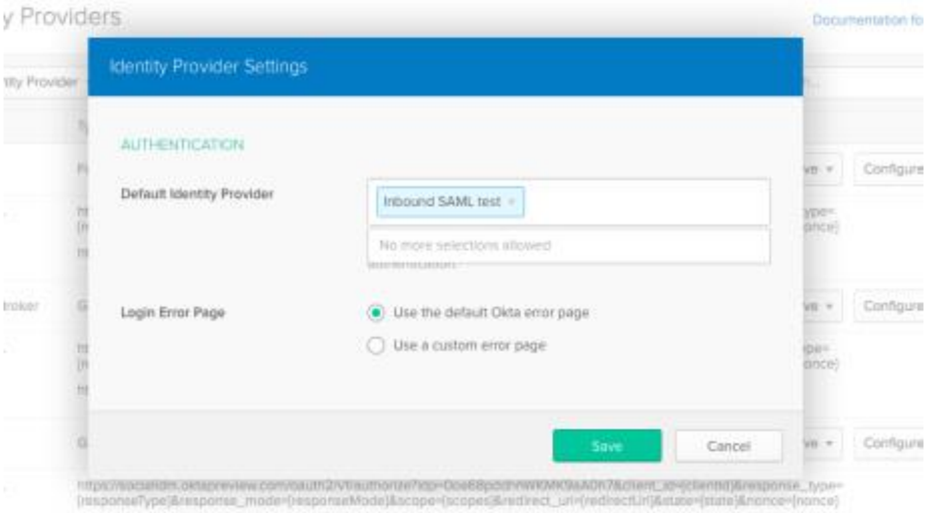
SAML PROTOCOL SETTINGS

IdP Issuer URI ? https://ec2-54-213-73-164.us-west-2.compute.amazona

IdP Single Sign-On URL ? https://ec2-54-213-73-164.us-west-2.compute.amazona

IdP Signature Certificate ? EMAILADDRESS=info@okta.com, CN=dev-568376, OU=SSOProvider, O=Okta, L=San Francisco, ST=California, C=US
Certificate expires in 3541 days

7. No changes to the advanced settings is needed.
8. Make the IDP as the default IDP



Identity Provider Settings

AUTHENTICATION

Default Identity Provider: Inbound SAML test ×
No more selections allowed

Login Error Page
● Use the default Okta error page
○ Use a custom error page

9. Let’s take an example app of the OIDC authentication and the routing. The following is the sample URL for the OIDC app https://socialidm.oktapreview.com/oauth2/v1/authorize?client_id=2ZZowgKy6rzwXyXfJMZp&response_type=id_token&scope=openid&redirect_uri=https%3A%2F%2Fec2-54-213-73-164.us-west-2.compute.amazonaws.com%2Fportal%2Fapplication.jsp&state=Af0ifjslDkj&nonce=n-0S6_WzA2Mj

10. Once the OIDC app hits the above URL, the user will get redirected to the login page that we set up in the identity provider tab.

11. Leverage a browser plugin to look at the relaystate. It will be something like –

    %2F%2Foauth2%2Fv1%2Fauthorize%2Fredirect%3Fokta_key%3DEDLZyIBpzUXAY1piPc56AEyTbFqieXI_TwpSRS22r5k

12. Okta transforms the complete path in the relaystate.
13. Now authenticate the user either via an and use the sessioncookieredirect endpoint with relaystate as the redirectURL. The sample URL is below (redirectURL highlighted in red)–

    https://socialidm.oktapreview.com/login/sessionCookieRedirect?token=20111DjxE9NqhGAxOzOd-BrbBmwE466qUfebFkGpA_jGqmcfOHAWYvF&redirectUrl=%2F%2Foauth2%2Fv1%2Fauthorize%2Fredirect%3Fokta_key%3DSN3XbOoLzNrOYzDNAIoWc4HpjpW_mbMj557ILkldc7g

14. One can also leverage Okta Sign-in widget to accomplish Step 13.
15. Step 13, will redirect the user back to the actual redirect uri that the OIDC client received as an authentication request.

The above steps can be applied to as many OIDC clients to accomplish the need of redirecting to a single login page.

Now let’s extend the above set up to implement more than one login pages.

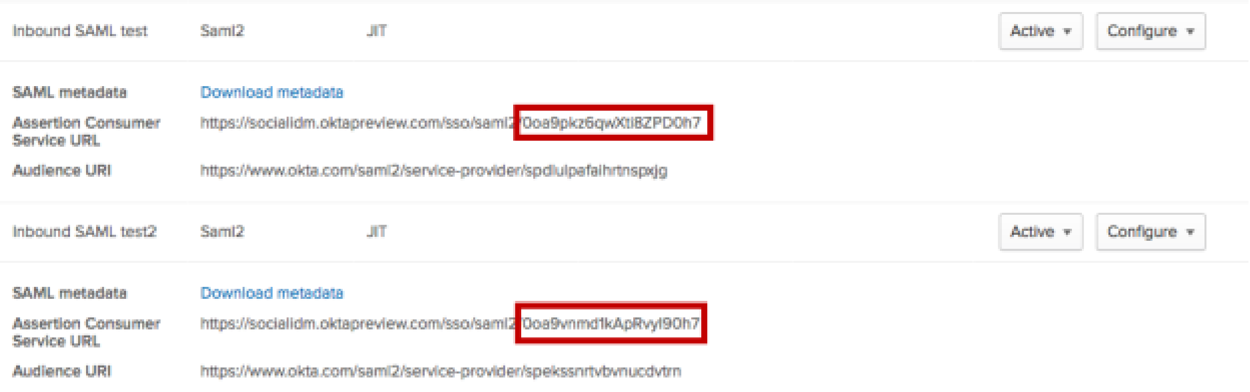
Common Requirements:

16. Need for many web apps in place to authenticate users from Okta.
17. The web apps leverage OIDC/SAML protocols for authentication.

18. The requirement is to have various login pages. The typical business case it to have custom branding for various customers or partners who access to the apps out of the Okta tenant.
19. Each of the application will initiate login process and the user needs to fall on the customer specific, custom branded login page.
20. Authenticate and gets redirected back to the app specific landing page.

Steps to be taken in Okta: -

21. Set up a SAML IDP in the Okta tenant. The IDP will redirect the user to the customer specific login page. Hypothetically, if there are 3 customers who need to have a custom branded login page, then set up 3 SAML IDPs.
22. Refer the steps 4 to 7 to set up the SAML IDP.
23. Please note the highlighted alphanumeric characters. It is the unique identifier of the IDP in the Okta tenant.



Inbound SAML test Saml2 JIT

SAML metadata Download metadata

Assertion Consumer Service URL https://socialidm.oktapreview.com/sso/saml2/0oa9pkz6qwXtl8ZPD0h7

Audience URI https://www.okta.com/saml2/service-provider/spdlulpafalhrtnspxjg

Inbound SAML test2 Saml2 JIT

SAML metadata Download metadata

Assertion Consumer Service URL https://socialidm.oktapreview.com/sso/saml2/0oa9vnmd1kApRvyl90h7

Audience URI https://www.okta.com/saml2/service-provider/spekssnrtvbvnucdvtrn

24. Refer Step 9, the authentication initiation URL for the OIDC Client, add the idp identifier highlighted in red.

    https://socialidm.oktapreview.com/oauth2/v1/authorize?idp={identifier}&client_id=2ZZowgKy6rzwXyXfJMZp&response_type=id_token&scope=openid&redirect_uri=https%3A%2F%2Fec2-54-213-73-164.us-west-2.compute.amazonaws.com%2Fportal%2Fapplication.jsp&state=Af0ifjslDkj&nonce=n-0S6_WzA2Mj

25. Step 24, will initiate the login to the OIDC client, and redirect the user to the custom login page set up for the specific IDP.
26. Upon authentication, the user will get redirected back to the app specific landing page.

27. The client application that initiates the login will need to associate the idp identifier to the specific customer.
28. There are APIs @ http://developer.okta.com/docs/api/resources/idps.html can help the external app automate the creation of the IDP and retrieving the IDP specific unique identifier.

This concludes the steps to set up a common login page or many login pages in an Okta Tenant depending on the requirements.