Single Sign On using SAML Authenticators in Weblogic Server

Steps to configure SAML Identity Asserter

1. Login to Weblogic console
2. Click on ‘Security Realm’
3. Open the Realm created for your application
4. Click on ‘Providers’
5. Click on ‘New’
6. Provide Authenticator name and type as ‘SAML2IdentityAsserter’

Steps to configure Service Provider

1. Login to Weblogic console
2. Click on **Servers-Admin Server-Federation Services-SAML 2.0 Service Provider**
3. Check ‘Enabled’
4. Check ‘POST Binding Enabled’
5. Provide Demantra App Default URL
6. Save the SP
7. Navigate to **Servers-Admin Server-Federation Services-SAML 2.0 General**
8. Check ‘Replicate Cashe Enabled’
9. Published site url https://<host-name>:<port>/saml2
10. Provide entity ID ex : SAML2\_Agile\_SP\_Destination
11. Check ‘Recepient Check Enabled’
12. Click Publish Metadata, save the xml file
13. Provide the above file to IAM team

Steps to configure Identity Provider Metadata in SAML Service Provider at destination

1. Login to Weblogic admin console
2. Click on Security Realm-‘<App> Realm’-Providers-Authentication-<Already Configured SAML Identity Asserter>-Management-New- New Web Single Sign On Identity Provider Partner
3. Select Identity Provider Metadata which is xml file
4. Click OK
5. Click on Web SSO which is created
6. Click on ‘Enabled’
7. Uncheck ‘Virtual User’
8. Add App specific URI in ‘Redirect URIs section ex: /Agile/\*

Configuring the Authenticator Order

1. Login to Weblogic admin console
2. Click on Security Realm-‘<App> Realm’-Providers-Authentication
3. Click on ‘Reorder’
4. Make sure SAML Identity Asserter need to be Immediately after ‘Trust Service Identity Asserter’
5. After this all other authenticators specific to application will be placed