# **Setting EBX to support SAML 2.0 SSO**

Configuring SSO with EBX, requires that we provide a URL that users will use to access EBX. The URL will redirect the access request to a IDP server that will manage the Authentication into EBX.

If the user is already logged in (to the IDP server) the IDP server will post a response to EBX with a SAML payload that will contain the user information.

EBX/SSO implementation will verify that the “post response” came from the correct IDP server and not another IdP server trying to spoof the authentication process.

If the SAML response is valid the user will be logged into EBX - a login page would not be presented to the user. If the response is invalid or the user is not defined on the IDP server the user will be requested user credentials through the EBX login page.

For EBX to do its part a few things need to be configured on the IdP Server so that it recognizes requests from EBX for authentication.

The following outlines the details required for configuration SSO Support within EBX.

## Customer Details

The following configuration details are need by the customer’s SSO Administrator.

1. EBX needs to be configured in the IdP server with support for SAML 2.0.
2. User credential to authenticate with the IDP server, for testing.
3. An IdP URL for redirecting users for authentication that support SAML 2.0
4. A SAML Issuer ID.
5. A 509 certificate that we use to validate the responses from The IdP Server as a file.
6. Attributes names for: email, first name and last name

## EBX Configuration Details

1. Tomcat server.xml need to be updated and have this value on the connector for http:
   1. **maxHttpHeaderSize="65536"**
2. Add the “ps-sso-auth” application to the EBX Server
   1. Pull the project into the workspace from Bitbucket.
   2. Build and export as a war file
   3. Deploy on tomcat by copying the war file to [Catalina.base]\webapps folder
   4. Customer should use the following URL to access EBX:
      1. HTTP[S]://[host name]:[port number]\[war file name]\ebxSSO
3. Edit the ebx.properties and set the following properties there are more details in the doc folder of the project in the ebx\_sso\_saml\_configuration.properties file:

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Value** | **Description** |
| ebx.directory.enableSSO | true/false | Enable SSO |
| ebx.directory.SSOClass | A class name | Class used to process SSO requests |
| ebx.directory.sso.ebxurl | HTTP[S]://[host name]:[port number]/ebx/ | EBX Server URL, note the forward slash, “/”, at the end of the URL is very important. |
| ebx.directory.sso.saml.samlresponseelementname | SAMLResponse | The header parameter from which the SAML payload will be placed. In case the IdP server returns the SAML payload under a different http header parameter this parameter can be used to modify the header parameter name. Default: SAMLResponse |
| ebx.directory.passwordencrypted | true/false | If this property is true all passwords in ebx.properties related to LDAP and SSO will expect an encrypted value.  <TBD> – Encryption Process |
| ebx.directory.sso.idp.url | IdP server URL | IdP server URL where we can redirect USERS that accept SAML authentication requests. |
| ebx.directory.sso.idp.isjksfile | true/false | Are certificates stored in a file or each file is one certificate. |
| ebx.directory.sso.idp.jkspassword | password | Encrypted password if ebx.directory.passwordencrypted=true or clear text.  The password to load certificates from a JKS file |
| ebx.directory.sso.idp.certificate.alias | Alias name | If certificate stored in a JKS file it is associated with an alias. An alias that is used to look up the certificate. |
| ebx.directory.sso.idp.certificate.file | File path | Either the file path to a certificate file or a file path to a JKS file.  The file path used depends on the value set for the “ebx.directory.sso.idp.isjksfile” property. |
| ebx.directory.sso.idp.issuerid | String | Provided by the IdP server Admin.  Used by the IdP server to identify EBX when exchanging authentication information when EBX issues the authentication request to the IdP server.  If this value does not match the IdP server configuration for EBX, the authentication request will be rejected. |
| ebx.directory.sso.saml.user.email | String | The attribute name in the SAML assertion response for the user’s email.  Used by the ps-directory when creating the User Profile in EBX. |
| ebx.directory.sso.saml.user.firstname | String | The attribute name in the SAML assertion response for the user’s first name.  Used by the ps-directory when creating the User Profile in EBX |
| ebx.directory.sso.saml.user.lastname | String | The attribute name in the SAML assertion response for the user’s last name.  Used by the ps-directory when creating the User Profile in EBX |
| ebx.directory.sso.idp.nameid.policy | string | Default – “persistent” |
| ebx.directory.sso.sp.issuerid | string | Service provider issue id. This can be any value as long as this property and the IdP server have the same value. |