Skills DB Pro©
Skills Management Made Easy

IDP Initiated Single Sign On - SAML Version 2.0

Quick Instructions:
1. Edit your setting below.
Add User Deny-denies a new user from registering in the system if they are not already in the system. Otherwise any new user passing validation will be brought to a new user registration screen.
2. Upload your public x509 certificate.
3. Either download the meta file for your Identity Provider or use the information below to manually set up your IDP.

Enable & Setup Saml Single Sign On						
#	Enable Saml 2.0?	Test Mode	Add User Deny	Identity Provider Login URL	Certificate Name	Expiration
Edit				http://skillsdbpro.com	1_SAP.cer	10/29/2110 2:36:47 PM

Upload your Identity Provider Public Certificate - Allowed File Extension:(.cer)

Browse...

Upload

Identity Provider Setup Information

Service Provider Metadata	Download Metadata File
Entity ID	http://SkillsDBPro.com
Assertion Consumer Service URL:	https://skillsdbsandbox.azurewebsites.net/modServiceProvider/ConsumerService.aspx?TempCompID=1 Example URL - Please login and use yours.
Assertion Method:	HTTPS Post
Assertion Signed	Yes (with your uploaded public key)
Request Signature Method	RSA-SHA1
Assertion Encryption Key:	N/A
SAML Identity Type*	Email address of user. This is the unique system identifier.
SAML Identity Location	Identity is in the NameIdentifier element of the Subject statement

UserID Mapping
Skills DB Pro uses email address in the Subject.NameId.NameIdentifier to map users from other security domains to Skills DB Pro. If your system cannot use the email address in the Subject.NameId.NameIdentifier you will need to add an AttributeStatement in the SAML Response; with Name/Friendly name as "EmailAddress". The AttributeStatement should follow the AuthnStatement. Here is a XML snippet as example:

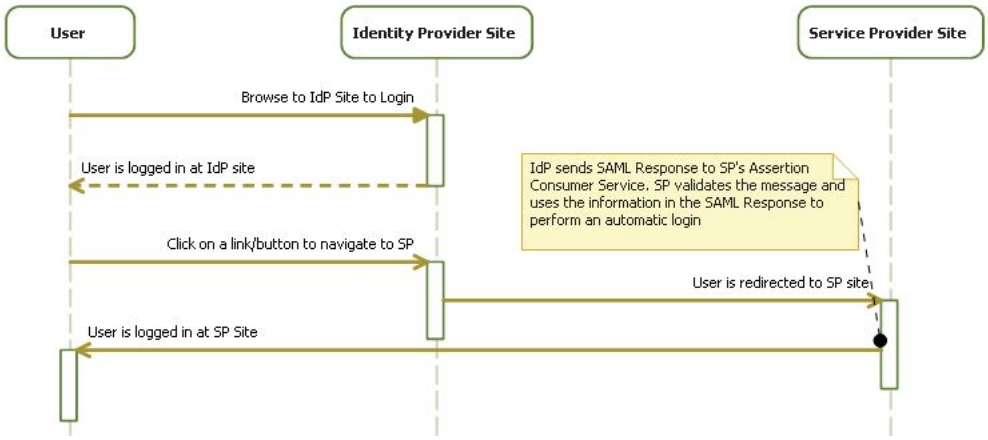
```
<saml:AttributeStatement>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
          Name="EmailAddress">
          <saml:AttributeValue xsi:type="xs:string">user@domain.com</saml:AttributeValue>
        </saml:Attribute>
</saml:AttributeStatement>
```

Other Attributes-For just in time provisioning of your people .

Attribute	Type	Max Len	Required	Notes
LastName	nvarchar	100	No	
FirstName	nvarchar	100	No	
YourPersonID	nvarchar	40	No	Refers to your employee id from another system.
GroupId	int	4	No	User Security Level 1=Default if not provided 1=Self 2=Expert 4=Manager 5=Executive 7=Admin

Skills DB Pro Single Sign-On Workflow

We use an IdP-Initiated SSO scenario, a user logs on to the IdP site and attempts to access a resource on the SP site.



Processing Steps:

1. A user browses to the IdP site
2. The IdP site will ask the user to provide his/her credentials if he or she is not logged in
3. After the user has logged in, he or she clicks on a link/button to navigate to the SP site. (Some sites may navigate the users automatically)
4. At this point, the IdP sends SAML Response containing the authentication assertion and any additional attributes to the SP's Assertion Consumer Service.
5. The SP validates the message. If the signature and assertion is valid, the SP uses the information in the SAML Response to perform an automatic login.