# Setting up SOBS SAML LOGIN

1) Login to SOBS website using localAccount and enter the following values after enabling SAML:

   *BaseDomain:* http://adfs.xxxxxx.edu.au/adfs/services/trust

   *SingleSignOnService:* https://adfs.xxxxxx.edu.au/adfs/ls/

   *SingleLogoutService:* https://adfs.xxxxxx.edu.au/adfs/ls/

   *NameIDFormat:* urn:oasis:names:tc:SAML:2.0:nameid-format:transient

   Upload the ADFS Token Signing Certificate from the ADFS server, the Base64 version.

2) Click on Generate metadata for IDP.

3) Import the above generated metadata file on your ADFS server under ADFS management Relying Party Trusts

4) Once imported, right click on that Relying Party Trust you have created and click on Edit Claim rules.

5) Click on Add rule and Select "Send Claims using a Custom Rule"
   1. Claim rule name: NameIDFormat
   2. Under Custom rule paste the following value:

      c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"]
       => issue(Type =
      "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
      Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value,
      ValueType = c.ValueType,
      Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimpropertie
      s/format"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient");

6) Add another rule and Select "Send LDAP Attributes as Claims"
1. Claim rule name: LDAP values
2. Select Attribute Store: Active Directory
And select the following LDAP attributes values and match it against the values on the right (Note: Right side values are case sensitive).

Claim rule name:

LDAP rules

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

| | LDAP Attribute (Select or type to add more) | | Outgoing Claim Type (Select or type to add more) | |
|---|---|---|---|---|
| ▶ | SAM-Account-Name | ∨ | User-Name | ∨ |
| | E-Mail-Addresses | ∨ | mail | ∨ |
| | Given-Name | ∨ | givenName | ∨ |
| | Surname | ∨ | Surname | ∨ |
| * | | ∨ | | ∨ |

View Rule Language...          OK          Cancel

7) Add an additional rule so that staff who are logging in for the first time will be configured with the SOBS security level of "Staff"

Add another custom Claims rule and using:

```
=> issue(Type = "Role", Value = "Staff");
```