Enabling Federated SSO to Service-Now using Oracle Identity Federation (OIF)

In this integration Oracle Identify Federation (OIF) is the Identity Provider (IdP) and Service-Now is the Service Provider.

Service-Now settings:

Obtain the OIF IdP meta. This can be downloaded from the OIF console, but you can also obtain the federation meta data at the following URL:

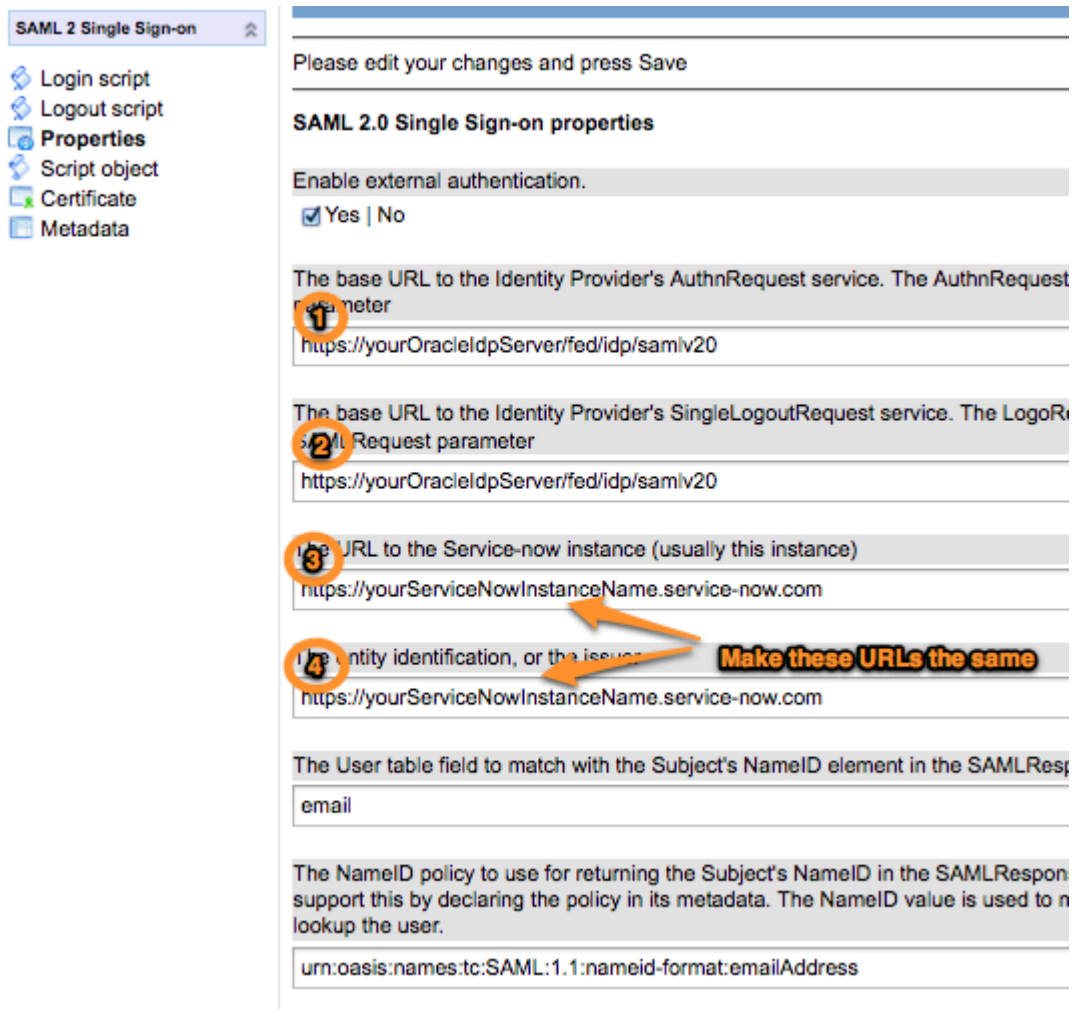
http://yourserver.com/fed/idp/metadata

From the Oracle IDP Metadata, look for:

1) SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect". Take the "Location" attribute and use it for our AuthnRequest service url
2) SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect". Take the "Location" attribute and use it for our SingleLogoutRequest service url

Put the Locations attribute values into positions (1) and (2) in the SAML properties as seen in the screenshot below.

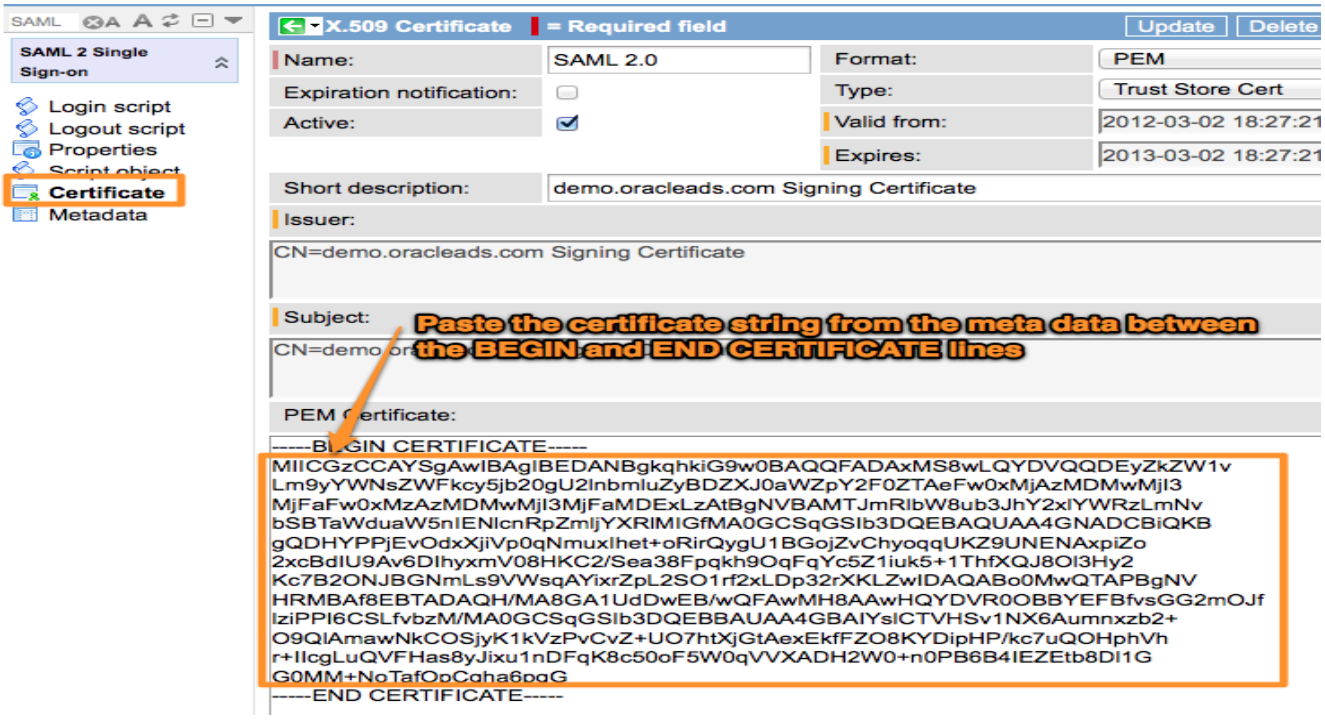
Change properties (3) and (4) (see the screen shot below) to be the ServiceNow instance URL that you are configuring. They will both need to be the same URL in this configuration. (Some instances have property (3) appended with "/navpage.do". Do not include that for this configuration).



From the Oracle IDP Metadata, look for the X509Certificate under the <md:KeyDescriptor use="signing"> section.

<md:EntityDescriptor ID="id-RnFY8rvc-e9i6SMiFlgLNKqJF4A-" cacheDuration="P0Y0M30DT0H0M0.0S" entityI
– <md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:
– <md:KeyDescriptor use="signing">
– <dsig:KeyInfo>
– <dsig:X509Data>
– <dsig:X509Certificate>
MIICGzCCAYSgAwIBAgIBEDANBgkqhkiG9w0BAQQFADAxMS8wLQYDVQQDEyZkZW1v Lm9y
MjFaFw0xMzAzMDMwMjI3MjFaMDExLzAtBgNVBAMTJmRlbW8ub3JhY2xlYWRzLmNv bSBTaW
gQDHYPPjEvOdxXjiVp0qNmuxIhet+oRirQygU1BGojZvChyoqqUKZ9UNENAxpiZo 2xcBdIU9Av6DI
Kc7B2ONJBGNmLs9VWsqAYixrZpL2SO1rf2xLDp32rXKLZwIDAQABo0MwQTAPBgNV HRMBAf8
/wQFAwMH8AAwHQYDVR0OBBYEFBfvsGG2mOJf lziPPI6CSLfvbzM/MA0GCSqGSIb3DQEBBAU
O9QlAmawNkCOSjyK1kVzPvCvZ+UO7htXjGtAexEkfFZO8KYDipHP/kc7uQOHphVh r+IIcgLuQVFH
G0MM+NoTafOpCgha6pgG
</dsig:X509Certificate>
– <dsig:X509IssuerSerial>
<dsig:X509IssuerName>CN=demo.oracleads.com Signing Certificate</dsig:X509IssuerName>
<dsig:X509SerialNumber>16</dsig:X509SerialNumber>
</dsig:X509IssuerSerial>
<dsig:X509SubjectName>CN=demo.oracleads.com Signing Certificate</dsig:X509SubjectName>
</dsig:X509Data>
</dsig:KeyInfo>
</md:KeyDescriptor>
– <md:KeyDescriptor use="encryption">
– <dsig:KeyInfo>
– <dsig:X509Data>
– <dsig:X509Certificate>
MIICITCCAYqgAwIBAgIBIDANBgkqhkiG9w0BAQQFADA0MTIwMAYDVQQDEylkZW1v Lm9yYW

Copy that string and place it between the -----BEGIN CERTIFICATE----- and ----END CERTIFICATE---- strings in the SAML 2.0 Certificate in your ServiceNow Instance as seen below:



Once this configuration is set up, click on the “Metadata” link and copy the metadata to a text editor. Add the following section to your meta data between the <SPSSODescriptor> element and the <SingleLogoutService> element:

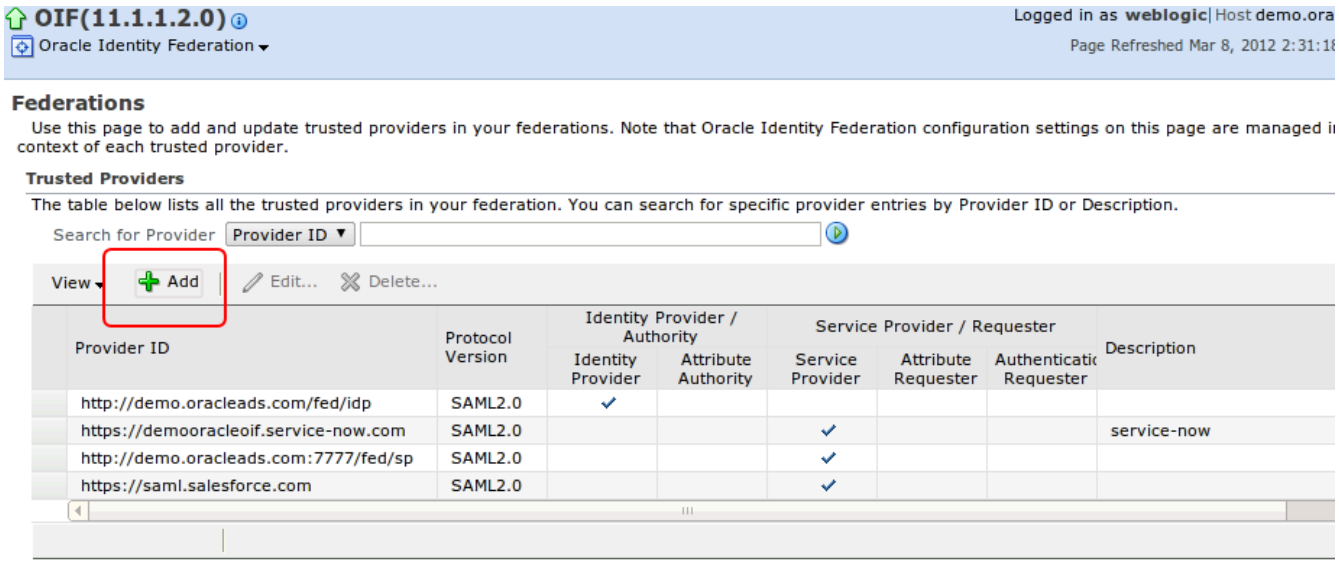
```
   <KeyDescriptor use="signing" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
     <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
       <ds:KeyName>*.service-now.com</ds:KeyName>
       <ds:X509Data xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
         <ds:X509Certificate xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
MIID6TCCAtGgAwIBAgIQaWG5DFrv6VYEv/tPlqZYbDANBgkqhkiG9w0BAQUFADA8
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMVGhhd3RlLCBJbmMuMRYwFAYDVQQDEw1U
aGF3dGUgU1NMIENBMB4XDTExMDcwNDAwMDAwMFoXDTEzMTAwMjIzNTk1OVowgYEx
CzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMRIwEAYDVQQHFAlTYW4g
RGllZ28xGDAWBgNVBAoUD1NlcnZpY2Utbm93LmNvbTETMBEGA1UECxQKT3BlcmF0
aW9uczEaMBgGA1UEAxQRKi5zZXJ2aWNlLW5vdy5jb20wggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQDACla2WcmR3wo3wxJZw/LJJJ9T5hMHmtCD+7Fgnfqy
+cnTeJ0QK7TbjVkkIR6VoDqurZ/vmul0d8RlqaAhdvErEf7zHd5Iv55IIpZVBmr0
iZ7nC0nHi8Zpu+GNxBptAQSmTldB/aiImb8VHItQTcq3qQM+mBGi+WqR31cPugDF
I2+03f+V5xob0nkE3y00I9dqCpjzrRNrIIZUMJGy4pkpXZDzNWyjPN/Bg7FIRjyo
XyLYHMI1ChOIkzq7yFrEgsI0qOo7j5jYX7DZOIAmX2TTvatYCoWqm1C3QrwRHUvI
2bSLdS+iEQp/fkue336btB1N8+VP5Q/Ri9KvHdJCiN1LAgMBAAGjgaAwgZ0wDAYD
VR0TAQH/BAIwADA6BgNVHR8EMzAxMC+gLaArhilodHRwOi8vc3ZyLW92LWNybC50
aGF3dGUuY29tL1RoYXd0ZU9WLmNybDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYB
BQUHAwIwMgYIKwYBBQUHAQEEJjAkMCIGCCsGAQUFBzABhhZodHRwOi8vb2NzcC50
aGF3dGUuY29tMA0GCSqGSIb3DQEBBQUAA4IBAQB9zifSRfQLsQIbFcfrBg9E1R0o
Nx5sco6WHQ3f8v4RrGO4ZAMGnqDlsAjEG88LzQfeVkqcAmsTWxCyCHW0iGWvUbfN
cAHvLdr9VlLmUnz3wg69VgnW+fwppPAyD1L1ZEafESw5eoivkjcQ5DIedjjKwYiI
FjkLngEOORkBhKmyGLlV7nXWG0VmJkDt5xHH5i3rVq1G8sEV743kSLtK/Dugn7Hf
HSYbiyDpHv8EJmFBYtFFYIPUyKOPowaTu2zj9qJz83X5oLulBd6eLZfaAgsjZ/Rb
1MTfRzgI2mur/IiTx9KL7Ymg+NJm7y7/wb1Fy438OwBANG6VrJUJqjxyYR/a
</ds:X509Certificate>
       </ds:X509Data>
     </ds:KeyInfo>
   </KeyDescriptor>
```

Your resulting Metadata will look like:

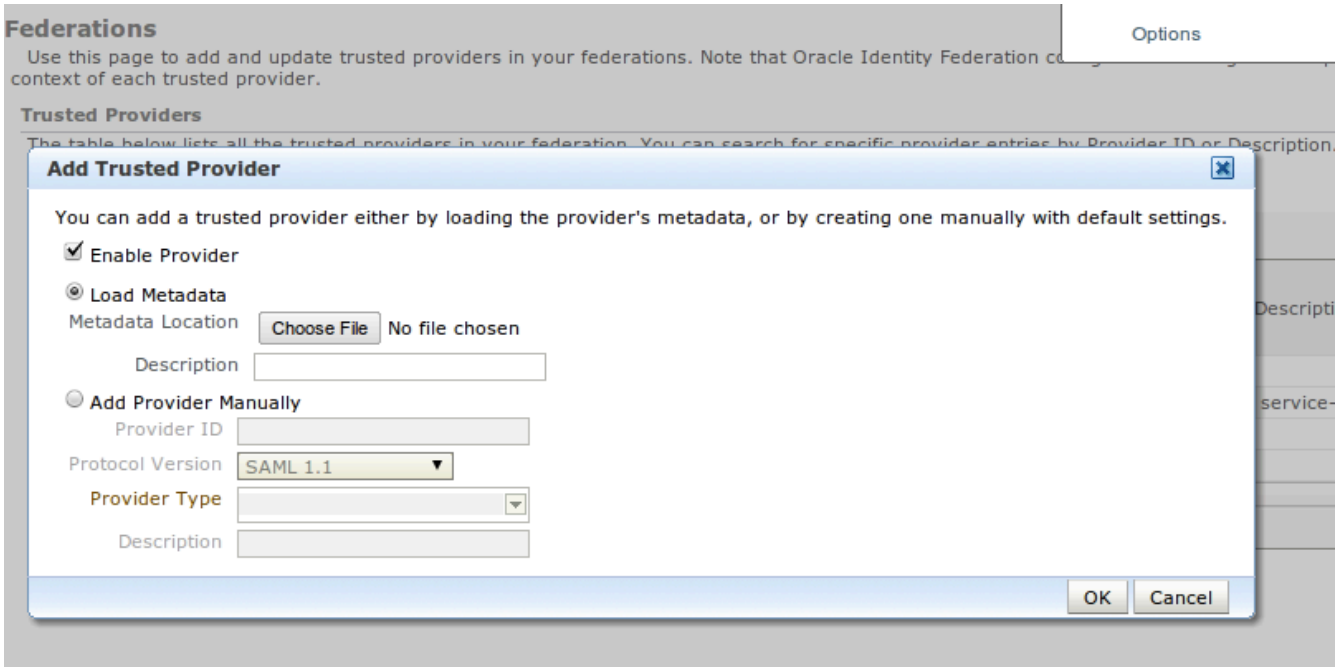
Save the meta data as a file and use it in the following steps for the OIF Server.

1. ## Oracle Identity Federation

Navigate to -> Administration -> Federation

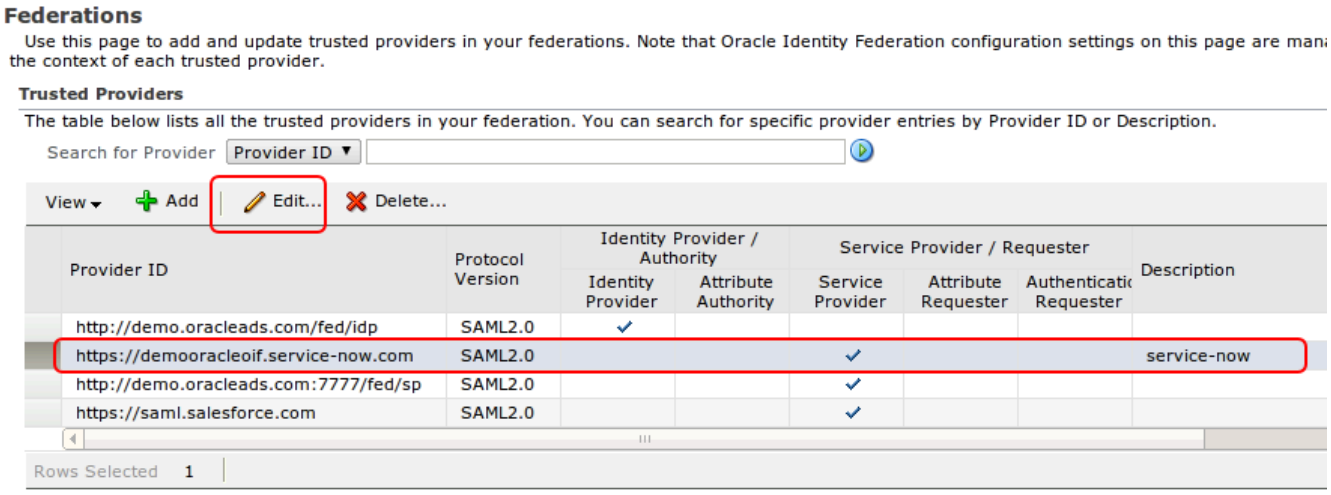


Click on the + Add button



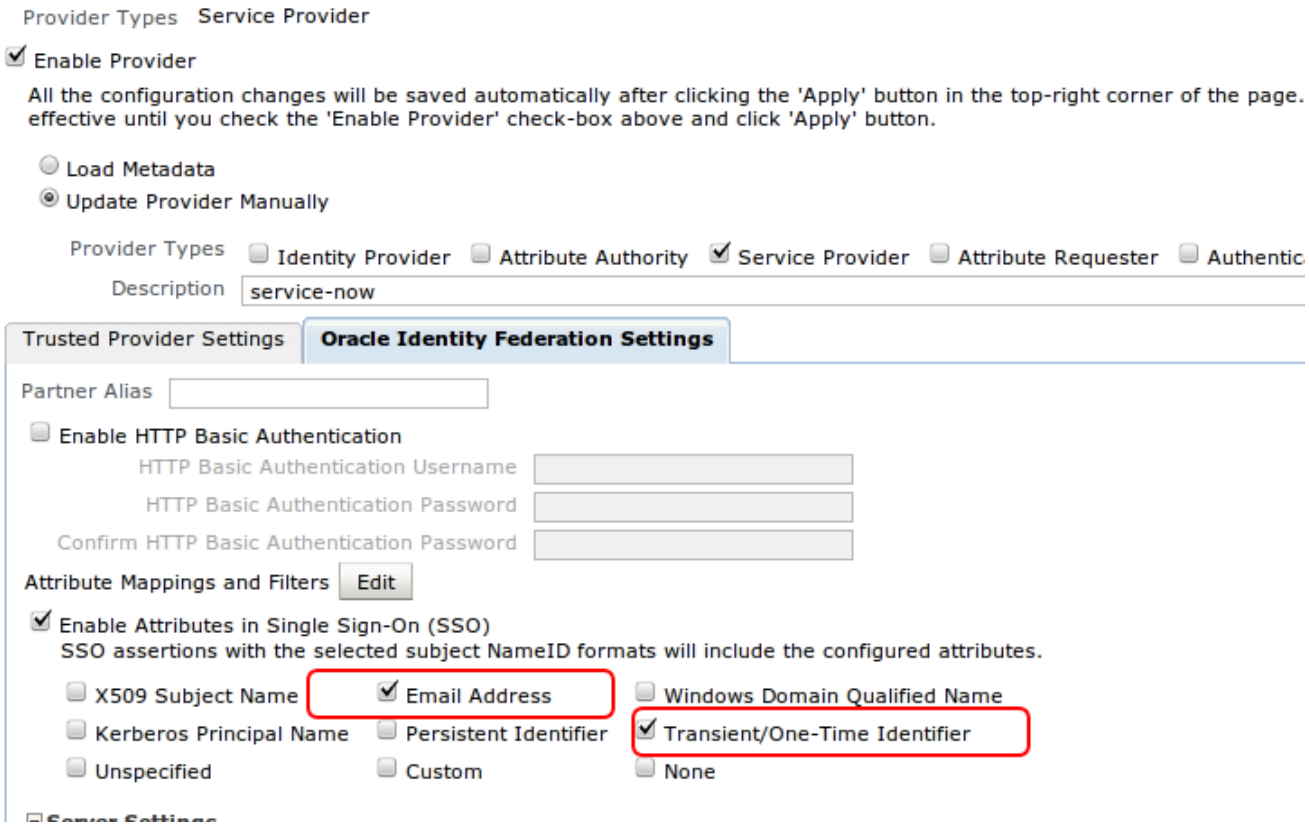
Load the meta data file that you downloaded for the Service-Now service provider.

This will create Relying Party Provider for OIF. Select the newly created provider and click on the "Edit" button to manually edit the provider settings:

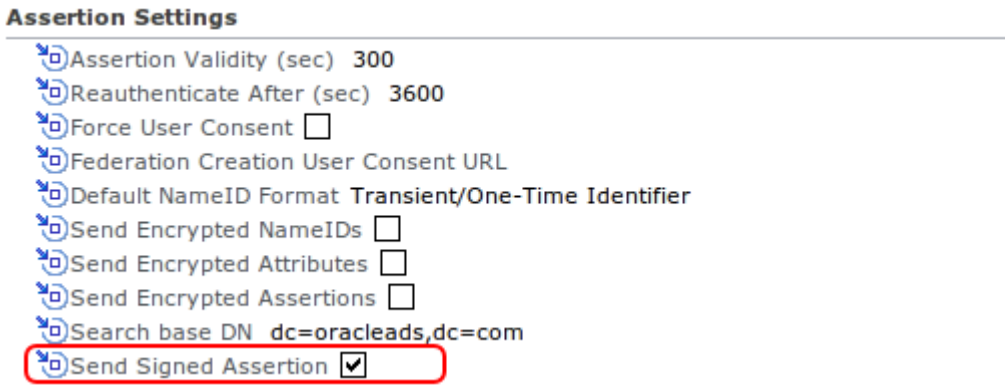


On the "Oracle Identity Federation Settings Tab" make sure you have the following settings:

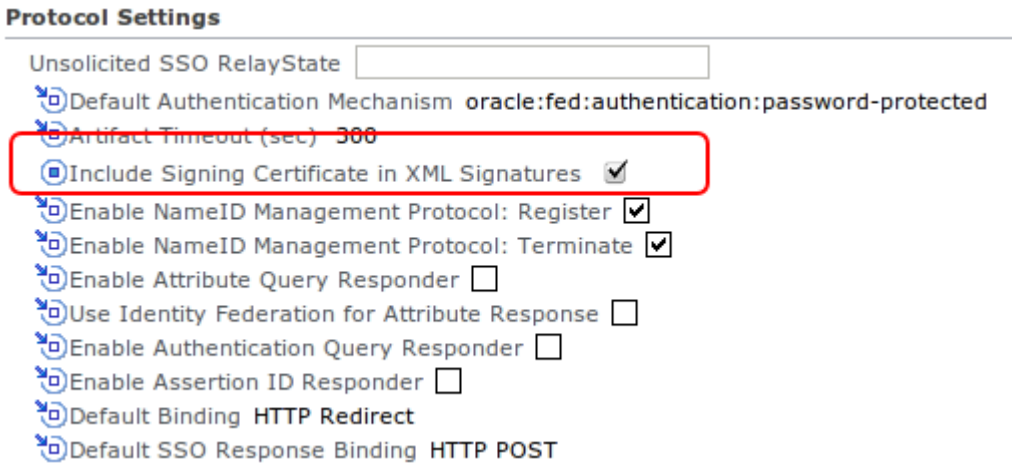
Under "Attribute Mappings and Filters" check "Email Address" and "Transient One Time Identifier"



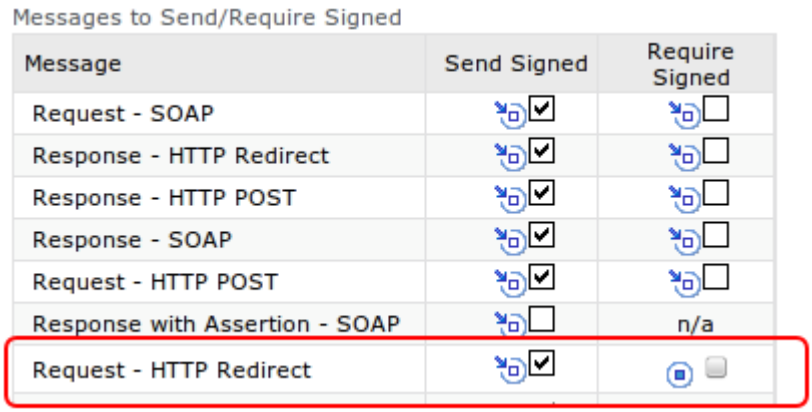
Under “Assertion Settings” enable “Send Signed Assertion”



Under “Protocol Settings” enable
“Include Signing Certificate in XML Signatures”



Under “Messages to Send/Require Signed” enable “Send Signed” for Request – HTTP Redirect



Testing the integration

For SSO the user is linked by their email address. The user must exist in the OIF datastore and must have a corresponding account on Service-now.com.

To initiate SSO go to your service-now domain. It it configured to use SP initiated SSO. You should see that you are re-directed to OIF for authentication. Once authenticated you will be redirected back again to Service-Now were you will be logged in.