

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

In this integration Oracle Identity 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).

SAML 2 Single Sign-on

- Login script
- Logout script
- Properties**
- Script object
- Certificate
- Metadata

Please edit your changes and press Save

SAML 2.0 Single Sign-on properties

Enable external authentication.

Yes | No

The base URL to the Identity Provider's AuthnRequest service. The AuthnRequest parameter

https://yourOracleIdpServer/fed/idp/samlv20

The base URL to the Identity Provider's SingleLogoutRequest service. The SingleLogoutRequest parameter

https://yourOracleIdpServer/fed/idp/samlv20

The base URL to the Service-now instance (usually this instance)

https://yourServiceNowInstanceName.service-now.com

The base URL to the Service-now instance (usually this instance)

https://yourServiceNowInstanceName.service-now.com

Make these URLs the same

The User table field to match with the Subject's NameID element in the SAMLResponse

email

The NameID policy to use for returning the Subject's NameID in the SAMLResponse. The NameID policy must support this by declaring the policy in its metadata. The NameID value is used to lookup the user.

urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

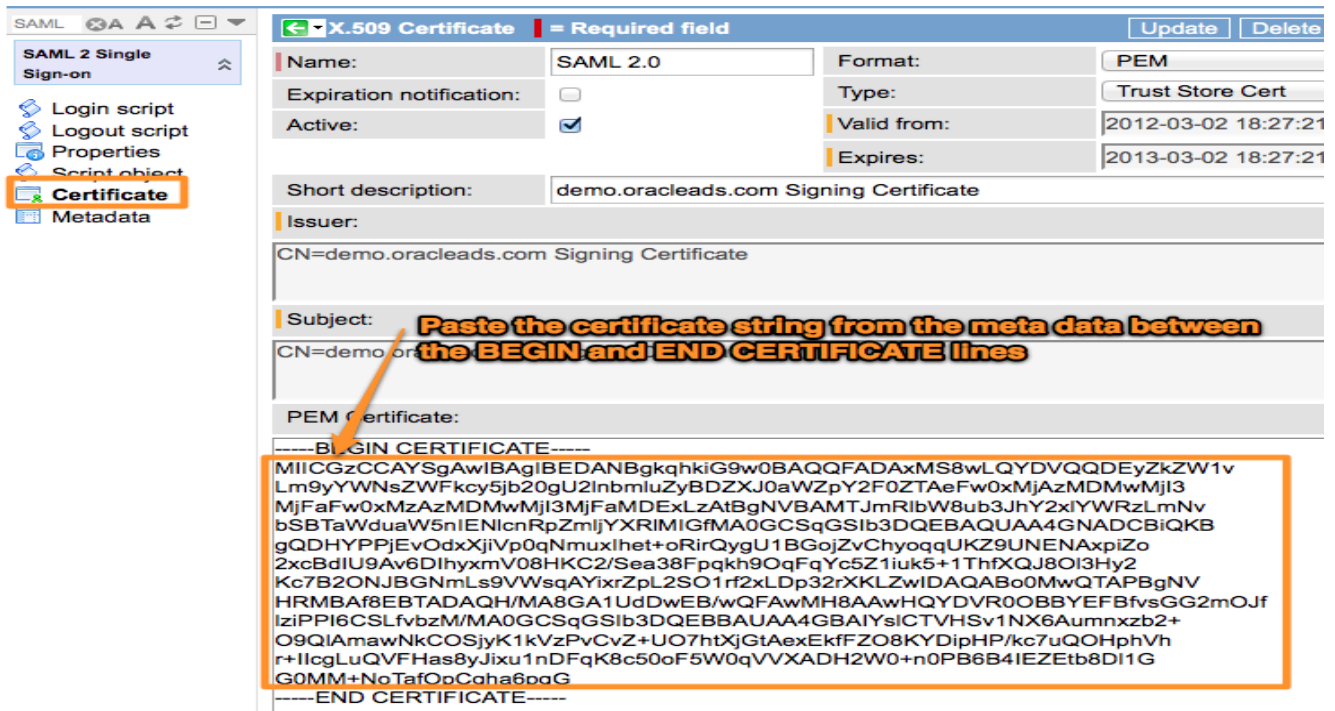
From the Oracle IDP Metadata, look for the X509Certificate under the <md:KeyDescriptor use="signing"> section.

```

<md:EntityDescriptor ID="id-RnFY8rvc-e9i6SMiFlgLNkqJF4A-" cacheDuration="POY0M30DT0H0M0.0S" entity]
- <md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:
  - <md:KeyDescriptor use="signing">
    - <dsig:KeyInfo>
      - <dsig:X509Data>
        - <dsig:X509Certificate>
          MIICGzCCAYSgAwIBAgIBEDANBgkqhkiG9w0BAQQFADAxMS8wLQYDVQQDEyZkZW1v Lm9yYy
          MjFaFw0xMzAzMDMwMjI3MjFaMDExLzAtBgNVBAMTJmRlbW8ub3JhY2x1YWRzLmNv bSBTaW
          gQDHYPPjEvOdxXjiVp0qNmuxIhet+oRirQygu1BG0jZvChyoqqUKZ9UNENAxpiZo 2xcBdlU9Av6DI
          Kc7B2ONJBGNmLs9VWsqAYixrZpL2SO1rf2xLDp32rXKLZwIDAQABo0MwQTAPBgNV HRMBAff
          /wQFAwMH8AAwHQYDVR0OBBYEFBfvsGG2mOJf lziPPI6CSLfvbzM/MA0GCSqGSIb3DQEBAU
          O9QlAmawNkCOSjyK1kVzPvCvZ+UO7htXjGtAexEkfFZO8KYDipHP/kc7uQOHphVh r+IicgLuQVVF
          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>
  </md:KeyDescriptor>
- <md:KeyDescriptor use="encryption">
  - <dsig:KeyInfo>
    - <dsig:X509Data>
      - <dsig:X509Certificate>
        MIICITCCAAYqAwIBAgIBIDANBgkqhkiG9w0BAQQFADA0MTIwMAYDVQQDEylkZW1v Lm9yYVY
        -----BEGIN CERTIFICATE-----
  -----END CERTIFICATE-----

```

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#">
MIID6TCCAAtGgAwIBAgIQaWG5DFrv6VYEv/tPlqZYbDANBgkqhkiG9w0BAQUFADA8
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMVGVhd3RILCBJbmMuMRYwFAYDVQQDEw1U
aGF3dGUuU1NMIENBMB4XDTEwMDAwMDAwMFAwMDAwMDAwMFAwMDAwMDAwMFAwMDAw
CzAJBgNVBAYTAiVUwvY290MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
RGllZ28xGDAWBgNVBAoUUD1NlcnZpY2Utbm93LmNvbTETMBEGA1UECzQKT3BlcmF0
aW9uc2EaMBGGA1UEAxQRK15zZXJ2aWNILW5vdy5jb20wggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIABAQDACL2WcmR3wo3wxJZw/LJJ9T5hMHmtCD+7Fgnfqy
+cnTeJ0QK7TbjVkkIR6VoDqurZ/vmul0d8RlqaAhdvErEf7zHd5Iv55IipZVBmr0
iZ7nC0nHi8Zpu+GNxBptAQSmTldB/ailmb8VHItQTcq3qQM+mBGi+WqR31cPugDF
I2+03f+V5xob0nkE3y0019dqCpjrRNrlIZUMJGy4pkpXZDzNWYjPN/Bg7FIRjyo
XyLYHMI1ChOIkzq7yFrEgsI0qOo7j5jYX7DZOIAmX2TTvatYCoWqm1C3QrwRHUvI
2bSLdS+iEQp/fkue336btB1N8+VP5Q/Ri9KvHdJcIN1LAgMBAAGjgaAwgZ0wDAYD
VR0TAQH/BAIwADA6BgNVHR8EMzAxMC+gLaArhilodHRwOi8vc3ZyLW92LWNybC50
aGF3dGUuY29tL1RoYXd0ZU9WLmNybDAdBgNVHSUEFjAUBgggrBgEFBQcDAQYIKwYB
BQUHAIwMgYIKwYBBQUHAQEELjAKMCIGCCsGAQUFBzABbhZodHRwOi8vb2NzcC50
aGF3dGUuY29tMA0GCSqGSIb3DQEBBQUAA4IBAQB9zifSRfQLsQIbFcfBg9E1R0o
Nx5sco6WHQ3f8v4RrGO4ZAMGnqDlsAjEG88LzQfeVkkqAmsTWxCyCHW0iGWvUbfN
cAHvLdr9VILmUnz3wg69VgnW+fwppPAyD1L1ZEafESw5eoivkjcQ5DledjjKwYil
FjkLngEOORkBhKmyGLIV7nXWGOVmJkDt5xHH5i3rVq1G8sEV743kSLtK/Dugn7Hf
HSYbiyDpHv8EJmFBYtFFYIPUyKOPowaTu2zj9qJz83X5oLulBd6eLZfaAgsjZ/Rb
1MTfRzgl2mur/IiTx9KL7Ymg+NJm7y7/wb1Fy438OwBANG6VrJUJqjxyYR/a
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</KeyDescriptor>
```

Your resulting Metadata will look like:

Federations

Use this page to add and update trusted providers in your federations. Note that Oracle Identity Federation configuration settings on this page are managed in context of each trusted provider.

Trusted Providers

The table below lists all the trusted providers in your federation. You can search for specific provider entries by Provider ID or Description.

Search for Provider Provider ID

View

Provider ID	Protocol Version	Identity Provider / Authority		Service Provider / Requester			Description
		Identity Provider	Attribute Authority	Service Provider	Attribute Requester	Authenticating Requester	
http://demo.oracleleads.com/fed/idp	SAML2.0	✓					
https://demooracleoif.service-now.com	SAML2.0			✓			service-now
http://demo.oracleleads.com:7777/fed/sp	SAML2.0			✓			
https://saml.salesforce.com	SAML2.0			✓			

Click on the + Add button

Federations

Options

Use this page to add and update trusted providers in your federations. Note that Oracle Identity Federation configuration settings on this page are managed in context of each trusted provider.

Trusted Providers

The table below lists all the trusted providers in your federation. You can search for specific provider entries by Provider ID or Description.

Add Trusted Provider

You can add a trusted provider either by loading the provider's metadata, or by creating one manually with default settings.

Enable Provider

Load Metadata

Metadata Location No file chosen

Description

Add Provider Manually

Provider ID

Protocol Version

Provider Type

Description

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:

Federations

Use this page to add and update trusted providers in your federations. Note that Oracle Identity Federation configuration settings on this page are managed in the context of each trusted provider.

Trusted Providers

The table below lists all the trusted providers in your federation. You can search for specific provider entries by Provider ID or Description.

Search for Provider

View

Provider ID	Protocol Version	Identity Provider / Authority		Service Provider / Requester			Description
		Identity Provider	Attribute Authority	Service Provider	Attribute Requester	Authentication Requester	
http://demo.oracleleads.com/fed/idp	SAML2.0	✓					
https://demooracleoif.service-now.com	SAML2.0			✓			service-now
http://demo.oracleleads.com:7777/fed/sp	SAML2.0			✓			
https://saml.salesforce.com	SAML2.0			✓			

Rows Selected 1

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”

Provider Types Service Provider

Enable Provider

All the configuration changes will be saved automatically after clicking the 'Apply' button in the top-right corner of the page. Changes are effective until you check the 'Enable Provider' check-box above and click 'Apply' button.

Load Metadata
 Update Provider Manually

Provider Types Identity Provider Attribute Authority Service Provider Attribute Requester Authentication Requester

Description

Trusted Provider Settings **Oracle Identity Federation Settings**

Partner Alias

Enable HTTP Basic Authentication

HTTP Basic Authentication Username

HTTP Basic Authentication Password

Confirm HTTP Basic Authentication Password

Attribute Mappings and Filters

Enable Attributes in Single Sign-On (SSO)

SSO assertions with the selected subject NameID formats will include the configured attributes.

X509 Subject Name Email Address Windows Domain Qualified Name

Kerberos Principal Name Persistent Identifier Transient/One-Time Identifier

Unspecified Custom None

Under “Assertion Settings” enable “Send Signed Assertion”

Assertion Settings

- ↳ Assertion Validity (sec) 300
- ↳ Reauthenticate After (sec) 3600
- ↳ Force User Consent
- ↳ Federation Creation User Consent URL
- ↳ Default NameID Format Transient/One-Time Identifier
- ↳ Send Encrypted NameIDs
- ↳ Send Encrypted Attributes
- ↳ Send Encrypted Assertions
- ↳ Search base DN dc=oracleads,dc=com
- ↳ Send Signed Assertion

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

Protocol Settings

- ↳ Unsolicited SSO RelayState
- ↳ Default Authentication Mechanism oracle:fed:authentication:password-protected
- ↳ Artifact Timeout (sec) 300
- ↳ Include Signing Certificate in XML Signatures
- ↳ Enable NameID Management Protocol: Register
- ↳ Enable NameID Management Protocol: Terminate
- ↳ Enable Attribute Query Responder
- ↳ Use Identity Federation for Attribute Response
- ↳ Enable Authentication Query Responder
- ↳ Enable Assertion ID Responder
- ↳ Default Binding HTTP Redirect
- ↳ Default SSO Response Binding HTTP POST

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

Messages to Send/Require Signed

Message	Send Signed	Require Signed
Request - SOAP	↳ <input checked="" type="checkbox"/>	↳ <input type="checkbox"/>
Response - HTTP Redirect	↳ <input checked="" type="checkbox"/>	↳ <input type="checkbox"/>
Response - HTTP POST	↳ <input checked="" type="checkbox"/>	↳ <input type="checkbox"/>
Response - SOAP	↳ <input checked="" type="checkbox"/>	↳ <input type="checkbox"/>
Request - HTTP POST	↳ <input checked="" type="checkbox"/>	↳ <input type="checkbox"/>
Response with Assertion - SOAP	↳ <input type="checkbox"/>	n/a
Request - HTTP Redirect	↳ <input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/>

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. If it is 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 where you will be logged in.