OracleInterop

When trying to interoperate with Oracle delivered applications there are a few options that are known to work using native Oracle technologies.

Weblogic Native - SAML1 RP

It is possible to setup a Weblogic container as a SAML1 RP that can work with your Shibboleth IdP.

More notes here later... but this does work.

Quick notes:

- NameID coming in (subject) needs to map to the userid at the Weblogic container.
  - There is an internal weblogic sudo-ldap facility that can be used for starters.
- You must specify the NameID format in the md on the IdP side
  - <md:NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</md:NameIDFormat>
- I believe pushing on the saml1 response was ok.. again i'll have to revisit

Oracle Identity Federation - SAML2 RP

It is possible to setup / configure Oracle Identity Federation (OIF) as a SAML2 RP that communicates with your Shibboleth IdP. The main reason one would want to do this is to enable access to any number of oracle specific applications that can use native OAM / OSSO for user access. Effectively what you are doing is creating a bridging service that will delegate some degree of SSO to your Shibboleth IdP.

The remainder of this article assumes you have OIF installed and are past the Oracle Middleware install idiosyncrasies.

> ⓘ You will be configuring OIF using the Oracle Enterprise Manger 11g (OEM) GUI.

Overall Steps

1. Bootstrap the "Federation" – upload metadata to define your IdP
2. Configure Server Properties – ports, etc
3. Configure your Service Provider
4. Export your Metadata
5. Fixup and import metadata to your Shibboleth Environment
6. Enable the SP Integration modules: Test SP and Oracle Single-Sign-On
7. Test round trip with the OIF Testing SP
8. Configure the mechanics between OIF and OAM
9. Configure release at your Shibboleth IdP

Locations of Interest (for config)

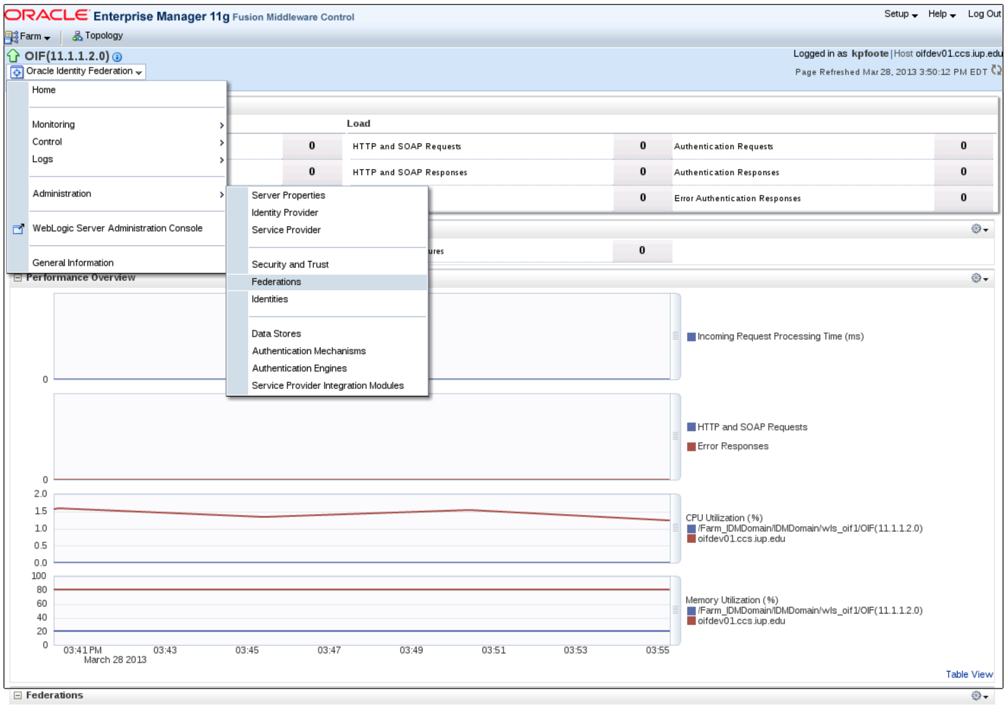
Oracle Enterprise Manageer	HTTP://OIF-HOST:OIF-ConsolePort/em
OIF Test SP	HTTP://OIF-SP-HOST:OIF-SP-PORT/fed/user/testspsso

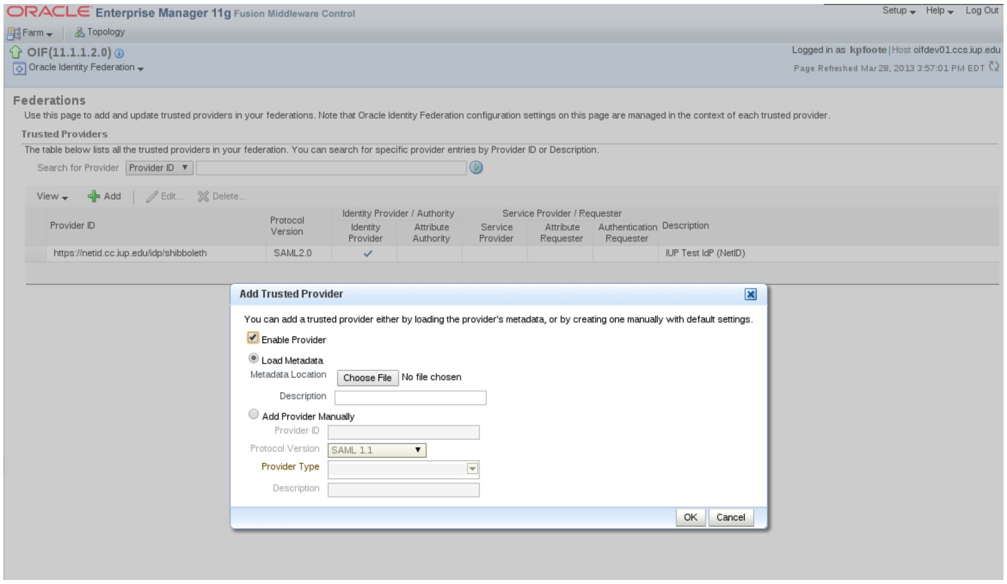
> ⓘ If you are taking defaults from the OIF / OAM install you will end up with the following ports: SP port 7499, Admin Console port 7001, OAM hooks port 14100

Create a Federation in OIF

To boot strap things to a running state in our environment we need to configure how our Federation will look (according to OIF).

```
OIF dropdown > Administration > Federations : Add , Enable Provider , Load Metadata (upload file)
```


ORACLE Enterprise Manager 11g Fusion Middleware Control
Setup
Help
Log Out
Farm
Topology
OIF(11.1.1.2.0)
Oracle Identity Federation
Logged in as kpfoote | Host oifdev01.ccs.iup.edu
Page Refreshed Mar 28, 2013 3:50:12 PM EDT
Home
Monitoring
Control
Logs
Administration
WebLogic Server Administration Console
General Information
Server Properties
Identity Provider
Service Provider
Security and Trust
Federations
Identities
Data Stores
Authentication Mechanisms
Authentication Engines
Service Provider Integration Modules
Load
HTTP and SOAP Requests 0
HTTP and SOAP Responses 0
Authentication Requests 0
Authentication Responses 0
Error Authentication Responses 0
Performance Overview
Incoming Request Processing Time (ms)
HTTP and SOAP Requests
Error Responses
CPU Utilization (%)
/Farm_IDMDomain/IDMDomain/wls_oif1/OIF(11.1.1.2.0)
oifdev01.ccs.iup.edu
Memory Utilization (%)
/Farm_IDMDomain/IDMDomain/wls_oif1/OIF(11.1.1.2.0)
oifdev01.ccs.iup.edu
0
2.0
1.5
1.0
0.5
0.0
100
80
60
40
20
03:41 PM
March 28 2013
03:43
03:45
03:47
03:49
03:51
03:53
03:55
Table View
Federations



ORACLE Enterprise Manager 11g Fusion Middleware Control

Farm | Topology

OIF(11.1.1.2.0)

Oracle Identity Federation

Logged in as kpfoote | Host oifdev01.ccs.iup.edu

Page Refreshed Mar 28, 2013 3:57:01 PM EDT

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: Provider ID

View | Add | Edit... | Delete...

Provider ID	Protocol Version	Identity Provider / Authority		Service Provider / Requester			Description
		Identity Provider	Attribute Authority	Service Provider	Attribute Requester	Authentication Requester	
https://netid.cc.iup.edu/idp/shibboleth	SAML2.0	✓					IUP Test IdP (NetID)

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: Choose File No file chosen

Description:

○ Add Provider Manually

Provider ID:

Protocol Version: SAML 1.1

Provider Type:

Description:

OK | Cancel

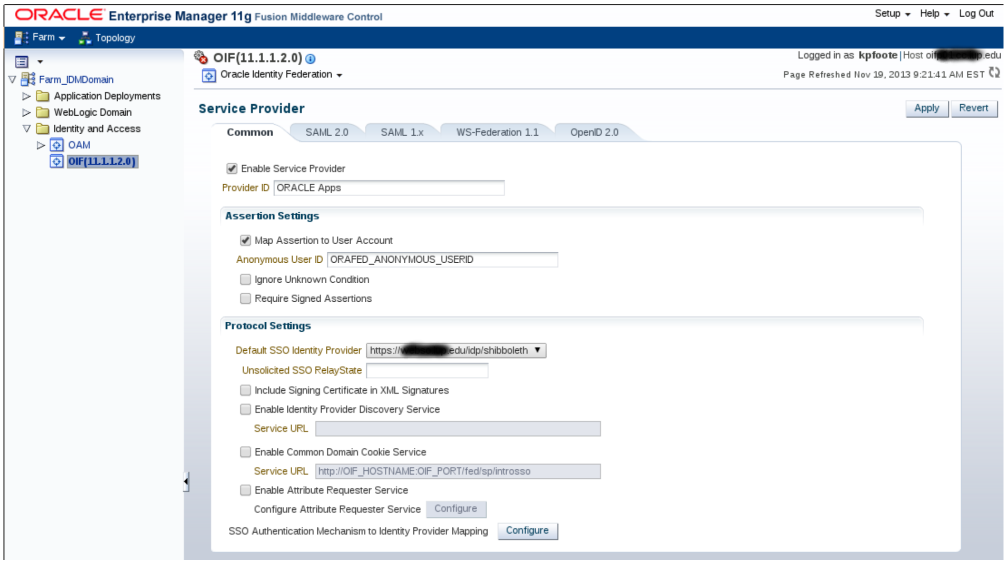
Configure the OIF SP

This is the piece we are after (SP) to create our bridge into the Oracle Single-Sign-On (OSSO) space.

```
OIF Dropdown >> Administration >> Service Provider
```

The Service Provider will be using the assertion sent by the IdP to map the user into an OSSO Id. Configure the Oracle SP to Map the Assertion to the User account, then configure to map the user via Attribute Query.

> ⚠ This is not an attribute query back to the IdP rather we are "querying" the attribute stack we have just received via the assertion.



OIF(11.1.1.2.0)
Oracle Identity Federation

Logged in as **kpfoote** | Host oif[redacted].edu
Page Refreshed Nov 19, 2013 9:21:41 AM EST

Service Provider

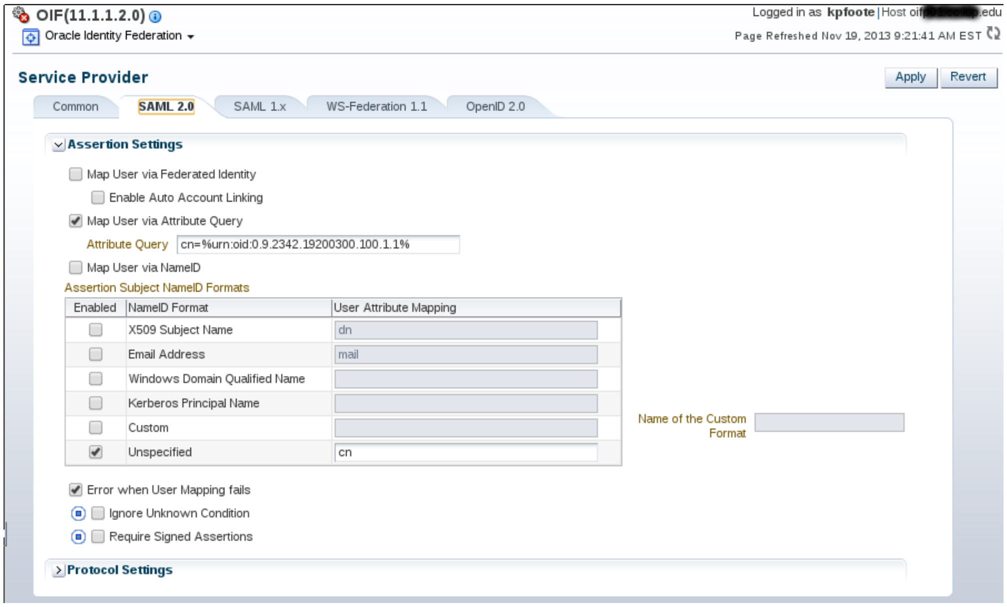
☑ Enable Service Provider
Provider ID: ORACLE Apps

Assertion Settings

☑ Map Assertion to User Account
Anonymous User ID: ORAFED_ANONYMOUS_USERID
☐ Ignore Unknown Condition
☐ Require Signed Assertions

Protocol Settings

Default SSO Identity Provider: https://[redacted].edu/idp/shibboleth ▼
Unsolicited SSO RelayState:
☐ Include Signing Certificate in XML Signatures
☐ Enable Identity Provider Discovery Service
Service URL:
☐ Enable Common Domain Cookie Service
Service URL: http://OIF_HOSTNAME:OIF_PORT/fed/sp/introsso
☐ Enable Attribute Requester Service
Configure Attribute Requester Service: Configure
SSO Authentication Mechanism to Identity Provider Mapping: Configure



OIF(11.1.1.2.0)
Oracle Identity Federation

Logged in as **kpfoote** | Host oif[redacted].edu
Page Refreshed Nov 19, 2013 9:21:41 AM EST

Service Provider

Assertion Settings

☐ Map User via Federated Identity
☐ Enable Auto Account Linking
☑ Map User via Attribute Query
Attribute Query: cn=%urn:oid:0.9.2342.19200300.100.1.1%
☐ Map User via NameID

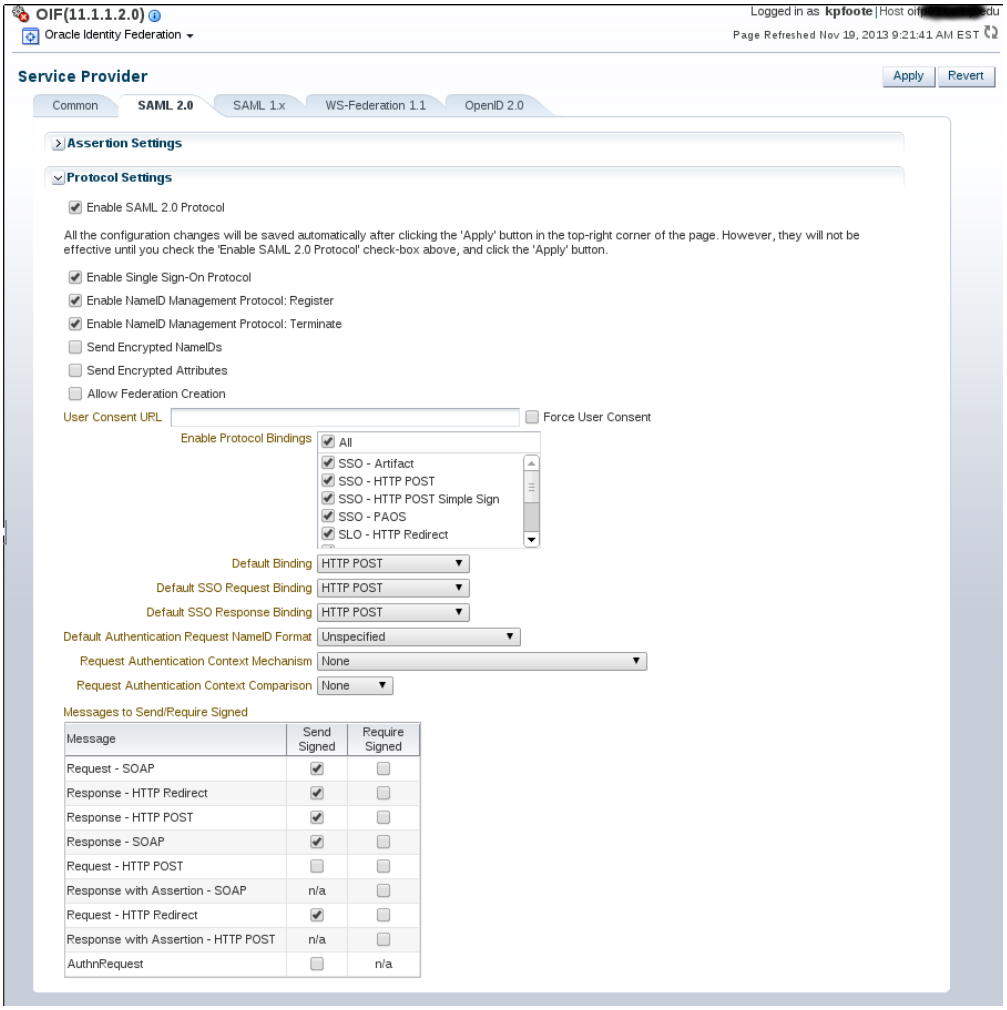
Assertion Subject NameID Formats

Enabled	NameID Format	User Attribute Mapping
☐	X509 Subject Name	dn
☐	Email Address	mail
☐	Windows Domain Qualified Name	
☐	Kerberos Principal Name	
☐	Custom	
☑	Unspecified	cn

Name of the Custom Format:

☑ Error when User Mapping fails
☐ Ignore Unknown Condition
☐ Require Signed Assertions

Protocol Settings



OIF(11.1.1.2.0)
Oracle Identity Federation
Logged in as kpfoote | Host oif[redacted]du
Page Refreshed Nov 19, 2013 9:21:41 AM EST
Apply
Revert
Common
SAML 2.0
SAML 1.x
WS-Federation 1.1
OpenID 2.0

Service Provider

Assertion Settings

Protocol Settings

☑ Enable SAML 2.0 Protocol

All the configuration changes will be saved automatically after clicking the 'Apply' button in the top-right corner of the page. However, they will not be effective until you check the 'Enable SAML 2.0 Protocol' check-box above, and click the 'Apply' button.

☑ Enable Single Sign-On Protocol

☑ Enable NameID Management Protocol: Register

☑ Enable NameID Management Protocol: Terminate

□ Send Encrypted NameIDs

□ Send Encrypted Attributes

□ Allow Federation Creation

User Consent URL ______ □ Force User Consent

Enable Protocol Bindings: ☑ All; ☑ SSO - Artifact; ☑ SSO - HTTP POST; ☑ SSO - HTTP POST Simple Sign; ☑ SSO - PAOS; ☑ SLO - HTTP Redirect

Default Binding: HTTP POST

Default SSO Request Binding: HTTP POST

Default SSO Response Binding: HTTP POST

Default Authentication Request NameID Format: Unspecified

Request Authentication Context Mechanism: None

Request Authentication Context Comparison: None

Messages to Send/Require Signed

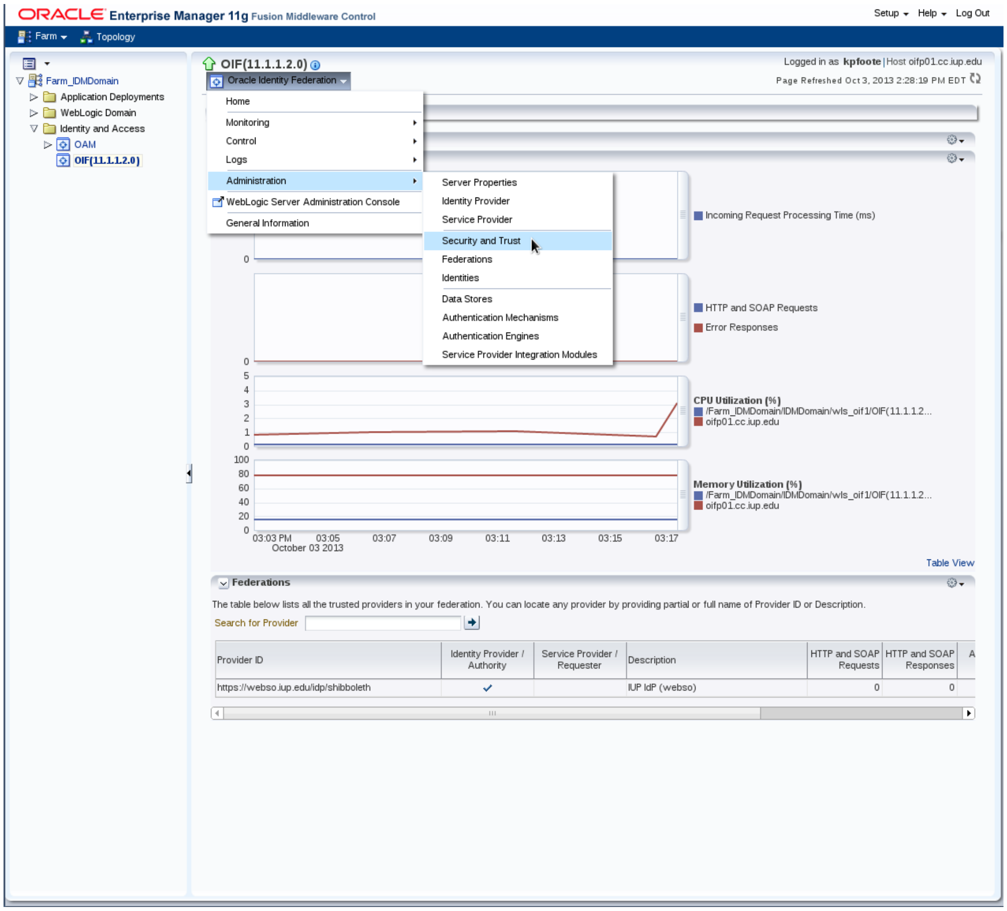
Message	Send Signed	Require Signed
Request - SOAP	☑	□
Response - HTTP Redirect	☑	□
Response - HTTP POST	☑	□
Response - SOAP	☑	□
Request - HTTP POST	□	□
Response with Assertion - SOAP	n/a	□
Request - HTTP Redirect	☑	□
Response with Assertion - HTTP POST	n/a	□
AuthnRequest	□	n/a

Obtain OIF Metadata

We need to produce some metadata on the OIF side so we can import this into our IdP metadata feed(s). Obtain the OIF metadata from here

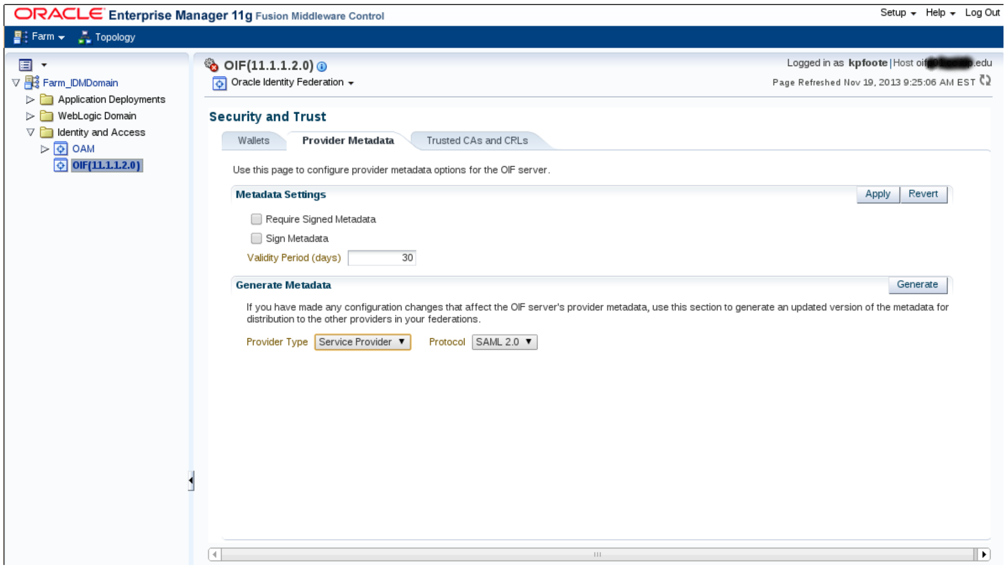
```
OIF Dropdown >> Administration >> Security and Trust
```

Use the Provider Metadata tab to find the Generate Metadata pane and button.



The table below lists all the trusted providers in your federation. You can locate any provider by providing partial or full name of Provider ID or Description.

Provider ID	Identity Provider / Authority	Service Provider / Requester	Description	HTTP and SOAP Requests	HTTP and SOAP Responses	A
https://webso.iup.edu/idp/shibboleth	✓		IUP IdP (webso)	0	0	



Logged in as kpfoote | Host oi[redacted].edu

Page Refreshed Nov 19, 2013 9:25:06 AM EST

Security and Trust

Use this page to configure provider metadata options for the OIF server.

Metadata Settings

☐ Require Signed Metadata

☐ Sign Metadata

Validity Period (days) 30

Generate Metadata

If you have made any configuration changes that affect the OIF server's provider metadata, use this section to generate an updated version of the metadata for distribution to the other providers in your federations.

Provider Type: Service Provider ▾ Protocol: SAML 2.0 ▾

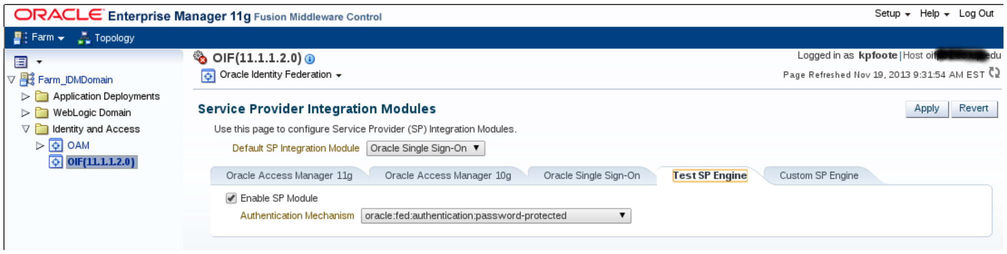
Save the generated XML metadata file and load that into your Shibboleth IdP config.

> ⓘ You will want to remove some XML properties / elements such as ValidUntil. You will also want to ensure that the NameId requested in metadata matches your release from the IdP.

Enable the SP Integration modules: Test SP and Oracle Single-Sign-On

Here we enable to integration points the Test SP and the Oracle Single-Sign-On module.

```
OIF Dropdown >> Service Provider Integration Modules
```



OIF(11.1.1.2.0)

Logged in as kpfoote | Host oif[redacted]edu

Page Refreshed Nov 19, 2013 9:31:54 AM EST

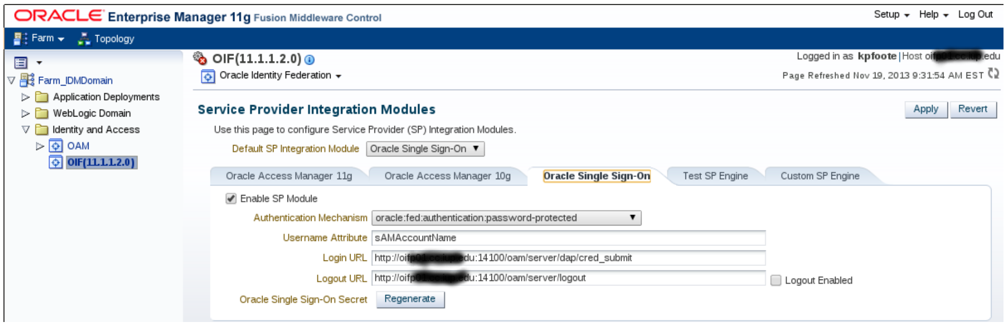
Service Provider Integration Modules

Use this page to configure Service Provider (SP) Integration Modules.

Default SP Integration Module: Oracle Single Sign-On

☑ Enable SP Module

Authentication Mechanism: oracle:fed:authentication:password-protected



OIF(11.1.1.2.0)

Logged in as kpfoote | Host oif[redacted]edu

Page Refreshed Nov 19, 2013 9:31:54 AM EST

Service Provider Integration Modules

Use this page to configure Service Provider (SP) Integration Modules.

Default SP Integration Module: Oracle Single Sign-On

☑ Enable SP Module

Authentication Mechanism: oracle:fed:authentication:password-protected

Username Attribute: sAMAccountName

Login URL: http://oif[redacted]du:14100/oam/server/dap/cred_submit

Logout URL: http://oifp[redacted]du:14100/oam/server/logout □ Logout Enabled

Oracle Single Sign-On Secret

Test round trip with Test SP module

http(s)://YOUROIFHOST:[PORT]/fed/user/testspsso

Register OAM with OIF

Register DAP token..

Configure release at Shibboleth IdP

You will need to configure a filter for this entityID such that only the NameID that you are expecting gets used in the assertion. This needs to be something that will be locatable on the RP side (OAM) as an actual user. In our case this is the netid of the user.