Oracle® Revenue Management and Billing

Version 2.6.0.1.0

Federated Identity (FI) – SSO Web Application

Revision 1.0

E97715-01

June, 2018

Oracle Revenue Management and Billing Federated Identity (FI) – SSO Web Application

E97715-01

Copyright Notice

Trademark Notice

License Restrictions Warranty/Consequential Damages Disclaimer

Warranty Disclaimer

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

Restricted Rights Notice

Hazardous Applications Notice

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Third Party Content, Products, and Services Disclaimer

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third party content, products, or services.

Preface

About This Document

This document describes the steps to be executed on Identity Provider (OAM), ORMB Application and External Identity Provider to complete the ORMB authentication configuration.

This document covers following Software and versions:

Software	Version
ORMB Application	2.6.0.1.0
OAM Server (cloud)	11.1.2.3.0
OAM Server (on- premise)	11.1.2.3.0

Intended Audience

This document is intended for the following audience:

- Cloud Engineering Team
- Application Management Support Team
- Consulting Team

Note: The person who is setting up SSO web application should have basic knowledge on how to install and maintain ORMB authentication configuration for web. The configuration also includes SAML Token.

Organization of the Document

The information in this document is organized into the following sections:

Section No.	Section Name	Description
Section 1	Introduction	Explains the Identity Federation feature. It also provides an overview of the configuration steps for Federated SSO Login.
Section 2	Federated Indentity Login Flow	Gives an overview of data flow between the user and federation systems.
Section 3	Steps to be executed on IDP (OAM server as IDP)	Explains how to enable and configure the identity federation service. It also provides steps to register external Identity Provider partners.

Section No.	Section Name	Description
Section 4	Steps to be executed on SP (OAM server as SP)	Lists and describes the steps to be followed to set up OAM server as SP.
Section 5	Steps to be executed on ORMB Application	Lists and describes the steps to be executed on ORMB application.
Section 6	Restarting Servers	Lists the scripts and commands to restart the respective instances.
Section 7	Verifying SSO Web Application	Lists the steps to be performed to verify SSO web application setup.
Section 8	Internal SSO Login Configuration	Explains how to configure Internal SSO Login.

Related Documents

You can refer to the following documents for more information:

Document	Description
Oracle Revenue Management and Billing Version 2.6.0.1.0 Release Notes	Provides a brief description about the new features, enhancements, UI and database level changes, supported platforms, framework upgrade, supported upgrades, and technology upgrade made in this release. It also highlights the discontinued features, bug fixes, and known issues in this release.
Oracle Revenue Management and Billing Banking User Guide	Lists and describes various banking features in Oracle Revenue Management and Billing. It also describes all screens related to these features and explains how to perform various tasks in the application.
Oracle Revenue Management and Billing Insurance User Guide	Lists and describes various insurance features in Oracle Revenue Management and Billing. It also describes all screens related to these features and explains how to perform various tasks in the application.

Contents

1. Introduction

Oracle Identity Federation enables companies to provide services and share identity information across their respective security domains. The end user does not need to log in again to access a remote entity where business is conducted. Users authenticate at their local sites, and the federation mechanism enables this information to be shared. Enterprises do not need to manage the identities of users who are already known to a partner organization.

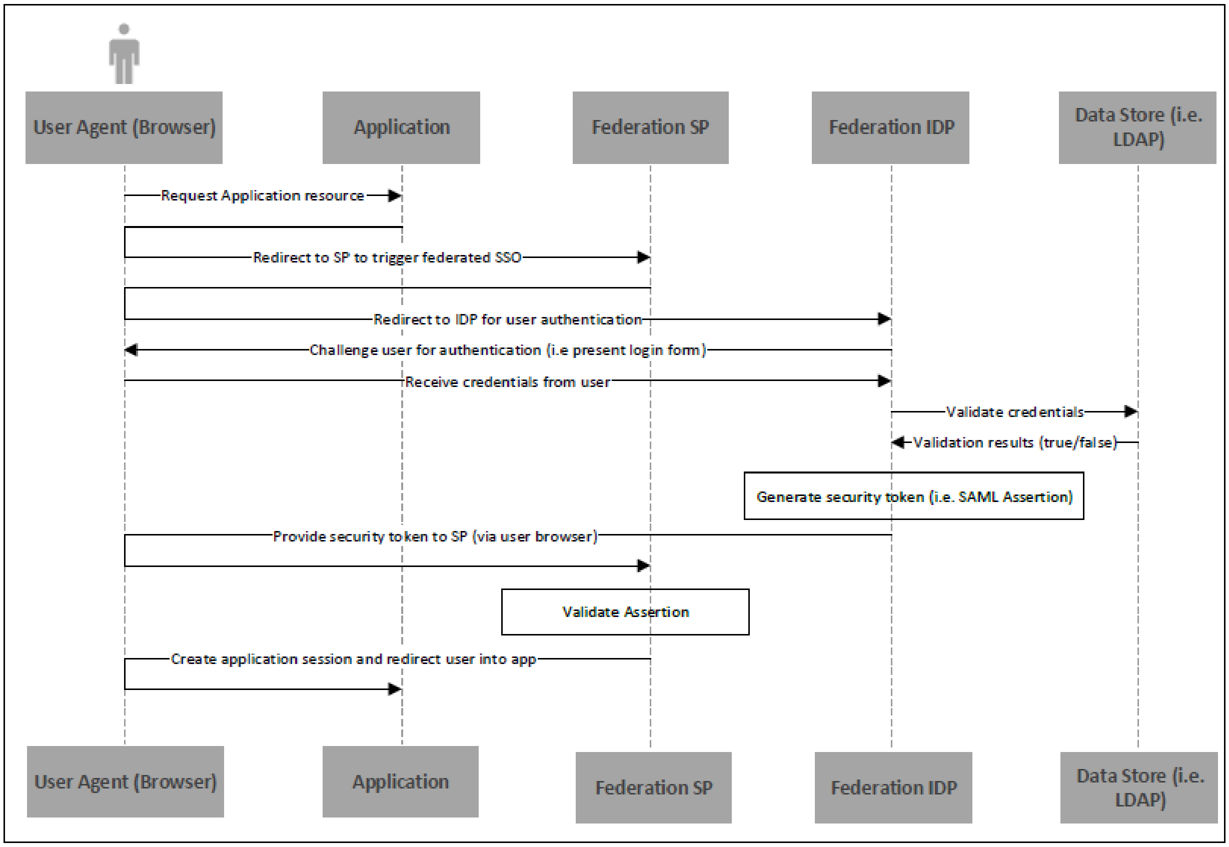
You can configure either Oracle Application Server Single Sign-On or Oracle Identity Federation to be the authentication mechanism for users who want to access resources that are protected by either product.

The below list gives an overview of the configuration steps for Federated SSO Login with each being described in detail later in this document.

1. IDP Configuration (OAM Server as IDP)
    - Enable OIF
    - Register OAM as IDP
    - Metadata XML file Import/Export
2. SP Configuration (OAM Server as SP)
    - Enable OIF
    - Register OAM as SP
    - Enable JIT User Provisioning in OIF
    - Configure OHS/WebGate Agent
    - Download WebGate Agent
    - Metadata XML file Import/Export
3. ORMB Application Configuration
    - Copy oamAuthnProvider jar file to OUAF domain
    - Copy ouaf-dbmsauth jar file to OUAF domain
    - Configure the OUAF app's web.xml
    - Add OAMIdentityAsserter
    - Add OuafDBMSAuthenticator

2. Federated Identity Login Flow

The flow of data between the two systems is illustrated below:


User Agent (Browser)
Application
Federation SP
Federation IDP
Data Store (i.e. LDAP)
Request Application resource
Redirect to SP to trigger federated SSO
Redirect to IDP for user authentication
Challenge user for authentication (i.e present login form)
Receive credentials from user
Validate credentials
Validation results (true/false)
Generate security token (i.e. SAML Assertion)
Provide security token to SP (via user browser)
Validate Assertion
Create application session and redirect user into app
User Agent (Browser)
Application
Federation SP
Federation IDP
Data Store (i.e. LDAP)

1. The user accesses the OUAF application via the OHS/WebGate URL.
2. The WebGate determines that the user has not been authenticated and responds with a redirect (302) back to the browser.
3. The browser accesses OAM to authenticate the user.
4. OAM determines that an external identity provider as configured in OAM should do the authentication. It creates a SAML 2.0 request and responds to the browser with a redirect to the IdP.
5. The IdP is invoked with the SAML request and the IdP challenges the user with a login prompt.
6. The IdP authenticates the user and responds with a SAML 2.0 assertion, which includes the authenticated user data.
7. The browser sends the SAML response to OAM.
8. OAM validates the assertion and responds with an OAM identity assertion for the SSO session.
9. The browser requests the original OUAF resource and this time WebGate grants access.
10. The OUAF response is returned to the browser.

3. Steps to be executed on IDP (OAM Server as IDP)

3.1 Enabling Identity Federation Service

Prerequisite

To set up federated identity on IDP, you should have:

- Access Manager Service and the Identity Federation service enabled in OAM.

Procedure

To enable the Identity Federation service, you need to follow the below steps:

1. Login to Oracle Access Management using the administrator's credentials.
2. Click the **Configuration** button. The **Launch Pad** tab appears.

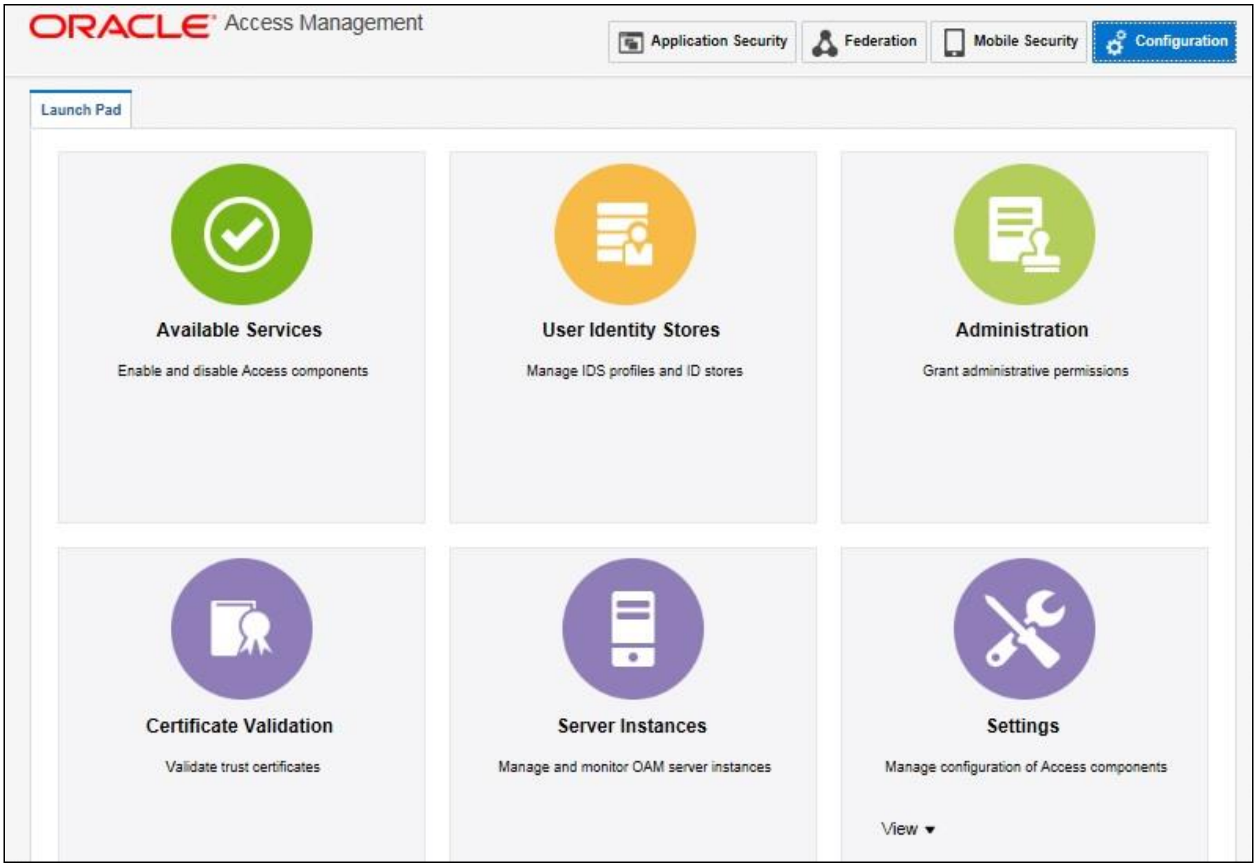
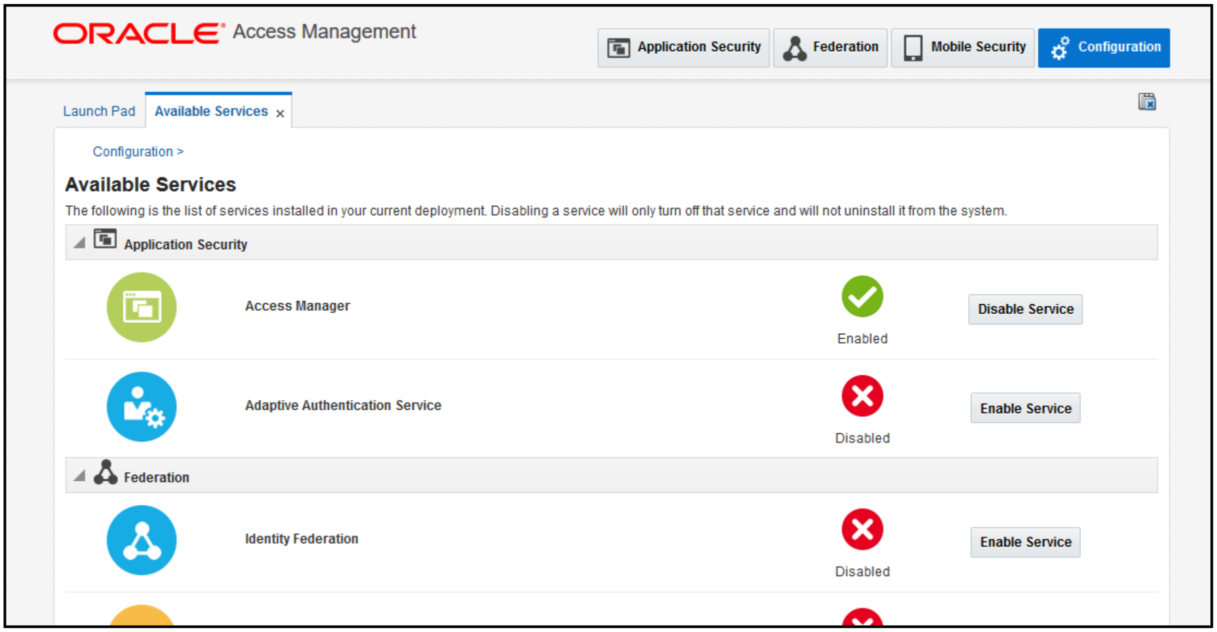

ORACLE Access Management
Application Security
Federation
Mobile Security
Configuration
Launch Pad
Available Services
Enable and disable Access components
User Identity Stores
Manage IDS profiles and ID stores
Administration
Grant administrative permissions
Certificate Validation
Validate trust certificates
Server Instances
Manage and monitor OAM server instances
Settings
Manage configuration of Access components
View ▾

Figure 1: Configuration - Launch Pad

3. Click the **Available Services** icon. The **Available Services** tab appears.



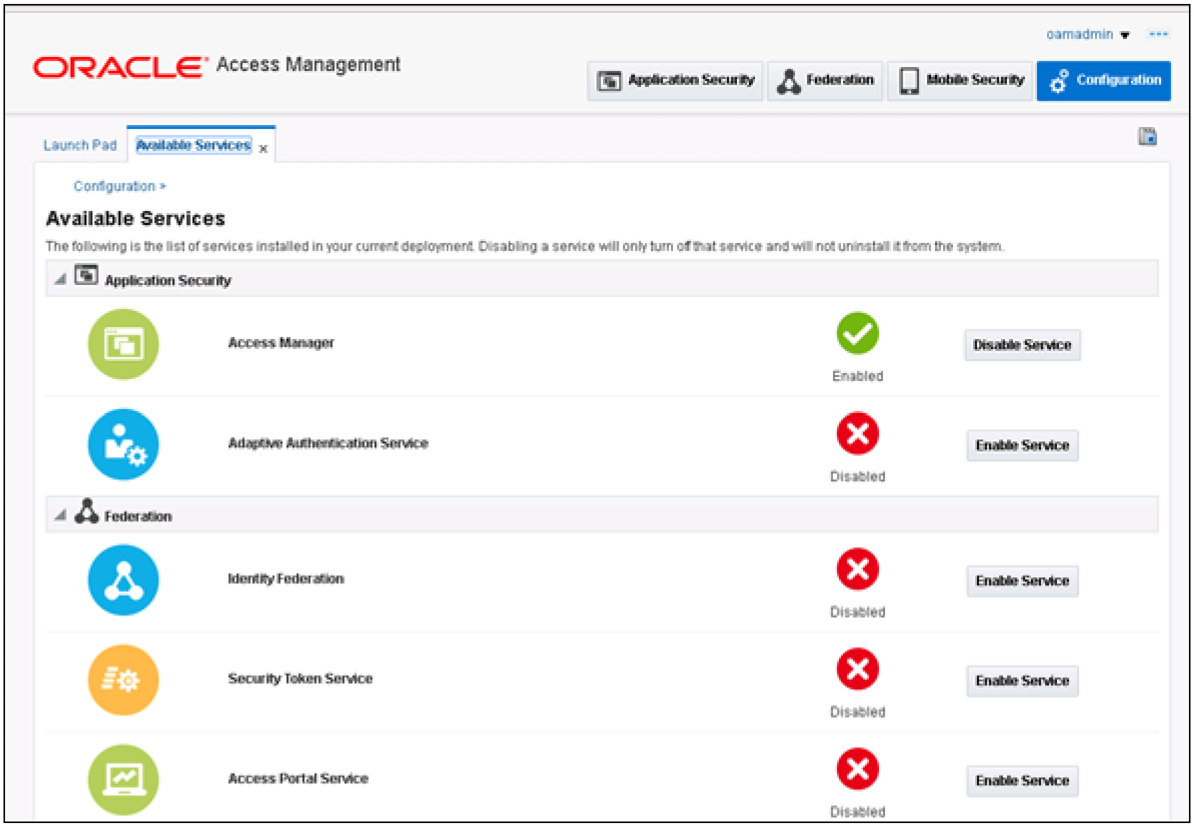
Available Services

The following is the list of services installed in your current deployment. Disabling a service will only turn off that service and will not uninstall it from the system.

Figure 2: Available Services

The list of services installed in current deployment appears. The green and red status symbols highlight whether the corresponding service is enabled or disabled. Green check mark indicates Enabled service and Red cross mark indicating Disabled service.

4. Click the **Enable Service** button corresponding to the Identity Federation service in the **Federation** section.



Available Services

The following is the list of services installed in your current deployment. Disabling a service will only turn off that service and will not uninstall it from the system.

Application Security

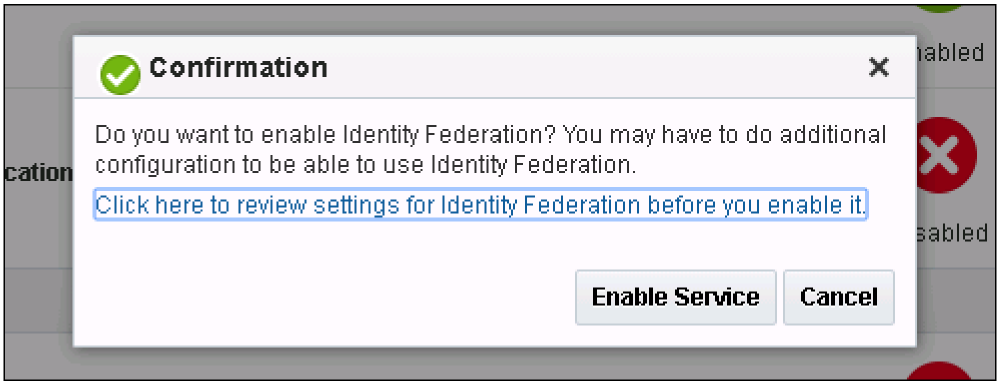
Access Manager	Enabled	Disable Service
Adaptive Authentication Service	Disabled	Enable Service

Federation

Identity Federation	Disabled	Enable Service
Security Token Service	Disabled	Enable Service
Access Portal Service	Disabled	Enable Service

Figure 3: Identity Federation - Disabled Service

5. A confirmation message appears. Click **Enable Service**.

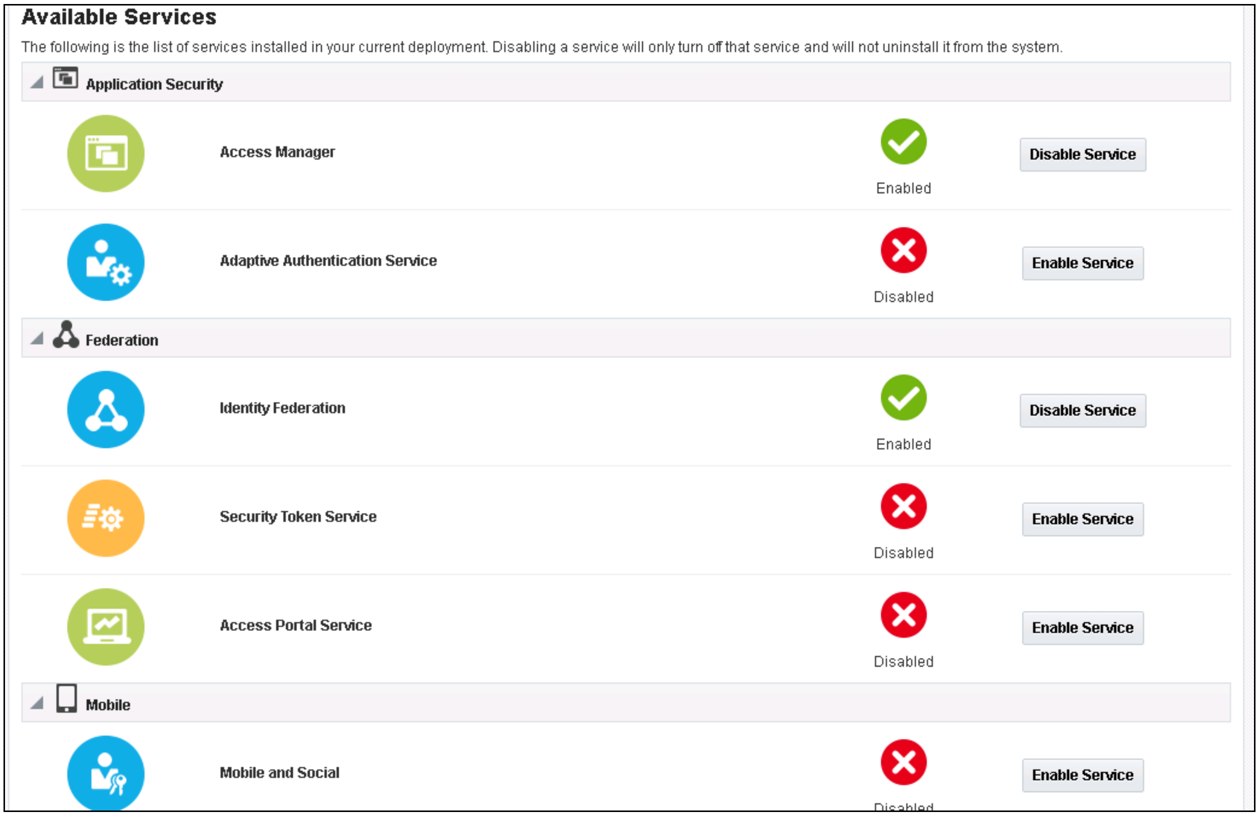


Do you want to enable Identity Federation? You may have to do additional configuration to be able to use Identity Federation.

Click here to review settings for Identity Federation before you enable it.

Figure 4: Confirmation Message

6. The **Enabled** icon appears corresponding to the adaptive authentication service indicating that the service is enabled.



Available Services

The following is the list of services installed in your current deployment. Disabling a service will only turn off that service and will not uninstall it from the system.

◢ Application Security

Access Manager	✓ Enabled	Disable Service
Adaptive Authentication Service	✕ Disabled	Enable Service

◢ Federation

Identity Federation	✓ Enabled	Disable Service
Security Token Service	✕ Disabled	Enable Service
Access Portal Service	✕ Disabled	Enable Service

◢ Mobile

Mobile and Social	✕ Disabled	Enable Service

Figure 5: Identity Federation - Enabled Service

3.2 Administering Identity Provider

When Access Manager is configured as a Federation Service Provider, you must register external Identity Provider partners to set up OAM server as IDP. To register an identity provider partner:

1. Login to Oracle Access Management using the administrator's credentials.
2. Click the **Federation** button. The **Launch Pad** tab appears.
3. Click the **Identity Provider Management** link in **Federation** section.

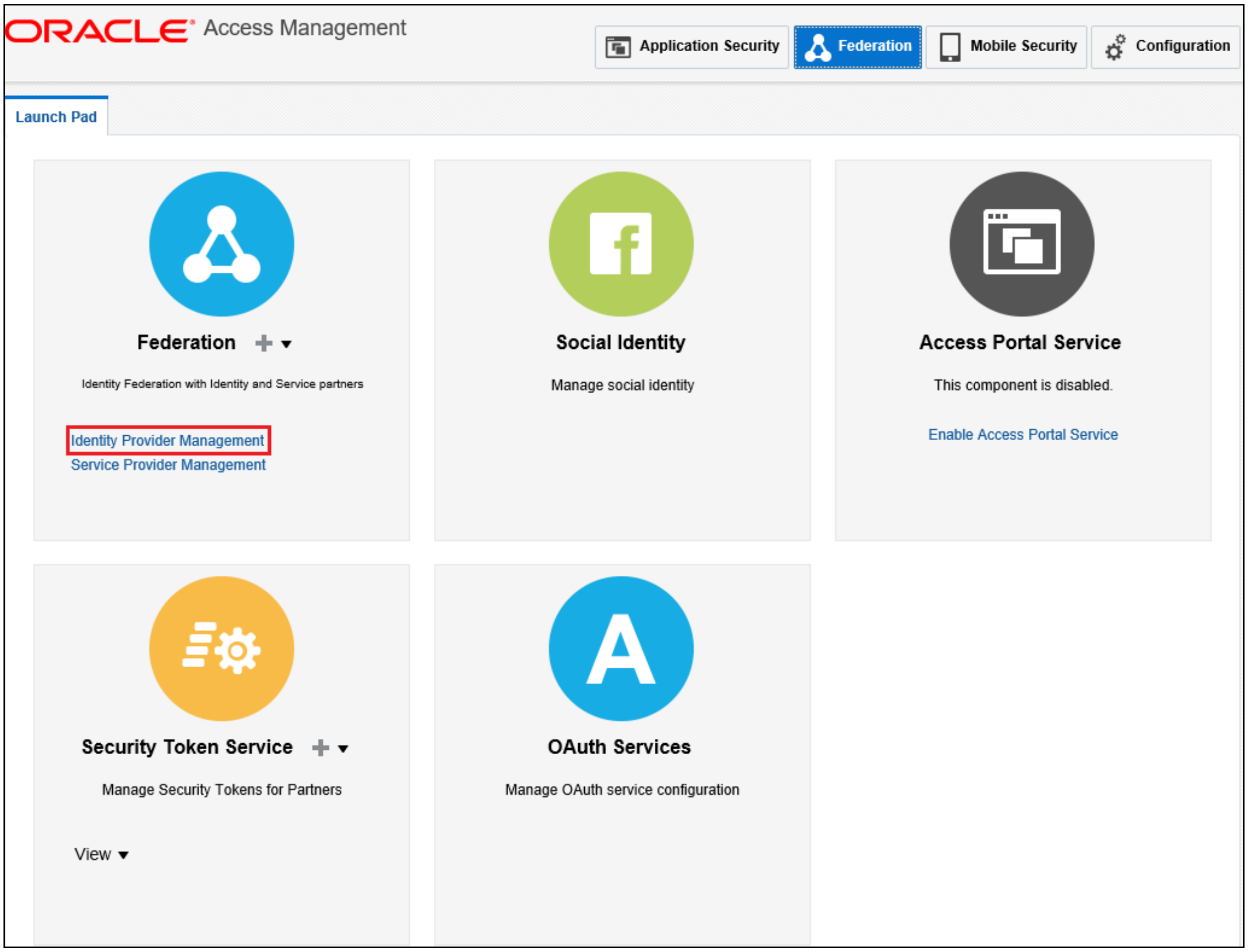
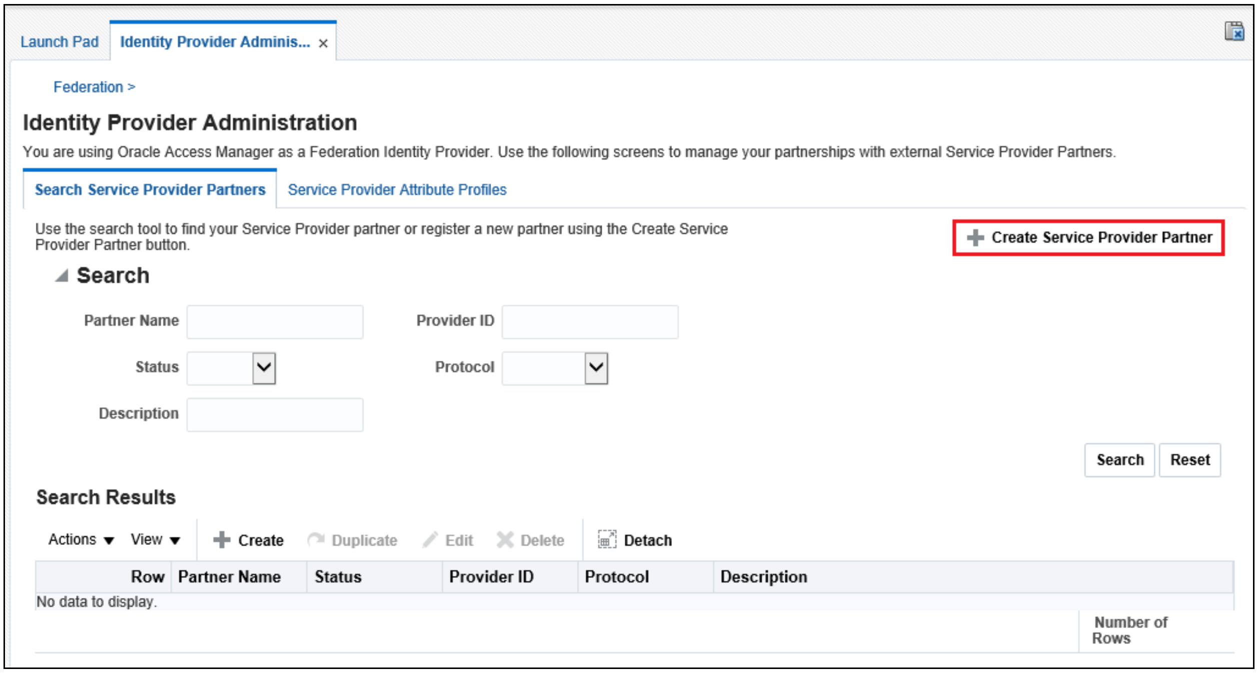

ORACLE Access Management
Application Security
Federation
Mobile Security
Configuration
Launch Pad
Federation
Identity Federation with Identity and Service partners
Identity Provider Management
Service Provider Management
Social Identity
Manage social identity
Access Portal Service
This component is disabled.
Enable Access Portal Service
Security Token Service
Manage Security Tokens for Partners
View
OAuth Services
Manage OAuth service configuration

Figure 6: Federation - Identity Provider Management

4. The **Identity Provider Administration** tab appears. Click **Create Service Provider Partner**.



Identity Provider Administration

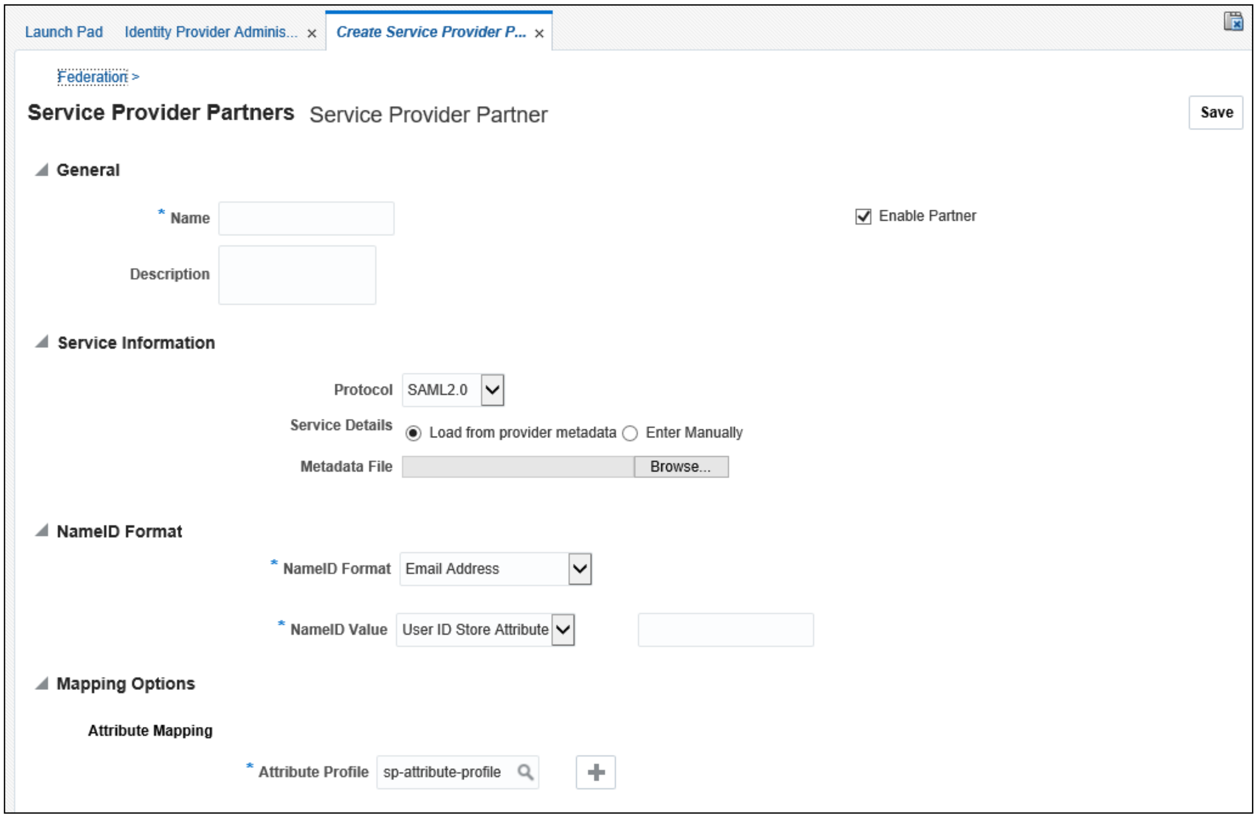
You are using Oracle Access Manager as a Federation Identity Provider. Use the following screens to manage your partnerships with external Service Provider Partners.

Use the search tool to find your Service Provider partner or register a new partner using the Create Service Provider Partner button.

No data to display.

Figure 7: Identity Provider Administration

5. **Create Service Provider Partner** screen appears.



Service Provider Partners Service Provider Partner

General

☑ Enable Partner

Service Information

Protocol: SAML2.0

Service Details: ● Load from provider metadata ○ Enter Manually

NameID Format

* NameID Format: Email Address

* NameID Value: User ID Store Attribute

Mapping Options

Attribute Mapping

* Attribute Profile: sp-attribute-profile

Figure 8: Service Provider Partners Screen

6. Enter a name for the Service Provider partner. For example, mum00xxx_sp.

7. Click **Browse** button corresponding to **Metadata File** to select and open the Metadata.xml file that you saved from Service Provider Server (SP).
8. Select 'User ID Store Attribute' from the **NameID Value** drop-down list and then specify **NameID Value**. For example uid.

Note: The user's uid attributes will be used to map the user to Service Provider Server.

9. Click **Save**.

3.3 Exporting OAM SAML Metadata

To export the metadata:

1. Login to Oracle Access Management using the administrator's credentials.
2. Click the **Configuration** button. The **Launch Pad** tab appears.
3. Click **View** button present within the **Settings** section.

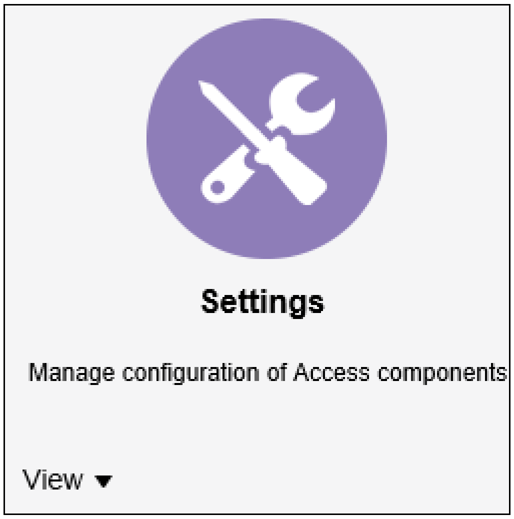
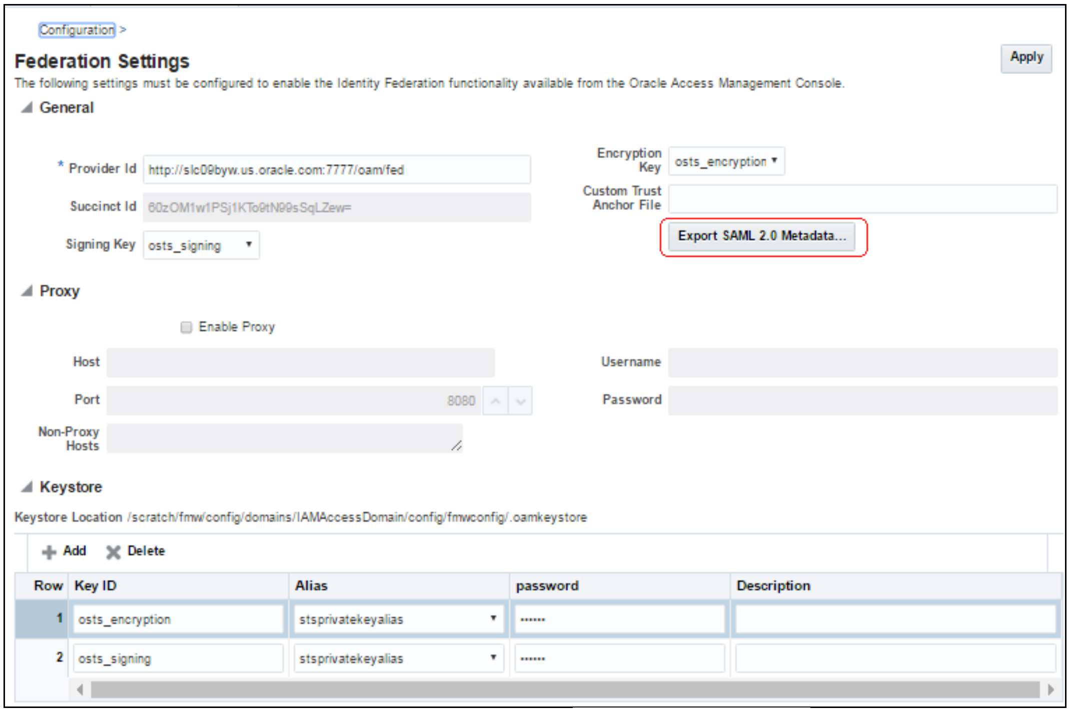


Figure 9: Configuration - Settings

4. Select **Federation** from the **View** list. The **Federation Settings** tab appears.

The unique Provider Id for the OIF instance is defined in these settings. This section also allows to export SAML 2.0 Metadata which can be exchanged with the Identity Provider.

Note that some IDPs can access the server directly and periodically download the metadata to keep it fresh whereas some IDPs require the metadata to be manually exchanged. You can export the metadata using this screen and import the same in the IDP.



Configuration >

Federation Settings

The following settings must be configured to enable the Identity Federation functionality available from the Oracle Access Management Console.

General

* Provider Id: http://slc09byw.us.oracle.com:7777/oam/fed

Succinct Id: 60zOM1w1PSj1KTo9tN99sSqLZew=

Signing Key: osts_signing

Encryption Key: osts_encryption

Custom Trust Anchor File:

Proxy

□ Enable Proxy

Host:

Port: 8080

Non-Proxy Hosts:

Username:

Password:

Keystore

Keystore Location /scratch/fmw/config/domains/IAMAccessDomain/config/fmwconfig/.oamkeystore

Row	Key ID	Alias	password	Description
1	osts_encryption	stsprivatekeyalias	••••••	
2	osts_signing	stsprivatekeyalias	••••••	

Figure 10: Federation Settings

4. Steps to be executed on SP (OAM Server as SP)

Prerequisite

To set up federated identity on IDP, you should have:

- Access Manager Service and the Identity Federation service enabled in OAM.

Procedure

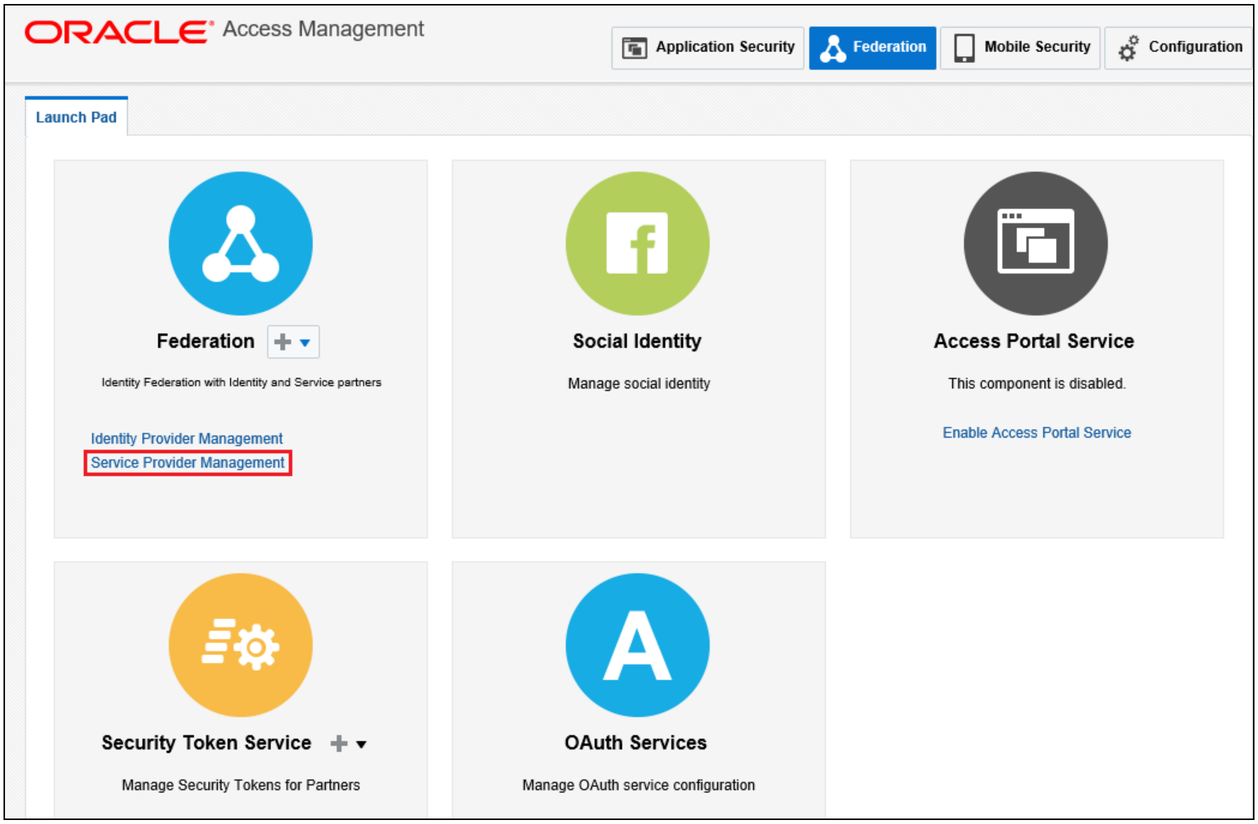
1. To enable Identity Federation Service, refer Enabling Identity Federation Service section.
2. Once Identity Federation Service is enabled, you need to complete the following activities in the specified order to set up OAM server as SP:
    1. Administer service provider
    2. Enabling JIT user provisioning in OIF
    3. Defining WebGate agent
    4. Configuring federated logout settings
    5. Downloading WebGate agent
    6. Configuring authentication policy for the application domain

4.1 Administering Service Provider

When Access Manager is configured as a Federation Service Provider, you must register external Service Provider partners to set up OAM server as SP.

To register a service provider partner:

1. Login to Oracle Access Management using the administrator’s credentials.
2. Click the **Federation** button. The **Launch Pad** tab appears.
3. Click the **Service Provider Management** link in **Federation** section.



Identity Federation with Identity and Service partners

Manage social identity

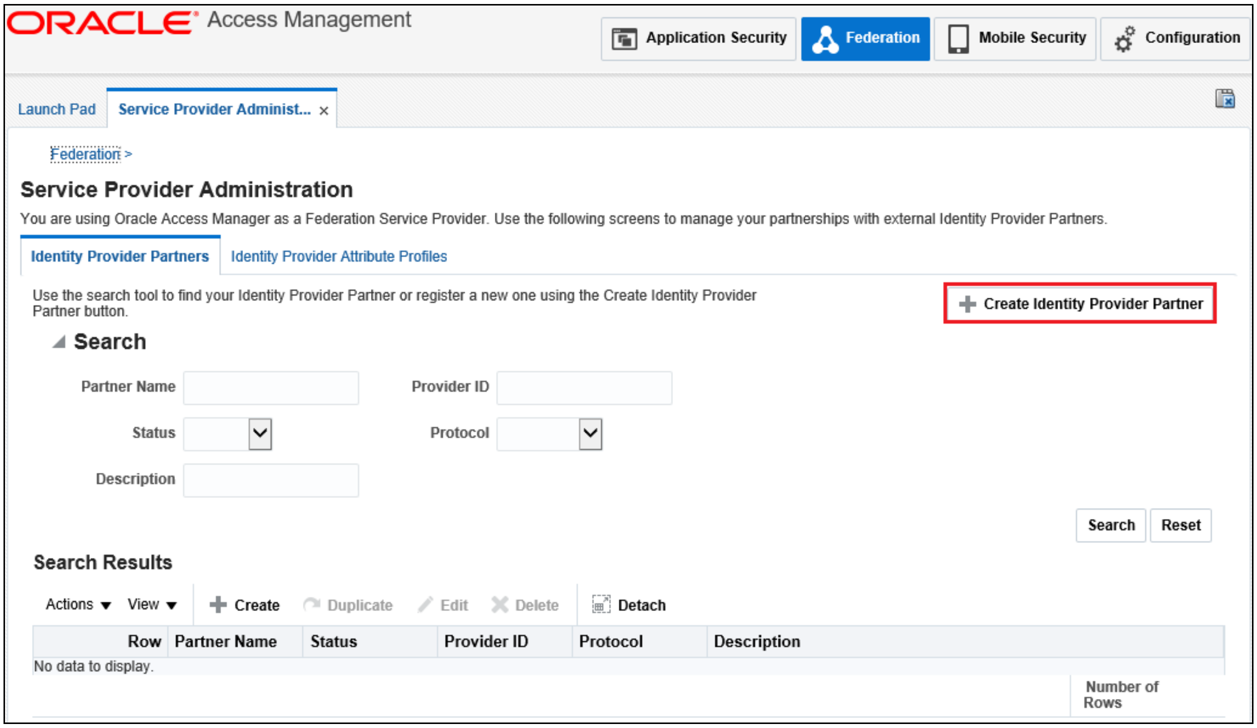
This component is disabled.

Manage Security Tokens for Partners

Manage OAuth service configuration

Figure 11: Federation – Service Provider Management

4. The **Service Provider Administration** tab appears. Click **Create Identity Provider Partner** button.



Service Provider Administration

You are using Oracle Access Manager as a Federation Service Provider. Use the following screens to manage your partnerships with external Identity Provider Partners.

Use the search tool to find your Identity Provider Partner or register a new one using the Create Identity Provider Partner button.

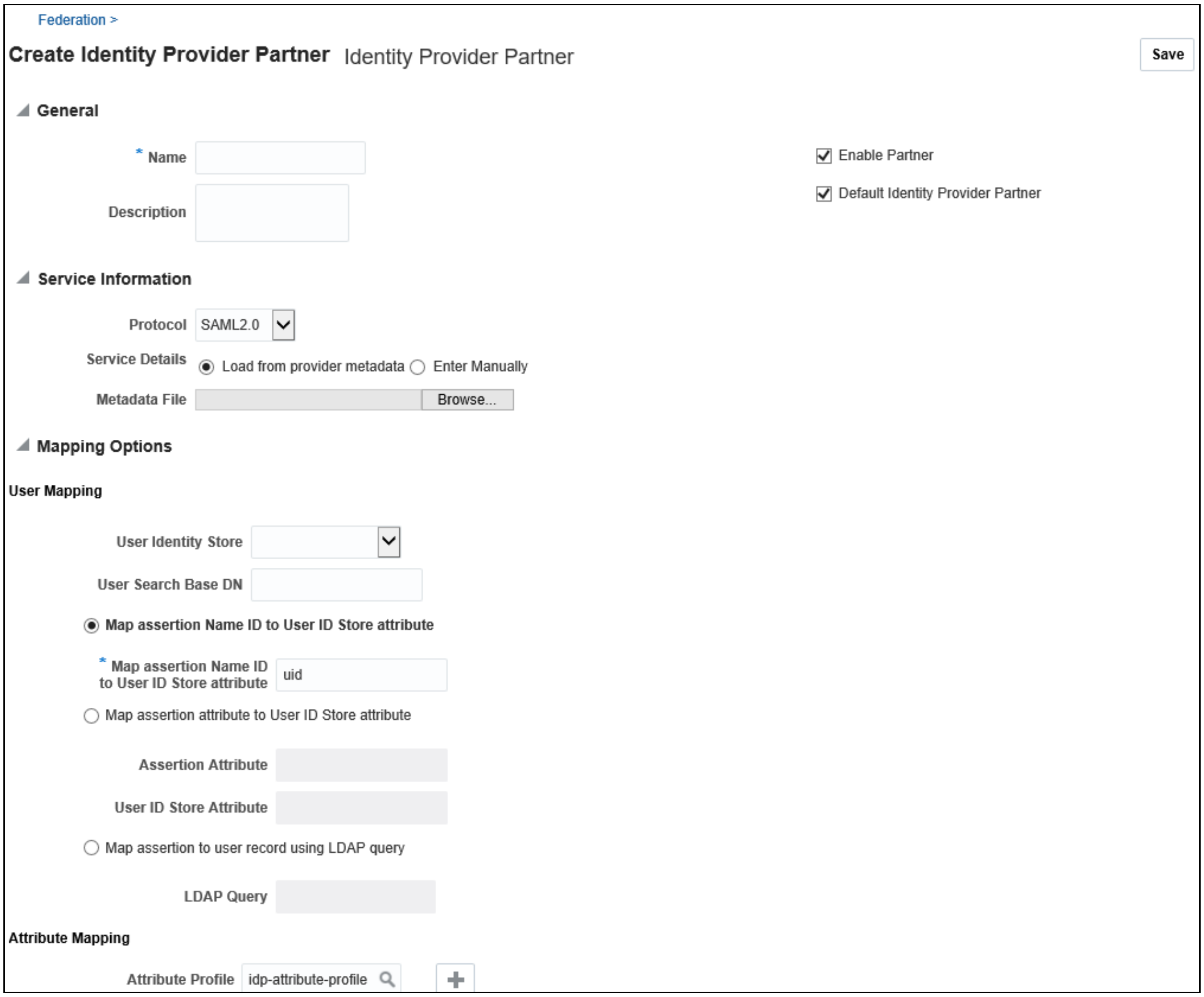
Search Results

Row	Partner Name	Status	Provider ID	Protocol	Description

No data to display.

Figure 12: Service Provider Administration

5. **Create Identity Provider Partner** screen appears.



Federation >

Create Identity Provider Partner Identity Provider Partner

Save

General

* Name

Description

☑ Enable Partner

☑ Default Identity Provider Partner

Service Information

Protocol SAML2.0

Service Details ● Load from provider metadata ○ Enter Manually

Metadata File Browse...

Mapping Options

User Mapping

User Identity Store

User Search Base DN

● Map assertion Name ID to User ID Store attribute

* Map assertion Name ID to User ID Store attribute uid

○ Map assertion attribute to User ID Store attribute

Assertion Attribute

User ID Store Attribute

○ Map assertion to user record using LDAP query

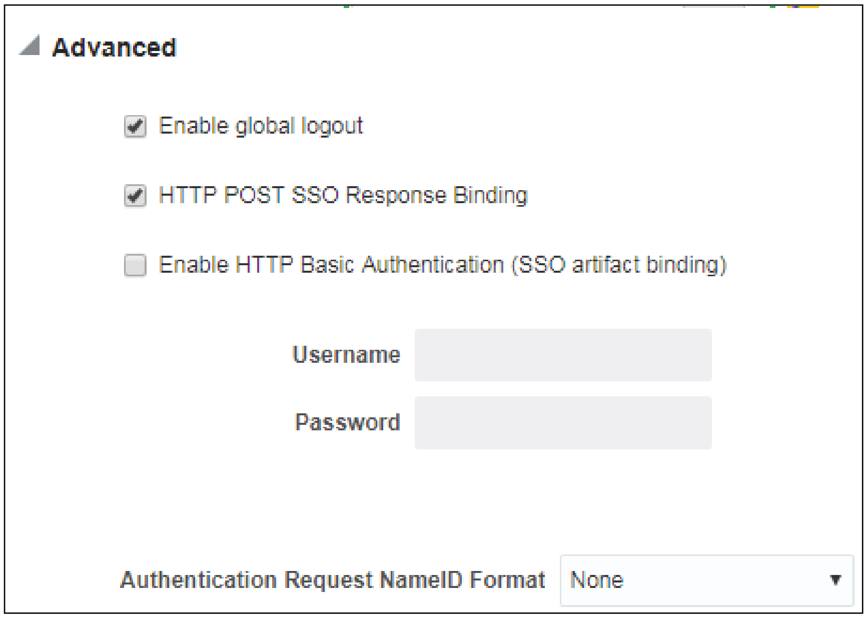
LDAP Query

Attribute Mapping

Attribute Profile idp-attribute-profile

Figure 13: Identity Provider Partner

6. Enter name for the Service Provider partner. For example, mum00xxx_Idp.
7. Select 'SAML 2.0' from the **Protocol** drop-down list.
8. Click **Browse** button corresponding to Metadata File to select and upload the SAML 2.0 Metadata file from the IDP.
9. Optionally set the OAM Identity Store that should be used.
10. Optionally set the User Search Base DN (If the value is not set, it will use the user search base DN configured in the Identity Store)
11. Enter value in **Map assertion Name ID to User ID Store attribute** to select how the mapping will occur. For example, 'uid'. This will map the Assertion via the NameID to the LDAP uid attribute.
12. Select the Attribute Profile that will be used to map the names of the attributes in the incoming SAML Assertion to local names.



Advanced

☑ Enable global logout

☑ HTTP POST SSO Response Binding

☐ Enable HTTP Basic Authentication (SSO artifact binding)

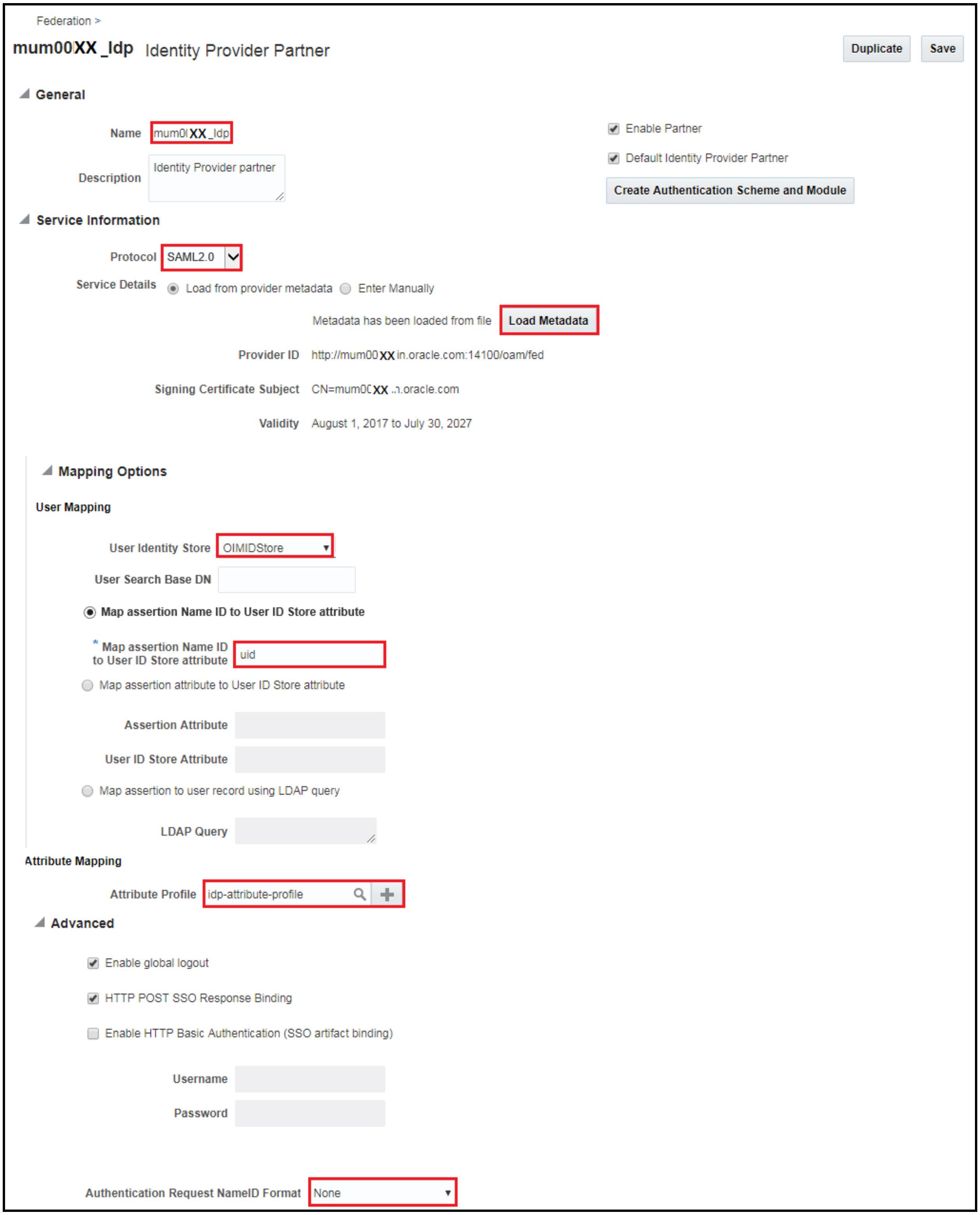
Username

Password

Authentication Request NameID Format: None

Figure 14: Identity Provider Partner - Advanced Option

13. When you enter all the required values, you will see an additional option ‘Advanced’.
14. Select **Enable global logout** and **HTTP POST SSO Response Binding** options.
15. Select ‘None’ from the **Authentication Request NameID Format** drop-down list.
16. Click **Save** button to save this information.



mum00XX _Idp Identity Provider Partner

◢ General

Name: mum0(XX_Idp

Description: Identity Provider partner

☑ Enable Partner

☑ Default Identity Provider Partner

◢ Service Information

Protocol: SAML2.0

Service Details: ● Load from provider metadata ○ Enter Manually

Metadata has been loaded from file

Provider ID: http://mum00XX in.oracle.com:14100/oam/fed

Signing Certificate Subject: CN=mum0(XX .n.oracle.com

Validity: August 1, 2017 to July 30, 2027

◢ Mapping Options

User Mapping

User Identity Store: OIMIDStore

User Search Base DN:

● Map assertion Name ID to User ID Store attribute

* Map assertion Name ID to User ID Store attribute: uid

○ Map assertion attribute to User ID Store attribute

Assertion Attribute:

User ID Store Attribute:

○ Map assertion to user record using LDAP query

LDAP Query:

Attribute Mapping

Attribute Profile: idp-attribute-profile

◢ Advanced

☑ Enable global logout

☑ HTTP POST SSO Response Binding

☐ Enable HTTP Basic Authentication (SSO artifact binding)

Username:

Password:

Authentication Request NameID Format: None

Figure 15: Service Provider Administration

4.2 Enabling JIT User Provisioning in OIF

Prerequisite

To enable JIT user provisioning in OIF, you should:

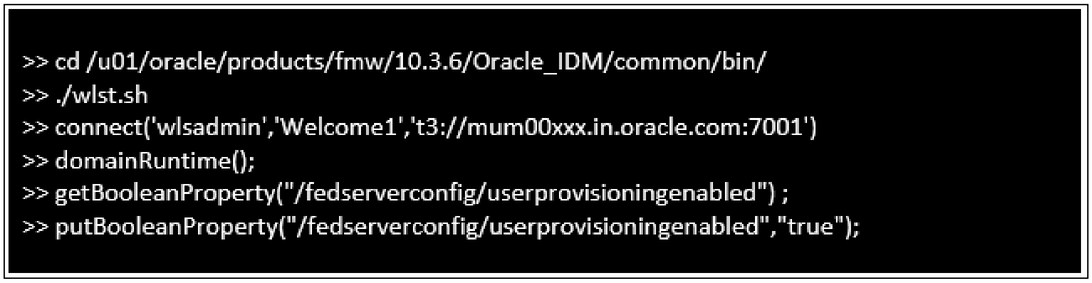
- Restart the WebLogic Admin and OAM manage server.

Procedure

To enable JIT user provisioning:

1. Execute below WLST commands using Putty:

```
connect('oamadmin','<password>','t3://<OAM-host>:7001');

cd /u01/oracle/products/fmw/10.3.6/Oracle_IDM/common/bin/

./wlst.sh

connect('wlsadmin','Welcome1','t3://mum00XXX.in.oracle.com:7001
');

domainRuntime();

getBooleanProperty("/fedserverconfig/userprovisioningenabled");

putBooleanProperty("/fedserverconfig/userprovisioningenabled","
true");
```



```
>> cd /u01/oracle/products/fmw/10.3.6/Oracle_IDM/common/bin/
>> ./wlst.sh
>> connect('wlsadmin','Welcome1','t3://mum00xxx.in.oracle.com:7001')
>> domainRuntime();
>> getBooleanProperty("/fedserverconfig/userprovisioningenabled") ;
>> putBooleanProperty("/fedserverconfig/userprovisioningenabled","true");
```

4.3 Defining WebGate Agent

1. Login to Oracle Access Management using the administrator’s credentials.
2. Click the **Application Security** button. The **Launch Pad** tab appears.
3. Click the **Agents** icon.

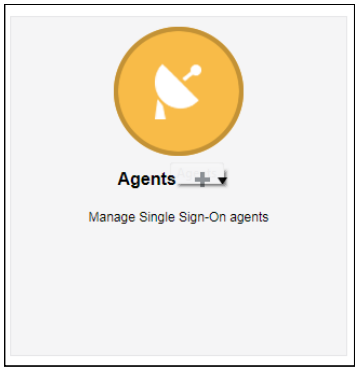
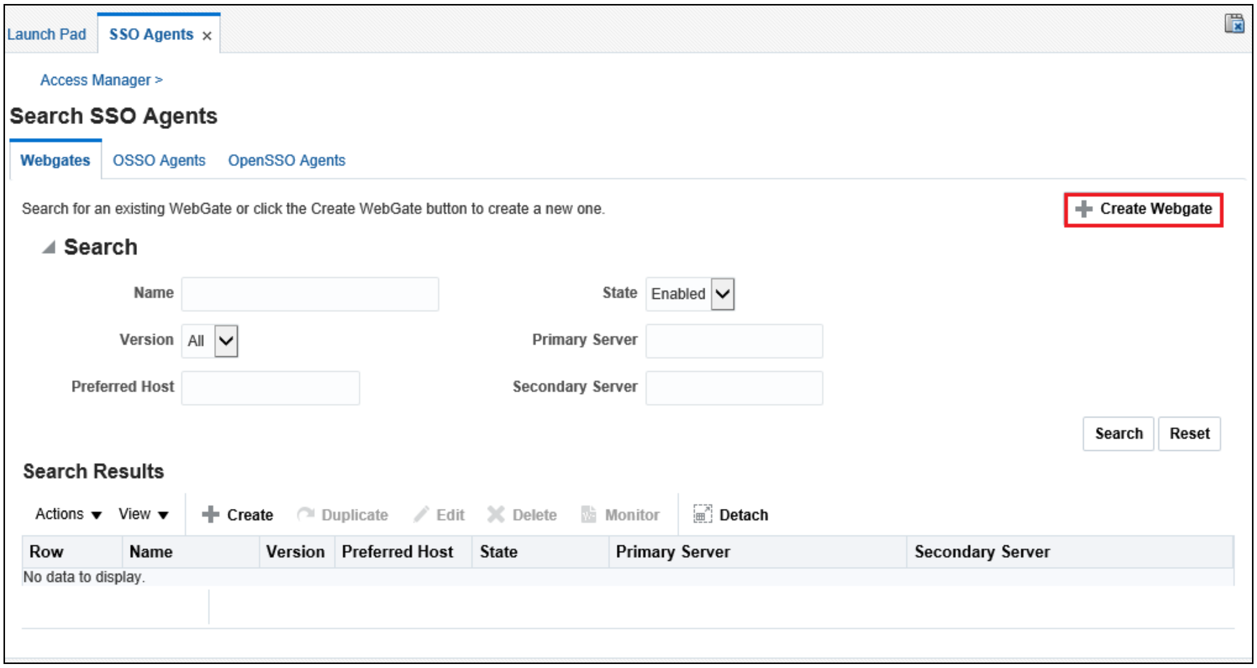


Figure 16: Application Security - Agents

4. **Search SSO Agents** tab appears. Click **Create Webgate**.



Search for an existing WebGate or click the Create WebGate button to create a new one.

Row	Name	Version	Preferred Host	State	Primary Server	Secondary Server

No data to display.

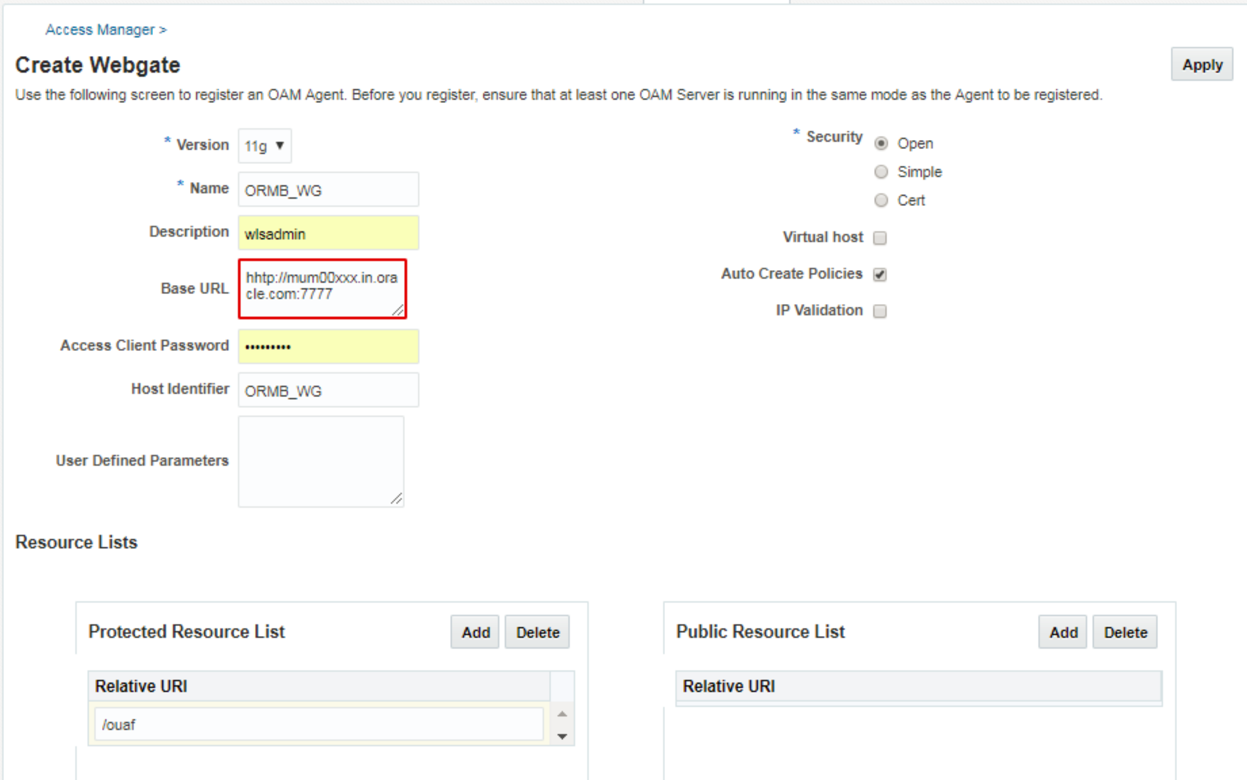
Figure 17: Search SSO Agents

5. **Create WebGate** screen appears. Enter the following parameter values.

Parameter	Description	Mandatory (Yes or No)
Version	Used to define WebGate version. For example, 11g.	Yes
Name	Used to define unique identifying name for this Agent registration. This is often the name of the computer that is hosting the web server used by WebGate.	Yes
Description	Used to define description.	No
Base URL	Used to define the host and port of the computer on which the Web server for the WebGate is installed. For example, http://example_host:port or https://example_host:port.	No

Parameter	Description	Mandatory (Yes or No)
Access Client Password	Used to authenticate a registered WebGate and prevent unauthorized WebGates from connecting to OAM Servers and obtaining policy information.	No
Security	Used to define the level of communication transport security between the Agent and the OAM Server (this must match the level specified for the OAM Server). The valid values are: • Open - No transport security. • Simple - SSL v3/TLS v1.0 secure transport using dynamically generated session keys. • Cert - SSL v3/TLS v1.0 secure transport using server side x.509 certificates. Choosing this option displays a field where you can enter the Agent Key Password.	No
Host Identifier	Used to represent the Web server host. This is automatically seeded with the value in the agent Name field.	No
User-defined Parameters	Used to define parameters to enable specific WebGate behaviors. **Note:** Specify multiple User Defined Parameters separated by a new line. They should be of the form 'Attribute=Value'.	No
Virtual Host	Flag to validate if a WebGate is installed on a Web server that contains multiple Web site and domain names. **Note:** The WebGate must reside in a location that enables it to protect all of the Web sites on that server.	No
Auto Create Policies	Flag to check whether authentication and authorization policies are to be created automatically during agent registration.	No If Selected, authentication and authorization policies are created automatically.
IP Validation	Flag to validate whether a client's IP address is the same as the IP address stored in the ObSSOCookie generated for single sign-on.	No

Parameter	Description	Mandatory (Yes or No)
IP Validation Exceptions	Used to define IP addresses to be excluded from validation using standard notation for the addresses. For example, 10.20.30.123.	No
Protected Resource (URI) List	Used to define URIs for the protected application. For example, /myapp/login **Note:** Each URI for the protected application should be specified in a new row of the table for the Protected Resource List. Default value: /**	No
Public Resource (URI) List	Used to define public application for the Public Resource List.	No



Access Manager >

Create Webgate

Use the following screen to register an OAM Agent. Before you register, ensure that at least one OAM Server is running in the same mode as the Agent to be registered.

* Version: 11g
* Name: ORMB_WG
Description: wlsadmin
Base URL: hhttp://mum00xxx.in.oracle.com:7777
Access Client Password: •••••••••
Host Identifier: ORMB_WG
User Defined Parameters:

* Security: ● Open ○ Simple ○ Cert
Virtual host: □
Auto Create Policies: ☑
IP Validation: □

Resource Lists

Protected Resource List

Relative URI
/ouaf

Public Resource List

Relative URI

Figure 18: Create WebGate

Note: It may be necessary to add “User Defined Parameter” authorizationResultCacheTimeout=0. The default for this is 15 seconds, but in local tests, it intermittently caused online logins to be rejected with “Invalid SAML Assertion” errors in the OUAF application’s log. Disabling this cache prevented these errors and made for a smoother login experience. It is not clear exactly what effect this setting has on performance or anything else; our tests so far have shown no noticeable differences.

4.4 Configuring Federated Logout Settings

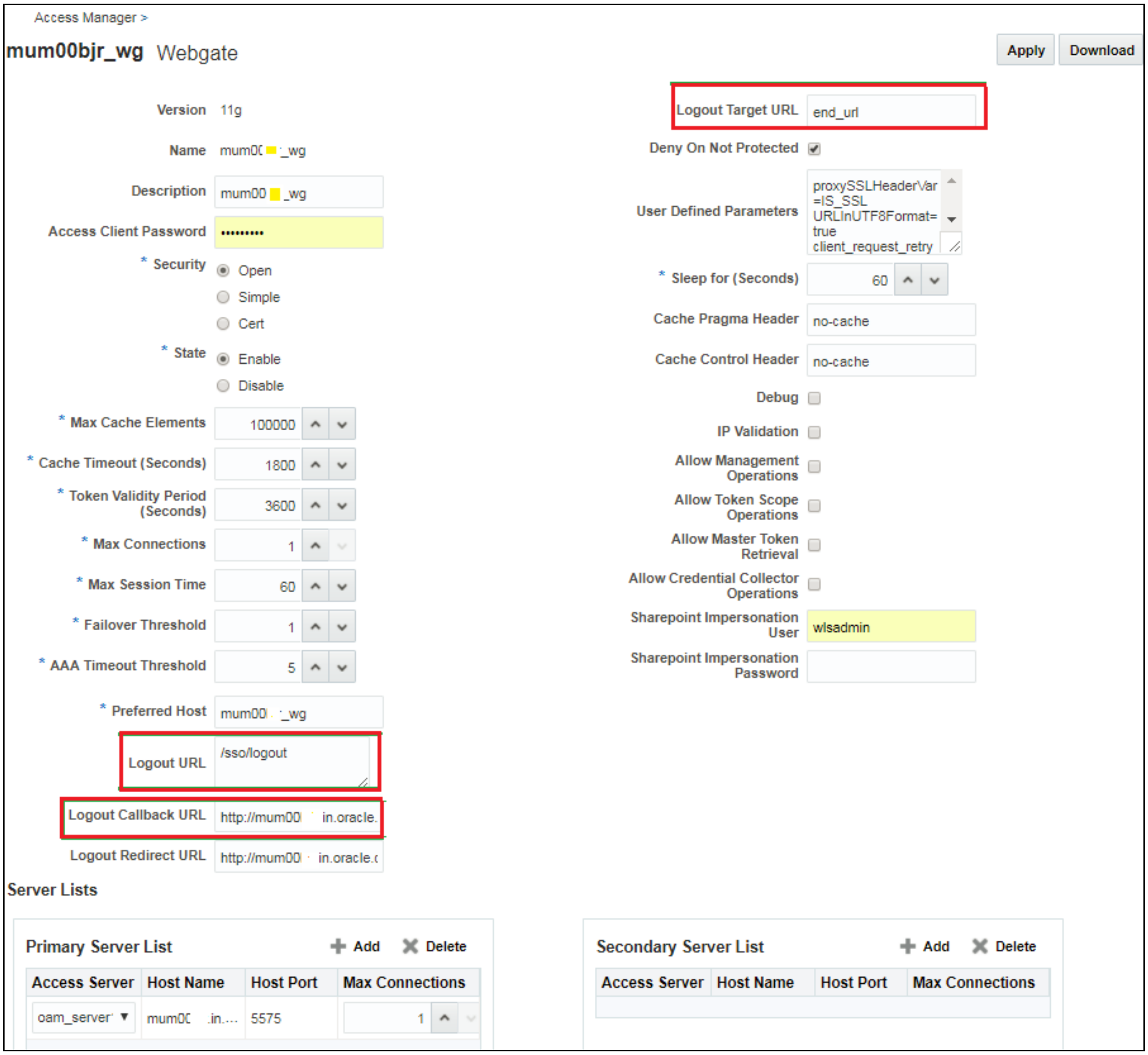
The WebGate configuration defined in Defining WebGate Agent can be modified to redirect to the third party IDP's logout URL.

For example, `http://<OAM server address>/oam/server/logout` must be called to end the OAM session.

To configure settings for Federated Logout:

1. Login to Oracle Access Management using the administrator's credentials.
2. Click the **Application Security**. The **Launch Pad** tab appears.
3. Click the **Agents** icon.
4. In the **Search** section, click **Search.**
5. In the **Search Results** section, select the newly created WebGate agent from the list.
6. Update the values in following fields:

Parameter	Description
Logout Callback URL	Specify the third party IDP's logout URL. OAM logout URL: http://mum00xxx.in.oracle.com:14100/oam/server/logout?end_url=http://mum00xxx.in.oracle.com:7001/oamconsole//faces/admin.jspx
Logout URL	/sso/logout
Logout Target URL	end_url



Version 11g

Name mum0C[redacted]_wg

Description mum00[redacted]_wg

Access Client Password ••••••••

* Security ● Open ○ Simple ○ Cert

* State ● Enable ○ Disable

* Max Cache Elements 100000

* Cache Timeout (Seconds) 1800

* Token Validity Period (Seconds) 3600

* Max Connections 1

* Max Session Time 60

* Failover Threshold 1

* AAA Timeout Threshold 5

* Preferred Host mum00 _wg

Logout URL /sso/logout

Logout Callback URL http://mum00 in.oracle.

Logout Redirect URL http://mum00 in.oracle.c

Logout Target URL end_url

Deny On Not Protected ☑

User Defined Parameters proxySSLHeaderVar =IS_SSL URLInUTF8Format= true client_request_retry

* Sleep for (Seconds) 60

Cache Pragma Header no-cache

Cache Control Header no-cache

Debug ☐

IP Validation ☐

Allow Management Operations ☐

Allow Token Scope Operations ☐

Allow Master Token Retrieval ☐

Allow Credential Collector Operations ☐

Sharepoint Impersonation User wlsadmin

Sharepoint Impersonation Password

Server Lists

Primary Server List

Access Server	Host Name	Host Port	Max Connections
oam_server' ▼	mum0C .in....	5575	1

Secondary Server List

Access Server	Host Name	Host Port	Max Connections

Figure 19: Configuring Federated Logout Settings

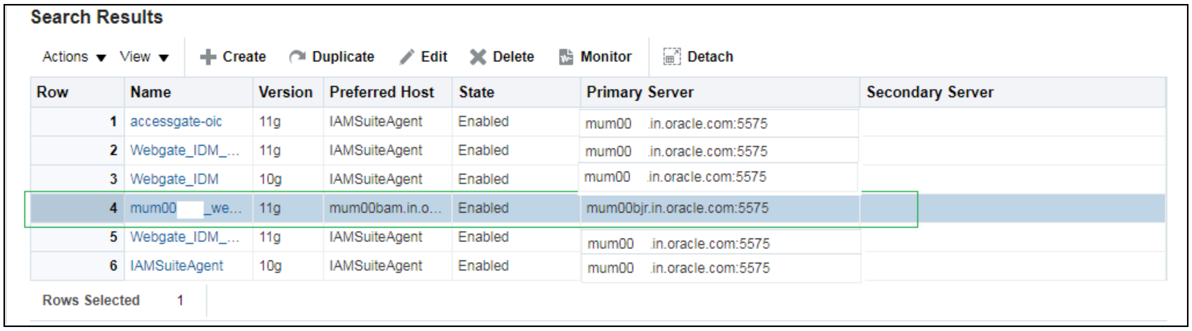
4.5 Downloading WebGate Agent

To download WebGate agent:

1. Login to Oracle Access Management using the administrator’s credentials.
2. Click the **Application Security**. The **Launch Pad** tab appears.
3. Click the **Agents** icon.
4. In the **Search Results** section, click **Search.**
5. Search for the required WebGate.

   Tip: You can click **Search** to view all existing WebGates.

6. In the **Search Results** section, select the newly created WebGate agent from the list.



Search Results

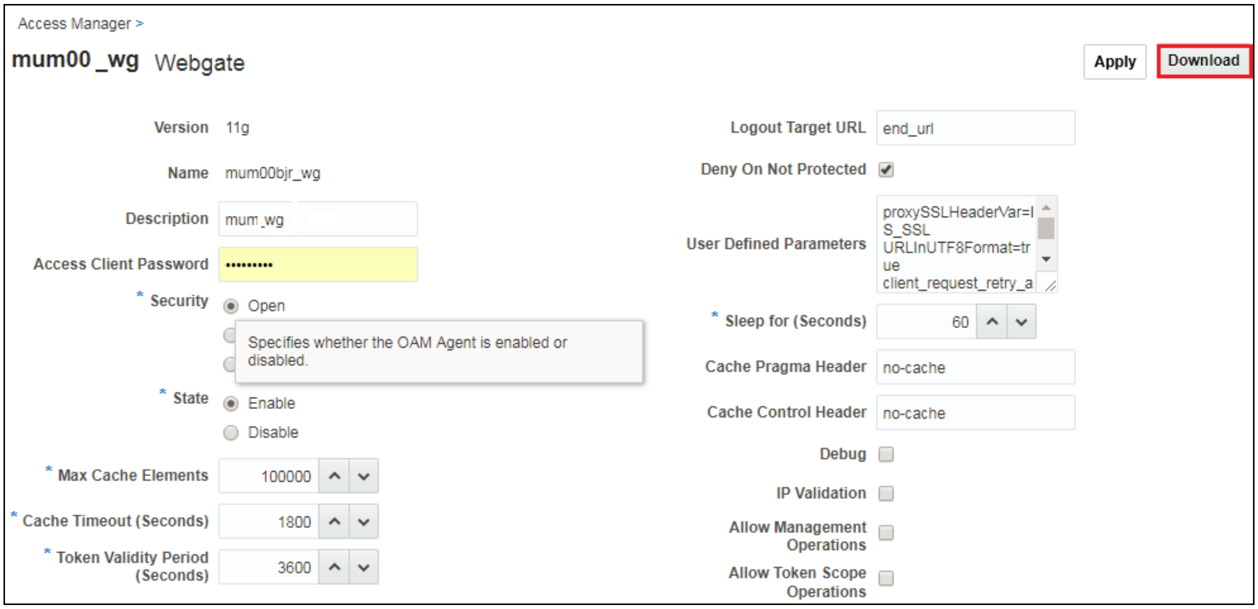
Actions ▾ View ▾ + Create Duplicate Edit Delete Monitor Detach

Row	Name	Version	Preferred Host	State	Primary Server	Secondary Server
1	accessgate-oic	11g	IAMSuiteAgent	Enabled	mum00 .in.oracle.com:5575	
2	Webgate_IDM_...	11g	IAMSuiteAgent	Enabled	mum00 .in.oracle.com:5575	
3	Webgate_IDM	10g	IAMSuiteAgent	Enabled	mum00 .in.oracle.com:5575	
4	mum00 _we...	11g	mum00bam.in.o...	Enabled	mum00bjr.in.oracle.com:5575	
5	Webgate_IDM_...	11g	IAMSuiteAgent	Enabled	mum00 .in.oracle.com:5575	
6	IAMSuiteAgent	10g	IAMSuiteAgent	Enabled	mum00 .in.oracle.com:5575	

Rows Selected 1

Figure 20: WebGate Agent Search Results

7. The WebGate screen appears. Click **Download**.



Access Manager >

mum00 _wg Webgate

Version 11g

Name mum00bjr_wg

Description mum wg

Access Client Password ••••••••••

* Security ● Open

Specifies whether the OAM Agent is enabled or disabled.

* State ● Enable ○ Disable

* Max Cache Elements 100000

* Cache Timeout (Seconds) 1800

* Token Validity Period (Seconds) 3600

Logout Target URL end_url

Deny On Not Protected ☑

User Defined Parameters proxySSLHeaderVar=I S_SSL URLInUTF8Format=true client_request_retry_a

* Sleep for (Seconds) 60

Cache Pragma Header no-cache

Cache Control Header no-cache

Debug □

IP Validation □

Allow Management Operations □

Allow Token Scope Operations □

Figure 21: Downloading WebGate Agent

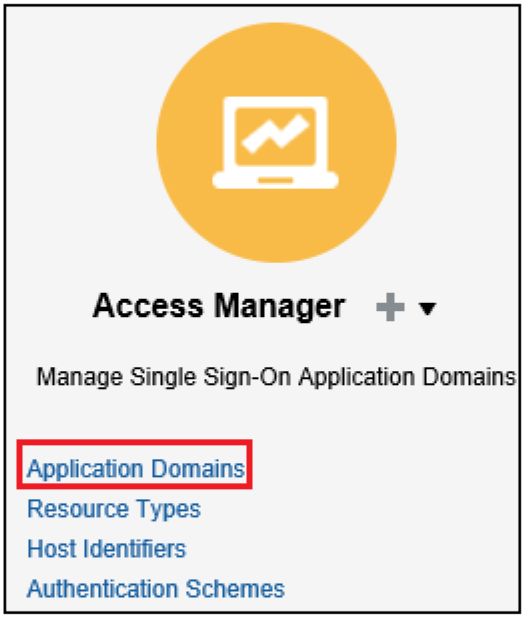
8. Save the zip file.

9. Copy downloaded files (cwallet.sso, ObAccessClient.xml, wallet) to ORMB server.

4.6 Configuring Authentication Policy for Application Domain

To configure authentication policies, follow the below steps:

1. Login to Oracle Access Management using the administrator's credentials.
2. Click the **Application Security** button. The **Launch Pad** tab appears.
3. Click the **Application Domains** link in the Access Manager section. The **Application Domain** tab appears.



Access Manager

Manage Single Sign-On Application Domains

Application Domains

Resource Types

Host Identifiers

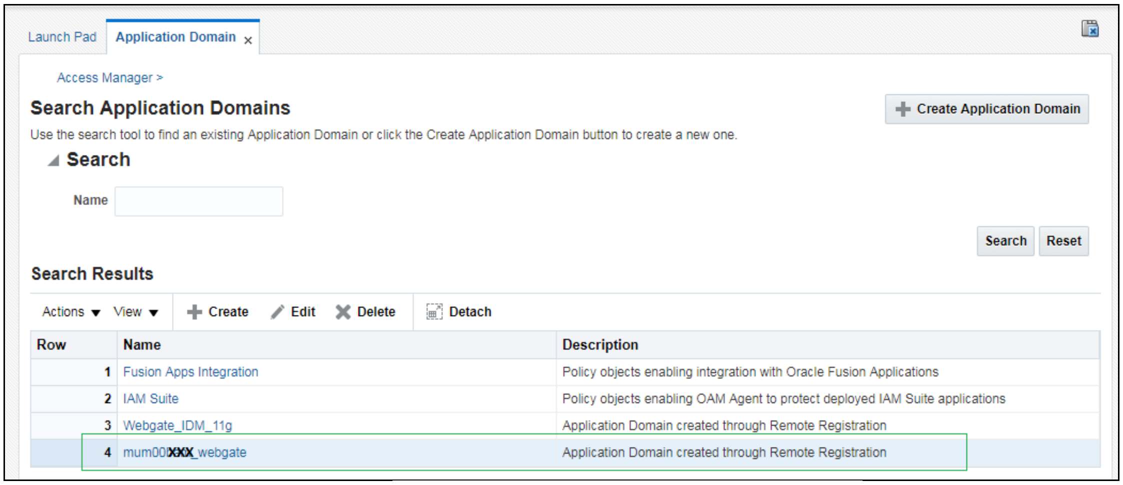
Authentication Schemes

Figure 22: Access Manager

4. Search for the required application domain in the **Application Domain** tab. For example, “mum00xxx_webgate”.

5. In the **Search Results** section, click Application Domain Name in the **Name** column whose resources you want to configure using the authentication policy.

> **Note:** The Application Domain should have been automatically generated when the WebGate Agent was created and it should have the same name as the WebGate Agent. Therefore, the given example, Application Domain “mum00xxx_webgate” should now exist.



Search Application Domains

Use the search tool to find an existing Application Domain or click the Create Application Domain button to create a new one.

Search

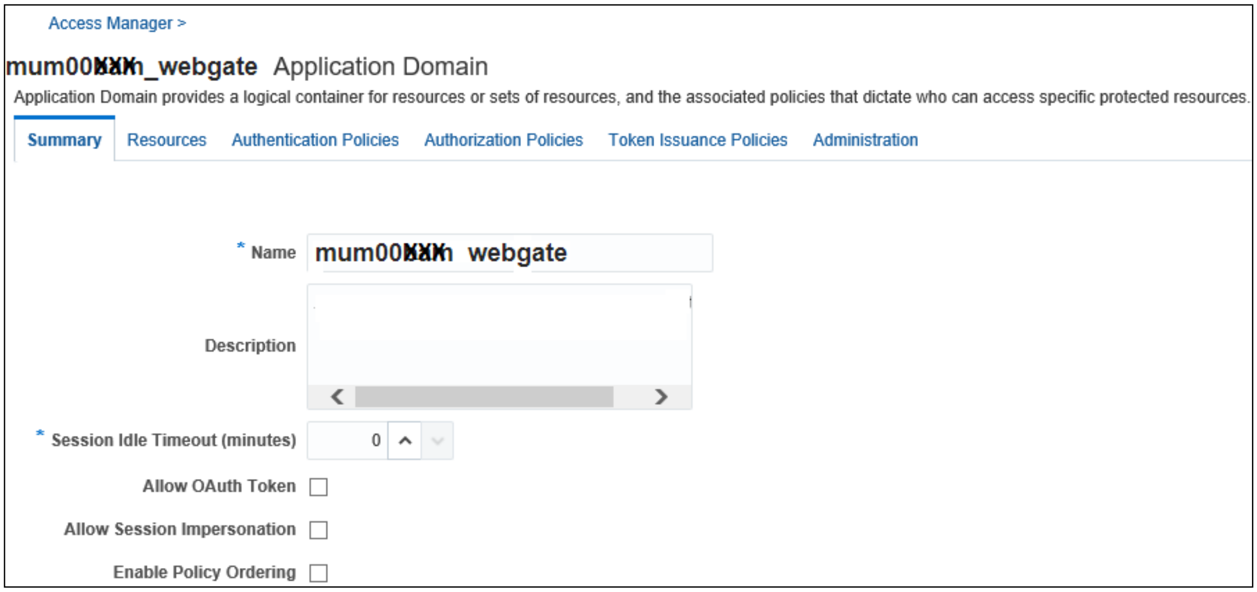
Name

Search Results

Row	Name	Description
1	Fusion Apps Integration	Policy objects enabling integration with Oracle Fusion Applications
2	IAM Suite	Policy objects enabling OAM Agent to protect deployed IAM Suite applications
3	Webgate_IDM_11g	Application Domain created through Remote Registration
4	mum00**XXX**_webgate	Application Domain created through Remote Registration

Figure 23: Search Application Domains

6. Selected Application Domain opens in a new tab.



Access Manager >

mum00[redacted]n_webgate Application Domain

Application Domain provides a logical container for resources or sets of resources, and the associated policies that dictate who can access specific protected resources.

* Name: mum00[redacted]n webgate

Description:

* Session Idle Timeout (minutes): 0

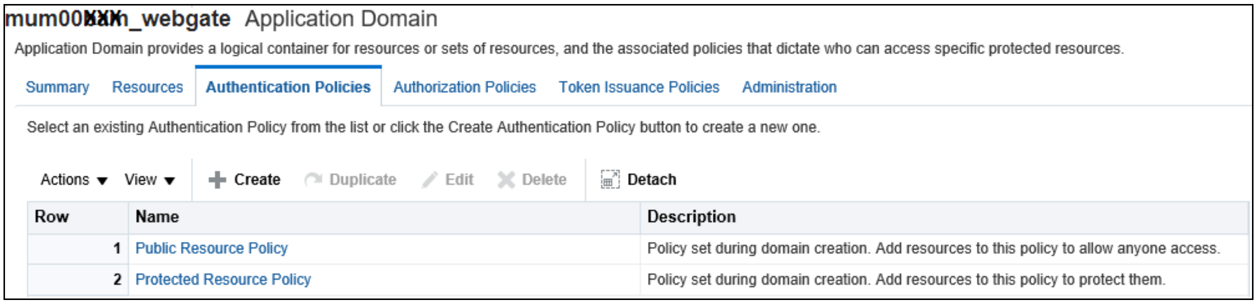
Allow OAuth Token □

Allow Session Impersonation □

Enable Policy Ordering □

Figure 24: Application Domain

7. Click the **Authentication Policies** tab. A list of existing Authentication Policies appears.



mum00[redacted]n_webgate Application Domain

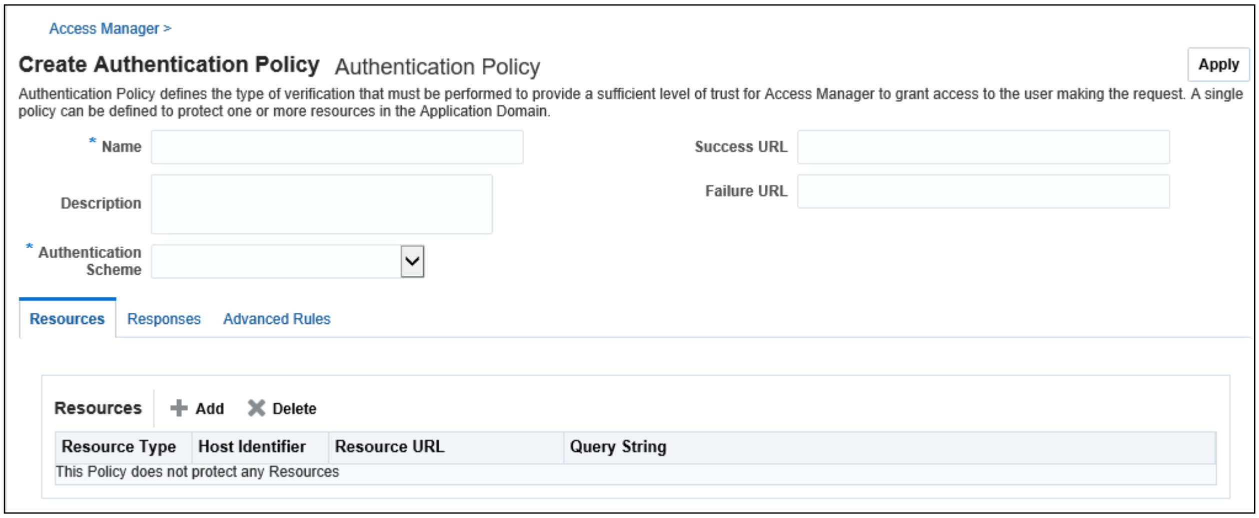
Application Domain provides a logical container for resources or sets of resources, and the associated policies that dictate who can access specific protected resources.

Select an existing Authentication Policy from the list or click the Create Authentication Policy button to create a new one.

Row	Name	Description
1	Public Resource Policy	Policy set during domain creation. Add resources to this policy to allow anyone access.
2	Protected Resource Policy	Policy set during domain creation. Add resources to this policy to protect them.

Figure 25: Application Domains - Authentication Policies

8. Click **Create** button to create a new authentication policy. The **Create Authentication Policy** tab appears.



Access Manager >

Create Authentication Policy Authentication Policy

Authentication Policy defines the type of verification that must be performed to provide a sufficient level of trust for Access Manager to grant access to the user making the request. A single policy can be defined to protect one or more resources in the Application Domain.

* Name	
Description	
* Authentication Scheme	
Success URL	
Failure URL	

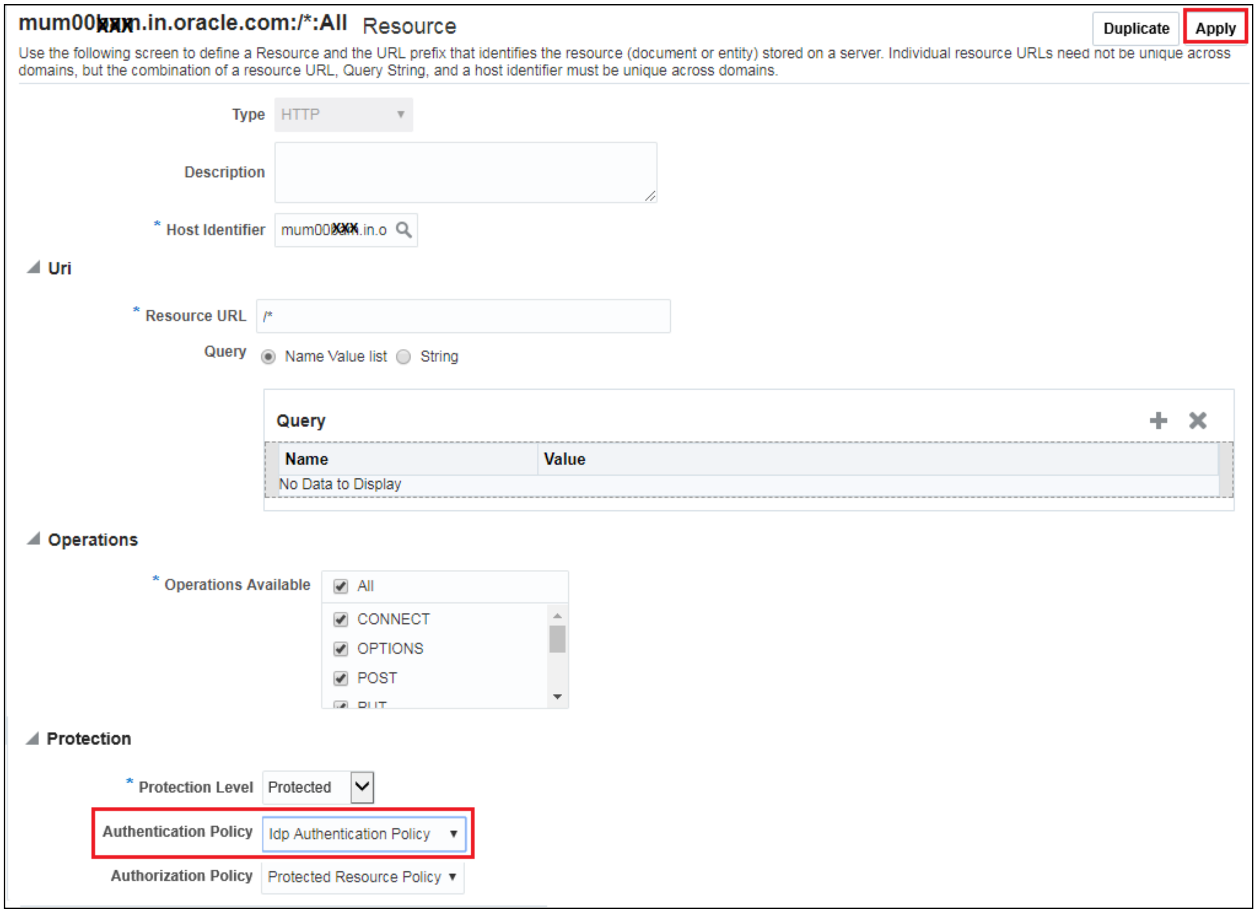
Resource Type	Host Identifier	Resource URL	Query String
This Policy does not protect any Resources			

Figure 26: Create Authentication Policy

9. Specify a name and the authentication scheme generated for the identity provider as defined Services Provider Administration section. Ensure that the entered name does not contain any punctuation marks.
10. Click **Apply**. The new authentication policy has been added.
11. To verify the policy, go to application domain’s Authentication Policies tab. The new authentication policy appears in the list.
12. Select the application domain’s Resources tab and click **Search**.
13. To add newly created Authentication Policy, click ‘HTTP’ text present in resource type field. The selected resource is highlighted. Click **Edit**.

Note: Repeat this step to attach authentication policy with all resource URLs.

14. Select the Authentication Policy name from the **Authentication Policy** drop-down list.
15. Click **Apply**.



mum00XXXn.in.oracle.com:/*:All Resource

Use the following screen to define a Resource and the URL prefix that identifies the resource (document or entity) stored on a server. Individual resource URLs need not be unique across domains, but the combination of a resource URL, Query String, and a host identifier must be unique across domains.

Type: HTTP

Description:

* Host Identifier: mum00XXX.in.o

Uri

* Resource URL: /*

Query: ● Name Value list ○ String

Query

Name	Value
No Data to Display	

Operations

* Operations Available: ☑ All

☑ CONNECT
☑ OPTIONS
☑ POST
☑ PUT

Protection

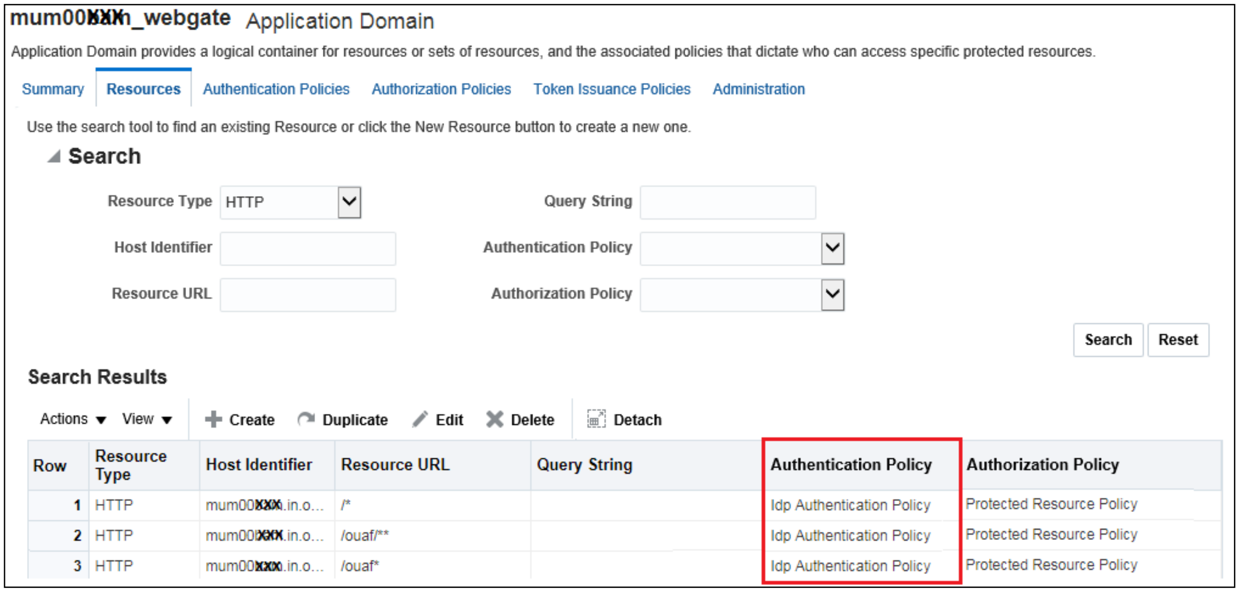
* Protection Level: Protected

Authentication Policy: Idp Authentication Policy

Authorization Policy: Protected Resource Policy

Figure 27: Attaching Authentication Policy

16. To confirm whether the authentication policy is attached, go to the Resources tab and search for the respective host.



mum00XXXn_webgate Application Domain

Application Domain provides a logical container for resources or sets of resources, and the associated policies that dictate who can access specific protected resources.

Use the search tool to find an existing Resource or click the New Resource button to create a new one.

Search

Resource Type: HTTP

Host Identifier:

Resource URL:

Query String:

Authentication Policy:

Authorization Policy:

Search Results

Row	Resource Type	Host Identifier	Resource URL	Query String	Authentication Policy	Authorization Policy
1	HTTP	mum00XXX.in.o...	/*		Idp Authentication Policy	Protected Resource Policy
2	HTTP	mum00XXX.in.o...	/ouaf/**		Idp Authentication Policy	Protected Resource Policy
3	HTTP	mum00xxx.in.o...	/ouaf*		Idp Authentication Policy	Protected Resource Policy

Figure 28: Authentication Policy

5. Steps to be executed on ORMB Application

This section lists and describes the following activities that you need to complete in the specified order to set up ORMB Application:

1. Copying WebGate Files
2. Copying required JAR files into application domain
3. Configuring the OUAF app's web.xml
4. Adding identity asserter
5. Adding WebLogic data sources
6. Adding OUAF DBMS authenticator
7. Configuring default authenticator
8. Reorder authentication providers

5.1 Copying WebGate Files

1. Download WebGate Agent by executing the steps mentioned in Downloading WebGate Agent.

   The WebGate configuration as per the section Defining WebGate Agent must be copied to the OHS/WebGate instance's config directory. For example,

   ```
   /u01/app/product/fmw/ohs/Oracle_WT1/
   instances/instance1/config/OHS/ohs1/webgate/config
   ```

5.2 Copying Required JAR Files into Application Domain

1. Copy the `<FMW_HOME>/oracle_common/modules/oracle.oamprovider_11.1.1/oamAuthnProvider.jar` from the OAM/OIF server to the ORMB application server's <domain>/lib directory.
2. Copy the `<FMW_HOME>/oracle_common/modules/oracle.oamprovider_11.1.1/oamAuthnProvider.jar` from the OAM/OIF server to the ORMB application server's "<WL_HOME>/wls12c/wlserver/server/lib/mbeantypes/" directory.
3. Copy the `…/oracle_common/modules/oracle.oamprovider_11.1.1/oamAuthnProvider.jar` from the OAM/OIF server to the WebLogic server's "<ORACLE_HOME>/oracle_common/modules/oracle.oamprovider/" directory.
4. Copy the `$SPLEBASE/tools/bin/auth/ ouaf-dbmsauth-4.3.0.4.0.jar` to the OUAF application server's <domain>/lib directory.
5. Restart the app server.

IMPORTANT: The oamAuthnProvider.jar must be the exact same one used by OAM. A version of this jar may already be in the OUAF app server's "oracle_common/modules" directory structure; that must be deleted so that the one from OAM that was copied (above) to the OUAF app's <domain>/lib directory gets used. If the same version of the OAM identity asserter is not used, SAML assertions may not be accepted and SSO logins will be mysteriously rejected.

5.3 Configuring OUAF app's web.xml

1. Specify the OUAF authentication login page type of CLIENT-CERT
   `configureEnv.sh -a` menu #52 can be used to do that
2. Change following web.xml templates from location:
   `/scratch/rmbbuild/spl/ORMB26000/templates`
   - web.xml.template
   - web.xml.appViewer.template
3. Update existing code

   From

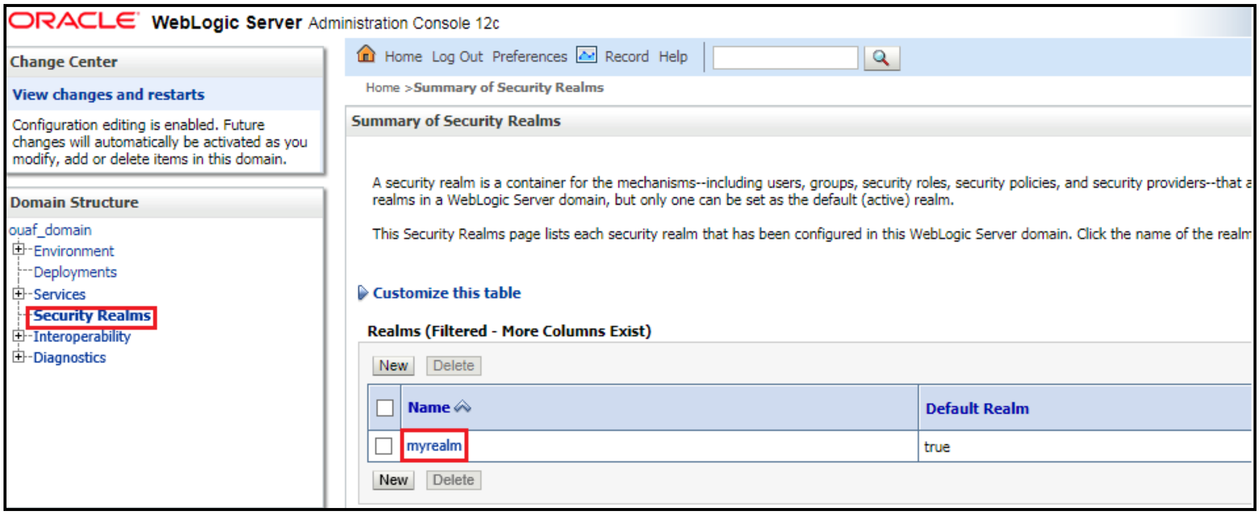
```
#ifdef WEB_WLAUTHMETHOD=CLIENT-CERT

<login-config>

     <auth-method>CLIENT-CERT</auth-method>

   </login-config>

#endif
```

   To

```
#ifdef WEB_WLAUTHMETHOD=CLIENT-CERT

   <login-config>

          <auth-method>CLIENT-CERT,FORM</auth-method>

           <form-login-config>

<form-login-page>@WEB_FORM_LOGIN_PAGE@</form-login-page>

<form-error-page>@WEB_FORM_LOGIN_ERROR_PAGE@</form-error-page>

            </form-login-config>

      </login-config>

#endif
```

5.4 Adding Identity Asserter

1. Login to the WebLogic console.
2. Click **Security Realms** and select myrealm.


ORACLE WebLogic Server Administration Console 12c
Change Center
View changes and restarts
Home Log Out Preferences Record Help
Home >Summary of Security Realms
Summary of Security Realms
Domain Structure
ouaf_domain
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
Customize this table
Realms (Filtered - More Columns Exist)
New Delete

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

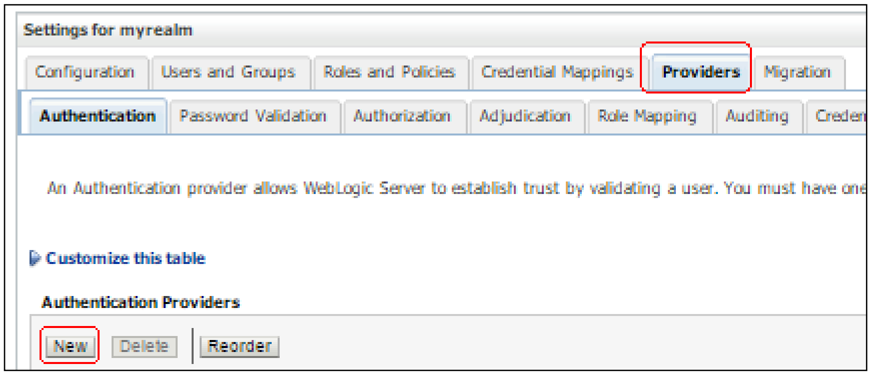
A security realm is a container for the mechanisms--including users, groups, security roles, security policies, and security providers--that a realms in a WebLogic Server domain, but only one can be set as the default (active) realm.

This Security Realms page lists each security realm that has been configured in this WebLogic Server domain. Click the name of the realm

□	Name	Default Realm
□	myrealm	true

Figure 29: WebLogic Security Realms

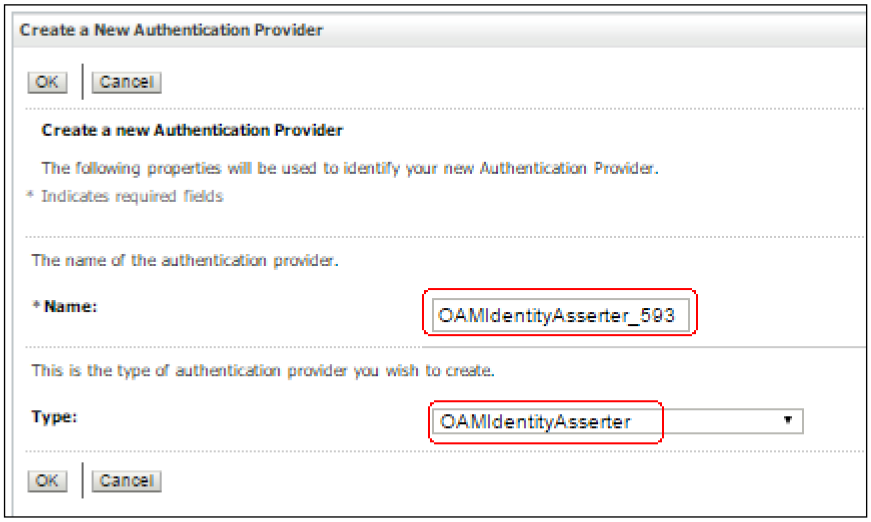
3. Select **Providers** tab and click on **Authentication** tab.
4. Click **New**.



An Authentication provider allows WebLogic Server to establish trust by validating a user. You must have one

Figure 30: myrealm Settings

5. The **Create a New Authentication Provider** window appears.
6. Specify a name for the new provider and select type “OAMIdentityAsserter” from the Type drop-down list.



Create a New Authentication Provider

OK | Cancel

Create a new Authentication Provider

The following properties will be used to identify your new Authentication Provider.
* Indicates required fields

The name of the authentication provider.

* Name: OAMIdentityAsserter_593

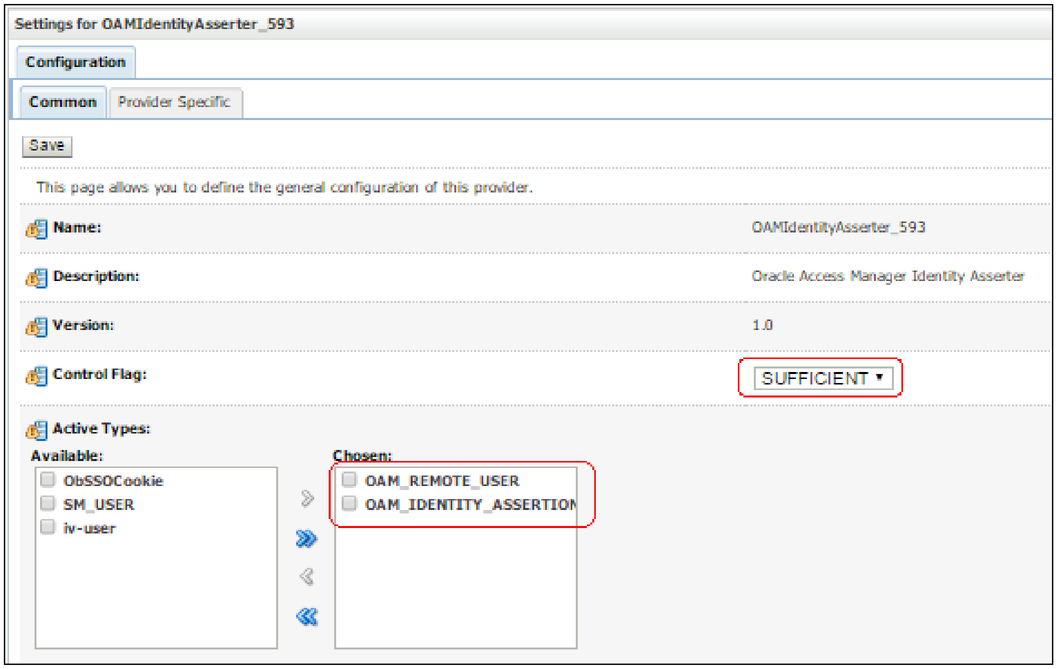
This is the type of authentication provider you wish to create.

Type: OAMIdentityAsserter

OK | Cancel

Figure 31: Creating New Authentication Provider

7. Click **OK**.
8. Click the newly created provider name. The configuration settings screen appears.
9. By default, Common tab appears. Select “SUFFICIENT” from the Control Flag drop-down list.
10. In Active Types field, select “OAM_REMOTE_USER” and “OAM_IDENTITY_ASSERTION” from ‘Available’ list and move the same to Chosen list.
11. Click **Save**.



Settings for OAMIdentityAsserter_593

This page allows you to define the general configuration of this provider.

Name: OAMIdentityAsserter_593

Description: Oracle Access Manager Identity Asserter

Version: 1.0

Control Flag: SUFFICIENT

Active Types:

Available:
□ ObSSOCookie
□ SM_USER
□ iv-user

Chosen:
□ OAM_REMOTE_USER
□ OAM_IDENTITY_ASSERTION

Figure 32: Authentication Provider - Configuration Settings

5.5 Adding WebLogic Data Sources

1. Login to the WebLogic console.
2. Expand the **Domain Structure** node in the left pane.
3. Expand Services and then click **Data Sources**.

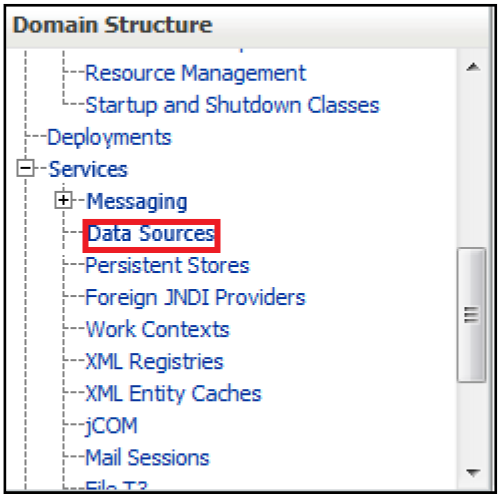
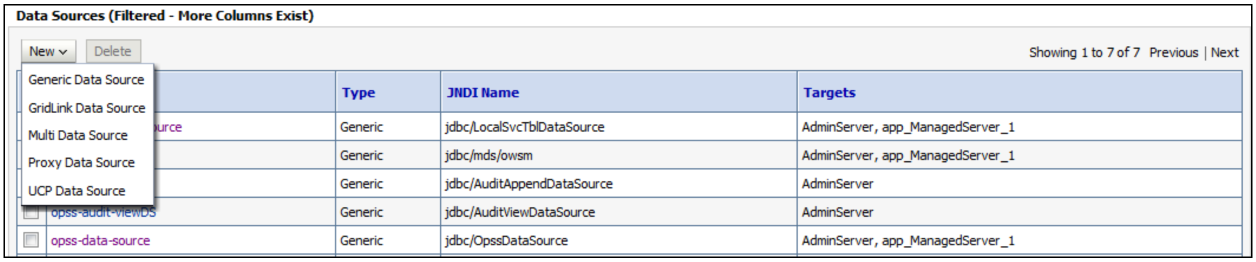


Figure 33: Domain Structure – Data Sources

4. The **Data Sources** section appears. It summarizes the JDBC data source objects that have been created in this domain.
5. Select **Generic Data Source** from the **'New'** drop-down list.



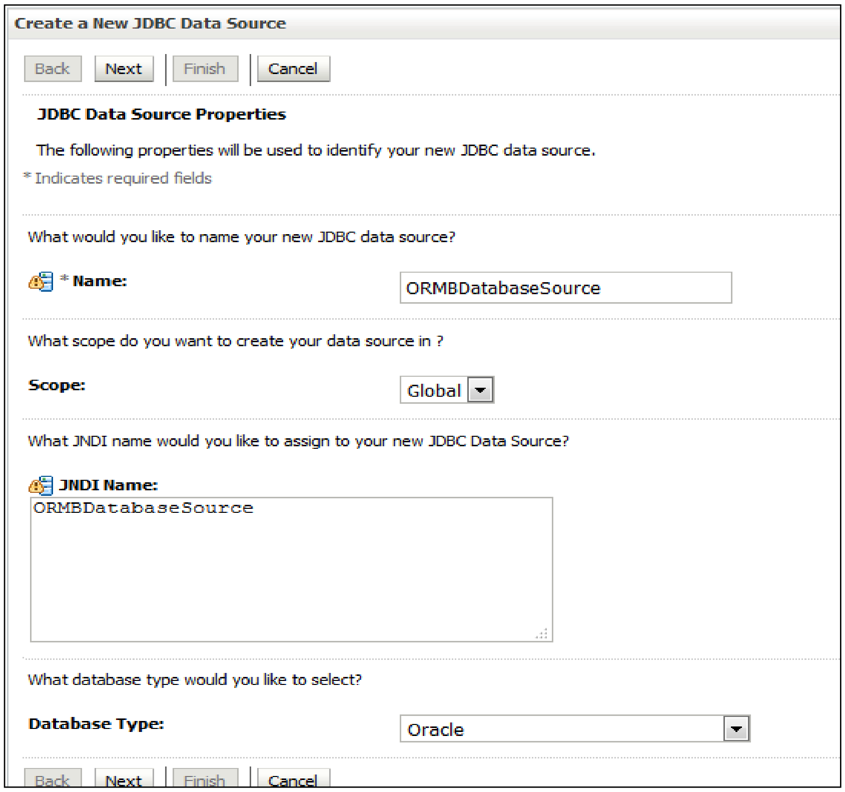
		Type	JNDI Name	Targets
	urce	Generic	jdbc/LocalSvcTblDataSource	AdminServer, app_ManagedServer_1
		Generic	jdbc/mds/owsm	AdminServer, app_ManagedServer_1
		Generic	jdbc/AuditAppendDataSource	AdminServer
□	opss-audit-viewDS	Generic	jdbc/AuditViewDataSource	AdminServer
□	opss-data-source	Generic	jdbc/OpssDataSource	AdminServer, app_ManagedServer_1

Figure 34: Generic Data Source

6. Enter the name of the data source. For example, **ORMBDatabaseSource**.
7. Enter the JNDI Name of the data source. For example, **ORMBDatabaseSource**.

Note: There is no requirement that the data source name and the JNDI name match.

8. Select **Oracle** from the **Database Type** drop-down list.
9. Click **Next**.



JDBC Data Source Properties

The following properties will be used to identify your new JDBC data source.

* Indicates required fields

What would you like to name your new JDBC data source?

* Name: ORMBDatabaseSource

What scope do you want to create your data source in ?

Scope: Global

What JNDI name would you like to assign to your new JDBC Data Source?

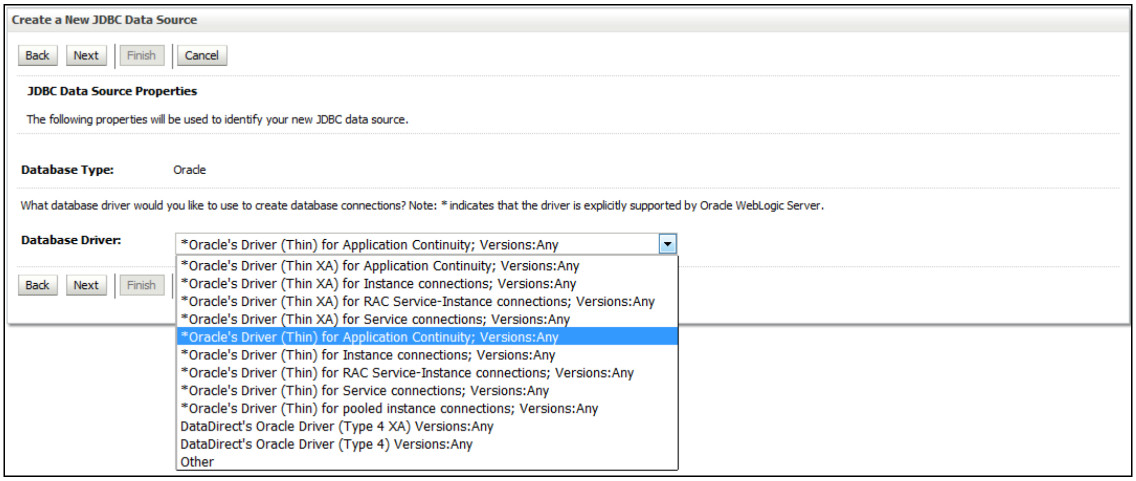
JNDI Name: ORMBDatabaseSource

What database type would you like to select?

Database Type: Oracle

Figure 35: Creating New JDBC Data Source

10. Select “*Oracle's Driver (Thin) for Application Continuity; Versions:Any” from the **Database Driver** drop-down list.


Create a New JDBC Data Source
Back
Next
Finish
Cancel
*Oracle's Driver (Thin XA) for Application Continuity; Versions:Any
*Oracle's Driver (Thin XA) for Instance connections; Versions:Any
*Oracle's Driver (Thin XA) for RAC Service-Instance connections; Versions:Any
*Oracle's Driver (Thin XA) for Service connections; Versions:Any
*Oracle's Driver (Thin) for Application Continuity; Versions:Any
*Oracle's Driver (Thin) for Instance connections; Versions:Any
*Oracle's Driver (Thin) for RAC Service-Instance connections; Versions:Any
*Oracle's Driver (Thin) for Service connections; Versions:Any
*Oracle's Driver (Thin) for pooled instance connections; Versions:Any
DataDirect's Oracle Driver (Type 4 XA) Versions:Any
DataDirect's Oracle Driver (Type 4) Versions:Any
Other

JDBC Data Source Properties

The following properties will be used to identify your new JDBC data source.

Database Type: Oracle

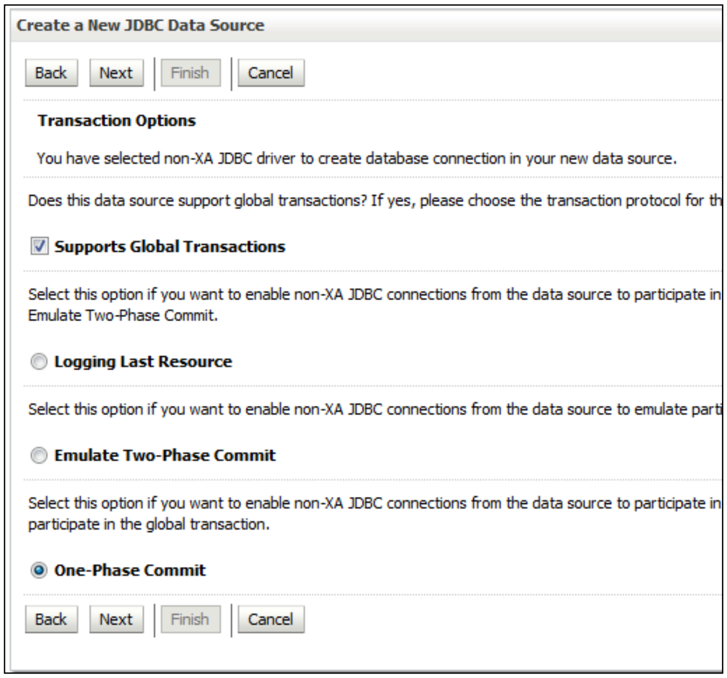
What database driver would you like to use to create database connections? Note: * indicates that the driver is explicitly supported by Oracle WebLogic Server.

Database Driver: *Oracle's Driver (Thin) for Application Continuity; Versions:Any

Figure 36: Selecting Database Driver

11. Click **Next**.

12. Keep all the default Transaction Options. Click **Next**.



Create a New JDBC Data Source

Transaction Options

You have selected non-XA JDBC driver to create database connection in your new data source.

Does this data source support global transactions? If yes, please choose the transaction protocol for th

☑ Supports Global Transactions

Select this option if you want to enable non-XA JDBC connections from the data source to participate in Emulate Two-Phase Commit.

○ Logging Last Resource

Select this option if you want to enable non-XA JDBC connections from the data source to emulate parti

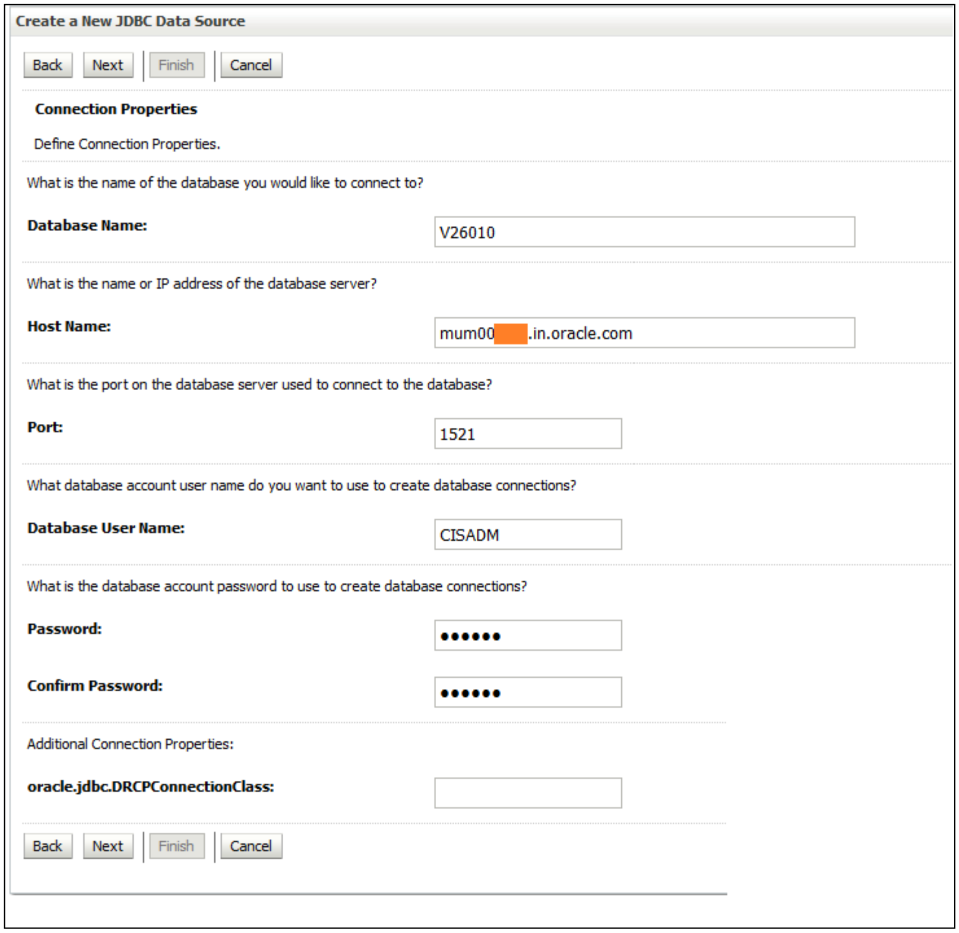
○ Emulate Two-Phase Commit

Select this option if you want to enable non-XA JDBC connections from the data source to participate in participate in the global transaction.

● One-Phase Commit

Figure 37: Default Transaction Options

13. Enter the Database Name. For example, V26010. The database name may vary at your end.
14. Enter the DB Host Name.
15. Enter the database Port. The default value is 1521. The value may vary at your end.
16. Enter the Database User Name.
17. Enter the database user's password in the Password and Confirm Password fields.
18. Click **Next**.



Create a New JDBC Data Source

Connection Properties

Define Connection Properties.

What is the name of the database you would like to connect to?

Database Name: V26010

What is the name or IP address of the database server?

Host Name: mum00[redacted].in.oracle.com

What is the port on the database server used to connect to the database?

Port: 1521

What database account user name do you want to use to create database connections?

Database User Name: CISADM

What is the database account password to use to create database connections?

Password: ••••••

Confirm Password: ••••••

Additional Connection Properties:

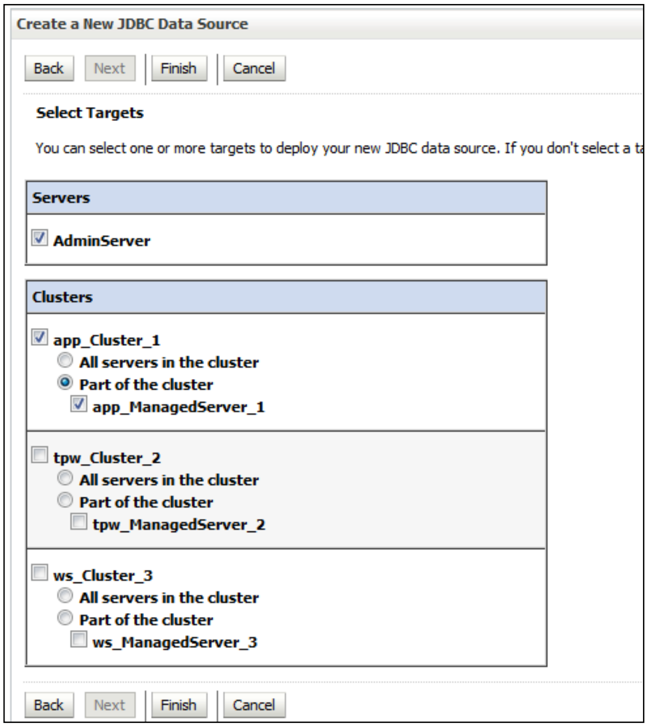
oracle.jdbc.DRCPConnectionClass:

Figure 38: Connection Properties

19. Click the Test Configuration button to check if a connection to the Database can be made, based upon the information entered.

20. A message "Connection test succeeded", informing that the connection test is successful appears. Click **Next**.

21. To target a data source to Admin and managed servers, select the check box next to servers.



Create a New JDBC Data Source

Select Targets

You can select one or more targets to deploy your new JDBC data source. If you don't select a t

Servers

☑ AdminServer

Clusters

☑ app_Cluster_1
○ All servers in the cluster
● Part of the cluster
☑ app_ManagedServer_1

□ tpw_Cluster_2
○ All servers in the cluster
○ Part of the cluster
□ tpw_ManagedServer_2

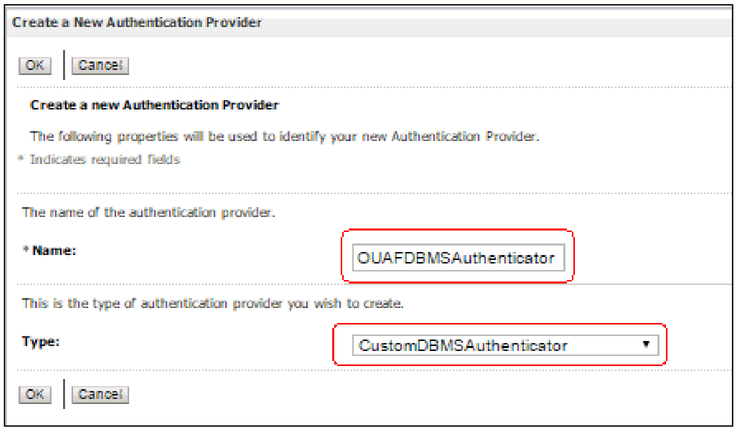
□ ws_Cluster_3
○ All servers in the cluster
○ Part of the cluster
□ ws_ManagedServer_3

Figure 39: Select Targets

22. Click **Finish**.

5.6 Adding OUAF DBMS Authenticator

1. Login to the WebLogic console.
2. Click **Security Realms** and select myrealm.
3. Select **Providers** tab and click on Authentication tab.
4. Click **New**.
5. Specify a name for the new provider and select “CustomDBMSAuthenticator” from the **Type** drop-down list.



Create a New Authentication Provider

Create a new Authentication Provider

The following properties will be used to identify your new Authentication Provider.
* Indicates required fields

The name of the authentication provider.

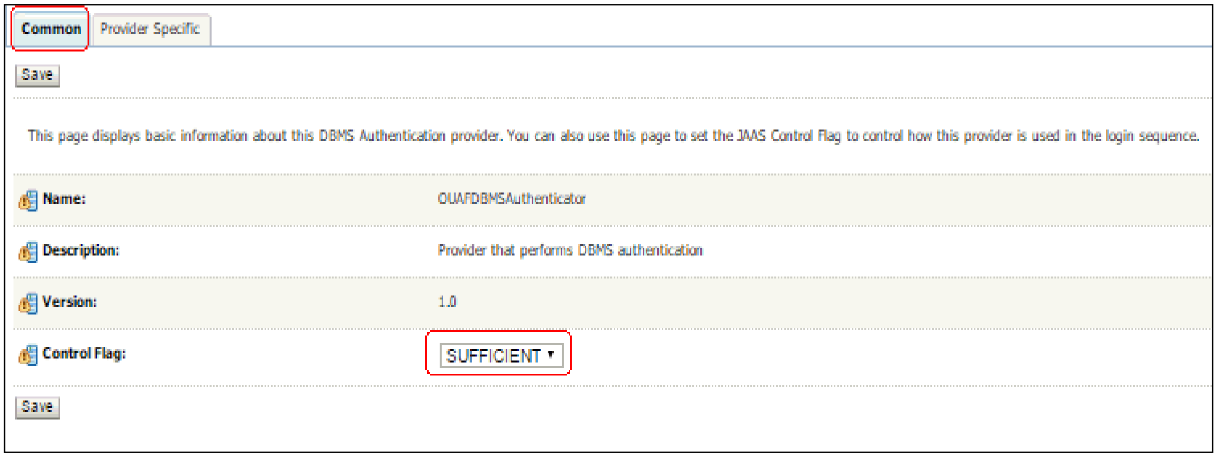
* Name: OUAFDBMSAuthenticator

This is the type of authentication provider you wish to create.

Type: CustomDBMSAuthenticator

Figure 40: Creating a New Authentication Provider

6. Click **OK**.
7. Click the newly created provider name. The configuration settings screen appears.
8. By default, Common tab appears. Select 'SUFFICIENT' from the **Control Flag** drop-down list.



This page displays basic information about this DBMS Authentication provider. You can also use this page to set the JAAS Control Flag to control how this provider is used in the login sequence.

Name: OUAFDBMSAuthenticator

Description: Provider that performs DBMS authentication

Version: 1.0

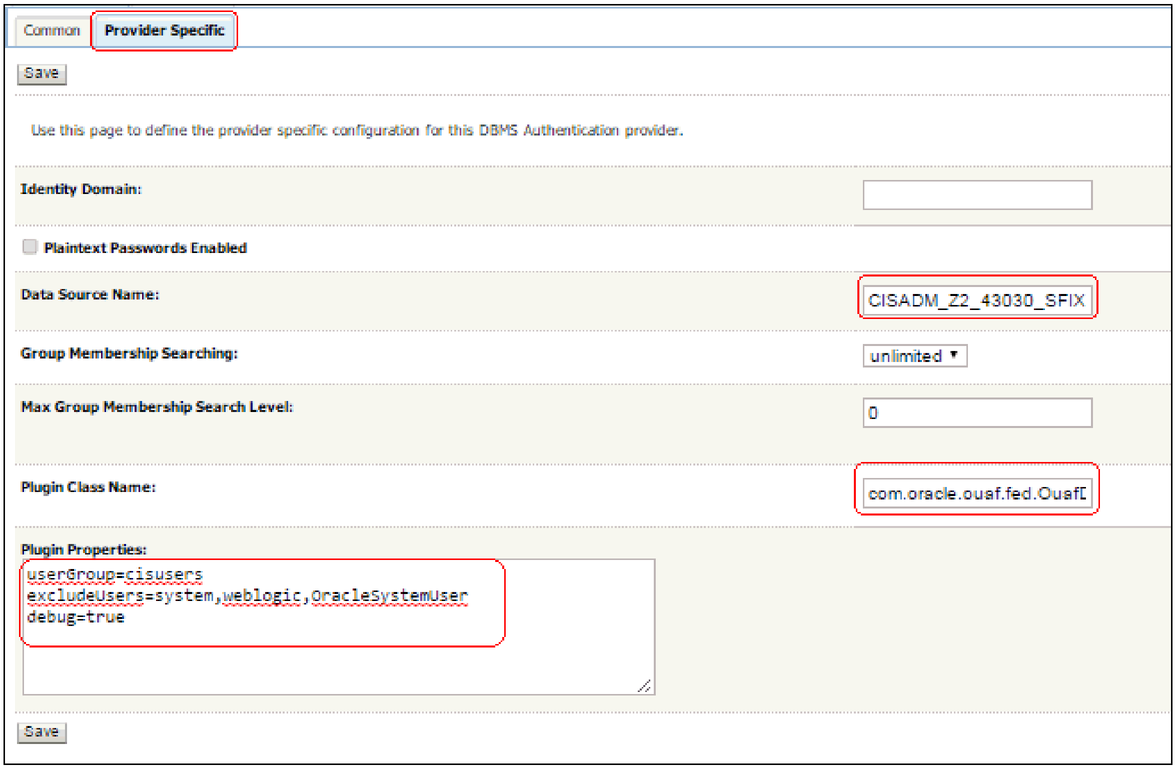
Control Flag: SUFFICIENT

Figure 41: Authentication Provider – Common Configuration Settings

9. Click **Save**.
10. Select the Provider Specific tab and enter the values in the fields as below:

Field Name	Values	Mandatory (Yes or No)
Data Source Name	The name of the data source to connect to the OUAF database. It is same as defined in Adding WebLogic Data Sources section.	Yes
Plugin Class Name	com.oracle.ouaf.fed.OuafDBMSAuthenticator	Yes
Plugin Properties	• userGroup=cisusers • excludeUsers= system,weblogic,OracleSystemUser • debug=true	No

Note: The debug property is set to true to troubleshoot the provider. To exclude troubleshooting the provider, set the property to false or do not specify.



Use this page to define the provider specific configuration for this DBMS Authentication provider.

Identity Domain:

□ Plaintext Passwords Enabled

Data Source Name: CISADM_Z2_43030_SFIX

Group Membership Searching: unlimited

Max Group Membership Search Level: 0

Plugin Class Name: com.oracle.ouaf.fed.OuafD

Plugin Properties:

```
userGroup=cisusers
excludeUsers=system,weblogic,OracleSystemUser
debug=true
```

Figure 42: Authentication Provider – Provider Specific Configuration Settings

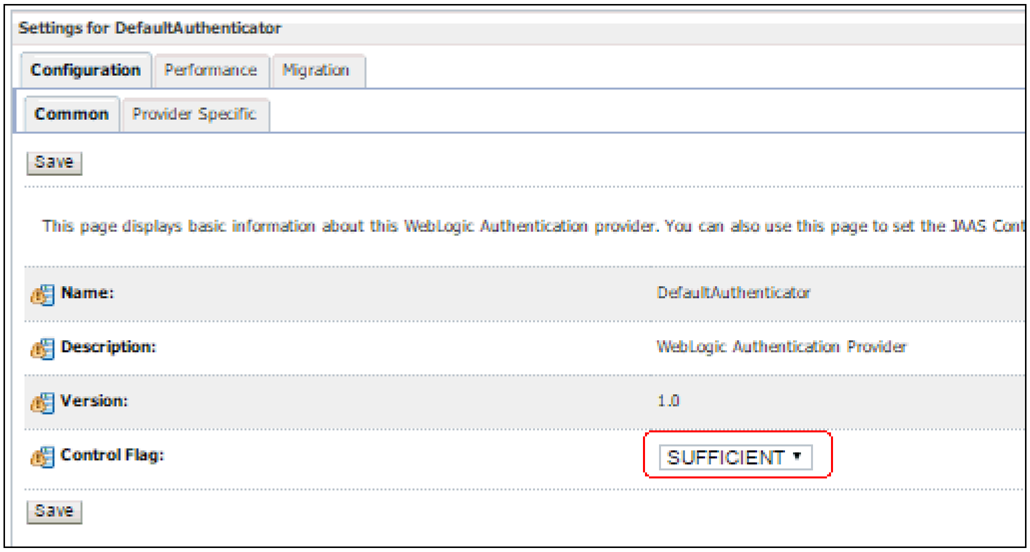
11. Click **Save**.

> **Note:** Important to note is that this authentication provider requires a data source to the OUAF database to access the SC_USER table.

5.7 Configuring Default Authenticator

The 'DefaultAuthenticator', which authenticates against the embedded LDAP, is always required in a typical WebLogic application server, but its Control Flag should be changed from REQUIRED to SUFFICIENT to prevent it from always prompting for a login.

1. Login to the WebLogic console.
2. Click **Security Realms** and select myrealm.
3. Select providers and click on Authentication Tab.
4. Select DefaultAuthenticator from the list.
5. Change the **Control Flag** to 'SUFFICIENT' and click **Save**.



This page displays basic information about this WebLogic Authentication provider. You can also use this page to set the JAAS Cont

Name:	DefaultAuthenticator
Description:	WebLogic Authentication Provider
Version:	1.0
Control Flag:	SUFFICIENT

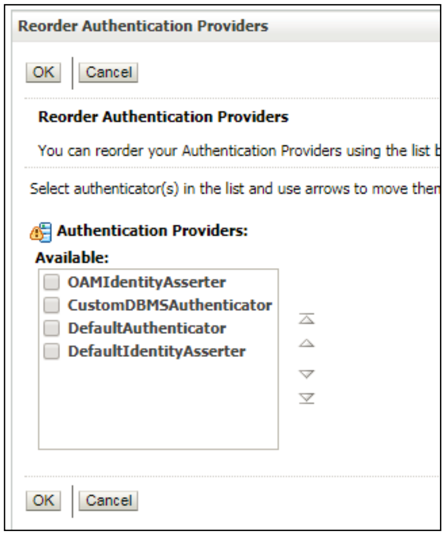
Figure 43: Authentication Provider – Common Configuration Settings

5.8 Reordering Authentication Providers

Authentication providers are called in the order in which they are configured. The Authentication Providers table lists the authentication providers in the order they are called. You can use the table to change the order of the providers. The two new providers should be ordered so that they are invoked before any other providers.

To change the ordering of Authentication providers:

1. Login to the WebLogic console.
2. Click **Security Realms** and select myrealm.
3. Select providers and click on Authentication Tab.
4. Click **Reorder**.
5. Select an Authentication provider from the list of configured Authentication providers and use the arrow buttons to move it up or down in the list. For example, OAMIdentityAsserter can appears in first position and OUAFDBMSAuthenticator appears in second position.



Reorder Authentication Providers

Reorder Authentication Providers

You can reorder your Authentication Providers using the list b

Select authenticator(s) in the list and use arrows to move ther

Authentication Providers:

Available:

□ OAMIdentityAsserter
□ CustomDBMSAuthenticator
□ DefaultAuthenticator
□ DefaultIdentityAsserter

Figure 44: Reorder Authentication Providers

6. Click **OK**.

6. Restarting Servers

Once you configure IDP, SP and ORMB application, you need to restart the instances associated with these services.

6.1 OAM (SP and IDP)

In general, the OAM system does not need to be restarted for any of the configurations described in this document to take effect. However, in case the system needs to be restarted, you can use the below scripts using Putty:

```
<FMW home>/config/scripts/stopall.sh
```

```
<FMW home>/config/scripts/startall.sh
```

6.2 OHS/WebGate

The OHS instance needs to be restarted to refresh its configuration from the WebGate agent configuration in OAM. To restart OHS instance:

1. Change directory to

```
<FMW home>/Oracle_WT1/instances/instance1/bin.
```

2. Run the following commands:

```
./opmnctl stopall
```

```
./opmnctl startall
```

6.3 ORMB Application Server

The application server may need to be restarted to activate the authentication providers. To restart the server, you can follow the standard process specified in Release specific SIQ.

7. Verifying SSO Web Application

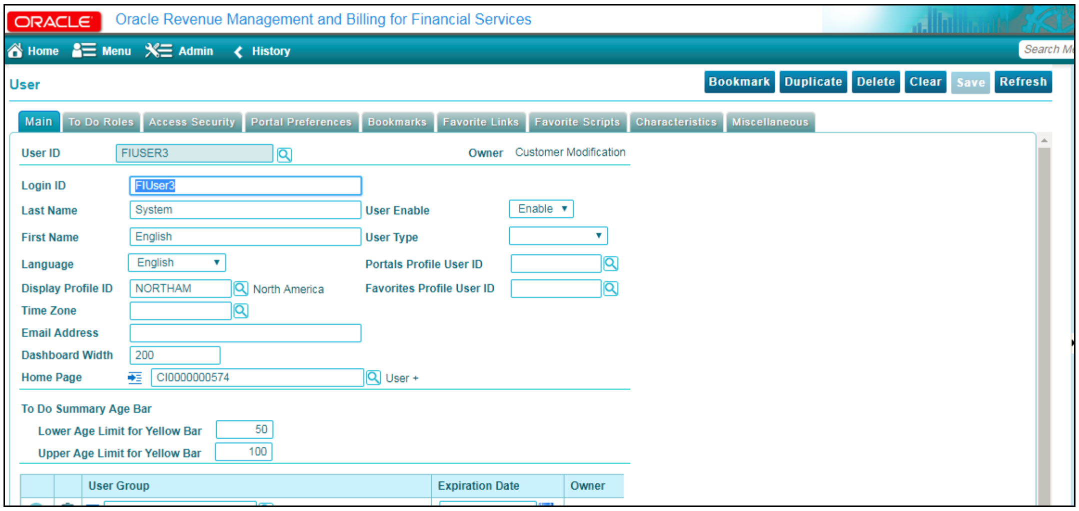
This section lists the steps to be performed to verify SSO web application setup.

7.1 Adding User into ORMB Application

The created user will be used to login from IDP Server into ORMB application. You can create user through application UI or Web service.

To create user through application:

1. Login into ORMB application.
2. Create new user. For example, “FIUser3”.



User

User ID	FIUSER3	Owner	Customer Modification
Login ID	FIUser3		
Last Name	System	User Enable	Enable
First Name	English	User Type	
Language	English	Portals Profile User ID	
Display Profile ID	NORTHAM North America	Favorites Profile User ID	
Time Zone			
Email Address			
Dashboard Width	200		
Home Page	CI0000000574 User +		

To Do Summary Age Bar

Lower Age Limit for Yellow Bar 50

Upper Age Limit for Yellow Bar 100

User Group	Expiration Date	Owner

Figure 45: Creating New User

7.2 Login to OUAF Application

Prerequisite

To login to OUAF Application, you must:

- Ensure that all the previous tests pass.
- Create a user with same user ID in IDP and ORMB application.

Procedure

To login to the WebGate-protected OUAF application:

1. Close all instances of the browser to invalidate the session for the following login.

2. Open the URL for the WebGate (typically the one on port 7777) – for example, `http://<OHS/Webgate-host>:7777/ouaf`

3. You will be redirected to the same OAM Server's (External IDP login page) login page.

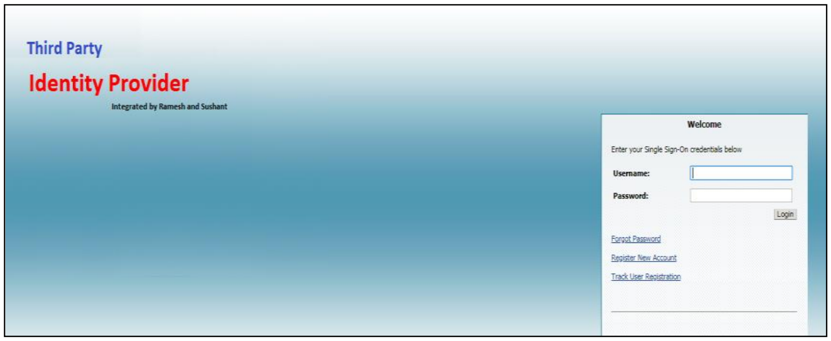
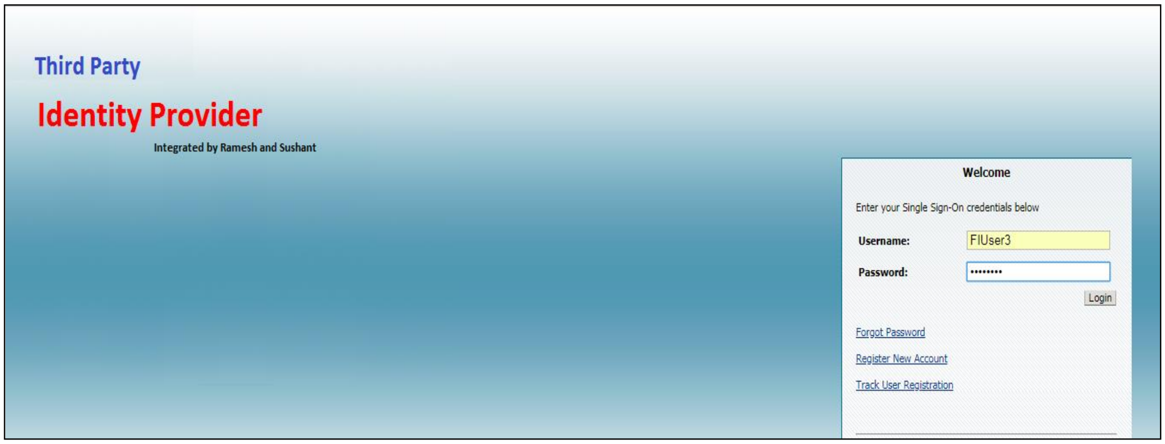


Figure 46: External IDP Login Screen

4. Login to a user id that exists in both External Providers LDAP and the OUAF application.



Username: FIUser3

Password: ••••••••

Figure 47: External IDP Login Screen

5. The browser should be redirected back to the OHS/WebGate and OUAF application server and the user should be logged in to the application.

7.3 Logout from OUAF Application

1. To validate the Logout Callback URL that was specified to end the IDP's session, logout from the OUAF application and verify that the logout was successful.

2. To verify successful logout, access the application `URL: http://<OHS/Webgate-host>:7777/ouaf`. The External Provider login page should appear.

3. Provide the authentication details and verify that the login was successful.

8. Configuring Internal SSO Login

The SSO login capability allows you to login to an OUAF application from an internal server. For example, an Oracle employee can login on behalf of any customer. To login to an OUAF application, you need to set up a second OHS/WebGate instance which will authenticate against the OAM user store (For example, OUD).

8.1 Configuring OHS/WebGate

Refer to Defining WebGate Agent section.

8.2 Defining WebGate Agent

Refer to Defining WebGate Agent section. Note that the name and base URL should be different and the base URL should reference the “internal” OHS/WebGate instance.

8.3 Copying WebGate Agent Configuration to OHS/WebGate

1. Download WebGate Agent as mentioned in Downloading WebGate Agent section.
2. Transfer the zip file to the “internal” OHS/WebGate instance’s config directory.

8.4 Modifying Authentication Scheme for Application Domain

1. Login to Oracle Access Management using the administrator’s credentials.
2. Click the **Application Security** button. The Launch **Pad** tab appears.

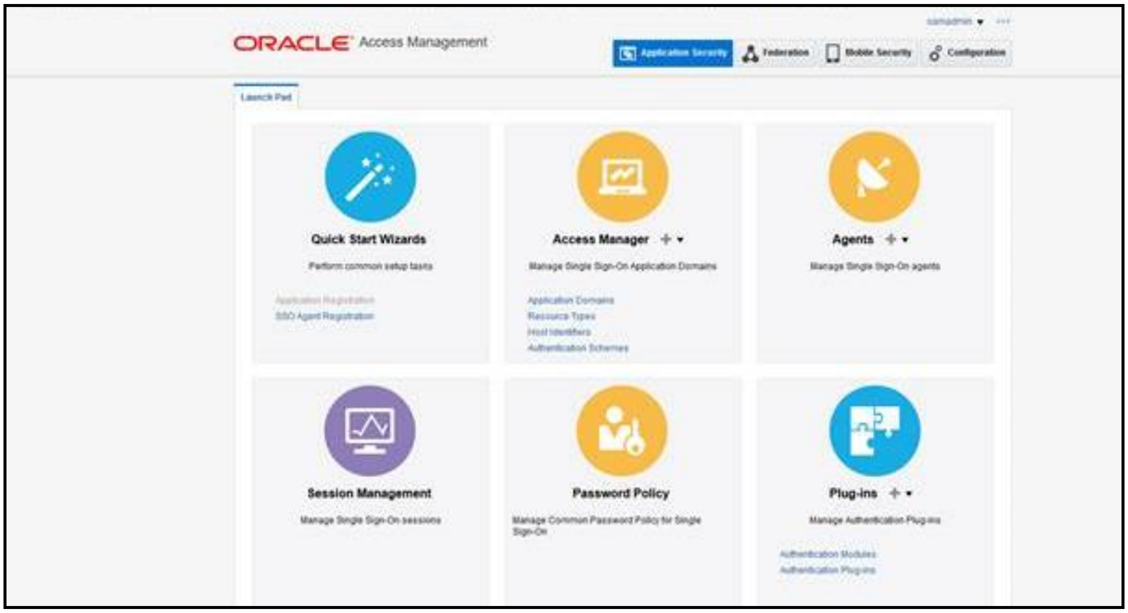
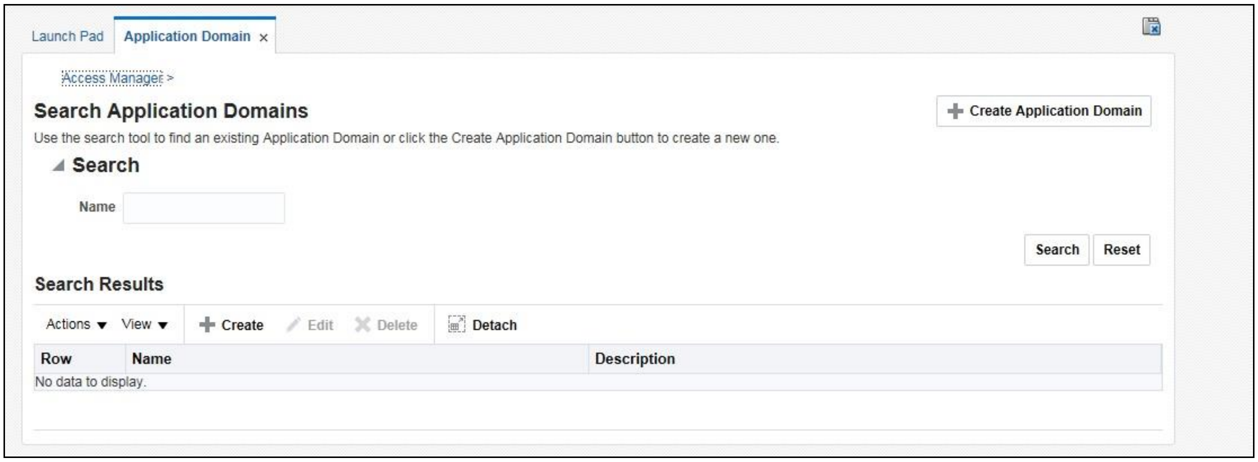


Figure 48: Application Security Launch Pad

3. Click the **Application Domains** link in the **Access Manager** section. The **Application Domain** tab appears.



Search Application Domains

Use the search tool to find an existing Application Domain or click the Create Application Domain button to create a new one.

Search

Name

Search Results

Row	Name	Description
No data to display.		

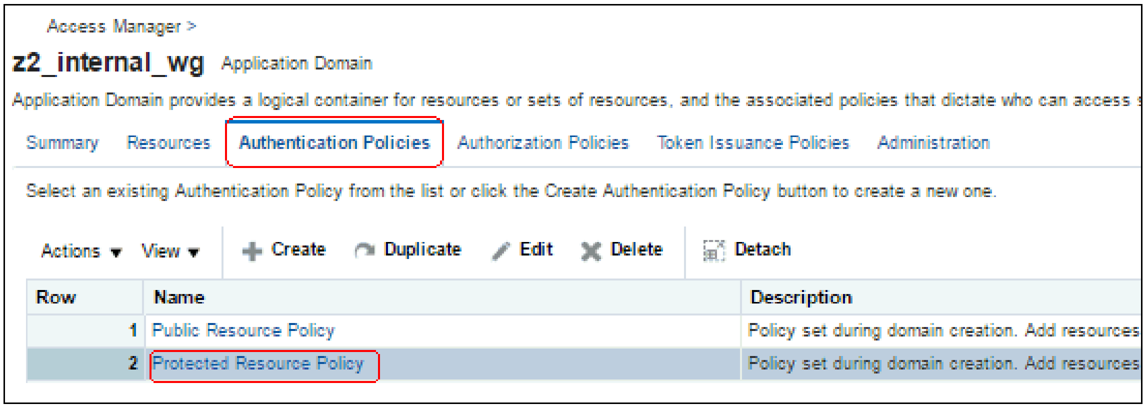
Figure 49: Application Domain Tab

4. Search for the required application domain in the Application Domain tab.

5. In the Search Results section, click the application domain name whose resources you want to protect using the authentication policy.

6. Click the **Authentication Policies** tab. The **Authentication Policies** tab appears.

7. Click the **Protected Resource Policy** link in the **Name** column. The {**Application Domain}: Protected Resource Policy** tab appears.



Access Manager >

z2_internal_wg Application Domain

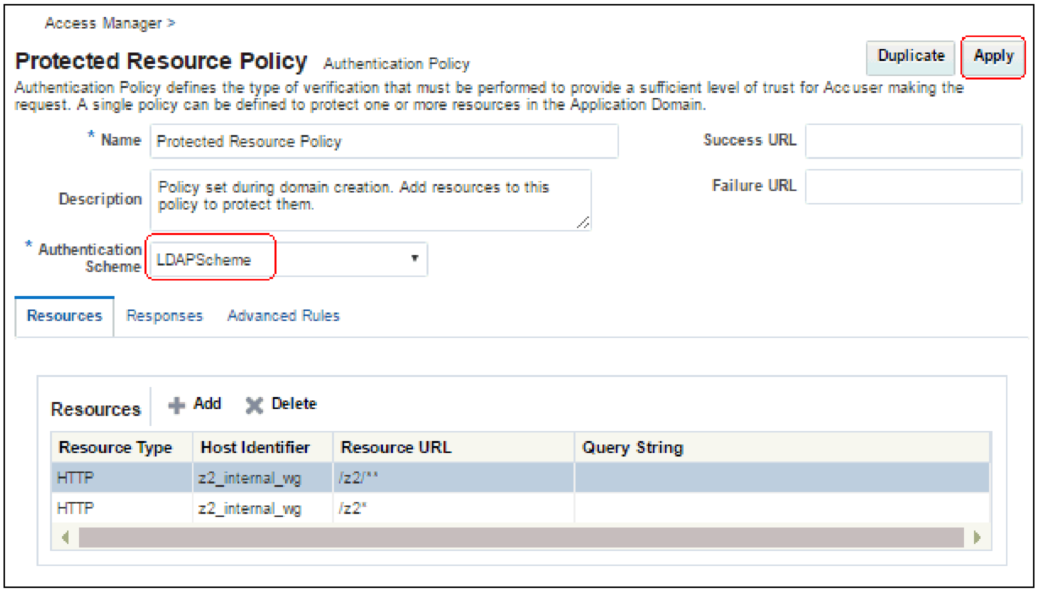
Application Domain provides a logical container for resources or sets of resources, and the associated policies that dictate who can access s

Select an existing Authentication Policy from the list or click the Create Authentication Policy button to create a new one.

Row	Name	Description
1	Public Resource Policy	Policy set during domain creation. Add resources
2	Protected Resource Policy	Policy set during domain creation. Add resources

Figure 50: {Application Domain} – Authentication Policies Tab

8. Click the **Resources** tab. The Resources section appears.
9. Change the Authentication Scheme to ‘LDAPScheme’ and click **Apply**.



Access Manager >

Protected Resource Policy Authentication Policy

Authentication Policy defines the type of verification that must be performed to provide a sufficient level of trust for Acc user making the request. A single policy can be defined to protect one or more resources in the Application Domain.

* Name: Protected Resource Policy

Description: Policy set during domain creation. Add resources to this policy to protect them.

* Authentication Scheme: LDAPScheme

Success URL:

Failure URL:

Resources

Resource Type	Host Identifier	Resource URL	Query String
HTTP	z2_internal_wg	/z2/**	
HTTP	z2_internal_wg	/z2*	

Figure 51: {Application Domain}: Protected Resource Policy Tab

Note: This assumes the default LDAPScheme authenticates against the OUD user store. If another user store is preferred, modify this appropriately.

8.5 Restarting OHS/WebGate

The OHS instance needs to be restarted to refresh its configuration from the WebGate agent configuration in OAM. To restart OHS instance:

1. Change directory to `<FMW home>/Oracle_WT1/instances/instance1/bin`.
2. Run the following commands:

```
./opmnctl stopall

./opmnctl startall
```