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
Copyright © 2018, Oracle and/or its affiliates. All rights reserved.

Trademark Notice
Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

License Restrictions Warranty/Consequential Damages Disclaimer
This software and related documentation are provided under a license agreement containing restrictions on use and disclosure, and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or de-compilation of this software, unless required by law for interoperability, is prohibited.

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
If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS
Oracle programs, including any operating system, integrated software, any programs installed on the hardware and/or documentation delivered to U.S. Government end users are “commercial computer software” pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware and/or documentation shall be subject to license terms and restrictions applicable to the programs. No other rights are granted to the U.S. Government.
**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:

<table>
<thead>
<tr>
<th>Software</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORMB Application</td>
<td>2.6.0.1.0</td>
</tr>
<tr>
<td>OAM Server (cloud)</td>
<td>11.1.2.3.0</td>
</tr>
<tr>
<td>OAM Server (on-premise)</td>
<td>11.1.2.3.0</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Section No.</th>
<th>Section Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 1</td>
<td>Introduction</td>
<td>Explains the Identity Federation feature. It also provides an overview of the configuration steps for Federated SSO Login.</td>
</tr>
<tr>
<td>Section 2</td>
<td>Federated Identity Login Flow</td>
<td>Gives an overview of data flow between the user and federation systems.</td>
</tr>
<tr>
<td>Section 3</td>
<td>Steps to be executed on IDP (OAM server as IDP)</td>
<td>Explains how to enable and configure the identity federation service. It also provides steps to register external Identity Provider partners.</td>
</tr>
<tr>
<td>Section No.</td>
<td>Section Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Section 4</td>
<td>Steps to be executed on SP (OAM server as SP)</td>
<td>Lists and describes the steps to be followed to set up OAM server as SP.</td>
</tr>
<tr>
<td>Section 5</td>
<td>Steps to be executed on ORMB Application</td>
<td>Lists and describes the steps to be executed on ORMB application.</td>
</tr>
<tr>
<td>Section 6</td>
<td>Restarting Servers</td>
<td>Lists the scripts and commands to restart the respective instances.</td>
</tr>
<tr>
<td>Section 7</td>
<td>Verifying SSO Web Application</td>
<td>Lists the steps to be performed to verify SSO web application setup.</td>
</tr>
<tr>
<td>Section 8</td>
<td>Internal SSO Login Configuration</td>
<td>Explains how to configure Internal SSO Login.</td>
</tr>
</tbody>
</table>

## Related Documents

You can refer to the following documents for more information:

<table>
<thead>
<tr>
<th>Document</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Oracle Revenue Management and Billing Version 2.6.0.1.0 Release Notes</em></td>
<td>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.</td>
</tr>
<tr>
<td><em>Oracle Revenue Management and Billing Banking User Guide</em></td>
<td>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.</td>
</tr>
<tr>
<td><em>Oracle Revenue Management and Billing Insurance User Guide</em></td>
<td>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.</td>
</tr>
</tbody>
</table>
# Contents

1. Introduction .................................................................................................................. 1

2. Federated Identity Login Flow ...................................................................................... 2

3. Steps to be executed on IDP (OAM Server as IDP) .................................................... 3
   3.1 Enabling Identity Federation Service ........................................................................ 3
   3.2 Administering Identity Provider ............................................................................. 7
   3.3 Exporting OAM SAML Metadata ............................................................................ 9

4. Steps to be executed on SP (OAM Server as SP) ......................................................... 11
   4.1 Administering Service Provider ............................................................................ 11
   4.2 Enabling JIT User Provisioning in OIF .................................................................. 16
   4.3 Defining WebGate Agent ..................................................................................... 16
   4.4 Configuring Federated Logout Settings .................................................................. 20
   4.5 Downloading WebGate Agent ............................................................................. 21
   4.6 Configuring Authentication Policy for Application Domain ................................... 22

5. Steps to be executed on ORMB Application ............................................................... 27
   5.1 Copying WebGate Files ....................................................................................... 27
   5.2 Copying Required JAR Files into Application Domain .......................................... 27
   5.3 Configuring OUAF app's web.xml ....................................................................... 28
   5.4 Adding Identity Asserter ...................................................................................... 29
   5.5 Adding WebLogic Data Sources .......................................................................... 31
   5.6 Adding OUAF DBMS Authenticator ...................................................................... 35
   5.7 Configuring Default Authenticator ...................................................................... 37
   5.8 Reordering Authentication Providers .................................................................... 38

6. Restarting Servers ........................................................................................................ 40
   6.1 OAM (SP and IDP) ............................................................................................. 40
   6.2 OHS/WebGate ..................................................................................................... 40
   6.3 ORMB Application Server .................................................................................... 40

7. Verifying SSO Web Application ................................................................................... 41
   7.1 Adding User into ORMB Application ................................................................... 41
   7.2 Login to OUAF Application .................................................................................. 41
   7.3 Logout from OUAF Application ............................................................................ 42
8. Configuring Internal SSO Login

8.1 Configuring OHS/WebGate

8.2 Defining WebGate Agent

8.3 Copying WebGate Agent Configuration to OHS/WebGate

8.4 Modifying Authentication Scheme for Application Domain

8.5 Restarting OHS/WebGate
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 oamAuthnP rovider 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:

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.

![Figure 1: Configuration - Launch Pad](image-url)
3. Click the **Available Services** icon. The **Available Services** tab appears.

![Figure 2: Available Services](image)

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

6. The Enabled icon appears corresponding to the adaptive authentication service indicating that the service is enabled.
<table>
<thead>
<tr>
<th>Available Services</th>
<th>Status</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application Security</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Manager</td>
<td>✔️</td>
<td>Disable Service</td>
</tr>
<tr>
<td>Adaptive Authentication Service</td>
<td>✔️</td>
<td>Disable Service</td>
</tr>
<tr>
<td>Federation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity Federation</td>
<td>✔️</td>
<td>Disable Service</td>
</tr>
<tr>
<td>Security Token Service</td>
<td>✗</td>
<td>Enable Service</td>
</tr>
<tr>
<td>Access Portal Service</td>
<td>✗</td>
<td>Enable Service</td>
</tr>
<tr>
<td>Mobile</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile and Social</td>
<td>✗</td>
<td>Enable Service</td>
</tr>
</tbody>
</table>

**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.

4. The Identity Provider Administration tab appears. Click Create Service Provider Partner.
Figure 7: Identity Provider Administration

5. Create Service Provider Partner screen appears.

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](image)

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.
Figure 10: Federation Settings

<table>
<thead>
<tr>
<th>Row</th>
<th>Key ID</th>
<th>Alias</th>
<th>password</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ots_encryption</td>
<td>integrationkeys</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>ots_signing</td>
<td>integrationkeys</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

- **General**
  - Provider ID: http://sso0byw.us.oracle.com:7777/damfed
  - Base URI: /sso0byw/psf
  - Signing Key: ots_signing

- **Proxy**
  - Enable Proxy
  - Host: (Enter host name)
  - Port: (Enter port number)
  - SSL/TLS Key: (Enter SSL/TLS key)

- **Keystore**
  - Keystore Location: /usr/local/sso0byw/psf/sso0byw-keystore
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.
4. The **Service Provider Administration** tab appears. Click **Create Identity Provider Partner** button.

---

**Figure 11: Federation – Service Provider Management**

**Figure 12: Service Provider Administration**
5. **Create Identity Provider Partner** screen appears.

![Identity Provider Partner](image)

**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.
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.
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");
   ```

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

![Figure 16: Application Security - Agents](image)

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Mandatory (Yes or No)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Used to define WebGate version. For example, 11g.</td>
<td>Yes</td>
</tr>
<tr>
<td>Name</td>
<td>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.</td>
<td>Yes</td>
</tr>
<tr>
<td>Description</td>
<td>Used to define description.</td>
<td>No</td>
</tr>
<tr>
<td>Base URL</td>
<td>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.</td>
<td>No</td>
</tr>
</tbody>
</table>

![Figure 17: Search SSO Agents](image)
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Mandatory (Yes or No)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Client Password</td>
<td>Used to authenticate a registered WebGate and prevent unauthorized WebGates from connecting to OAM Servers and obtaining policy information.</td>
<td>No</td>
</tr>
<tr>
<td>Security</td>
<td>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:</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>- Open - No transport security.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Simple - SSL v3/TLS v1.0 secure transport using dynamically generated session keys.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
<td></td>
</tr>
<tr>
<td>Host Identifier</td>
<td>Used to represent the Web server host. This is automatically seeded with the value in the agent Name field.</td>
<td>No</td>
</tr>
<tr>
<td>User-defined Parameters</td>
<td>Used to define parameters to enable specific WebGate behaviors.</td>
<td>No</td>
</tr>
<tr>
<td>Virtual Host</td>
<td>Flag to validate if a WebGate is installed on a Web server that contains multiple Web site and domain names.</td>
<td>No</td>
</tr>
<tr>
<td>Auto Create Policies</td>
<td>Flag to check whether authentication and authorization policies are to be created automatically during agent registration.</td>
<td>No</td>
</tr>
<tr>
<td>IP Validation</td>
<td>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.</td>
<td>No</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Mandatory (Yes or No)</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>IP Validation Exceptions</td>
<td>Used to define IP addresses to be excluded from validation using standard notation for the addresses. For example, 10.20.30.123.</td>
<td>No</td>
</tr>
<tr>
<td>Protected Resource (URI) List</td>
<td>Used to define URIs for the protected application. For example, /myapp/login</td>
<td>No</td>
</tr>
<tr>
<td>Note: Each URI for the protected application should be specified in a new row of the table for the Protected Resource List.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Default value: /**</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public Resource (URI) List</td>
<td>Used to define public application for the Public Resource List.</td>
<td>No</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logout Callback URL</td>
<td>Specify the third party IDP’s logout URL. OAM logout URL: <a href="http://mum00xxx.in.oracle.com:14100/oam/server/logout?end_url=http://mum00xxx.in.oracle.com:7001/oamconsole//faces/admin.jspx">http://mum00xxx.in.oracle.com:14100/oam/server/logout?end_url=http://mum00xxx.in.oracle.com:7001/oamconsole//faces/admin.jspx</a></td>
</tr>
<tr>
<td>Logout URL</td>
<td>/sso/logout</td>
</tr>
<tr>
<td>Logout Target URL</td>
<td>end_url</td>
</tr>
</tbody>
</table>

Copyright © 2018, Oracle and/or its affiliates. All rights reserved.
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.

![WebGate Agent Search Results](image)

**Figure 20: WebGate Agent Search Results**

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

![Downloading WebGate Agent](image)

**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.
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.
6. **Selected Application Domain** opens in a new tab.

![Application Domain](image)

**Figure 24: Application Domain**

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

![Application Domains - Authentication Policies](image)

**Figure 25: Application Domains - Authentication Policies**

8. Click **Create** button to create a new authentication policy. The **Create Authentication Policy** tab appears.
9. Specify a name and the authentication scheme generated for the identity provider as defined in the 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**.
16. To confirm whether the authentication policy is attached, go to the Resources tab and search for the respective host.
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 asseter 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
   ```bash
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.

![Figure 29: WebLogic Security Realms](image)

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

![Figure 30: myrealm Settings](image)

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.
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**.

---

**Figure 31: Creating New Authentication Provider**

**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.

![Domain Structure](image)

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.

![Generic Data Source](image)

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

11. Click Next.

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

![Figure 41: Authentication Provider – Common Configuration Settings](image)

9. Click Save.

10. Select the Provider Specific tab and enter the values in the fields as below:

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

**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.
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.
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 appear in first position and OUAFDBMSAuthenticator appears in second position.
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”.

![Figure 45: Creating New User](image)

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](image)

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

![Figure 47: External IDP Login Screen](image)

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

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.
8. Click the Resources tab. The Resources section appears.

9. Change the Authentication Scheme to ‘LDAPScheme’ and click **Apply**.

**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
   ```