Copyright © 2011, 2012, Oracle and/or its affiliates. All rights reserved.

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 decompilation of this software, unless required by law for interoperability, is prohibited.

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.

If this is software or related documentation that 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 Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software or hardware 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 or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle 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.

This software or hardware 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.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>v</td>
</tr>
<tr>
<td>Audience</td>
<td>v</td>
</tr>
<tr>
<td>Documentation Accessibility</td>
<td>v</td>
</tr>
<tr>
<td>Related Documents</td>
<td>v</td>
</tr>
<tr>
<td>Conventions</td>
<td>v</td>
</tr>
<tr>
<td>1  Architecture Overview</td>
<td>1-1</td>
</tr>
<tr>
<td>1.1 JD Edwards EnterpriseOne and WebCenter Single Sign-On Architecture</td>
<td>1-1</td>
</tr>
<tr>
<td>1.1.1 Architecture Overview</td>
<td>1-1</td>
</tr>
<tr>
<td>1.1.2 Configuring the SSO Environment</td>
<td>1-3</td>
</tr>
<tr>
<td>1.1.3 Software Versions</td>
<td>1-3</td>
</tr>
<tr>
<td>2  Oracle Access Manager Server</td>
<td>2-1</td>
</tr>
<tr>
<td>2.1 Understanding Oracle Access Manager</td>
<td>2-2</td>
</tr>
<tr>
<td>2.2 Installing Oracle Internet Directory</td>
<td>2-2</td>
</tr>
<tr>
<td>2.2.1 Installing Oracle Internet Directory 11.1.1.2.0</td>
<td>2-2</td>
</tr>
<tr>
<td>2.2.2 Upgrading to Oracle Internet Directory 11.1.1.5</td>
<td>2-13</td>
</tr>
<tr>
<td>2.2.3 Verifying Oracle Internet Directory Installation</td>
<td>2-17</td>
</tr>
<tr>
<td>2.3 Installing Oracle Access Manager 11g</td>
<td>2-20</td>
</tr>
<tr>
<td>2.4 Configuring Oracle Access Manager to Use the External LDAP Server</td>
<td>2-34</td>
</tr>
<tr>
<td>3  Oracle WebCenter Spaces</td>
<td>3-1</td>
</tr>
<tr>
<td>3.1 Understanding WebCenter Server</td>
<td>3-1</td>
</tr>
<tr>
<td>3.2 Installing Oracle WebCenter Spaces</td>
<td>3-1</td>
</tr>
<tr>
<td>3.2.1 Post Installation Configuration</td>
<td>3-8</td>
</tr>
<tr>
<td>3.3 Configuring the WebLogic Domain for Oracle Access Manager</td>
<td>3-9</td>
</tr>
<tr>
<td>3.3.1 Configuring the Oracle Internet Directory Authenticator</td>
<td>3-10</td>
</tr>
<tr>
<td>3.3.2 Configuring the OAM Identity Asserter</td>
<td>3-12</td>
</tr>
<tr>
<td>3.3.2.1 Adding the OAM Identity Asserter</td>
<td>3-13</td>
</tr>
<tr>
<td>3.3.2.2 Configuring the Default Authenticator and Provider Order</td>
<td>3-14</td>
</tr>
<tr>
<td>3.3.2.3 Adding an OAM Single Sign-On Provider</td>
<td>3-15</td>
</tr>
<tr>
<td>3.4 Installing Oracle WebGate</td>
<td>3-16</td>
</tr>
<tr>
<td>3.4.1 Post-Installation Steps</td>
<td>3-20</td>
</tr>
<tr>
<td>3.5 Configuring Oracle HTTP Server for WebCenter Spaces</td>
<td>3-22</td>
</tr>
<tr>
<td>3.6 Registering the WebGate Agent for WebCenter Spaces</td>
<td>3-23</td>
</tr>
</tbody>
</table>
4 JD Edwards EnterpriseOne HTML Server

4.1 Understanding JD Edwards EnterpriseOne HTML Server .............................................. 4-1
4.2 Installing SOA Suite 11g .............................................................................................. 4-1
4.2.1 Verify the Installation ............................................................................................ 4-12
4.3 Installing Oracle WebGate .......................................................................................... 4-14
4.3.1 Post-Installation Steps .......................................................................................... 4-19
4.4 Configuring the KeyStore Connection ........................................................................ 4-21
4.4.1 Generate the KeyStore from the Oracle WebCenter Server .................................. 4-21
4.4.2 Configure KeyStore on EnterpriseOne ................................................................. 4-22
4.5 Installing JD Edwards EnterpriseOne HTML Server .................................................. 4-23
4.6 Configuring Oracle HTTP Server for EnterpriseOne HTML Server ....................... 4-24
4.7 Registering the WebGate Agent for EnterpriseOne HTML Server ............................. 4-24
4.8 Enabling OAM SSO on the EnterpriseOne HTML Server ......................................... 4-29
4.9 Copying JAR File to the HTML Web Server .............................................................. 4-30
4.10 Granting Permission to the Client Application to Request a Token from OpenSSO.... 4-31
4.11 Synchronizing the System Clock on all Servers ......................................................... 4-31
4.12 Testing the SSO Configuration .................................................................................... 4-32

A Create Database Schemas with Repository Creation Utility

B Installing WebLogic Server

C Installing Oracle HTTP Server

C.1 Installing HTTP Server 11.1.1.2................................................................................... C-1
C.2 Upgrading Oracle HTTP Server to Version 11.1.1.5 ................................................... C-9
Preface

Welcome to the JD Edwards EnterpriseOne Related Information Application Framework for WebCenter Installation and Configuration Guide.

Audience

This guide is intended for system administrators and technical consultants who are responsible for installing and configuring JD Edwards EnterpriseOne.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

You can access related documents from the JD Edwards EnterpriseOne Release Documentation Overview pages on My Oracle Support. Access the main documentation overview page by searching for the document ID, which is 876932.1, or by using this link:

https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=876932.1

This guide contains references to server configuration settings that JD Edwards EnterpriseOne stores in configuration files (such as jde.ini, jas.ini, jdbj.ini, jdelog.properties, and so on). Beginning with the JD Edwards EnterpriseOne Tools Release 8.97, it is highly recommended that you only access and manage these settings for the supported server types using the Server Manager program. See the Server Manager Guide.

Conventions

The following text conventions are used in this document:
<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold</strong></td>
<td>Indicates field values.</td>
</tr>
<tr>
<td><em>Italics</em></td>
<td>Indicates emphasis and JD Edwards EnterpriseOne or other book-length publication titles.</td>
</tr>
<tr>
<td>Monospace</td>
<td>Indicates a JD Edwards EnterpriseOne program, other code example, or URL</td>
</tr>
</tbody>
</table>
This chapter contains this topic:

- Section 1.1, "JD Edwards EnterpriseOne and WebCenter Single Sign-On Architecture".

1.1 JD Edwards EnterpriseOne and WebCenter Single Sign-On Architecture

JD Edwards EnterpriseOne and WebCenter single sign-on (SSO) supports creating contextually linked group spaces in JD Edwards EnterpriseOne, and opening the group space in WebCenter for collaboration among authorized users. Contextually linked group spaces are group spaces that are tied to a JD Edwards EnterpriseOne application form. SSO enables one-time login with multiple access between EnterpriseOne and WebCenter Spaces.

To support JD Edwards EnterpriseOne and WebCenter Spaces SSO, you deploy three major Oracle components:

- EnterpriseOne HTML Web Server
- Oracle Access Manager Server (OAM)
- WebCenter Spaces

OAM ensures SSO security between JD Edwards EnterpriseOne and WebCenter. Oracle Web Service Manager (OWSM) ensures server-to-server security between JD Edwards EnterpriseOne and WebCenter Spaces.

1.1.1 Architecture Overview

This diagram shows the architecture for SSO between JD Edwards EnterpriseOne and Web Center:
In summary:

1. Users access JD Edwards EnterpriseOne by entering their JD Edwards EnterpriseOne URL in a Web browser, and then entering their SSO user ID and password on the sign-on page.

2. The WebGate component on the Oracle HTTP Server (OHS) captures the user credentials and sends them to Oracle Access Manager (OAM) for authentication.

3. OAM compares the user credentials against the Oracle Internet Directory (OID). If the SSO user credentials are not in OID, OAM notifies WebGate and the user is denied access to JD Edwards EnterpriseOne. If OAM finds the SSO user credentials in OID, OAM authenticates the user credentials.

4. After successful authentication, the user accesses the JD Edwards EnterpriseOne HTML client. If the user is WebCenter enabled, the My Web Center Group Spaces link appears under the Action section of the EnterpriseOne menu. Clicking the link opens another browser that opens the WebCenter home page without requiring the user to sign in again.

5. The EnterpriseOne HTML client calls a Web Center web service through OWSM. For example, the EnterpriseOne HTML client fetches a list of group spaces from WebCenter. This creates group space links in the Related Information Application Framework. OWSM secures the communication.

6. When the user clicks the group space link in JD Edwards EnterpriseOne, a new Web browser opens and tries to connect to the WebCenter group space.
4. The WebGate on the WebCenter server determines that the user has been authenticated and allows the user to access the group space without logging in again.

1.1.2 Configuring the SSO Environment

One way to configure SSO is to deploy different components to three machines. The following diagram shows this configuration strategy:

1.1.3 Software Versions

You download the software components from Oracle Technology Network (OTN). This table identifies the software versions that JD Edwards EnterpriseOne used to configure the SSO solution, and these software versions have been tested:

<table>
<thead>
<tr>
<th>Software</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebCenter Spaces</td>
<td>11.1.1.5</td>
</tr>
<tr>
<td>WebLogic Server</td>
<td>10.3.5.0</td>
</tr>
<tr>
<td>Repository Creation Utility (RCU)</td>
<td>11.1.1.5</td>
</tr>
<tr>
<td>Oracle Database</td>
<td>11.2.0.1</td>
</tr>
<tr>
<td>Oracle Internet Directory (OID)</td>
<td>11.1.1.5</td>
</tr>
</tbody>
</table>
The remaining chapters in this document, Chapters 2, 3, and 4, provide information for installing the Oracle software components on three different servers. These chapters are excerpts from the Oracle Fusion Middleware documents, which discuss how to install many other components that you do not need. You can use these three chapters as a guide for understanding which components you need to deploy for your platform. If you need more detail, you can find the component installation information in Oracle documents, which are located on Oracle Technology Network (OTN).

### Software

<table>
<thead>
<tr>
<th>Software</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Access Manager (OAM)</td>
<td>11.1.1.5</td>
</tr>
<tr>
<td>Oracle WebGate</td>
<td>11.1.1.5</td>
</tr>
<tr>
<td>OWSM (Oracle Web Services Manager) / SOA</td>
<td>11.1.1.5</td>
</tr>
<tr>
<td>FMW Web Tier (OHS)</td>
<td>11.1.1.5</td>
</tr>
</tbody>
</table>

**See Also:**

- Oracle Fusion Middleware Installation Guide for Oracle Identity Management 11g Release 1 (11.1.1)
  
  http://docs.oracle.com/cd/E21764_01/install.1111/e12002/toc.htm

- Oracle Fusion Middleware Administrator’s Guide for Oracle Access Manager with Oracle Security Token Service 11g Release (11.1.1)
  
  http://docs.oracle.com/cd/E23943_01/doc.1111/e15478.pdf

- Oracle Fusion Middleware Installation Guide for Oracle WebCenter 11g Release 1 (11.1.1.5) on Oracle Technology Network
  
  http://docs.oracle.com/cd/E21764_01/install.1111/e12001/toc.htm

- Oracle Fusion Middleware Administrator’s Guide for Oracle WebCenter 11g Release 1 (11.1.1.5) on Oracle Technology Network
  
  http://docs.oracle.com/cd/E21764_01/webcenter.1111/e12405/toc.htm

- Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server 11g Release 1 (10.3.5) on Oracle Technology Network
  
  http://docs.oracle.com/cd/E21764_01/doc.1111/e14142/toc.htm
This chapter contains these topics:

- Section 2.1, "Understanding Oracle Access Manager"
- Section 2.2, "Installing Oracle Internet Directory"
- Section 2.3, "Installing Oracle Access Manager 11g"
- Section 2.4, "Configuring Oracle Access Manager to Use the External LDAP Server"

### 2.1 Understanding Oracle Access Manager

Oracle Access Manager 11g provides a full range of Web perimeter security functions that include Web single sign-on, authentication and authorization, policy administration, auditing, and more.

Single sign-on (SSO) enables users and groups of users to access multiple applications after authentication. SSO eliminates multiple sign-on requests. Oracle Access Manager 11g is the Oracle Fusion Middleware 11g single sign-on solution.

Oracle Access Manager 11g is a Java Platform, Enterprise Edition (Java EE) based enterprise-level security application that provides restricted access to confidential information and centralized authentication and authorization services.

A web server, application server, or any third-party application must be protected by a webgate that is registered with Oracle Access Manager as an agent. To enforce policies, the agent acts as a filter for HTTP requests. Oracle Access Manager enables administrators to define authentication and authorization policies.

**Prerequisites**

- Create local user ID and password credentials.
- Log into the machine that will contain your OAM components.
- Install a supported database level. For example: 11.2.0.1

---

**Note:** Check the EnterpriseOne Minimum Technical Requirements for supported database level if this database is also used for EnterpriseOne.

- Create database schemas using Repository Creation Utility (RCU) 11.1.1.5.0. See Create Database Schemas with Repository Creation Utility.
2.2 Installing Oracle Internet Directory

Before installing Oracle Access Manager 11g, you must have Oracle WebLogic Server and Oracle Internet Directory 11.1.1.5 installed and configured.

First, you install Oracle Internet Directory (OID), version 11.1.1.2. After you install this version, you upgrade to version 11.1.1.5. After installing and upgrading OID to the appropriate version, you verify the installation.

2.2.1 Installing Oracle Internet Directory 11.1.1.2.0

Use these steps to install OID 11.1.1.2.0.

1. Download and unzip ofm_idm_<platform>_11.1.1.2.0_64_disk1_1of1.zip.
2. Open the OID download directory.
3. Launch the installer:
   - On Windows: setup.exe with Run as administrator option.
   - On UNIX: ./runInstaller as a non-root user.

   This action starts the Oracle Universal Installer.
4. Select **Install and Configure** type.

5. Click **Next**.

6. The installer performs prerequisite checks. Be sure to correct any failures before continuing.
7. Click Next.

8. Select Create New Domain and enter the Domain Name, User Name, and Password.
9. Click Next.

10. Specify the installation location.

11. Click Next.

12. Specify the Security Update option. Oracle recommends enabling this option to receive any security updates.
13. Click Next.
14. Clear any components that you do not want the installer to configure.
15. Click Next.

16. Select Auto Port Configuration.

17. Click Next.

18. On Specify Schema Database page, enter the appropriate information for the following fields:
   - Database connect String
   - Schema Name = Default to ODS
   - Password
19. Click Next.

20. In the Realm field, enter the domain address of your Oracle Internet Directory.

21. Enter Oracle Internet Directory Administrator User Password. The default administrator user is **cn=orcladmin**.
22. Click Next.

23. Enter the Federation Details if you have selected this component to be configured.
24. Click Next.

25. Accept the default values on the following page.

26. Click Next.

27. Review the Install Summary.
28. Click Install.

29. Click Next when the installation process is completed.
30. The Configuration Progress begins.

31. Click Next.

32. On Installation Complete, you can click Save to create an Installation Summary for future reference.

   Also ensure you have noted all of the passwords you entered during the installation.

33. Click Finish.
2.2.2 Upgrading to Oracle Internet Directory 11.1.1.5

After you successfully install Oracle Internet Directory version 11.1.1.2, run Patch to upgrade Oracle Internet Directory to version 11.1.1.5. Use these steps to upgrade OID 11.1.1.2.0 to OID 11.1.1.5.

1. Stop the Oracle Process Manager using OPMN:
   - On Windows, open the Windows Services and stop the OID process.
   - On Unix/Linux, go to `<MW_Home>/<oid_instance_name>/bin` and enter this command:
     ```bash
     ./opmnctl stopall
     ```


3. Open the Oracle Internet Directory 11.1.1.5 directory.

4. Double click `setup.exe` (with Run as administrator) or `runInstaller`.
   This action starts the Oracle Universal Installer.

5. On Oracle Universal Installer Welcome, click **Next**.
6. Specify the existing Middleware Home and Oracle Internet Directory Home.

7. Click Next.
8. Specify the Security Updates information.

9. Click Next.

10. Review the Installation Summary.
11. Click **Install**.

12. Click **Next** when the Installation process is completed.
13. Review the install process or save the installation summary.

14. Click **Finish** to exit the installer.

15. Stop and restart the Oracle Process Manager using OPMN:
   
   - On Windows, open the Windows Services and stop and restart the OID process.
   - On Unix/Linux, go to `<MW_Home>/<oid_instance_name>/bin` and enter these commands:
     
     ```
     ./opmnctl stopall
     ./opmnctl startall
     ```

### 2.2.3 Verifying Oracle Internet Directory Installation

After you upgrade Oracle Internet Directory to 11.1.1.5, use these steps to verify the installation.

1. Verify the Oracle Directory Server Manager (ODSM) is active:
   
   a. Open the WebLogic Administration Console.
   
   b. Navigate to Servers.
   
   c. Verify `wls_ods1` is in a running status.
2. Open an Internet Browser and enter the ODSM URL:
   
   http://server:port/odsm

   For example:
   
   http://denptw23.mlab.jdedwards.com:7005/odsm

3. Click **Connect to a directory** to create a new connection.

4. Click **Create A New Connection**.

5. Enter the Admin user and password.
6. The Oracle Directory Server Manager appears.

7. Select the **Data Browser** tab to view user information.
Upon successful installation verification, close Directory Manager.

2.3 Installing Oracle Access Manager 11g

Use these steps to install the Oracle Access Manager (OAM) 11.1.1.5.

1. Download and unzip `ofm_iam_generic_11.1.1.5.0.zip` file.
2. Change directory to Disk 1.
3. Execute this command:
   - On Windows, run `setup.exe` with the Run as Administrator option.
   - On UNIX/Linux, run `runInstaller`.
4. Enter the JRE/JDK location.
5. On the Welcome page, click Next.
6. Select **Skip Software Updates** option.

7. Click **Next**.

8. The install performs Prerequisite Checks.
9. Specify the Oracle Middleware Home and the Oracle Access Directory Home. The default home is Oracle_OAM.

10. Click Next.

11. Review the Installation Summary.
12. Click Install.

13. Wait for the installation process to complete.

14. Click Next.
15. Review the installation location.

16. Click **Finish** to exit the installer.

17. Run the domain configure from `<MW_Home>/Oracle_OAM/common/bin`:
   - On Windows = config.cmd
   - On UNIX = config.sh

18. The Fusion Middleware Configuration Wizard screen appears.

19. Select **Create a new WebLogic domain** option.
20. Click Next.

21. Select the components to configure.
   For OAM Server, you need Oracle Access Manager with Database Policy Store and Oracle Enterprise Manager. Oracle JRF - 11.1.1.0 is selected by default.

22. Click Next.

23. Enter a domain name and accept the default locations.
24. Click Next.

25. Enter the Administrator User Name and Password.

26. Click Next.

27. Select Production Mode and verify the JDK version and location.
28. Click Next.

29. Enter the JDBC Component Schema, complete these fields:

- DBMS/Service
- Host Name and Port
- Schema Password
- Schema Owner

If you are not using the default schema prefix (Dev), you must select each schema component individually and modify the prefix only.
30. Click Next.

31. The installer verifies all of the component schema connections.

32. Click Next.

33. Select Administration Server and Managed Servers, Clusters and Machines options.
34. Click Next.

35. Enter the Administration Server Name; for example, AdminServerOAM

Do not accept the default listen port (7001) if you have Oracle Internet Directory Server already installed because it might have used the default port. Enter a unique listen port for this OAM server. For example, port 8001.

36. Click Next.
37. Accept the default values on the Configure Managed Servers page.

38. Click Next.

39. The Configure Clusters page appears.

40. Click Next.

41. Select the Machine Type:
   - On Windows select the Machine tab.
- On UNIX and Linux, select the **UNIX Machine** tab.

42. Select the **Add** tab.

43. Enter a logical machine name.

44. Click **Next**.

45. Assign the servers to this logical machine.

46. Click **Next**.
47. Review the Configuration Summary.

48. Click Create.

49. Click Done once the domain creation is completed.

50. Start the Admin Server:
   - On Windows, open a command window, change the directory to `<MW_Home>\user_projects\domains\OAMdomain\bin`
Run startWebLogic.cmd

- On UNIX, run `startWebLogic.sh` from `<MW_Home>/user_projects/domains/OAMdomain/bin`

51. Connect to the OAM Domain Administration console

http://full-qualified-oamserver:domain-port/console

52. Select the Servers and start the oam_server1 managed server.

53. Verify the OAM installation by opening the OAM Admin Console

http://full-qualified-oamserver:oamport/oamconsole

**Note:** The oamport is the same as the WebLogic Console port.
2.4 Configuring Oracle Access Manager to Use the External LDAP Server

Oracle Access Manager 11g by default uses the Oracle WebLogic embedded LDAP Server. You must create a custom User Identity Store to use the external LDAP Server.

1. Log on to the OAM Administration Console.
2. Select the Data Sources from the System Configuration tab.
3. Open the **UserIdentityStore1** from User Identity Stores.
   
   This is the default embedded LDAP server.

4. To create a new user identity store, focus on **User Identity Stores** and click the **Create** button.

5. Enter your LDAP information, and then click **Test Connection**.
6. Set this newly created store to the Default and System Store.

Also you might want to add the additional system administrators.

7. Restart the OAM Server.
This chapter contains these topics:

- Section 3.1, "Understanding WebCenter Server"
- Section 3.2, "Installing Oracle WebCenter Spaces"
- Section 3.3, "Configuring the WebLogic Domain for Oracle Access Manager"
- Section 3.4, "Installing Oracle WebGate"
- Section 3.5, "Configuring Oracle HTTP Server for WebCenter Spaces"
- Section 3.6, "Registering the WebGate Agent for WebCenter Spaces"

3.1 Understanding WebCenter Server

The WebCenter server ensures the SSO credentials are valid without the user logging in again.

**Prerequisites**

- Install WebCenter Database Schemas (See Appendix A)
- Install WebLogic Server (See Appendix B)

Important: The WebCenter database schemas must be created, and the WebLogic Server must be installed before you install Oracle WebCenter Spaces.

3.2 Installing Oracle WebCenter Spaces

You install Oracle WebCenter Spaces 11.1.1.5.0.

When you install the WebCenter components on your machine, be sure to enter the correct data (machine name, ports, and so on) for your configuration. When you download the software from Oracle Technology Network (OTN) note the directories to which you downloaded the software and replace the directory location specified in this chapter with your directory locations. Be sure to install the executable files for your platform.

Use these steps to install Oracle WebCenter spaces 11.1.1.5.0.

1. Download and unzip the WebCenter installation file:
   
   ofm_wc_generic_11.1.1.5.0_disk1_1of1.zip

2. Execute the install process from Disk1 folder:
   - On Windows: *setup.exe* with Run as administrator option
3. Review the Welcome page information, and then click Next.
4. Select your **Software Updates** option.
5. The installer performs prerequisite checks.
7. Select the application server.

**Note:** EnterpriseOne supports only a WebLogic Server as the application server.
8. Click Next.

9. Review the Install Summary.

10. Click Install to start the install process.
11. Click **Next** to continue.

12. Click **Finish** when the install process is completed.
13. Run config.cmd (.sh) from <MW_Home>\Oracle_WC1\common\bin folder to create the WebCenter domain.

14. Select Create a new WebLogic domain option.

15. Select the products to be part of this domain. You can add more products later.

16. Click Next.

17. Enter the domain name.
18. Enter the domain Administrator user and password.

19. Select Production Mode.

20. Verify the available JDK.

21. Enter the JDBC Component Schema database connection.
22. Test JDBC Schema connection.

23. Select the Administration Server and Managed Server, Cluster and Machine.

24. See Appendix B to complete the domain creation.
3.2.1 Post Installation Configuration

1. Start the WebCenter Admin Server (startWebLogic.cmd (.sh)) from <MW_Home>\user_projects\domains\<webcenter_domain>\bin folder.

2. Start WebLogic NodeManager (startNodeManager.cmd/sh) from <MW_home>\wlserver_10.3\server\bin.

3. The startNodeManager process creates a nodemanager.properties file in <MW_home>\wlserver_10.3\common\nodemanager folder.

4. Once the file is created, run setNMProps.cmd/.sh from <MW_home>oracle_common\common\bin folder.

5. After the value is changed, you must stop and restart NodeManager.

6. Start the domain Admin Server and WC_Spaces.

7. After the Admin Server is started, you can access the domain console, Enterprise Manager, and WebCenter Spaces.

   http://server:7001/console (Enterprise Manager)
   http://server:7001/em  (Domain Console)

---

Note: Another option is that you can edit the nodemanager.properties by opening the file with an editor and change StartScriptEnabled to true.

Important: WebCenter Spaces will not start correctly if this value is not set.
8. Click About WebCenter Spaces on the bottom right to verify the version level.

### 3.3 Configuring the WebLogic Domain for Oracle Access Manager

Configuring the WebLogic Domain for OAM consists of these tasks:

- Configuring the Oracle Internet Directory Authenticator
- Configuring the OAM Identity Asserter
3.3.1 Configuring the Oracle Internet Directory Authenticator

Assuming Oracle Internet Directory is backing the Oracle Access Manager (OAM) identity store, an Oracle Internet Directory authenticator (OracleInternetDirectoryAuthenticator) should be configured for the LDAP server that is used as the identity store of OAM, and the provider should be set to SUFFICIENT.

Use these steps to configure the Oracle Internet Directory Authenticator.

1. Log in to the WebCenter WebLogic Server Administration Console.
2. From the Domain Structure pane, click Security Realms.
3. Select the realm entry for which to configure the OID authenticator.
4. Select the Providers tab.
5. Click New to create a provider.
6. Enter a name for the new provider (for example, OID Authenticator), select OracleInternetDirectoryAuthenticator as the type, and then click OK.
7. On the Providers tab, click the newly added provider. The common setting pane appears.
8. Set the control flag to SUFFICIENT and click Save.

9. Open the Provider Specific tab.
10. Complete the fields as shown in the table below. Leave the rest of the fields set to their default values.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>The host ID for the LDAP server</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>The LDAP server port number</td>
<td></td>
</tr>
<tr>
<td>Principal</td>
<td>The LDAP administrator principal</td>
<td></td>
</tr>
<tr>
<td>Credential</td>
<td>&lt;password&gt;</td>
<td>The administrator principal password</td>
</tr>
<tr>
<td>Confirm Credential</td>
<td>&lt;password&gt;</td>
<td></td>
</tr>
<tr>
<td>User Base DN</td>
<td>(&amp;(uid=*)(objectclass=person))</td>
<td>User Search Base - this value should be the same as for the OAM Access Manager setup.</td>
</tr>
<tr>
<td>User Name Attribute</td>
<td>uid</td>
<td></td>
</tr>
<tr>
<td>Group Base DN</td>
<td>Group search base - same as user base DN</td>
<td></td>
</tr>
<tr>
<td>Use Retrieved User Name as Principal</td>
<td>Checked</td>
<td>User login IDs are usually case insensitive. This flag is required so that the subject established contains the user name as stored in the OID.</td>
</tr>
</tbody>
</table>

11. Click Save.

### 3.3.2 Configuring the OAM Identity Asserter

In a WebLogic Server domain where JRF is installed, the JRF template is present as part of the domain in an Oracle Fusion Middleware product. In this case, the OAM Identity Asserter and OAM Authentication Provider are automatically available for configuration. If JRF is not installed in your WebLogic domain, you must add the OAMAuthnProvider.jar to a specific location in your domain.

Configuring the OAM Identity Asserter consists of these tasks:
- Adding the OAM Identity Asserter
- Configuring the Default Authenticator and Provider Order
- Adding an OAM Single sign-On Provider

### Prerequisites

Confirm the required JAR and WAR files as follows:

- Confirm the location of required JAR files in the following Fusion Middleware path:
  `<MW_Home>/oracle_common/modules/oracle.oamprovider_11.1.1/oamAuthnProvider.jar`
- Locate the console-extension WAR file in the following path:
  `<MW_Home>/oracle_common/modules/oracle.oamprovider_11.1.1/oamauthenticationprovider.war`
- Copy the WAR file to the following path in the WebLogic Server home:
  <MW_Home>/wlserver_10.3/server/lib/console-ext/autodeploy/oamauthenticationprovider.war

### 3.3.2.1 Adding the OAM Identity Asserter

An OAM identity asserter must be configured with the provider control flag set to required.

Use these steps to add the OAM Identity Asserter.

1. Log in to the WebCenter WebLogic Server Administration Console.
2. From the Domain Structure pane, click **Security Realms**.
3. Click the realm entry for which to configure the OAM identity asserter.
4. From the **Providers** tab, click **New**.

![Create a New Authentication Provider](image)

5. Enter a name for the new provider (for example, OAM ID Asserter), select OAMIdentityAsserter as its type and click **OK**.
6. On the Providers tab, click the newly added provider.
7. Set the control flag to **REQUIRED** and check that **OAM_REMOTE_USER** and **ObSSOCookie** are set for Active Types.

8. Click **Save** to save your settings.

### 3.3.2.2 Configuring the Default Authenticator and Provider Order

After configuring the OAM identity assister, ensure that the default authenticator’s control flag is set to **SUFFICIENT** and reorder the providers.

Use these steps to configure the default authenticator and provider order.

1. Navigate to the Provider Settings pane.
2. Open the Default Authenticator and set the control flag to **SUFFICIENT**.
3. Do the same for any providers other than the two you just created.
4. On the Setting Pane, reset the provider order to:
   - **OAMIdentityAsserter(REQUIRED)**
   - **OracleInternetDirectoryAuthenticator (SUFFICIENT)**
   - **DefaultAuthenticator (SUFFICIENT)**
   - **DefaultIdentityAsserter**
You can use these steps to add an Administrators group and add your user in it.

1. Connect to Oracle Directory Manager
2. Create a new Group, Administrators. You can use the Create Like option.
3. Add your admin user to this group

Now, you should able to start the WebLogic Admin Server.

3.3.2.3 Adding an OAM Single Sign-On Provider
After checking that the default authenticator’s control flag is set correctly and that the order of the providers is correct, add an OAM SSO provider and restart all servers.

1. Connect to the WebLogic domain using WLST and run the following command:
   
   Start WLST.cmd or WLST.sh from `<MW_Home>oracle_common\common\bin` folder
   
   Connect (‘admin-user’,’admin-password’,’t3://localhost:7001’)

   **Note:** On Windows platform, if your WebLogic user is not part of the OID Administrators group, you will not be able to restart the WebLogic Admin Server.
addOAMSSOProvider
(loginuri="/${app.context}/adfAuthentication",logouturi="/oamsso/logout.html")

2. Exit the tool.
3. Restart all servers.

### 3.4 Installing Oracle WebGate

Next, you install Oracle WebGate 11.1.1.5.

Oracle HTTP Server WebGate is a web server plug-in that is shipped out-of-the-box with Oracle Access Manager. The Oracle HTTP Server WebGate intercepts HTTP requests from users for web resources and forwards them to the Access Server for authentication and authorization. Oracle HTTP Server WebGate installation packages are found on media and virtual media that is separate from the core components.

**Prerequisites**

Install Oracle HTTP Server *(See Appendix C)*

- If you are installing Oracle HTTP Server 11g WebGate for Oracle Access Manager on a Linux or Solaris operating system, you must download and install third-party GCC libraries on your machine.

  You can download the appropriate GCC library from the following third-party website:


<table>
<thead>
<tr>
<th>Operating System</th>
<th>Architecture</th>
<th>GCC Libraries</th>
<th>Required Library Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux 64-bit</td>
<td>x64</td>
<td>libgcc_s.so.1</td>
<td>3.4.6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>libstdc++.so.6</td>
<td></td>
</tr>
<tr>
<td>Solaris 64-bit</td>
<td>SPARC</td>
<td>libgcc_s.so.1</td>
<td>3.3.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>libstdc++.so.5</td>
<td></td>
</tr>
</tbody>
</table>

- If you are using Windows 2008 64-bit operating systems, you must install Microsoft Visual C++ 2005 libraries on the machine hosting the Oracle HTTP Server 11g WebGate.

  The libraries are included in the Microsoft Visual C++ 2005 SP1 Redistributable Package (x64), which can be downloaded from the following website:


Use these steps to install Oracle HTTP 11g WebGate.

1. Download and unzip `ofm_oam_webgates_generic_11.1.1.5.0_disk1_1of1.zip`.
2. Launch the installer:
   - On Windows: `setup.exe` with **Run as administrator** option.
   - On UNIX: `./RunInstaller` as a non-root user.
3. Specify JRE/JDK location.
4. Click **Next** on the Welcome page.

   Oracle HTTP WebGate supports Oracle HTTP version 11.1.1.2 or 11.1.1.3. EnterpriseOne configuration supports version 11.1.1.5. See Appendix A to upgrade to Version 11.1.1.5.

5. The installer performs prerequisite checks.

   ![Prerequisite Checks](image.png)

   This image shows the prerequisite checks on Linux operating system:

7. Review the installation Summary.
8. Click Install.

9. Click Next when the installation is completed.
10. Click **Finish** when the installation is completed.

### 3.4.1 Post-Installation Steps

You must complete the following steps after installing Oracle HTTP Server 11g WebGate for Oracle Access Manager:

1. Move to the following directory under your Oracle Home for WebGate:
   - On UNIX operating systems:
     ```
     <webgate_home>/webgate/ohs/tools/deployWebGate
     ```
   - On Windows operating systems:
     ```
     <webgate_home>\webgate\ohs\tools\deployWebGate
     ```

2. On the command line, run the following command to copy the required bits of agent from the Webgate_Home directory to the WebGate instance location:
   - On UNIX operating systems:
     ```
     ./deployWebgateInstance.sh -w <Webgate_Instance_Directory> -oh <Webgate_Oracle_Home>
     ```
   - On Windows operating systems:
deploy WebgateInstance.bat -w <Webgate_Instance_Directory> -oh <Webgate_Oracle_Home>

Where <Webgate_Oracle_Home> is the directory where you have installed Oracle HTTP Server WebGate and created as the Oracle Home for WebGate.

For example: <MW_HOME>/Oracle_OAMWebGate1

The <Webgate_Instance_Directory> is the location of WebGate Instance Home, which is same as the Instance Home of Oracle HTTP Server.

For example: <MW_HOME>/Oracle_WT1/instances/instance1/config/OHS/ohs1

3. Run the following command to ensure that the LD_LIBRARY_PATH variable contains <Oracle_Home_for_Oracle_HTTP_Server>/lib:

   - On UNIX operating systems:
     ```bash
     Export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:<Oracle_Home_for_Oracle_HTTP_Server>/lib
     ```
   - On Windows operating systems:
     ```<Webgate_Installation_Directory>\webgate\ohs\lib location in the PATH environment variable.```

4. From your present working directory, move up one directory level:
   - On UNIX operating systems:
     ```bash
     <webgate_home>/webgate/ohs/tools/setup/InstallTools
     ```
   - On Windows operating systems:
     ```bash
     <webgate_home>\webgate\ohs\tools\editHttpConf
     ```

5. On the command line, run the following command to copy the apache_webgate.template from the Webgate_Home directory to the Webgate Instance location (renamed to webgate.conf) and update the httpd.conf file to add one line to include the name of webgate.conf:

   - On UNIX operating systems:
     ```bash
     ./EditHttpConf -w <Webgate_Instance_Directory> [-oh <Webgate_Oracle_Home>] [-o <output_file>]
     ```
6. Verify the updated httpd.conf.

   The following line is added to the bottom of the file:

   ```
   include "z:\oracle\Middleware\Oracle_WT1\instances\instance1\config\ohs\ohs1/webgate.conf"
   ```

**Note:** Do not restart the Oracle HTTP server until the WebGate agent is registered for WebCenter Spaces; errors will continue to display in the command line if the Oracle HTTP server processes are restarted.

### 3.5 Configuring Oracle HTTP Server for WebCenter Spaces

After you install and configure Oracle HTTP Server and Oracle HTTP WebGate, you configure the Oracle HTTP server for WebCenter Spaces.

Use the following example to configure `mod_wl_ohs.conf`. Verify that WebLogic port numbers match your configuration.
Registering the WebGate Agent for WebCenter Spaces

You must register the WebGate Agent for WebCenter Spaces.

Prerequisites:

- Install and configure Oracle HTTP Server and WebGate.
- Install and configure OID and OAM Server.
- Install and configure Oracle WebCenter Spaces.

3.6.1 Registering the WebGate Agent

Use these steps to register the WebGate Agent.

1. Open an internet browser and connect to Oracle Access Manager.

2. Open the OAM console.

   http://oamserver:oamport/oamconsole

3. Enter the Admin user and Password.

4. Select New OAM 11g Webgate option.
5. Enter a WebGate agent name and select the Open security option.
6. Enter your WebCenter URL in Base URL.
7. Click **Apply** to create the agent. Authorization and authentication policies will be created.

8. A Host Identifier and an Application Domain is generated as well.
9. Create the Resource URL from the Resources option

10. Click the **Create** button

11. Enter the following information:
   - Type = HTTP
   - Host Identifier = Select your Host Identifier
   - Resource URL = /webcenter
   - Protection Level = Protected
   - Authentication Policy = Protected Resource Policy
   - Authorization Policy = Protected Resource Policy
12. Repeat the above step and add the resource URL = /console and /em (if you plan to use SSO on the Admin Console and Enterprise Manager.)

You should see the newly added resources listed.

14. Review all registered agents.

15. Select the **System Configuration** tab.

16. Open the Access Manager Settings section and open the **SSO Agents** option.

17. Double-click **OAM Agents**, and then click the **Search** button.
The system displays a list of registered agents.
Registering the WebGate Agent for WebCenter Spaces

18. The agent registration creates a cwallet.sso and ObAccessClient.xml file.

19. Copy these two files to the WebCenter server:
   
   `<MW_HOME>/user_projects/domain/OAMDomain/output/<Agent_name>`
   
   `<MW_Home>/Oracle_WT1/instances/instance1/config/OHS/ohs1/webgate/config` directory

   A system property tells WebCenter that the application is configured in SSO mode
   and some special handling is required.

20. To set this property, edit the `setDomainEnv.sh (.cmd)` script located in your
    `<domain>/bin` directory, and add an entry similar to the following at the end of
    the file:

    ```
    EXTRA_JAVA_PROPERTIES="-Doracle.webcenter.spaces.osso=true ${EXTRA_JAVA_PROPERTIES}"
    export EXTRA_JAVA_PROPERTIES
    ```

21. After changing the property, restart all the WebCenter Services: Admin Server,
    WC_Spaces server.

22. Stop and restart the Oracle HTTP server process using OPMN:

    - On Windows, open the Windows Services and stop and restart the Oracle
      HTTAP server process.
    - On Unix/Linux, go to `<MW_Home>/<oid_instance_name>/bin` and enter
      these commands:
      
      ```
      ./opmnctl stopall
      ./opmnctl startall
      ```

23. Test your SSO with the WebCenter URL:

    ```
    ```

    The SSO process switches to the Oracle Access Manager and display the SSO page.
24. Log in with your WebCenter user name and password.
This chapter contains these topics:

- Section 4.1, "Understanding JD Edwards EnterpriseOne HTML Server"
- Section 4.2, "Installing SOA Suite 11g"
- Section 4.3, "Installing Oracle WebGate"
- Section 4.4, "Configuring the KeyStore Connection"
- Section 4.5, "Installing JD Edwards EnterpriseOne HTML Server"
- Section 4.6, "Configuring Oracle HTTP Server for EnterpriseOne HTML Server"
- Section 4.7, "Registering the WebGate Agent for EnterpriseOne HTML Server"
- Section 4.8, "Enabling OAM SSO on the EnterpriseOne HTML Server"
- Section 4.9, "Copying JAR File to the HTML Web Server"
- Section 4.10, "Granting Permission to the Client Application to Request a Token from OpenSSO"
- Section 4.11, "Synchronizing the System Clock on all Servers"
- Section 4.12, "Testing the SSO Configuration"

4.1 Understanding JD Edwards EnterpriseOne HTML Server

The JD Edwards EnterpriseOne HTML server is a WebLogic server. This server works with the OAM to ensure that SSO credentials are valid. When valid SSO credentials are entered, the user is granted access to JD Edwards EnterpriseOne.

When you download the software from Oracle Technology Network (OTN) note the directories to which you downloaded the software and replace the directory location specified in this chapter with your directory locations. This chapter also specifies executable files for a Windows platform. Be sure to install the executable files for your platform.

*Note:* The JD Edwards EnterpriseOne HTML server is installed on a different server than the OAM/OID server.

4.2 Installing SOA Suite 11g

You install SOA Suite 11g, version 11.1.1.5. You use the installer to download the Oracle Fusion Middleware 11g SOA Suite.
Prerequisites

■ Install WebLogic Server 10.3.5. See Appendix B, "Installing WebLogic Server."
■ Download the Oracle Fusion Middleware 11g SOA Suite.

Use these steps to install Oracle SOA Suite 11.1.1.5.0

1. Launch the installer:
   ■ On Windows: setup.exe with Run as administrator option.
   ■ On Unix: ./runInstaller as a non-root user.

2. On the Welcome page, click Next.

3. Select the appropriate update option for your company.
4. The installer performs prerequisite checks.

5. Enter the Middleware Home and a SOA Home Directory.
6. Select WebLogic as the application server.

   EnterpriseOne does not support the configuration with WebSphere Application Server.
7. Review the Installation Summary.

8. Click Next when the installation process is completed.
9. Click **Finish** to exit the installer.

10. Launch the Domain Configuration Wizard (config.cmd or config.sh) from `<MW_Home>/Oracle_SOA/common/bin/`.  

![Image of the Installation Complete window]

![Image of the Fusion Middleware Configuration Wizard]
11. Select Oracle WSM Policy Manager-11.1.1.0 and Oracle JRF-11.1.1.0 options.

12. Enter a domain name.

13. Enter the Administrator User and Password.
14. Select **Production Mode** and verify the JDK location.

15. Enter the JDBC Schema information.
16. Verify the schema connections.

17. Select Administration Server and Managed Servers, Clusters and Machines options.
18. Enter the Administration Server Name and Port.

19. Click Next on the Configure Managed Servers page.

20. Click Next on the Configure Clusters page.

21. Add a logic machine name.
22. Assign a server to the machines.

23. Review the Configuration Summary and Click Create.
24. Click **Done** and start the Administration Server.

Refer to Appendix B on how to start and stop the Administration Server.

### 4.2.1 Verify the Installation

You must have the Administration Server running.

1. Open an internet browser, and enter the following URL:

   ```
   http://server:port:/wsm-pm/validator
   ```

2. Enter the Admin user and password.

3. The Policy Manager Status screen appears.

4. If the following error message occurs, use the steps in the next task to resolve the error.
Use these steps to fix errors:

1. Access Data Sources using this path from the left navigation:
   base_domain -> Services -> JDBC -> Data Sources

2. Click the mds-owsm link.

3. On the Settings for mds-owsm page, click the Targets tab.
4. On the Targets page, select AdminServer, and then click **Save**.

5. Activate the change and restart the WLS Admin Server.

6. Launch the URL again.

### 4.3 Installing Oracle WebGate

Next, you install Oracle WebGate 11.1.1.5.0.

Oracle HTTP Server WebGate is a Web server plug-in that is shipped out-of-the-box with Oracle Access Manager. The Oracle HTTP Server WebGate intercepts HTTP requests from users for Web resources and forwards them to the Access Server for authentication and authorization. Oracle HTTP Server WebGate installation packages are found on media and virtual media that is separate from the core components.
Prerequisites

- You must have Oracle HTTP Server installed and configured. See Appendix C, "Installing Oracle HTTP Server."

- If you are installing Oracle HTTP Server 11g WebGate for Oracle Access Manager on a Linux or Solaris operating system, you must download and install third-party GCC libraries on your machine.

You can download the appropriate GCC library from the following third-party website:

http://gcc.gnu.org/

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Architecture</th>
<th>GCC Libraries</th>
<th>Required Library Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux 64-bit</td>
<td>x64</td>
<td>libgcc_s.so.1, libstdc++ .so.6</td>
<td>3.4.6</td>
</tr>
<tr>
<td>Solaris 64-bit</td>
<td>SPARC</td>
<td>libgcc_s.so.1, libstdc++ .so.5</td>
<td>3.3.2</td>
</tr>
</tbody>
</table>

- If you are using Windows 2008 64-bit operating systems, you must install Microsoft Visual C++ 2005 libraries on the machine hosting the Oracle HTTP Server 11g WebGate.

The libraries are included in the Microsoft Visual C++ 2005 SP1 Redistributable Package (x64), which can be downloaded from the following website:


Use these steps to install Oracle HTTP 11g WebGate.

1. Download and unzip ofm_oam_webgates_generic_11.1.1.5.0_disk1_1of1.zip.

2. Launch the installer.
   - On Windows: setup.exe with **Run as administrator** option
   - On UNIX: /RunInstaller as a non-root user

3. Specify JRE/JDK location.

4. Click **Next** on the Welcome page.

   Oracle HTTP WebGate supports Oracle HTTP version 11.1.1.2 or 11.1.1.3. EnterpriseOne configuration supports version 11.1.1.5. See Appendix A, "Create Database Schemas with Repository Creation Utility" to upgrade to version 11.1.1.5.

5. The installer performs prerequisite checks.
7. Review the installation Summary.

8. Click **Next** when the installation is completed.
9. Click Finish to exit the installer.
4.3.1 Post-Installation Steps

You must complete the following steps after installing Oracle HTTP Server 11g WebGate for Oracle Access Manager:

1. Move to the following directory under your Oracle Home for WebGate:
   - On UNIX operating systems:
     ```bash
     <webgate_home>/webgate/ohs/tools/deployWebGate
     ```
   - On Windows operating systems:
     ```bash
     <webgate_home>\webgate\ohs\tools\deployWebGate
     ```

2. On the command line, run the following command to copy the required bits of the agent from the Webgate Home directory to the WebGate Instance location:
   - On UNIX operating systems:
     ```bash
     ./deployWebgateInstance.sh -w <Webgate_Instance_Directory> -oh <Webgate_Oracle_Home>
     ```
   - On Windows operating systems:
     ```bash
     deployWebgateInstance.bat -w <Webgate_Instance_Directory> -oh <Webgate_Oracle_Home>
     ```

Where `<Webgate_Oracle_Home>` is the directory where you have installed Oracle HTTP Server WebGate and created as the Oracle Home for WebGate. For example: `<MW_Home>/Oracle_OAMWebGate1`

The `<Webgate_Instance_Directory>` is the location of Webgate Instance Home, which is same as the Instance Home of Oracle HTTP Server. For example: `<MW_Home>/Oracle_WT1/instances/instance1/config/OHS/ohs1`

3. Run the following command to ensure that the LD_LIBRARY_PATH variable contains `<Oracle_Home_for_Oracle_HTTP_Server>/lib`
   - On UNIX operating systems:
     ```bash
     Export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:<Oracle_Home_for_Oracle_HTTP_Server>/lib
     ```
   - On Windows operating systems:
Set the `<Webgate_Installation_Directory>`\webgate\ohs\lib location in the PATH environment variable.

4. From your present working directory, move up one directory level:
   - On UNIX operating systems:
     ```
     <webgate_home>/webgate/ohs/tools/setup/InstallTools
     ```
   - On Windows operating systems:
     ```
     <webgate_home>\webgate\ohs\tools\editHttpConf
     ```

5. On the command line, run the following command to copy the `apache_webgate.template` from the Webgate Home directory to the WebGate Instance location (renamed to `webgate.conf`) and update the `httpd.conf` file to add one line to include the name of `webgate.conf`
   - On UNIX operating systems:
     ```
     ./EditHttpConf -w <Webgate_Instance_Directory> [-oh <Webgate_Oracle_Home>] [-o <output_file>]
     ```
   - On Windows operating systems:
     ```
     EditHttpConf.exe -w <Webgate_Instance_Directory> [-oh <Webgate_Oracle_Home>] [-o <output_file>]
     ```

6. Verify the updated `httpd.conf`.
   The following line is added to the bottom of the file
   ```
   include "z:\oracle\Middleware\Oracle_WT1\instances\instance1\config\ohs\ohs1/webgate.conf"
   ```

7. Restart the Oracle HTTP server process.
   Run `opmnctl (stopall and startall)` from `<MW_Home>`\Oracle_WT1\instances\instance1\bin
Configuring the KeyStore Connection

This section discusses configuring the KeyStore connection for WebCenter and EnterpriseOne.

Prerequisites
Verify your Node Manger on your EnterpriseOne machine has the StartScriptEnable set to true:

- Open the NodeManager.properties file from NMW_HOME>/wlserver_10.3/common/nodemanager folder and enter the following:
  
  `StartScriptEnable=true`

- Restart Node Manager.

4.4.1 Generate the KeyStore from the Oracle WebCenter Server

Use these steps to generate the KeyStore.

1. Log onto your WebCenter server.

2. From the `<JDK_Home>/bin` directory, enter the following:

   ```
   ./keytool -genkeypair -v -keyalg RSA -dname "cn=den60208jems,dc=us,dc=oracle,dc=com" -alias webcenter -keypass welcome1 -keystore webcenter.jks -storepass welcome1 -validity 365
   ``

   Generating 1,024 bit RSA key pair and self-signed certificate (SHA1withRSA) with a validity of 365 days
   for: CN=den60208jems, DC=us, DC=oracle, DC=com
   [Storing webcenter.jks]

   ```
   ./keytool -exportcert -v -alias webcenter -keystore webcenter.jks -storepass welcome1 -rfc -file webcenter.cer
   
   Certificate stored in file <webcenter.cer>
   ```

3. Copy the KeyStore files (keystore.jks and keystore.cer) to this location:

   `<MW_HOME>user_projects/domains/<your_domain>/config/fmwconfig`

   **Note:** If you launched the keytool from the JRockit/bin directory, then the KeyStore files will be generated in the same location.

5. Click **Configure** to set up the keystore.

6. Enter the KeyStore file name and password.

7. Enter the Key Alias and Crypt Alias, these value are from your key export process.

8. Enter the passwords for both Signature Key and Encryption Key.

   .;/keytool -exportcert -v -alias webcenter -keystore webcenter.jks -storepass welcome1 -rfc -file webcenter.cer

   In this example, we used webcenter as the key alias and the certificate name is webcenter.cer.

9. Click **OK**.

10. Restart WebCenter Admin and WC_Spaces.

### 4.4.2 Configure KeyStore on EnterpriseOne

Use these steps to configure the KeyStore on EnterpriseOne.
1. Log onto your EnterpriseOne machine.

2. Change the directory to `<MW_HOME>/user_projects/domains/your_domain/config/fmwconfig`.

3. Copy these files from your WebCenter machine:
   - `cwallet.sso`
     This file is different than the OAM configuration; do not copy it from your OAM server.
   - `your keystore.jks`
     For example, `webcenter.jks`
   - `your keystore.cer`
     For example, `webcenter.cer`

4. Open `jps-config.xml` from the same location.

5. Search for `default-keystore.jks`.

6. Replace the KeyStore location with your `<keystore>.jks`.
   You can adjust the description as illustrated here:

   ```xml
   <serviceInstance>
   <property name="keystore.provider" value="keystore.provider" location="webcenter.jks">
   <description>WebCenter KeyStore Service</description>
   <property name="keystore.file.path" value="/"></property>
   <property name="keystore.type" value="JKS"></property>
   <property name="keystore.csf.map" value="oracle.wsm.security"></property>
   <property name="keystore.pass.csf.key" value="keystore-csf-key"></property>
   <property name="keystore.sign.csf.key" value="sign-csf-key"></property>
   <property name="keystore.enc.csf.key" value="enc-csf-key"></property>
   </serviceInstance>
   ``

7. Save the file.

4.5 Installing JD Edwards EnterpriseOne HTML Server

You must install the JD Edwards EnterpriseOne HTML Server.


**Prerequisites**
- For Related Information Application Framework configuration, EnterpriseOne HTML server must be installed within the SOA domain.
- Install and configure the JD Edwards EnterpriseOne Server Manager.
- Install Server Manager Agent on the EnterpriseOne HTML Server.
- Start the EnterpriseOne HTML Server.
4.6 Configuring Oracle HTTP Server for EnterpriseOne HTML Server

After you install and configure the Oracle HTTP Server and Oracle HTTP WebGate, use the following example to configure mod_wl_ohs.conf (located at <MW_Home>/OracleWT1/instance/instance1/config/OHS/ohs1.). Verify that WebLogic port numbers match your configuration.

4.7 Registering the WebGate Agent for EnterpriseOne HTML Server

Prerequisites

- Install Oracle HTTP Server and WebGate.
- Install and configure OID and OAM Server.
- Install and configure EnterpriseOne HTML Server.

Use these steps to register the WebGate Agent.

1. Open an internet browser and connect to the Oracle Access Manager.
2. Open the OAM console.
3. Enter the Admin user and Password.

4. Select the New OAM 11g Webgate option.

5. Enter a WebGate agent name and select the **Open** Security option.

6. Enter the EnterpriseOne HTML URL in Base URL. Use the http port number.

7. Click **Apply**.
8. Host Identifiers and Application Domains are generated.
9. Select Resources, and then click **Create** to create the Resource URL.

10. Enter the following information:
   - **Type** = HTTP
   - **Host Identifier** = Select your Host Identifier
   - **Resource URL** = /jde
- Protection Level = Protected
- Authentication Policy = Protected Resource Policy
- Authorization Policy = Protected Resource Policy

11. Repeat the above step and add the resource URL = /.../*
12. Double-click the Protected Resource Policy to see the newly added resources listed.

13. Click the **Responses** tab, and then click the **Add** button
14. Enter the JDE SSO header field as follows:
   - Response Name = JDE_SSO_UID
   - Type = Header
   - Value = $user.userid

15. Review all registered agents.

16. Select the System Configuration tab.

17. Open the Access Manager Settings section and open the SSO Agents option.

18. Double click OAM Agents, and then click the Search button.

   The system displays a list of registered agents.

19. The registered agent creates a cwallet.sso and ObAccessClient.xml file.

20. Copy these two file to the EnterpriseOne Server:
    
    `<MW_HOME>/user_projects/domain/OAMDomain/output/<Agent_name>` location
    
    `<MW_Home>Oracle_WT1/config/instances/instance1/OHS/ohs1/webgate/config directory.

4.8 Enabling OAM SSO on the EnterpriseOne HTML Server

Use these steps to enable OAM SSO on the JD Edwards EnterpriseOne HTML server through JD Edwards EnterpriseOne Server Manger:

1. Open Server Manager from a browser.
2. Select your instance.
3. Select Network Settings from the Configuration section.

4. Select the Enable Oracle Access Manager option.

5. Enter the Sign-Off URL


   For example:


6. Click **Apply**.

   You are prompted to synchronize the ini changes.

7. Stop and restart the HTML server.

### 4.9 Copying JAR File to the HTML Web Server

Copy the following jar files from the WebCenter server to the HTML Web server:

- spaces-api.jar
- spaces-webservice-client.jar
- webcenter-core-api.jar

The spaces-api.jar and webcenter-core-api.jar files are typically located at

<WebCenter>/lib/java/internal/oracle.webcenter.spaces/11.1.1.0.0.

For example:

C:\oracle\Middleware\Oracle_WC1\lib\java\internal\oracle.webcenter.spaces\11.1.1.0.0
Synchronizing the System Clock on all Servers

The spaces-webservice-client.jar file is typically located at
<WebCenter>\webcenter\modules\oracle.webcenter.framework_11.1.1.

For example:
C:\oracle\Middleware\Oracle_WC1\webcenter\modules\oracle.webcenter.framework_11.1.1

Copy the jar files to the following location on the HTML Web server:
<Middleware>/user_projects/domains/<domain>/servers/<EnterpriseOne HTML server>/stage/<jas instance>/app/webclient.war/WEB-INF/lib

After you copy the files to the HTML Web server, restart the HTML Web server.

4.10 Granting Permission to the Client Application to Request a Token from OpenSSO


2. Search for the oracle.wsm.security.WSIdentityPermission class.

3. Add the following permission section:

```xml
<permission>
  <class>oracle.wsm.security.WSIdentityPermission</class>
  <name>resource={your_JAS_server_name}</name>
  <actions>assert</actions>
</permission>
```

4. Save the file, and then stop and restart your EnterpriseOne Server using Server Manager.

4.11 Synchronizing the System Clock on all Servers

**Important:** After all three of the machines (WebCenter, JD Edwards EnterpriseOne HTML Web Server, and the Oracle Access Manager (SSO Server) are successfully installed and configured, you MUST synchronize the clocks of all three machines. Otherwise you will not able to log in.

See "Synchronizing Clocks" in the *JD Edwards EnterpriseOne Tools System Administration Guide*
4.12 Testing the SSO Configuration

Use these steps to test the SSO configuration.

1. Enter the following in the Address line:
   
   http://<your host:your sso port>/jde/E1Menu.maf

   **Note:** Ensure you provide the HTTP port instead of the actual JAS port. You will not be able to log in with your original JAS port.

2. The Oracle Access Manager 11g login page appears.

3. After the sign-on is working, create a WebCenter connection and enable an application form.

   See “Creating a WebCenter Connection” in the *JD Edwards EnterpriseOne Tools System Administration Guide*

   See “Enabling Application Forms” in the *JD Edwards EnterpriseOne Tools System Administration Guide*

4. After the configuration is done, log onto EnterpriseOne and test the WebCenter Spaces configuration.

   The WebCenter Spaces appear on your configured application.

5. You can click the green **Plus** icon to add new WebCenter Spaces.
Testing the SSO Configuration
Create Database Schemas with Repository Creation Utility

This appendix discusses creating database schemas with Repository Creation Utility (RCU) 11.1.1.5. Prior running this utility, you must have a functioning database such as Oracle database 11g. RCU is a 32-bit application and is available on only Windows x86 and Linux x86 platforms, but you can create schemas on other supported platforms.

The previous version of RCU, such as 11.1.1.2, is not compatible with OFMW 11.1.1.5. You must use 11.1.1.5.

Prerequisites

- You must have a database installed and configured.
  
  If your existing database is not UTF-8 format, you will get a warning message that you can ignore.
  
- You must alter these Oracle database parameters:
  
  - Alter system set processes=500 scope=spfile
  - Alter system set open Cursors=800 scope=spfile
  - Restart database before running RCU

Use these steps to launch the Repository Creation Utility.

1. Download and unzip the ofm_rcu_win_11.1.1.5.0_disk1_1of1.zip file.

2. Run rcu.bat on Windows and rcu on UNIX.

3. Click Next on the Welcome page.
4. Select the **Create** option.

5. Enter the database connection information.
6. The utility performs a prerequisites check.

7. On Select Components, enter the prefix that identifies your environment in the **Create a new Prefix** field.

   - For WebCenter - select the WebCenter Suite
   - For OAM/OID - select Identity management
   - For SOA - select SOA and BPM Infrastructure

**Note:** You can rerun this utility anytime to add more database schemas.
9. The utility performs the prerequisites again.

10. Enter the schema passwords.
11. Enable the Activity Graph and Analytics option.

12. Review the tablespace mapping.

Note: This example shows a different schema prefix than the default, which is DEV.
13. The utility creates any tablespaces that do not already exist.

14. The utility validates and creates the tablespaces.

15. Review the summary.

16. Click Create to start the tablespace creation.
17. Click Close to exit Repository Creation Utility.

18. Verify the schemas creation from Oracle Database console.
This appendix discusses installing WebLogic Server 10.3.5.0. Prior running WebLogic Server installation, you must install a 64-bit JDK and set it to the system path.

**Prerequisites**
- Install a 64-bit JDK based on your platform.
  - Sun JDK 1.6.0_24+
  - Oracle JRockit 1.6.0_24-R28.1.3+
  - IBM JDK 6 (SR9 with FP1+)
- Add the JDK to your system path.

---

**Note:** A plus sign (+) after the fourth digit in the version number indicates that this and its subsequent versions are supported.

---

Use these steps to install WebLogic Server 10.3.5.0

1. Download the wls1035_generic.jar file.
2. Run this command:
   - On Windows and Linux: `>java -jar wls1035_generic.jar`
   - On Solaris with Sun JDK: `>java -d64 -jar wls1035_generic.jar`
3. Click Next on the Welcome page.
4. Click **Create a New Middleware Home** option, and then enter the Home Directory.

5. Enter the contact information for Security Updates.
6. Select **Typical** as the installation type.

7. Verify the JDK location.
8. Confirm the install location.

9. On Windows platform, the system prompts you for a shortcut location.
10. Review the Installation Summary page.

11. Click Run Quickstart to launch the domain configuration wizard.
12. Select Getting started with WebLogic Server 10.3.5.

**Note:** Some Oracle applications (such as WebCenter and OID/OAM) create the domain during installation. If so, you can skip the Quickstart process.

13. Select Create a new WebLogic domain.
14. Select only the WebLogic Server Domain - 10.3.4.0 (Selected as default).

Note: The 10.3.4.0 version shows that you are installing 10.3.5.0 version.
15. Enter a domain name.

16. Enter the Administrator user name and password.

17. Select Production Mode.
18. Select Administration Server and Managed Servers, Clusters and Machine options.

19. Enter the Admin Server name and port. The default port is 7001.
20. On Configured Managed Servers, click **Next**.

21. On Configure Clusters, click **Next**.
22. Click **Add** to configure the machine information.

**Note:** On UNIX platform, select the Unix Machine tab prior to clicking the **Add** button.
23. Enter a logical machine name.

24. Assign the server to your newly created machine name.

25. Review the Configuration Summary page.
26. Click Create.

27. Review the domain information.

Now you can start the Admin Server process.
Launch the Admin Server console:
This appendix discusses installing the Oracle HTTP Server. First you install version 11.1.1.2, and then you upgrade to version 11.1.1.5.

### C.1 Installing HTTP Server 11.1.1.2

1. Download `ofm_webtier_win_11.1.1.2.0_64_disk1_1of1.zip` file.
2. Unzip the file.
3. Double-click `setup.exe`.
   
   This action opens the Oracle Fusion Middleware 11g Web Tier Utilities Installer.
4. Click Next.
5. On Select Installation Type, select the Install and Configure option.
6. Click Next.

7. On Prerequisite Checks, click Next.

9. Click Next. Ignore the error message about WebLogic server needs to be installed in the same directory.

10. On Configure Components, select only the Oracle HTTP Server option.
11. Click Next.
12. On Specify Component Details, complete these fields:
   - Instance Home Location
   - Instance Name
   - OHS Component Name
13. Click Next.

14. On Configure Ports, accept the default option, Auto Port Configuration.
15. Click Next.

16. On Specify Security Updates, provide your contact information.

17. Click Next.

18. On Installation Summary, review the information.
19. Click Install.

20. Click Next after the install is completed.

21. On Configuration Progress, review the information.
22. Click Next.
23. On Installation Complete, click Finish.
C.2 Upgrading Oracle HTTP Server to Version 11.1.1.5

After you successfully install Oracle HTTP Server 11.1.1.2, run Patch to upgrade Oracle HTTP Server to version 11.1.1.5.

1. Open the Windows Services and stop the HTTP process from the previous installation or from the bin directory of the HTTP instance, run the `opmnctl stopall` command.

2. Download `p12395115_webtier_111150_MSWIN-x86-64.zip` file or the one that matches your platform.

3. Unzip the file.

   This action opens the Oracle Fusion Middleware 11g WebTier Patchset Installer

5. Click Next.

6. Select the existing Web Tier Home.
7. Enter the Security Updates information.

8. Review the Installation Summary.
9. Click Install.

10. Click Next when the install completed.
11. Click **Finish** to exit the installer.

12. Restart the process from Windows Services or use the `opmnctl startall` command.