Oracle® Fusion Middleware

Tutorial for Oracle Identity Management

11*g* Release 1 (11.1.1)

E10276-01

May 2009

Oracle Fusion Middleware Tutorial for Oracle Identity Management, 11*g* Release 1 (11.1.1)

E10276-01

Primary Authors: Ellen Desmond, Vinaye Misra

Contributing Author: Stephen Lee

Contributors: Sophia Maler, Olaf Stullich, Mark Wilcox

Contents

6 Setting up Oracle Directory Integration Platform Synchronization and Attribute Mapping

7 Configuring Wallets and Data Stores for Oracle Identity Federation

8 Configuring Oracle Identity Federation for Single Sign-On to Trusted Provider

A Accessing Administrative Interfaces

Index

Preface

This book contains the tutorial exercises for *Oracle Fusion Middleware Getting Started with Oracle Identity Management*.

Identity Management components are integral to the correct functioning of an enterprise. Inappropriate modifications can render essential services inaccessible and might violate company protocol. For this reason, we recommend that you do not actually perform these exercises unless you have an isolated test system.

Audience

Oracle Fusion Middleware Tutorial for Oracle Identity Management is intended for anyone who performs administration tasks for Oracle Identity Management components.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at `http://www.oracle.com/accessibility/`.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process. Information about TRS is available at `http://www.fcc.gov/cgb/consumerfacts/trs.html`, and a list of phone numbers is available at `http://www.fcc.gov/cgb/dro/trsphonebk.html`.

Related Documents

For more information, see the following documents in the Oracle Fusion Middleware 11*g* Release 1 (11.1.1) documentation set:

- *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*
- *Oracle Fusion Middleware Integration Guide for Oracle Identity Management*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*
- *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*
- *Oracle Fusion Middleware High Availability Guide*
- *Oracle Fusion Middleware Security Guide*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Adding Users and Groups to Oracle Internet Directory

In this exercise, you use Oracle Directory Services Manager to add a user and a group to Oracle Internet Directory.

Before you Begin

You need access to an instance of Oracle Directory Services Manager and to an Oracle Internet Directory instance.

Perform this exercise before performing the Oracle Virtual Directory exercise. The Oracle Virtual Directory exercise requires access to an instance of Oracle Internet Directory that has at least one entry.

Adding User Entries

In this example, we create a user and assign a password.

1. Access Oracle Directory Services Manager, as described in "Accessing Oracle Directory Services Manager" on page A-1.
2. From the task selection bar, select **Data Browser**.
3. On the toolbar, click the **Create a new entry** icon. The Entry Properties page of the Create New Entry wizard appears.
4. Click the **Add** icon next to Object Class. The Add Object Class dialog box appears.
5. In the Add Object Class dialog box, search for, then select, the `inetOrgPerson` object class.
6. Click **OK**. This returns you to the Create New Entry wizard.
7. In the **Parent of the entry** field, type the full DN of the parent entry, for example `cn=users,dc=us,dc=oracle,dc=com`. You can also click the **Browse** button to locate the DN of the parent for this entry.
8. Click **Next**. The **Mandatory Properties** dialog appears.
9. Enter **Anne Smith** in the cn text box and **Smith** in the sn text box.
10. Select **cn** in the Relative Distinguished Name list as the property to use as the RDN.
11. Click **Next**. The entry is created.
12. Click **Finish**.

13. Select the Anne Smith entry in the data tree. (You can search for it to save time.)
14. Click the **Attributes** tab.
15. Click the icon under **Optional Attributes** to manage which optional attributes are shown. In the All Attributes list, select **userPassword**, then click `Move` to move it into the Shown Attributes list. Click **Add Attributes**. A userPassword text box now appears under Optional Attributes in the Anne Smith entry.
16. Enter a password in the **Password** text box.
17. Click **Apply**.

Create another user, as follows:

1. Select the Anne Smith entry in the data tree. (You can search for it to save time.)
2. On the toolbar above the entry click the **Create a new entry line this one** icon. The Entry Properties page of the Create New Entry: Create Like wizard appears.
3. Use the same object classes and parent that you used for Anne Smith.

   Click **Next**. The **Mandatory Properties** dialog appears.
4. Enter a user name in the **cn** text box and the user's surname in the **sn** text box.
5. Select **cn** in the Relative Distinguished Name list as the property to use as the RDN.
6. Click **Next**. The entry is created.
7. Click **Finish**.
8. Select the new user's entry in the data tree.
9. Follow steps 14-17 in the previous list of steps to assign a password for the new user.

Creating A Static Group and Adding Members

In this example, we create a group and add the user Anne Smith to the group.

To add a static group entry:

1. From the task selection bar, select **Data Browser**.
2. On the toolbar, click the **Create a new entry** icon. The Entry Properties page of the Create New Entry wizard appears.
3. Click the **Add** icon next to Object Class. The Add Object Class dialog box appears.
4. In the Add Object Class dialog box, search for, then select, the `groupOfNames` object class.
5. Click **OK**. This returns you to the Create New Entry wizard.
6. In the **Parent of the entry** field, type the full DN of the parent entry, for example `cn=groups,dc=us,dc=oracle,dc=com`. You can also click the **Browse** button to locate the DN of the parent for this entry.
7. Enter **NewGroup** in the cn text box.
8. Select **cn** in the Relative Distinguished Name list as the property to use as the RDN.
9. Click **Next**. The entry is created.
10. Click **Finish**.

11. Select the NewGroup entry in the data tree. (You can search for it to save time.)
12. Click the **Group** tab.
13. Click the **Add** icon next to **Members**.
14. Select the DN of Anne Smith.
15. Click **OK**.
16. Click **Apply**.

2

Modifying the Oracle Internet Directory Schema

In this exercise, you use Oracle Directory Services Manager to create a new object class, conferenceRoom, which extends the object class room.

Before you Begin

You need the following information in order to perform this exercise:

- The host and port for ODSM. If you are invoking ODSM from Fusion Middleware Control, this information will be filled in for you.
- Whether the ODSM port is using SSL.
- The ODSM user and password.
- An Object ID that is not already in use.

Adding an Object Classes by Using Oracle Directory Services Manager

To add an object class:

1. Access Oracle Directory Services Manager as described in "Accessing Oracle Directory Services Manager" on page A-1.
2. Go to the **Schema** page.
3. Expand the Object Classes panel on the left.
4. Enter room in the Search field and click **Go**. The search returns at least one object class, called **room**.
5. Select **room** in the Object Classes panel. Information about the object class appears in the right panel
6. Click the **Create an object class like the selected one** icon. The New Object Class dialog box displays the attributes of the room object class.
7. Enter the name conferenceRoom and an available Object ID. Leave Type set to Structural.
8. In the Superclass section of the page, click the **Add Super Object Class** icon. The Add Super Object Class dialog appears. Enter **room** into the search field and click **Go**. When the search returns, click **room** in the search result and click **OK**.
9. In the Optional Attributes section of the page, click the **Add optional attributes to list** icon. The Optional Attribute Selector dialog appears. Enter buildingName

into the search field and click **Go**. Select **buildingName** in the search result and click **OK**.

3

Setting up Oracle Internet Directory Replication

In this exercise, you use Fusion Middleware Control to set up LDAP-based multimaster replication between two Oracle Internet Directory nodes.

Before you Begin

To complete this exercise, you need the following prerequisites:

- Two Oracle Internet Directory instances in separate domains. Each instance must be registered with a WebLogic domain and have anonymous binds enabled.
- The host, port, and replication DN password for each of the nodes. (If you provide the correct host, port, and password, the replication wizard fills in the replication DN.)

Setting Up an LDAP-Based Multimaster Replication Agreement

You configure a one-way, two-way, or multimaster LDAP replica by using the Replication Wizard in Oracle Enterprise Manager Fusion Middleware Control. In this exercise, we will configure a multimaster agreement between two nodes.

Proceed as follows.

1. Access Oracle Enterprise Manager Fusion Middleware Control as described in "Accessing Fusion Middleware Control" on page A-1.
2. From the Oracle Enterprise Manager Fusion Middleware Control domain home page, under Fusion Middleware, under Identity and Access, select the Oracle Internet Directory component you want to use as the first node in the multimaster agreement. The home page for that instance of Oracle Internet Directory appears.
3. From the Oracle Internet Directory menu, select **Administration**, then **Manage Replication**. This takes you to the Replication Agreements page. If this Oracle Internet Directory instance is not yet configured to be part of any replication agreement, the list is blank.
4. Log in, by providing the host, port, and replication DN password. The replication DN fills in.
5. Click the **Create** icon to invoke the Replication Wizard.
6. On the Type page, select the replication type: **Multimaster Replication**.
7. Click **Next**. The **Replicas** screen displays the replication type you selected.
8. Provide the agreement name Testreplica. This must be unique across all the nodes.

9. Primary node will be filled in with information about the current (primary) host. You must enter the information about the secondary host. Enter the host, port, and replication password for the for the secondary node. The Username (replication DN), will fill in automatically.
10. Click **Next** to go the Settings page.
11. In the LDAP Connection field, select **Keep Alive**. This specifies that the replication server use same connection for performing multiple LDAP operations.
12. Use the default **Replication Frequency**.
13. Use the default **Human Intervention Queue Schedule**. This is the interval, in minutes, at which the directory replication server repeats the change application process.
14. The settings page also contains a section called Replication Server Start Details. Leave these disabled.
15. Click **Next** to go to the Scope page.
16. Leave the default naming context.
17. Click **Next**. The Summary page displays a summary of the replication agreement you are about to create.
18. Click **Finish** to create the replication agreement.

4

Setting up Auditing of Oracle Internet Directory

In this exercise, you use Fusion Middleware Control to manage auditing.

Before you Begin

You must have access to the administrative user account for the domain.

Managing Auditing by Using Fusion Middleware Control

You use Oracle Enterprise Manager Fusion Middleware Control to manage auditing.

1. Connect to Fusion Middleware Control as described in "Accessing Fusion Middleware Control" on page A-1.
2. Log in as the WebLogic administrator.
3. From the domain home page, under Fusion Middleware, expand Identity and Access, if necessary. Instances of Oracle Internet Directory are listed.
4. Select the Oracle Internet Directory component to manage.
5. From the Oracle Internet Directory menu, select **Security**, then **Audit Policy**.
6. From the Audit Level list, select **Custom** to configure your own filters.
7. Under User Sessions, User Logins, enable **Failure**.
8. Click the **Edit Filter** icon next to the **Failure** item you enabled. The Edit Filter dialog for the filter appears.
9. From the **Condition** list, select **Initiator**.

   From the list to the right, select **-eq**.

   In the text box to the right, enter the name of the administrative user that you used when logging in, for example, **weblogic**.
10. Click the **Add** icon.
11. Click **OK**.
12. Click **Apply** to save the changes.
13. To obtain a report of your current settings, click **Export**. Save the report to a file.
14. Open the file in a text editor, such as Wordpad and view the audit configuration you just created.

5

Creating Oracle Virtual Directory Adapters

In this exercise, you use Oracle Directory Services Manager to create a local store and add an entry to it. Then you create an adapter for an LDAP directory and an adapter for a database.

Before you Begin

The prerequisites for setting up Oracle Virtual Directory adapters are as follows:

- An instance of Oracle Directory Services Manager. You need to know the URL.
- An instance of Oracle Virtual Directory
- An instance of Oracle Internet Directory with some user entries. You can use the instance from the Oracle Internet Directory tutorial.
- An Oracle Database. For this exercise, you can use the Oracle Database associated with Oracle Internet Directory, although you would not do that on a production system. When an Oracle Database is installed, it already has the HR example scema that we will use in this exercise.
- For the Oracle Virtual Directory, Oracle Internet Directory, and Oracle Database, you will need to supply the following information:
  - Hostname
  - Port
  - Administrator’s name
  - Password

Creating a Local Store Adapter

Create Local Store Adapter dc=oracle,dc=com, as follows:

1. Access Oracle Directory Services Manager, as described in "Accessing Oracle Directory Services Manager" on page A-1.
2. Click the **Adapter** tab. On the Adapter page:
   a. Click the **Create Adapter** icon and choose Local Store Adapter.
   b. Enter the Adapter name **LSA**.
   c. Leave Template set to Default.
   d. Click **Next**.
3. On the Settings page:

   a. Enter the Adapter Suffix / Namespace dc=oracle,dc=com.
   b. Enter data / localDB for Database File.
   c. Use the default values for the rest of the fields on the Settings page.
   d. Click **Next**.

4. Review the summary page and click **Finish** if everything looks correct.

> **Note:** If, for some reason, you decide to delete the adapter and create a new one, use a different Adapter name and a different Database File name.

Adding Entries

Create an entry in the local store as follows:

1. Using a text editor, create an LDIF file that looks like this:

```
version: 1

dn: dc=oracle,dc=com
objectclass: top
objectclass: domain
dc: oracle
```

2. Access Oracle Directory Services Manager, as described in "Accessing Oracle Directory Services Manager" on page A-1.
3. Click the **Data Browser** tab.
4. Highlight dc=oracle,dc=com under Client View.
5. Click the **Import LDIF** icon.
6. Browse to the LDIF file you created and click Open.

Creating an LDAP Adapter

Create LDAP adapter as a branch cn=Users,dc=mydomain,dc=com).

1. Access Oracle Directory Services Manager, as described in "Accessing Oracle Directory Services Manager" on page A-1.
2. Click the Adapter tab. On the Adapter page:
   a. Click **Create Adapter** icon and choose **LDAP**
   b. Since we will be connecting to an OID server, leave the adapter template at Default.
   c. Enter LDAP as name
   d. Click Next.
3. On the Connection Page:
   a. Click the **Add Host** icon.
   b. Leave Use DNS for Auto Discovery set to No.
   c. Enter **hostname** and **port** values for your LDAP server.

   d. For server proxy Bind DN and proxy password enter the admin DN (typically cn=orcladmin) and password for your LDAP server.
   e. Use the default values for the rest of the fields on the page.
   f. Click **Next**.
4. You should see `Success!! Oracle Virtual Directory connected to all hosts`. on the Connection Test page. Click **Next**.
5. On the Name Space page:
   a. SetPassThrough Credentials to **Always**.
   b. Set the remote base to where you wish to connect in the remote directory tree. Browse to the Users container, cn=Users,dc=mydomain,dc=com
   c. Set the Mapped Namespace to ou=LDAP,dc=oracle,dc=com
   d. Use the default values for the rest of the fields on the page.
   e. Click **Next**.
6. Review the Summary page. Click **Finish**.
7. Click the Data Browser tab. On the Data Browser page;
   a. Click the **Refresh** icon
   b. Expand the containers under Adapter Browser to view the entries.
   c. Expand ou=LDAP,dc=oracle,dc=com under Client View to view the entries as they appear to a client.
8. Click the **Adapter** tab.
9. Highlight the LDAP adapter and click the **Routing** tab. On the Routing tab:
   a. Under General Settings, select No for Visibility so that this adapter will look like a normal branch to an LDAP client.
   b. Click Apply.
10. Go to the **Data Browser** tab, refresh and verify that the data tree from the LDAP adapter is visible.
11. Expand the containers under Client View to see if they have changed.

Creating an Oracle Database Adapter

Create a database adapter that maps the Oracle DB sample HR schema as a branch, as follows:

1. Access Oracle Directory Services Manager, as described in "Accessing Oracle Directory Services Manager" on page A-1.
2. Click the **Adapter** tab. On the Adapters page:
   1. Click the **Create Adapter** icon. The Adapter navigation tree appears.
   2. Select **Database** from the Adapter Type list.
   3. Enter DB as adapter name
   4. Leave the Adapter Template set to Default.
   5. Click **Next**. The Connection screen appears.
3. On the Connection screen:

   a. For Adapter Suffix / Namespace, enter ou=db,dc=oracle,dc=com.
   b. For URL type, select Use Predefined Database.
   c. For Database type, select the proper driver type for your database, such as Oracle Thin Drivers. JDBC Driver Class and Database URL will fill in automatically.
   d. For Host, enter the hostname / IP address of your database (sta00730)
   e. For Port, enter the port of your database (5521)
   f. For Database name, enter dapmain.
   g. For Database user, enter HR.
   h. For Database password, enter the password. (welcome1)
   i. Click **Next** which takes you to the Mapped Database Tables page.

4. On the Mapped Database Tables Page:
   a. Click **Browse**.
   b. Scroll down to HR, expand the container, and click EMPLOYEES.
   c. Click **OK**. The Map Database Tables page will now show HR.EMPLOYEES.
   d. Click **Next** to go to the Map Object Classes page.
5. On the Map Object Classes page:
   a. Click the **Create a New Object Class** icon.
   b. Enter Object Class inetorgperson.
   c. Enter RDN Attribute UID.
   d. Click **OK**.
6. Highlight the object class you just created and click the **Add Mapping Attribute** icon.
7. On the Add Mapping Attribute page:
   a. Enter the LDAP attribute uid and the Database Table:Field HR.EMPLOYEES:EMAIL
   b. Leave Datatype blank.
   c. Click **OK**.
   d. Map the LDAP iterate givenname to HR.EMPLOYEES:FIRST_NAME.
   e. Click **Next**.
8. Click **Finish**. The new DB adapter appears on the Adapter page.
9. On the Adapter page, select the new Database adapter and click the **Routing** tab.
10. On the Routing page:
    a. Under General Settings, select No for Visibility so that this adapter will look like a normal branch to an LDAP client.
    b. Select DB adapter criticality False so that if DB is not available OVD still responds
    c. Click **Apply**.

Verify Adapters

You should see three adapters listed on the left side of the Adapter page, one for Local store, one for LDAP and one for Database adapter.

Click on each adapter to make sure that it displays the correct namespace and configuration information you set in the adapter configuration setup.

Go to the Data Browser, click the refresh icon, and observer the Client View and Adapter Browser.

6

Setting up Oracle Directory Integration Platform Synchronization and Attribute Mapping

In this tutorial, you use Fusion Middleware Control to set up an Active Directory synchronization profile and add a customized attribute mapping. Then you enable and test synchronization.

Before you Begin

The prerequisites for setting up Oracle Directory Integration Platform synchronization with Active Directory are as follows:

- An Oracle Enterprise Manager Fusion Middleware Control environment with an Oracle Directory Integration Platform component instance.
- A container in the Oracle Internet Directory instance associated with the Oracle Directory Integration Platform instance, for example: `cn=adusers,cn=users,dc=example,dc=com`.
- An Active Directory server. You will need to supply the following information about the server:
  - Hostname
  - Port
  - Administrator's name
  - Password
  - Host container, usually`cn=users, dc=`*`domain`*. For example: `cn=users,dc=example,dc=com`.

Set up Synchronization

Perform the following steps to create a profile using Oracle Enterprise Manager Fusion Middleware Control:

1. Access Oracle Directory Services Manager, as described in "Accessing Oracle Directory Services Manager" on page A-1.
2. Log in to the domain that is running the Oracle Directory Integration Platform instance you want to manage.
3. Locate and select the Oracle Directory Integration Platform instance that you want to manage, for example, DIP1.

4. Click the **DIP Server** menu, point to **Administration**, and then click **Synchronization Profiles**. The Manage Synchronization Profiles page appears.
5. Click **Create**. The Create Synchronization Profile page appears with tabs for the various types of profile settings.
6. Click the **General** tab to configure the general settings for the profile.
   a. Choose a Profile Name
   b. Select Destination for DIP-OID.
   c. Select Active Directory for Type.
   d. Enter the host and port of the Active Directory server.
   e. Do not enable SSL.
   f. For User Name and Password, enter the administrator name and password on the Active Directory server.
7. Click **Test Connection**. It should return `Test Passed. Authentication Successful.`
8. Click the **Mapping** tab to configure Domain and Attribute Mapping Rules.
   a. Click **Create** in the Domain Mapping Rules section to create mapping rules for the domain or container from which objects are synchronized into Oracle Internet Directory. The Add Domain Mapping Rule dialog box appears.

      You can use the Lookup button or enter the values directly.
   b. For Source Container enter the source container in AD, for example: `cn=users,dc=example,dc=com`.
   c. For DIP-OID Container enter the DIP-OID container on the Oracle Internet Directory instance, for example: `cn=adusers,cn=users,dc=example,dc=com`.
   d. Leave the Mapping Rule box empty
   e. Click OK
   f. Keep the default set for the Attribute Mapping Rules section.
   g. Click **OK**.
   h. Use the **Validate All Mapping Rules** button to test your mapping rules after you create them. You can ignore warnings, but not errors.
9. Click the **Filtering** tab to configure the filter settings for the profile. Do not make any changes.
10. Click the **Advanced** tab to configure the advanced settings for the profile. Set the following values
    a. Scheduling Interval MM:SS: 1 Minute
    b. Maximum Number of Retries: 1
    c. Log Level: Error
11. Click **OK** to return to the Manage Synchronization Profile page and create the profile. The profile appears, along with a confirmation that the profile was saved successfully.

Customize Attribute Mappings

In this exercise, you will add an attribute mapping rule to the synchronization profile you created in Set up Synchronization.

1. Access Oracle Enterprise Manager Fusion Middleware Control as described in "Accessing Fusion Middleware Control" on page A-1.
2. Click the **DIP Server** menu, point to **Administration**, and then click **Synchronization Profiles**. The Manage Synchronization Profiles appears.
3. Click the Profile that you created in Set up Synchronization.
4. Click the Edit icon
5. Verify that Profile Name is correct.
6. Click the Mapping tab
7. In the Attribute Mapping Rules section select the Create icon
8. In the Mapping Rule window:
   a. From the Source ObjectClass drop down list select: user
   b. Select Source Attribute: Single Attribute
   c. From the Source Attribute drop down list select: telephonenumber
   d. From the DIP-OID ObjectClass drop down list select: inetorgperson
   e. From the DIP-OID Attribute drop down list select: inetorgperson
   f. From the DIP-OID Attribute type drop down list select: telephonenumber
   g. Click OK
9. Use the **Validate All Mapping Rules** button to test your mapping rules after you create them.

Enable and Test Synchronization

1. On the Manage Synchronization Profile page, click **Enable**. A confirmation that the profile was enabled appears.
2. Add an entry to Active Directory and wait a few minutes.
3. Using Oracle Directory Services Manager, verify that the entry now exists in Oracle Internet Directory.

7

Configuring Wallets and Data Stores for Oracle Identity Federation

In this series of exercises, you use Fusion Middleware Control to manage Oracle Identity Federation. The exercises include:

- Configuring a Wallet for Signing Certificates
- Configuring Data Stores
- Integrating Oracle Identity Federation with Oracle Access Manager

Configuring a Wallet for Signing Certificates

Create a wallet for the Oracle Identity Federation server's signing certificates.

1. Access Oracle Enterprise Manager Fusion Middleware Control as described in "Accessing Fusion Middleware Control" on page A-1.
2. Select the Oracle Identity Federation instance in the navigation pane on the left.
3. Navigate to Oracle Identity Federation, then **Administration**, then **Security and Trust**.
4. Click the **Update** button corresponding to Wallet Properties - Signatures.
5. For JCE Keystore Type, select the PKCS#12 radio button.
6. For Wallet Location, click **Browse**. Locate the operating system file for the wallet, and click **Open** in the file dialog.
7. For Password, enter the password that is used to encrypt the private key.
8. For Signing Key Alias, enter the alias under which the private key is stored in the wallet.
9. Click **OK**.

Configuring Data Stores

In this section you will learn how to configure Oracle Identity Federation to use Oracle Database and Oracle Internet Directory as data stores.

Configure a database as the user data store:

1. Create a JDBC Data Source
   a. Log in to the WebLogic Administration Console, as described in "Accessing the Oracle WebLogic Server Administration Console" on page A-2.

   b. Navigate to Services, then JDBC, then Data Sources.
   c. Click **New**.
   d. Choose a name and a JNDI name for the new data source, and enter the database information. Choose the WebLogic managed server where Oracle Identity Federation is deployed as the target of this data source.

2. Configure an RDBMS user data store
   a. Log in to Fusion Middleware Control and navigate to the Oracle Identity Federation instance.
   b. Navigate to **Administration**, then **Data Stores**.
   c. In the User Data Store section, click **Edit**.
   d. Select **Database** from the **Repository Type** dropdown list.
   e. Enter the following properties:

      - For JNDI Name, enter the JNDI of the data source created in the WebLogic Administration Console.

      - For Login Table, enter the name of the user table.

      - For User ID Attribute, enter the name of the User ID column in the user table.

      - For User Description Attribute, enter the name of the User Description column in the user table.
   f. Click **OK**.

Configure Oracle Internet Directory as the LDAP user data store:

1. Log in to Fusion Middleware Control and navigate to the Oracle Identity Federation instance.
2. Navigate to **Administration**, then **Data Stores**.
3. In the **User Data Store** section, click **Edit**.
4. Select **LDAP Directory** from the **Repository Type** dropdown list.
5. Provide the following details:
   - For Connection URL, enter the LDAP URL to connect to the server. For example, `ldap://ldap.oif.com:389`.
   - For Bind DN, enter the administrator account DN to use to connect to the LDAP server. For example, `cn=orcladmin`.
   - For Password, enter the administrator password to connect to the LDAP server.
   - For UserID attribute, enter `uid`.
   - For User Description attribute, enter `uid`.
   - For Person Object Class, enter `inetOrgPerson`.
   - For Base DN, enter the directory to which the search for users should be confined.
   - For Maximum Connections, enter the maximum number of LDAP connections that Oracle Identity Federation will simultaneously open to the LDAP server.
   - For Connection Wait Timeout, enter the timeout, in minutes, to use when Oracle Identity Federation opens a connection to the LDAP server.

6. Click **OK**.

Integrating Oracle Identity Federation with Oracle Access Manager

This integration enables Oracle Identity Federation to interact with Oracle Access Manager to create an authenticated user session. You can:

- Configure Oracle Access Manager as an Authentication Engine
- Configure Oracle Access Manager as an SP Integration Module

For details, see Deploying Oracle Identity Federation with Oracle Access Manager in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

8

Configuring Oracle Identity Federation for Single Sign-On to Trusted Provider

In this series of exercises, you use Fusion Middleware Control to create a trusted provider in Oracle Identity Federation. The exercises include:

- Exporting Service Provider Metadata
- Creating a Trusted Provider
- Executing Single Sign-On to a Provider

Exporting Service Provider Metadata

In this exercise, the service provider administrator exports SAML 2.0 metadata to a file:

1. Access Oracle Enterprise Manager Fusion Middleware Control as described in "Accessing Fusion Middleware Control" on page A-1.
2. Select the Oracle Identity Federation instance in the navigation pane on the left.
3. Navigate to Oracle Identity Federation, then **Administration**, then **Security and Trust**.
4. Click the Provider Metadata tab.
5. Under Metadata Settings:
   - check the Require Signed Metadata box
   - check the Sign Metadata box
6. Click **Apply**.
7. In the Generate Metadata area of the page:
   - in the Provider Type drop-down, select Service Provider
   - in the Protocol drop-down, select SAML 2.0
8. Click **Apply**.
9. Click **Generate**.
10. In the file dialog box, click **Save**.
11. Click Open to view the generated XML file.
12. Note the service provider URL in the entity ID and Location tags in the file.

Creating a Trusted Provider

In this exercise, an administrator adds a new service provider to the Oracle Identity Federation server's trusted providers.

1. Access Oracle Enterprise Manager Fusion Middleware Control as described in "Accessing Fusion Middleware Control" on page A-1.
2. Select the Oracle Identity Federation instance in the navigation pane on the left.
3. Review key statistics for the server on the home page, including:
   - SOAP Requests
   - SOAP Responses
4. Navigate to Oracle Identity Federation, then **Administration**, then **Federations**.
5. Click **Add**.
6. In the Add Trusted Provider dialog:
   - check Enable Provider
   - select Load Metadata
7. Click the **Browse** button next to the Metadata Location field.
8. In the browse dialog box, navigate to the folder that contains the service provider metadata.

   Service provider metadata was generated on page 8-1.
9. Select the XML file containing the metadata. Click **Open**.
10. In the Add Trusted Provider dialog, the Metadata Location field now fills in the path of the metadata file you selected.
11. Click **OK**. The Federations page appears.
12. Note that the newly added provider is listed in the Trusted Provider table, with the correct protocol version.

Executing Single Sign-On to a Provider

This exercise demonstrates a user performing an SP-initiated single sign-on operation using HTTP Redirect / Artifact processing.

Before You Begin

This exercise assumes that:

- the IdP and SP have exchanged metadata as demonstrated in a previous exercise.
- the IdP administrator has added the SP to its trusted providers as demonstrated in a previous exercise.

The steps to perform the exercise are as follows:

1. Open a browser window.
2. Initiate an SSO flow using a URL of the form:

   ```
   HTTP://OIF-SP-HOST:OIF-SP-PORT/fed/user/testspsso
   ```
3. The Federation SSO / authentication page appears.
4. Provide this information on the page:

- From the IdP Provider ID drop-down, select the IdP URL.
- Under Authentication Request Binding, select HTTP Redirect.
- Check Allow Federation Creation.
- From the SSO Response Binding drop-down, select Artifact.

5. Click **Start SSO**. A request is sent to the service provider to start single sign-on.
6. A login page appears. Enter your username and password.
7. Click **Sign In**.
8. The SSO operation completes and a results page is displayed.
9. Note the information displayed on the page, including the User ID, the IdP Provider ID, session start and end dates, and so on.

A

Accessing Administrative Interfaces

This appendix explains how to access Oracle Enterprise Manager Fusion Middleware Control, Oracle Directory Services Manager, and the Oracle WebLogic Server Administration Console.

This appendix contains the following sections:

- Accessing Fusion Middleware Control
- Accessing Oracle Directory Services Manager
- Accessing the Oracle WebLogic Server Administration Console

Accessing Fusion Middleware Control

1. Connect to Fusion Middleware Control.

   The URL is of the form:

   ```
   https://host:port/em
   ```

2. Log in using the administrator's name and password.
3. From the domain home page, under Fusion Middleware, expand Identity and Access, if necessary. Instances of Oracle Internet Directory, Oracle Virtual Directory, Oracle Directory Integration Platform, and Oracle Identity Federation are listed.

Accessing Oracle Directory Services Manager

1. Invoke Oracle Directory Services Manager in one of the following ways:

   - To invoke Oracle Directory Services Manager from Fusion Middleware Control, select an Oracle Internet Directory or an Oracle Virtual Directory component, select **Directory Services Manager** from the Oracle Internet Directory or Oracle Virtual Directory menu in the Oracle Internet Directory target, then select the specific screen in Oracle Directory Services Manager. Oracle Directory Services Manager displays the connection dialog for the same Oracle Internet Directory or Oracle Virtual Directory instance.
   - To invoke Oracle Directory Services Manager directly:

     Enter the following URL into your browser's address field:

     ```
     http://host:port/odsm
     ```

     In the URL to access Oracle Directory Services Manager, *host* is the name of the managed server where Oracle Directory Services Manager is running. *port* is the managed server port number from the WebLogic server. You can determine the exact port number by examining the $*Fusion_Middleware_Home* / *Oracle_Identity_Management_domain* / servers / wls_ods / data / nodemanager / wls_ods1.url file, where *Fusion_Middleware_Home* represents the root directory where Fusion Middleware is installed.

When the Oracle Directory Services Manager home page appears, click the small arrow to the right of the label **Click to connect to a directory**.

2. Connect to an Oracle Internet Directory or Oracle Virtual Directory instance with Oracle Directory Services Manager.

   If you have previously logged into the directory, click the entry for that directory and supply the user and password.

   If you have not previously logged in to the directory, click **Create a New Connection** or type Ctrl+N. The New Connection Dialog appears.

   a. Optionally, enter an alias name to identify this entry on the Disconnected Connections list.

   b. Enter the server and non-SSL port for the Oracle Internet Directory or Oracle Virtual Directory instance you want to manage.

   c. Select or deselect **SSL Enabled**, based on whether your Oracle Internet Directory instance is using SSL.

   d. Enter the user (usually `cn=orcladmin`) and password.

   e. Select the Start Page you want to go to after logging in.

   f. Click **Connect**.

   g. If using an SSL port, you might be presented with a certificate from the server. After manually verifying the authenticity of the server certificate, accept the certificate.

Accessing the Oracle WebLogic Server Administration Console

1. Enter the following URL in a browser:

   ```
   http://hostname:port_number
   ```

   The port number is the number of the Administration Server. By default, the port number is 7001.

   The login page is displayed

2. Log in using the user name and password supplied during installation or another administrative user that you created.

   Oracle WebLogic Server Administration Console is displayed.

Alternatively, you can access the Administration Console from Fusion Middleware Control, from the home pages of targets such as the Administration Server or Managed Servers.

Index