# Oracle® Fusion Middleware

Installation Guide for Oracle Identity and Access Management

11*g* Release 1 (11.1.1.7.0)

**E36891-01**

March 2013

ORACLE®

Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management, 11*g* Release 1 (11.1.1.7.0)

E36891-01



Primary Author: Nisha Singh

Contributors: Don Biasotti, Niranjan Ananthapadmanabha, Heeru Janweja, Deepak Ramakrishnan, Madhu Martin, Sergio Mendiola, Svetlana Kolomeyskaya, Sid Choudhury, Javed Beg, Eswar Vandanapu, Harsh Maheshwari, Sidhartha Das, Mark Karlstrand, Daniel Shih, Don Bosco Durai, Kamal Singh, Rey Ong, Gail Flanegin, Ellen Desmond, Priscilla Lee, Vinaye Misra, Toby Close, Ashish Kolli, Ashok Maram, Peter LaQuerre, Srinivasa Vedam, Vinay Shukla, Sanjeev Topiwala, Shaun Lin, Prakash Hulikere, Debapriya Dutta, Sujatha Ramesh, Ajay Keni, Ken Vincent

# Contents

## Part II Installing and Configuring Oracle Identity and Access Management (11.1.1.7.0)

## 3 Installing and Configuring Oracle Identity and Access Management (11.1.1.7.0)



## 4 Configuring Oracle Identity Navigator



## 5 Configuring Oracle Identity Manager

## 6 Configuring Oracle Access Manager



## 7 Configuring Oracle Adaptive Access Manager



## 8 Installing and Configuring Oracle Entitlements Server

## H OAAM Partition Schema Reference



## I Software Deinstallation Screens

# Preface

This Preface provides supporting information for the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management* and includes the following topics:



## Audience

The *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management* is intended for administrators that are responsible for installing Oracle Identity and Access Management components.

This document assumes you have experience installing enterprise components. Basic knowledge about the Oracle Identity and Access Management components and Oracle Application Server is recommended.

This document does not cover the information for installing Oracle Identity Management components. For information on installing Oracle Identity Management components, refer to *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

## 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

This section identifies additional documents related to Oracle Identity Management. You can access Oracle documentation online from the Oracle Technology Network (OTN) Web site at the following URL:

`http://docs.oracle.com/`

Refer to the following documents for additional information on each subject:

### Oracle Fusion Middleware

- *Oracle Fusion Middleware Administrator's Guide*
- *Oracle Fusion Middleware Security Guide*

### High Availability

*Oracle Fusion Middleware High Availability Guide*

### Oracle Fusion Middleware Repository Creation Utility

*Oracle Fusion Middleware Repository Creation Utility User's Guide*

### Oracle Identity Manager

*Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*

### Oracle Access Manager

*Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager*

### Oracle Adaptive Access Manager

*Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*

### Oracle Identity Navigator

*Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*

### Oracle Entitlements Server

*Oracle Fusion Middleware Administrator's Guide for Oracle Entitlements Server*

# 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. |

# Part I

## Introduction and Preparation

Part I introduces Oracle Identity and Access Management 11*g* Release 1 (11.1.1.7.0) installation and describes how to perform preparatory tasks. It contains the following chapters:

- Chapter 1, "Introduction"
- Chapter 2, "Preparing to Install"

# 1 Introduction

This chapter provides an overview of Oracle Identity and Access Management 11*g* Release 1 (11.1.1.7.0). This chapter includes the following topics:

- Overview of Oracle Identity and Access Management 11g Release 1 (11.1.1.7.0)
- Additional 11g Release 1 (11.1.1.7.0) Deployment Information
- Silent Installation
- Understanding the State of Oracle Identity and Access Management Components After Installation
- Using This Guide

## 1.1 Overview of Oracle Identity and Access Management 11*g* Release 1 (11.1.1.7.0)

Oracle Identity and Access Management 11*g* Release 1 (11.1.1.7.0) includes the following components:

- Oracle Identity Manager
- Oracle Access Manager
- Oracle Adaptive Access Manager
- Oracle Identity Navigator
- Oracle Entitlements Server

> **Note:** This document does not cover the information for installing Oracle Identity Management components. For information on installing Oracle Identity Management components, refer to *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

## 1.2 Additional 11*g* Release 1 (11.1.1.7.0) Deployment Information

This topic describes additional sources for 11*g* Release 1 (11.1.1.7.0) deployment information, including documentation on the following subjects:

- Upgrading to Oracle Identity and Access Management 11g Release 1 (11.1.1.7.0)
- Installing Oracle Identity and Access Management 11g Release 1 (11.1.1.7.0) for High Availability

**See:** The "Related Documents" section in this guide's Preface for a list of documents that provide additional information about Oracle Identity and Access Management components.

### 1.2.1 Upgrading to Oracle Identity and Access Management 11*g* Release 1 (11.1.1.7.0)

This guide does not explain how to upgrade previous versions of Oracle Identity and Access Management components, including any previous database schemas, to 11*g* Release 1 (11.1.1.7.0). To upgrade an Oracle Identity and Access Management component that is earlier than 11*g*, refer to *Oracle Fusion Middleware Upgrade Guide for Oracle Identity and Access Management*.

If you have an existing Oracle Identity and Access Management 11*g* Release 1 installation, refer to the "Patching Oracle Identity and Access Management" topic in the *Oracle Fusion Middleware Patching Guide*.

### 1.2.2 Installing Oracle Identity and Access Management 11*g* Release 1 (11.1.1.7.0) for High Availability

This guide does not explain how to install Oracle Identity and Access Management components in High Availability (HA) configurations. To install an Oracle Identity and Access Management component in a High Availability configuration, refer to *Oracle Fusion Middleware High Availability Guide*.

Specifically, see the "Configuring High Availability for Identity and Access Management Components" topic in the *Oracle Fusion Middleware High Availability Guide*.

## 1.3 Silent Installation

In addition to the standard graphical installation option, you can perform silent installation of the Oracle Identity and Access Management 11*g* software. A silent installation runs on its own without any intervention, and you do not have to monitor the installation and provide input to dialog boxes.

For more information, see Appendix F.4, "Performing a Silent Installation".

## 1.4 Understanding the State of Oracle Identity and Access Management Components After Installation

This topic provides information about the state of Oracle Identity and Access Management components after installation, including:

- Default SSL Configurations
- Default Passwords

### 1.4.1 Default SSL Configurations

By default, most of the Oracle Identity and Access Management 11*g* components are not installed with SSL configured. Only Oracle Adaptive Access Manager is configured with SSL. For other components, you must configure SSL for the Oracle WebLogic Administration Server and Oracle WebLogic Managed Server after installation.

**See:** The "SSL Configuration in Oracle Fusion Middleware" topic in the *Oracle Fusion Middleware Administrator's Guide* for more information.

### 1.4.2 Default Passwords

By default, the passwords for all Oracle Identity and Access Management components are set to the password for the Oracle Identity and Access Management Instance. For security reasons, after installation, you should change the passwords of the various components so they have different values.

**See:** The following documents for information about changing passwords for Oracle Identity and Access Management components:

- The "Getting Started Managing Oracle Fusion Middleware" topic in the *Oracle Fusion Middleware Administrator's Guide*.
- Component-specific guides listed in the "Related Documents" section in this guide's Preface.

## 1.5 Using This Guide

Each document in the Oracle Fusion Middleware Documentation Library has a specific purpose. The specific purpose of this guide is to explain how to:

1. Install single instances of Oracle Identity and Access Management 11*g* Release 1 (11.1.1.7.0) components.
2. Verify the installation was successful.
3. Get started with the component after installation.

This guide covers the most common, certified Oracle Identity and Access Management deployments. The following information is provided for each of these deployments:

- **Appropriate Installation Environment**: Helps you determine which installation is appropriate for your environment.
- **Components Installed**: Identifies the components that are installed in each scenario.
- **Dependencies**: Identifies the components each installation depends on.
- **Procedure**: Explains the steps for the installation.

Part II of this guide explains how to install Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager,Oracle Entitlements Server, and Oracle Identity Navigator by using the Oracle Identity and Access Management 11.1.1.7.0 Installer and the Oracle Fusion Middleware Configuration Wizard. The Oracle Identity Manager 11*g* Configuration Wizard is used for configuring Oracle Identity Manager only.

The following is a list of recommendations on how to use the information in this guide to install Oracle Identity and Access Management 11*g* Release 1 (11.1.1.7.0):

1. Review Chapter 1, "Introduction," for context.
2. Review Chapter 2, "Preparing to Install," for information about what you should consider before you deploy Oracle Identity and Access Management.
3. Review Chapter 3, "Installing and Configuring Oracle Identity and Access Management (11.1.1.7.0)," for general installation and configuration information

which applies to all Oracle Identity and Access Management 11*g* Release 1 (11.1.1.7.0) components.

4. Install, verify, and get started with your Oracle Identity and Access Management component by referring to its specific chapter in this guide.
5. Use the appendixes in this guide as needed.

**See Also:** The "Related Documents" section in this guide's Preface for a list of documents that provide additional information about Oracle Identity and Access Management components.

# 2

# Preparing to Install

This chapter provides information you should review before installing Oracle Identity and Access Management 11*g* Release 1 (11.1.1.7.0).

This chapter discusses the following topics:



## 2.1 Reviewing System Requirements and Certification

Before performing any installation, you should read the system requirements and certification documents to ensure that your environment meets the minimum installation requirements for the products you are installing.

- *Oracle Fusion Middleware System Requirements and Specifications*

  This document contains information related to hardware and software requirements, minimum disk space and memory requirements, and required system libraries, packages, or patches.

- *Oracle Fusion Middleware Supported System Configurations*

  This document contains information related to supported installation types, platforms, operating systems, databases, JDKs, and third-party products.

- For interoperability and compatibility issues that may arise when installing, refer to *Oracle Fusion Middleware Interoperability and Compatibility Guide*.

  This document contains important information regarding the ability of Oracle Fusion Middleware products to function with previous versions of other Oracle Fusion Middleware, Oracle, or third-party products. This information is applicable to both new Oracle Fusion Middleware users and existing users who are upgrading their existing environment.

## 2.2 Installing and Configuring Java Access Bridge (Windows Only)

If you are installing Oracle Identity and Access Management on a Windows operating system, you have the option of installing and configuring Java Access Bridge for Section 508 Accessibility. This is only necessary if you require Section 508 Accessibility features:

1. Download Java Access Bridge from the following URL:

   `http://java.sun.com/javase/technologies/accessibility/accessbridge/`

2. Install Java Access Bridge.
3. Copy `access-bridge.jar` and `jaccess-1_4.jar` from your installation location to the `jre\lib\ext` directory.
4. Copy the `WindowsAccessBridge.dll`, `JavaAccessBridge.dll`, and `JAWTAccessBridge.dll` files from your installation location to the `jre\bin` directory.
5. Copy the `accessibility.properties` file to the `jre\lib` directory.

## 2.3 Identifying Installation Directories

This topic describes directories you must identify in most Oracle Identity and Access Management installations and configurations—it does not describe one particular Installer screen. During installation, you will have to identify other component-specific directories not described in this topic.

The common directories described in this section include the following:

- Oracle Middleware Home Location
- Oracle Home Directory
- Oracle Common Directory
- Oracle WebLogic Domain Directory
- WebLogic Server Directory

### 2.3.1 Oracle Middleware Home Location

Identify the location of your Oracle Middleware Home directory. The Installer creates an Oracle Home directory for the component you are installing under the Oracle Middleware Home that you identify in this field. The Oracle Middleware Home directory is commonly referred to as *MW_HOME*.

### 2.3.2 Oracle Home Directory

Enter a name for the Oracle Home directory of the component. The Installer uses the name you enter in this field to create the Oracle Home directory under the location you enter in the Oracle Middleware Home Location field.

The Installer installs the files required to host the component, such as binaries and libraries, in the Oracle Home directory. The Oracle Home directory is commonly referred to as *ORACLE_HOME*.

---

**Note:** Avoid using spaces in the directory names, including Oracle Home. Spaces in such directory names are not supported.

---

### 2.3.3 Oracle Common Directory

The Installer creates this directory under the location you enter in the Oracle Middleware Home Location field.

The Installer installs the Oracle Java Required Files (JRF) required to host the components, in the Oracle Common directory. There can be only one Oracle Common Home within each Oracle Middleware Home. The Oracle Common directory is commonly referred to as *oracle_common*.

### 2.3.4 Oracle WebLogic Domain Directory

A WebLogic domain includes a special WebLogic Server instance called the Administration Server, which is the central point from which you configure and manage all resources in the domain. Usually, you configure a domain to include additional WebLogic Server instances called Managed Servers. You deploy Java components, such as Web applications, EJBs, and Web services, and other resources to the Managed Servers and use the Administration Server for configuration and management purposes only.

Managed Servers in a domain can be grouped together into a cluster.

The directory structure of a domain is separate from the directory structure of the WebLogic Server home. It can reside anywhere; it need not be within the Middleware home directory. A domain is a peer of an Oracle instance.

The Oracle Fusion Middleware Configuration Wizard creates a domain in a directory named *user_projects* under your Middleware Home (*MW_HOME)*.

### 2.3.5 WebLogic Server Directory

Enter the path to your Oracle WebLogic Server Home directory. This directory contains the files required to host the Oracle WebLogic Server. It is commonly referred to as *WL_HOME*.

## 2.4 Determining Port Numbers

If you want to install an Oracle Identity and Access Management 11*g* Release 1 (11.1.1) component against an existing Oracle Identity and Access Management 11*g* Release 1 (11.1.1) component, you may need to identify the ports for the existing component. For example, if you want to install Oracle Identity Manager 11*g* Release 1 (11.1.1) against an existing Oracle Internet Directory 11*g* Release 1 (11.1.1) component, you must identify its port when you install Oracle Identity Manager.

## 2.5 Locating Installation Log Files

The Installer writes log files to the `ORACLE_INVENTORY_LOCATION/logs` directory on UNIX systems and to the `ORACLE_INVENTORY_LOCATION\logs` directory on Windows systems.

On UNIX systems, if you do not know the location of your Oracle Inventory directory, you can find it in the `ORACLE_HOME/oraInst.loc` file.

On Microsoft Windows systems, the default location for the inventory directory is `C:\Program Files\Oracle\Inventory\logs`.

The following install log files are written to the log directory:

- install*DATE-TIME_STAMP*.log

- install*DATE-TIME_STAMP*.out
- installActions*DATE-TIME_STAMP*.log
- installProfile*DATE-TIME_STAMP*.log
- oraInstall*DATE-TIME_STAMP*.err
- oraInstall*DATE-TIME_STAMP*.log
- opatch*DATE-TIME_STAMP*.log

## 2.6 Optional: Updating the WebLogic Administrator Server User Name in Oracle Enterprise Manager Fusion Middleware Control (OIM Only)

Read this section only if the user name for the WebLogic Administrator for the domain is not **weblogic**. This task is required only if you are using Oracle Identity Manager.

If your WebLogic administrator user name is not **weblogic**, complete the following steps:

1. Ensure that the Oracle Identity Manager Managed server is up and running.
2. Log in to Oracle Enterprise Manager Fusion Middleware Control using your WebLogic Server administrator credentials.
3. Click **Identity and Access** > **oim** > **oim(11.1.1.7.0)**. Right-click and select **System MBean Browser**. The System MBean Browser page is displayed.
4. Under Application Defined MBeans, select `oracle.iam` > `Server:oim_server1` > `Application: oim` > `XMLConfig` > `config` > `XMLConfig.SOAConfig` > SOAConfig.
5. View the attribute username. By default, the value of the attribute is weblogic. Change this value to your WebLogic administrator user name.
6. Click **Apply**. Exit Oracle Enterprise Manager Fusion Middleware Control.
7. On the command line, use the `cd` command to move from your present working directory to the `IAM_Home/common/bin` directory. `IAM_Home` is the example IDM_Home directory for Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Entitlements Server, and Oracle Identity Navigator.
8. Launch the WebLogic Scripting Tool (WLST) interface as follows:

   On UNIX: Run `./wlst.sh` on the command line.

   On Windows: Run `wlst.cmd`.

   At the WLST command prompt (`wls:/offline>`), type the following:

   ```
   connect()
   ```

   You are prompted to enter the WebLogic Administration Server user name, password, and URL. For more information about using the WLST interface, see the topic "Using the WebLogic Scripting Tool" in the guide *Oracle Fusion Middleware Oracle WebLogic Scripting Tool*.

   a. Run the `deleteCred` WLST command:

      ```
      deleteCred(map="oim", key="SOAAdminPassword");
      ```

   b. Run the `createCred` WLST command, and replace the `ADMIN_PASSWORD` with your WebLogic administrator password:

```
createCred(map="oim", key="SOAAdminPassword",
user="xelsysadm",password="<ADMIN_PASSWORD>");
```

c. Run the following WLST command to verify the values:

```
listCred(map="oim", key="SOAAdminPassword");
```

d. Type `exit()` to exit the WLST command shell.

9. Open the Oracle Identity Manager Administration Console, and log in as user `xelsysadm`.
10. Create a new user for the user name of your WebLogic administrator.
11. Search for the **Administrators** role. Open the role details, and click the **Members** tab.
12. Remove all the existing members of the **Administrators** role.
13. Add the newly created user (the one with your WebLogic administrator user name) as a member of the **Administrators** role.
14. Restart Oracle Identity Manager Managed Server, as described in Starting the Stack.

# Part II

# Installing and Configuring Oracle Identity and Access Management (11.1.1.7.0)

Part III provides information about installing and configuring the following Oracle Identity and Access Management products:

- Oracle Identity Manager
- Oracle Access Manager
- Oracle Adaptive Access Manager
- Oracle Entitlements Server
- Oracle Identity Navigator

Additionally, Part III provides information about installing and configuring Oracle HTTP Server 11*g* Webgate for Oracle Access Manager, and migrating from Domain Agent to Oracle HTTP Server 10*g* Webgate for Oracle Access Manager.

Part III contains the following chapters:

# 3

# Installing and Configuring Oracle Identity and Access Management (11.1.1.7.0)

This chapter includes the following topics:

- Installation and Configuration Roadmap
- Installing and Configuring Oracle Identity and Access Management 11g Release 1 (11.1.1.7.0)

## 3.1 Installation and Configuration Roadmap

Table 3–1 lists the general installation and configuration tasks that apply to Oracle Identity and Access Management 11*g* Release 1 (11.1.1.7.0) products.

***Table 3–1 Installation and Configuration Flow for Oracle Identity and Access Management***

| No. | Task | Description |
|---|---|---|
| 1 | Review installation concepts in the Installation Planning Guide. | Read the *Oracle Fusion Middleware Installation Planning Guide*, which describes the process for various users to install or upgrade to Oracle Fusion Middleware 11*g* Release 1 (11.1.1.7.0) depending on the user's existing environment. |
| 2 | Review the system requirements and certification documents to ensure that your environment meets the minimum installation requirements for the components you are installing. | For more information, see Section 2.1, "Reviewing System Requirements and Certification". |
| 3 | Obtain the Oracle Fusion Middleware Software. | For more information, see Section 3.2.1, "Obtaining the Oracle Fusion Middleware Software" |
| 4 | Review the Database requirements. | For more information, see Section 3.2.2, "Reviewing Database Requirements". |
| 5 | Run Oracle Fusion Middleware Repository Creation Utility (RCU) to create and load the appropriate schemas for Oracle Identity and Access Management products. | For more information, see Section 3.2.3, "Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)". |
| 6 | Review WebLogic Server and Middleware Home requirements. | For more information, see Section 3.2.4, "Reviewing WebLogic Server and Middleware Home Requirements". |
| 7 | For Oracle Identity Manager users only:<br>Install Oracle SOA Suite 11*g* Release 1 (11.1.1.7.0). | For more information, see Section 3.2.5, "Installing Oracle SOA Suite (Oracle Identity Manager Users Only)". |

*Table 3–1 (Cont.) Installation and Configuration Flow for Oracle Identity and Access Management*

| No. | Task | Description |
|---|---|---|
| 8 | Start the Oracle Identity and Access Management Installer. | For more information, see Section 3.2.6, "Starting the Oracle Identity and Access Management Installer". |
| 9 | Install the Oracle Identity and Access Management 11*g* software. | For more information, see Section 3.2.7, "Installing Oracle Identity and Access Management (11.1.1.7.0)". |
| 10 | Run the Oracle Fusion Middleware Configuration Wizard to configure your Oracle Identity and Access Management products in a new or existing WebLogic domain. | For more information, see Section 3.2.8, "Configuring Oracle Identity and Access Management Products".<br>**Note:** If you are using Oracle Identity Manager, you must perform additional configuration after configuring Oracle Identity and Access Management in a WebLogic domain.<br>For more information, see Chapter 5, "Configuring Oracle Identity Manager". |
| 11 | Start the servers. | You must start the Administration Server and all Managed Servers. For more information, see Section C.1, "Starting the Stack". |

## 3.2 Installing and Configuring Oracle Identity and Access Management 11*g* Release 1 (11.1.1.7.0)

Follow the instructions in this section to install and configure the latest Oracle Identity and Access Management software.

Installing and configuring the latest version of Oracle Identity and Access Management 11*g* components involves the following steps:

- Obtaining the Oracle Fusion Middleware Software
- Reviewing Database Requirements
- Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)
- Reviewing WebLogic Server and Middleware Home Requirements
- Installing Oracle SOA Suite (Oracle Identity Manager Users Only)
- Starting the Oracle Identity and Access Management Installer
- Installing Oracle Identity and Access Management (11.1.1.7.0)
- Configuring Oracle Identity and Access Management Products
- Starting the Servers

### 3.2.1 Obtaining the Oracle Fusion Middleware Software

For installing Oracle Identity and Access Management, you must obtain the following software:

- Oracle WebLogic Server 11*g* Release 1 (10.3.6) or Oracle WebLogic Server 11*g* Release 1 (10.3.5)
- Oracle Database
- Oracle Repository Creation Utility
- Oracle Identity and Access Management Suite
- Oracle SOA Suite 11*g* Release 1 (11.1.1.7.0)

**Note:** Oracle SOA Suite is required only for Oracle Identity Manager.

For more information on obtaining Oracle Fusion Middleware 11*g* software, see *Oracle Fusion Middleware Download, Installation, and Configuration ReadMe*.

## 3.2.2 Reviewing Database Requirements

Some Oracle Identity and Access Management components require an Oracle Database. Ensure that you have an Oracle Database installed on your system before installing Oracle Identity and Access Management. The database must be up and running to install the relevant Oracle Identity and Access Management component. The database does not have to be on the same system where you are installing the Oracle Identity and Access Management component.

**Note:** For information about certified databases, see the "Certified Databases" topic in the *Oracle Fusion Middleware System Requirements and Specifications* 11*g* Release 1 (11.1.1) document.

For information about RCU requirements for Oracle Databases, see the "RCU Requirements for Oracle Databases" topic in the *Oracle Fusion Middleware System Requirements and Specifications* 11*g* Release 1 (11.1.1) document.

### 3.2.2.1 Oracle Database 11.1.0.7 Patch Requirements for Oracle Identity Manager

To identify the patches required for Oracle Identity Manager 11.1.1.7.0 configurations that use Oracle Database 11.1.0.7, refer to the Oracle Identity Manager section of the 11*g* Release 1 *Oracle Fusion Middleware Release Notes*.

## 3.2.3 Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)

You must create and load the appropriate Oracle Fusion Middleware schema in your database before installing the following Oracle Identity and Access Management components and configurations:

- Oracle Identity Manager
- Oracle Access Manager
- Oracle Adaptive Access Manager
- Oracle Entitlements Server

You create and load Oracle Fusion Middleware schema in your database using the Oracle Fusion Middleware Repository Creation Utility (RCU), which is available on the Oracle Technology Network (OTN) web site. You can access the OTN web site at:

`http://www.oracle.com/technetwork/index.html`

For more information on obtaining Oracle Fusion Middleware Repository Creation Utility, see *Oracle Fusion Middleware Download, Installation, and Configuration ReadMe*.

**Notes:**

- For information on RCU requirements, refer to the "Repository Creation Utility (RCU) Requirements" topic in the *Oracle Fusion Middleware System Requirements and Specifications* document.
- For information about launching and running RCU, see the "Launching RCU with a Variety of Methods" and "Running Oracle Fusion Middleware Repository Creation Utility (RCU)" topics in the guide *Oracle Fusion Middleware Repository Creation Utility User's Guide*.
- For information on creating schemas, see the "Creating Schemas" topic in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

Before running RCU, ensure that you have the database connection string, port, administrator credentials, and service name ready.

When you run RCU, create and load only the following schema for the Oracle Identity and Access Management component you are installing—do not select any other schema available in RCU:

- For Oracle Identity Manager, select the **Identity Management - Oracle Identity Manager** schema. The **SOA Infrastructure** schema, the **User Messaging Service** schema, and the **Metadata Services** schema are also selected, by default.
- For Oracle Adaptive Access Manager, select the **Identity Management - Oracle Adaptive Access Manager** schema. By default, the **AS Common Schemas - Metadata Services** schema is also selected.

  For Oracle Adaptive Access Manager with partition schema support, select the **Identity Management - Oracle Adaptive Access Manager (Partition Supp...)** schema. By default, the **AS Common Schemas - Metadata Services** schema is also selected.

  **Note:** For information about Oracle Adaptive Access Manager schema partitions, see Section H, "OAAM Partition Schema Reference".

- For Oracle Access Manager, select the **Identity Manager - Oracle Access Manager** schema. By default, the **AS Common Schema - Audit Services** schema is also selected.
- For Oracle Entitlements Server, select the **Identity Management - Oracle Entitlements Server** schema. By default, the **AS Common Schemas - Metadata Services** schema is also selected.

**Note:** When you create a schema, be sure to remember the schema owner and password that is shown in RCU.

If you are creating schemas on databases with Oracle Database Vault installed, note that statements such as `CREATE USER`, `ALTER USER`, `DROP USER`, `CREATE PROFILE`, `ALTER PROFILE`, and `DROP PROFILE` can only be issued by a user with the `DV_ACCTMGR` role. SYSDBA can issue these statements by modifying the Can Maintain Accounts/Profiles rule set only if it is allowed.

### 3.2.4 Reviewing WebLogic Server and Middleware Home Requirements

Before you can install Oracle Identity and Access Management 11*g* Release 1 (11.1.1.7.0) components, you must ensure that you have installed Oracle WebLogic Server 11*g* Release 1 (10.3.6) or Oracle WebLogic Server 11*g* Release 1 (10.3.5), and created a Middleware Home directory.

**Note:** On 64-bit platforms, when you install Oracle WebLogic Server using the generic jar file, JDK is not installed with Oracle WebLogic Server. You must install JDK separately, before installing Oracle WebLogic Server.

Ensure that the JDK version you select is Java SE 6 Update 24 or higher.

For more information, see "Install Oracle WebLogic Server" in *Oracle Fusion Middleware Installation Planning Guide*. In addition, see *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server* for complete information about installing Oracle WebLogic Server.

**Note:** By default, WebLogic domains are created in a directory named `domains` located in the `user_projects` directory under your Middleware Home. After you configure any of the Oracle Identity and Access Management products in a WebLogic administration domain, a new directory for the domain is created in the `domains` directory. In addition, a directory named `applications` is created in the `user_projects` directory. This `applications` directory contains the applications deployed in the domain.

### 3.2.5 Installing Oracle SOA Suite (Oracle Identity Manager Users Only)

If you are installing Oracle Identity Manager, you must install Oracle SOA Suite 11*g* Release 1 (11.1.1.7.0). Note that only Oracle Identity Manager requires Oracle SOA Suite. This step is required because Oracle Identity Manager uses process workflows in Oracle SOA Suite to manage request approvals.

For more information about installing Oracle SOA Suite, see *Oracle Fusion Middleware Installation Guide for Oracle SOA Suite and Oracle Business Process Management Suite*.

**Note:** If you have already created a Middleware Home before installing Oracle Identity and Access Management components, do not create a new Middleware Home again. You must use the same Middleware Home for installing Oracle SOA Suite.

### 3.2.6 Starting the Oracle Identity and Access Management Installer

This topic explains how to start the Oracle Identity and Access Management Installer.

**Notes:**

- If you are installing on an IBM AIX operating system, you must run the `rootpre.sh` script from the `Disk1` directory before you start the installer.
- Starting the Installer as the `root` user is not supported.

Start the Installer by executing one of the following commands:

**UNIX**: `<full path to the runInstaller directory>/runInstaller -jreLoc <full path to the JRE directory>`

**Windows**: `<full path to the setup.exe directory>\setup.exe -jreLoc <full path to the JRE directory>`

**Note:** The installer prompts you to enter the absolute path of the JRE that is installed on your system. When you install Oracle WebLogic Server, the `jrockit_1.6.0_29` directory is created under your Middleware Home. You must enter the absolute path of the JRE folder located in this JDK when launching the installer. For example, on Windows, if the JDK is located in `D:\oracle\Middleware\jrockit_1.6.0_29`, then launch the installer from the command prompt as follows:

```
D:\setup.exe -jreLoc D:\oracle\Middleware\jrockit_
1.6.0_29\jre
```

If you do not specify the `-jreLoc` option on the command line when using the Oracle JRockit JDK, the following warning message is displayed:

```
-XX:MaxPermSize=512m is not a valid VM option.
Ignoring
```

This warning message does not affect the installation. You can continue with the installation.

On 64 bit platforms, when you install Oracle WebLogic Server using the generic jar file, the `jrockit_1.6.0_29` directory will not be created under your Middleware Home. You must enter the absolute path of the JRE folder from where your JDK is located.

### 3.2.7 Installing Oracle Identity and Access Management (11.1.1.7.0)

This topic describes how to install the Oracle Identity and Access Management 11*g* software, which includes Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Identity Navigator, and Oracle Entitlements Server.

It includes the following sections:

- Products Installed
- Dependencies
- Procedure
- Understanding the Directory Structure After Installation

#### 3.2.7.1 Products Installed

Performing the installation in this section installs the following products:

- Oracle Identity Manager
- Oracle Access Manager

> **Note:** When you are installing Oracle Access Manager, Oracle Secure Token Service will also be installed. For more information on Oracle Secure Token Service, see *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service*.

- Oracle Adaptive Access Manager

> **Note:** For Oracle Identity and Access Management 11.1.1.7.0, Oracle Adaptive Access Manager includes two components
>
> - Oracle Adaptive Access Manager (Online)
> - Oracle Adaptive Access Manager (Offline)

- Oracle Identity Navigator
- Oracle Entitlements Server

> **Note:** When you are installing Oracle Identity and Access Management, only the Administration Server of Oracle Entitlements Server is installed.
>
> To install and configure Oracle Entitlements Server Client, see Installing Oracle Entitlements Server Client.

#### 3.2.7.2 Dependencies

The installation in this section depends on the following:

- Oracle WebLogic Server 11*g* Release 1 (10.3.6) or Oracle WebLogic Server 11*g* Release 1 (10.3.5)
- Oracle Database and any required patches
- Oracle SOA Suite 11*g* Release 1 (11.1.1.7.0)

> **Note:** Oracle SOA Suite is required only for Oracle Identity Manager.

- JDK (Java SE 6 Update 24 or higher) or JRockit

### 3.2.7.3 Procedure

Complete the following steps to install the Oracle Identity and Access Management suite that contains Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Identity Navigator, and Oracle Entitlements Server:

1. Start your installation by performing all the steps in Section 3.2.6, "Starting the Oracle Identity and Access Management Installer". After you complete those steps, the Welcome screen appears.
2. Click **Next** on the Welcome screen. The Install Software Updates screen appears. Select whether or not you want to search for updates. Click **Next**.
3. The Prerequisite Checks screen appears. If all prerequisite checks pass inspection, click **Next**. The Specify Installation Location screen appears.
4. On the Specify Installation Location screen, enter the path to the Oracle Middleware Home installed on your system. Ensure that Oracle WebLogic Server is already installed on the system in the same Middleware Home. This directory is the same as the Oracle Home created in the Oracle WebLogic Server installation.

   ---

   **Note:** If you do not specify a valid Middleware Home directory on the Specify Installation Location screen, the Installer displays a message and prompts you to confirm whether you want to proceed with the installation of only Oracle Identity Manager Design Console and Oracle Identity Manager Remote Manager. These two components of Oracle Identity Manager do not require a Middleware Home directory.

   If you want to install only Oracle Identity Manager Design Console or Remote Manager, you do not need to install Oracle WebLogic Server or create a Middleware Home directory on the machine where Design Console or Remote Manager is being configured.

   Before using Oracle Identity Manager Design Console or Remote Manager, you must configure Oracle Identity Manager Server on the machine where the Administration Server is running. When configuring Design Console or Remote Manager on a different machine, you can specify the Oracle Identity Manager Server host and URL information.

   ---

5. In the **Oracle Home Directory** field, enter a name for the Oracle Home folder that will be created under your Middleware Home. This directory is also referred to as `IAM_Home` in this book.

   ---

   **Note:** The name that you provide for the Oracle Home for installing the Oracle Identity and Access Management suite should not be same as the Oracle Home name given for the Oracle Identity Management suite.

   Oracle Identity Management 11*g* Release 1 is part of Oracle Fusion Middleware and includes components like Oracle Internet Directory, Oracle Virtual Directory, Oracle Directory Services Manager, Oracle Directory Integration Platform, and Oracle Identity Federation.

   ---

   Click **Next**. The Installation Summary screen appears.

6. The Installation Summary screen displays a summary of the choices that you made. Review this summary and decide whether to start the installation. If you want to modify any of the configuration settings at this stage, select a topic in the left navigation page and modify your choices. To continue installing Oracle Identity and Access Management, click **Install**. The Installation Progress screen appears. Click **Next**.

   **Note:** If you cancel or abort when the installation is in progress, you must manually delete the `IAM_Home` directory before you can reinstall the Oracle Identity and Access Management software.

   To invoke online help at any stage of the installation process, click the **Help** button on the installation wizard screens.

7. The Installation Complete screen appears. On the Installation Complete screen, click **Finish**.

   This installation process copies the Identity Management software to your system and creates an *IAM_Home* directory under your Middleware Home.

   After installing the Oracle Identity and Access Management software, you must proceed to Section 3.2.8, "Configuring Oracle Identity and Access Management Products," to configure Oracle Identity and Access Management products in a new or existing WebLogic domain.

#### 3.2.7.4 Understanding the Directory Structure After Installation

This section describes the directory structure after installation of Oracle WebLogic Server and Oracle Identity and Access Management. It also shows the structure of directories created after the Oracle Identity and Access Management software is installed.

After you install the Oracle Identity and Access Management suite, an Oracle Home directory for Oracle Identity and Access Management, such as `Oracle_IDM1`, is created under your Middleware Home. This home directory is also referred to as `IAM_Home` in this guide.

For more information about identifying installation directories, see Section 2.3, "Identifying Installation Directories".

### 3.2.8 Configuring Oracle Identity and Access Management Products

After Oracle Identity and Access Management 11*g* is installed, you are ready to configure the WebLogic Server Administration Domain for Oracle Identity and Access Management components. A domain includes a special WebLogic Server instance called the Administration Server, which is the central point from which you configure and manage all resources in the domain.

When you configure an Oracle Identity and Access Management 11.1.1.7.0 component, you can choose one of the following configuration options:

- Create a New Domain
- Extend an Existing Domain

You can use the Oracle Fusion Middleware Configuration Wizard to create a WebLogic domain or extend an existing domain.

#### Create a New Domain

Select the **Create a new WebLogic domain** option on the Welcome screen in the Oracle Fusion Middleware Configuration Wizard to create a new WebLogic Server domain.

#### Extend an Existing Domain

Select the **Extend an existing WebLogic domain** option on the Welcome screen in the Oracle Fusion Middleware Configuration Wizard to add Oracle Identity and Access Management components in an existing Oracle WebLogic Server administration domain.

> **See:** The "Understanding Oracle WebLogic Server Domains" chapter in the *Oracle Fusion Middleware Understanding Domain Configuration for Oracle WebLogic Server* guide for more information about Oracle WebLogic Server administration domains.
>
> In addition, see the *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard* guide for complete information about how to use the Configuration Wizard to create or extend WebLogic Server domains. This guide also provides the Oracle Fusion Middleware Configuration Wizard Screens.

For component-specific configuration information about Oracle Identity and Access Management products, see the following chapters:

- Chapter 4, "Configuring Oracle Identity Navigator"
- Chapter 5, "Configuring Oracle Identity Manager"
- Chapter 6, "Configuring Oracle Access Manager"
- Chapter 7, "Configuring Oracle Adaptive Access Manager"
- Chapter 8, "Installing and Configuring Oracle Entitlements Server"

If you are configuring Oracle Identity Manager, you must run the Oracle Identity Manager Configuration Wizard after configuring a domain, to configure Oracle Identity Manager Server, Oracle Identity Manager Design Console, and Oracle Identity Manager Remote Manager as described in "Section 5.5, "Starting the Oracle Identity Manager 11g Configuration Wizard"". For more information, see the following sections:

- Section 5.6, "Configuring Oracle Identity Manager Server",
- Section 5.7, "Optional: Configuring Oracle Identity Manager Design Console"
- Section 5.8, "Optional: Configuring Oracle Identity Manager Remote Manager"

### 3.2.9 Starting the Servers

After installing and configuring Oracle Identity and Access Management, you must run the Oracle WebLogic Administration Server and various Managed Servers, as described in Section C.1, "Starting the Stack".

# 4

# Configuring Oracle Identity Navigator

This chapter explains how to configure Oracle Identity Navigator. It includes the following topics:



## 4.1 Important Note Before You Begin

Before you start installing and configuring Oracle Identity and Access Management products in any of the scenarios discussed in this chapter, note that **IAM_Home** is used to refer to the Oracle Home directory that includes Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Entitlements Server, and Oracle Identity Navigator. You can specify any name for this Oracle Home directory.

## 4.2 Configuring Oracle Identity Navigator in a New WebLogic Domain

This topic describes how to configure only Oracle Identity Navigator in a new WebLogic administration domain. It includes the following sections:



### 4.2.1 Appropriate Deployment Environment

Perform the configuration in this topic if you want to configure Oracle Identity Navigator with Oracle Identity Manager, Oracle Access Manager, and Oracle Adaptive Access Manager in a new WebLogic domain and then run the Oracle Identity Navigator discovery feature. This feature populates links to the product consoles for Oracle Identity Manager, Oracle Access Manager, and Oracle Adaptive Access Manager. You can then access those product consoles from within the Oracle Identity Navigator interface, without having to remember the individual console URLs.

### 4.2.2 Components Deployed

Performing the configuration in this section deploys the Oracle Identity Navigator application on a new WebLogic Administration Server.

### 4.2.3 Dependencies

The configuration in this section depends on the following:

- Oracle WebLogic Server 11*g* Release 1 (10.3.6) or Oracle WebLogic Server 11*g* Release 1 (10.3.5).
- Installation of the Oracle Identity and Access Management 11*g* Release 1 (11.1.1.7.0) software.

### 4.2.4 Procedure

Perform the following steps to configure only Oracle Identity Navigator in a new WebLogic administration domain:

1. Start the Oracle Fusion Middleware Configuration Wizard by running the `<IAM_Home>/common/bin/config.sh` script (on UNIX), or `<IAM_Home>\common\bin\config.cmd` (on Windows). The Welcome screen of the Oracle Fusion Middleware Configuration Wizard appears.

   **Note:** `IAM_Home` is used as an example here. You must run this script from your Oracle Identity and Access Management Home directory that contains Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Entitlements Server, and Oracle Identity Navigator.

2. On the Welcome screen, select **Create a new WebLogic domain**, and click **Next**. The Select Domain Source screen appears.
3. On the Select Domain Source screen, ensure that the **Generate a domain configured automatically to support the following products:** option is selected. Create a WebLogic administration domain, which supports Oracle Identity Navigator (choose **Oracle Identity Navigator - 11.1.1.3.0 [Oracle_IDM2]**), and click **Next**. The Specify Domain Name and Location screen appears.

   **Note:** When you select the **Oracle Identity Navigator - 11.1.1.3.0 [Oracle_IDM2]** check box, the **Oracle JRF 11.1.1.0 [oracle_common]** option is also selected, by default.

4. Enter a name and a location for the domain to be created, and click **Next**. The Configure Administrator User Name and Password screen appears.
5. Configure a user name and a password for the administrator. The default user name is `weblogic`. Click **Next**.
6. The Configure Server Start Mode and JDK screen appears. Choose a JDK from the **Available JDKs** and select a **WebLogic Domain Startup Mode**. Click **Next**.
7. On the Select Optional Configuration screen, you can configure **Administration Server** and **Managed Servers, Clusters, and Machines, Deployments and Services**, and **RDBMS Security Store** options. Click **Next**.

8. Optional: Configure the following Administration Server parameters:
   - Name
   - Listen address
   - Listen port
   - SSL listen port
   - SSL enabled or disabled
9. Optional: Configure Managed Servers, as required.
10. Optional: Configure Clusters, as required.

    For more information about configuring clusters for Oracle Identity and Access Management products, see the "Configuring High Availability for Identity Management Components" topic in the guide *Oracle Fusion Middleware High Availability Guide*.
11. Optional: Assign Managed Servers to clusters, as required.
12. Optional: Configure Machines, as needed. This step is useful when you want to run the Administration Server on one machine and Managed Servers on another physical machine.

    **Tip:** Before configuring a machine, use the `ping` command to verify whether the machine or host name is accessible.
13. Optional: Assign the Administration Server to a machine.
14. Optional: Select Deployments, such as applications and libraries, and Services to target them to a particular cluster or server.
15. Optional: Configure RDBMS Security Store, as required.
16. On the Configuration Summary screen, you can view summaries of your configuration for deployments, application, and service. Review the domain configuration, and click **Create** to start creating the domain.

A new WebLogic domain to support Oracle Identity Navigator is created in the `<MW_HOME>\user_projects\domains` directory (on Windows). On UNIX, the domain is created in the `<MW_HOME>/user_projects/domains` directory.

## 4.3 Starting the Servers

After installing and configuring Oracle Identity Navigator, you must run the Oracle WebLogic Administration Server and various Managed Servers, as described in Appendix C.1, "Starting the Stack".

## 4.4 Verifying Oracle Identity Navigator

To verify the installation of Oracle Identity Navigator, complete the following steps:

1. Launch Oracle Identity Navigator in a browser by using the following URL:

   `http://<host>:7001/oinav/faces/idmNag.jspx`

   The Oracle Identity Navigator dashboard and the resource catalog are displayed.
2. Click the **Customize link** on the upper right corner of the screen to switch to the Edit mode.

3. Click the **Add Content** button on the page. A resource catalog pops up.
4. In the pop-up dialog, click the **Open** link for the folder IDM Product Launcher. The Launcher task flow pops up.
5. In the pop-up dialog, click the **Add** link. Verify that the Launcher portlet is added to the page content. Continue to add News task flows to the page, without closing the pop-up dialog. Click the up arrow at the upper left corner. The top folder layout is displayed again. Click the **Open** link for the folder News. The News and Announcements task flow pops up.
6. In the News and Announcements pop-up dialog, click the **Add** link. Verify that the Report portlet is added to the page content. Continue to add Reports task flows to the page, without closing the pop-up dialog. Click the up arrow at the upper left corner. The top folder layout is displayed again. Click the **Open** link for the folder My Reports. Click the **Add** link and the Close button (X). All the three workflows are added to the page content.
7. Change the default layout, if necessary, by clicking the Pencil icon located on the upper right area of the screen.
8. To exit the Edit mode, click the **Close** button.

   If the task flows are properly added to the page content, the screen displays the task flow content.
9. Test the Product Registration functionality as follows:
   a. Create, edit, or delete the product information by clicking the **Administration** tab.
   b. To add a new product, click the **Create image** icon in the Product Registration section. The New Product Registration dialog pops up.
   c. Enter the relevant information in this dialog, and the new product registration is updated accordingly. The new product registration data is updated on the Launcher portlet after you click the **Dashboard** tab.
   d. Click the product link and ensure that a new browser window or tab opens with the registered product URL.
10. Test the News functionality as follows:
    a. Click the **refresh** icon to update the RSS feed content.
    b. Click the news item link to open the source of content in a new browser window or tab.
11. Test the Reports functionality as follows:
    a. Add a report by clicking the **Add** icon. The Add Report dialog pops up.
    b. In this dialog, select a report to add, and click the **Add Report** button. Verify that the report is added.
    c. Run a report by clicking the report icon. The report opens in a new browser window or tab.

## 4.5 Getting Started with Oracle Identity Navigator After Installation

After installing Oracle Identity Navigator, refer to the "Using Identity Navigator" chapter in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*.

# 5

# Configuring Oracle Identity Manager

This chapter explains how to configure Oracle Identity Manager.

It includes the following topics:



> **Note:** To invoke online help at any stage of the Oracle Identity Manager configuration process, click the **Help** button on the Oracle Identity Manager Configuration Wizard screens.

## 5.1 Important Notes Before You Start Configuring Oracle Identity Manager

Before you start configuring Oracle Identity Manager, keep the following points in mind:

- Before you start installing and configuring Oracle Identity and Access Management products in any of the scenarios discussed in this chapter, note that **IAM_Home** is used to refer to the Oracle Home directory that includes Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Entitlements Server, and Oracle Identity Navigator. You can specify any name for this Oracle Home directory.
- By performing the domain configuration procedures described in this chapter, you can create Managed Servers on a local machine (the machine on which the Administration Server is running). However, you can create and start Managed

Servers for Oracle Identity and Access Management components on a remote machine. For more information, see the "Creating and Starting a Managed Server on a Remote Machine" topic in the guide *Oracle Fusion Middleware Creating Templates and Domains Using the Pack and Unpack Commands*.

- You must use the Oracle Identity Manager Configuration Wizard to configure Oracle Identity Manager Server, Oracle Identity Manager Design Console (on Windows only), and Oracle Identity Manager Remote Manager.

  If you are configuring Oracle Identity Manager Server, you must run the Oracle Identity Manager configuration wizard on the machine where the Administration Server is running. For configuring the Server, you can run the wizard only once during the initial setup of the Server. After the successful setup of Oracle Identity Manager Server, you cannot run the Oracle Identity Manager Configuration Wizard again to modify the configuration of Oracle Identity Manager Server. For such modifications, you must use Oracle Enterprise Manager Fusion Middleware Control.

  If you are configuring only Design Console or Remote Manager, you can run the Oracle Identity Manager Configuration Wizard on the machine where Design Console or Remote Manager is being configured. You can configure Design Console or Remote Manager after configuring the Oracle Identity Manager Server. Note that you can run the Oracle Identity Manager Configuration Wizard to configure Design Console or Remote Manager as and when you need to configure them on new machines.

  Note that Oracle Identity Manager requires Oracle SOA Suite 11*g* Release 1 (11.1.1.7.0), which should be exclusive to Oracle Identity and Access Management. You must install Oracle SOA Suite before configuring Oracle Identity Manager. If you are setting up integration between Oracle Identity Manager and Oracle Access Manager, ensure that Oracle Identity Manager, Oracle Access Manager, and Oracle SOA Suite are configured in the same domain.

## 5.2 Creating a new WebLogic Domain for Oracle Identity Manager and SOA

This topic describes how to create a new WebLogic domain for Oracle Identity Manager and SOA. It includes the following sections:



### 5.2.1 Appropriate Deployment Environment

Perform the configuration in this topic if you want to install Oracle Identity Manager in an environment where you may use Oracle Identity Manager as a provisioning or request solution. This option is also appropriate for Oracle Identity Manager environments that do not use Single Sign-On (SSO) or Oracle Access Manager.

### 5.2.2 Components Deployed

Performing the configuration in this section installs the following components:

- Administration Server

- A Managed Server for Oracle Identity Manager
- Oracle Identity Administration Console, Oracle Identity Manager Self Service Console, and Oracle Identity Manager Advanced Administration Console on the Oracle Identity Manager Managed Server

### 5.2.3 Dependencies

The configuration in this section depends on the following:

- Oracle WebLogic Server 11*g* Release 1 (10.3.6) or Oracle WebLogic Server 11*g* Release 1 (10.3.5).
- Installation of the Oracle Identity and Access Management 11*g* Release 1 (11.1.1.7.0) software.
- Installation of Oracle SOA Suite 11*g* Release 1 (11.1.1.7.0).
- Database schemas for Oracle Identity Manager and Oracle SOA 11*g* Suite. For more information, see Section 3.2.3, "Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)".

### 5.2.4 Procedure

Complete the following steps to create a new WebLogic domain for Oracle Identity Manager and SOA and to configure Oracle Identity Manager Server, Design Console, and Remote Manager:

1. Review the section Important Notes Before You Start Configuring Oracle Identity Manager.
2. Run the `<IAM_Home>/common/bin/config.sh` script (on UNIX). (`<IAM_Home>\common\bin\config.cmd` on Windows). The Welcome screen of the Oracle Fusion Middleware Configuration Wizard appears.
3. On the Welcome screen, select **Create a new WebLogic domain**, and click **Next**. The Select Domain Source screen appears.
4. On the Select Domain Source screen, ensure that the **Generate a domain configured automatically to support the following products:** option is selected.

   Select **Oracle Identity Manager - 11.1.1.3.0 [IAM_Home]**.

   ---

   **Note:** When you select the **Oracle Identity Manager - 11.1.1.3.0 [IAM_Home]** option, the following options are also selected, by default:

   - **Oracle SOA Suite - 11.1.1.1.0 [Oracle_SOA1]**
   - **Oracle JRF 11.1.1.0 [oracle_common]**
   - **Oracle Enterprise Manager - 11.1.1.0 [oracle_common]**
   - **Oracle WSM Policy Manager 11.1.1.0 [oracle_common]**

   ---

   Click **Next**. The Specify Domain Name and Location screen appears.
5. Enter a name and a location for the domain to be created, and click **Next**. The Configure Administrator User Name and Password screen appears.
6. Configure a user name and a password for the administrator. The default user name is `weblogic`. Click **Next**.

7. The Configure Server Start Mode and JDK screen appears. Choose a JDK from the **Available JDKs** and select a **WebLogic Domain Startup Mode**. Click **Next**. The Configure JDBC Component Schema screen appears. This screen displays a list of the following component schemas:
   - SOA Infrastructure
   - User Messaging Service
   - OIM MDS Schema
   - OWSM MDS Schema
   - SOA MDS Schema
   - OIM Infrastructure
8. On the Configure JDBC Component Schema screen, for the Oracle Identity Manager and its dependant schemas, specify the schema owner and password that you set in RCU when creating and loading the schemas. Click **Next**. The Test JDBC Component Schema screen appears. After the test succeeds, the Select Optional Configuration screen appears.
9. On the Select Optional Configuration screen, you can configure the **Administration Server**, **JMS Distributed Destination**, **Managed Servers, Clusters, and Machines, Deployments and Services**. Click **Next**.
10. Optional: Configure the following Administration Server parameters:
    - Name
    - Listen address
    - Listen port
    - SSL listen port
    - SSL enabled or disabled

    Click **Next**.
11. Optional: Configure JMS Distributed Destination, as required. Click **Next**.
12. Optional: Configure Managed Servers, as required. Click **Next**.
13. Optional: Configure Clusters, as required. Click **Next**.

    For more information about configuring clusters for Oracle Identity and Access Management products, see the "Configuring High Availability for Identity Management Components" topic in the guide *Oracle Fusion Middleware High Availability Guide*.
14. Optional: Assign Managed Servers to Clusters, as required. Click **Next**.
15. Optional: Configure Machines, as needed. This step is useful when you want to run the Administration Server on one machine and Managed Servers on another physical machine.Click **Next**.

    **Tip:** Before configuring a machine, use the `ping` command to verify whether the machine or host name is accessible.
16. Optional: Assign servers to machines. Click **Next**.
17. Optional: Select Deployments, such as applications and libraries, and Services to target them to a particular cluster or server. Click **Next**.

18. On the Configuration Summary screen, you can view summaries of your configuration for deployments, application, and service. Review the domain configuration, and click **Create** to start creating the domain.

    After the domain configuration is complete, click **Done** to close the configuration wizard.

    A new WebLogic domain to support Oracle Identity Manager is created in the `<MW_HOME>\user_projects\domains` directory (on Windows). On UNIX, the domain is created in the `<MW_HOME>/user_projects/domains` directory.

19. Start the Administration Server, as described in Appendix C, "Starting or Stopping the Oracle Stack".

20. Start the SOA Managed Server, as described in Appendix C, "Starting or Stopping the Oracle Stack".

21. Start the Oracle Identity Manager Configuration Wizard, as described in Section 5.5, "Starting the Oracle Identity Manager 11g Configuration Wizard".

22. Configure the Oracle Identity Manager Server, Design Console, or Remote Manager, as described in Section 5.6, "Configuring Oracle Identity Manager Server", Section 5.7, "Optional: Configuring Oracle Identity Manager Design Console", and Section 5.8, "Optional: Configuring Oracle Identity Manager Remote Manager".

> **Note:** If **weblogic** is not your WebLogic administrator user name, you must complete a set of manual steps after starting the servers. For more information, see Section 2.6, "Optional: Updating the WebLogic Administrator Server User Name in Oracle Enterprise Manager Fusion Middleware Control (OIM Only)".

## 5.3 Starting the Servers

After installing and configuring Oracle Identity Manager in a WebLogic domain, you must run the Oracle WebLogic Administration Server and various Managed Servers, as described in Appendix C.1, "Starting the Stack".

> **Notes:**
>
> - If **weblogic** is not your WebLogic administrator user name, you must complete a set of manual steps after starting the servers. For more information, see Section 2.6, "Optional: Updating the WebLogic Administrator Server User Name in Oracle Enterprise Manager Fusion Middleware Control (OIM Only).".
> - Oracle Identity Manager requires Oracle SOA Suite. In order to avoid concurrent update, Oracle Identity Manager and SOA servers should not be started simultaneously. Start the SOA server first, wait for the SOA server to come up and then start the Oracle Identity Manager server.

## 5.4 Overview of Oracle Identity Manager Configuration

This section discusses the following topics:

- Before Configuring Oracle Identity Manager Server, Design Console, or Remote Manager

- Oracle Identity Manager Configuration Scenarios

## 5.4.1 Before Configuring Oracle Identity Manager Server, Design Console, or Remote Manager

Before configuring Oracle Identity Manager using the Oracle Identity Manager Wizard, ensure that you have installed and configured Oracle Identity Manager and SOA in a WebLogic.

The Oracle Identity Manager 11*g* Configuration Wizard prompts you to enter information about certain configurations, such as Database, Schemas, WebLogic Administrator User Name and Password, and LDAP Server. Therefore, keep this information ready with you before starting the Identity Management 11*g* Configuration Wizard.

This section discusses the following topics:

- Prerequisites for Configuring Oracle Identity Manager Server
- Prerequisites for Configuring Only Oracle Identity Manager Design Console on a Different Machine
- Prerequisites for Configuring Only Oracle Identity Manager Remote Manager on a Different Machine

### 5.4.1.1 Prerequisites for Configuring Oracle Identity Manager Server

Before you can configure Oracle Identity Manager Server using the Oracle Identity Manager Configuration Wizard, you must complete the following prerequisites:

1. Installing a supported version of Oracle database. For more information, see Section 3.2.2, "Reviewing Database Requirements".
2. Creating and loading the required schemas in the database. For more information, see Section 3.2.3, "Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU),".
3. Installing Oracle WebLogic Server and creating a Middleware Home directory. For more information, see Section 3.2.4, "Reviewing WebLogic Server and Middleware Home Requirements".
4. Installing Oracle SOA Suite 11*g* Release 1 (11.1.1.7.0) under the same Middleware Home directory. For more information, see Section 3.2.5, "Installing Oracle SOA Suite (Oracle Identity Manager Users Only)".
5. Installing the Oracle Identity and Access Management Suite (the suite that contains Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Entitlements Server, and Oracle Identity Navigator) under the Middleware Home directory. For more information, see Installing Oracle Identity and Access Management (11.1.1.7.0).
6. Creating a new WebLogic domain or extending an existing Identity Management 11.1.1.7.0 domain for Oracle Identity Manager and Oracle SOA. For more information, see Section 5.2, "Creating a new WebLogic Domain for Oracle Identity Manager and SOA".
7. Starting the Oracle WebLogic Administration Server for the domain in which the Oracle Identity Manager application is deployed. For more information, see Appendix C.1, "Starting the Stack".
8. Starting the SOA Managed Server, as described in Appendix C.1, "Starting the Stack".

#### 5.4.1.2 Prerequisites for Configuring Only Oracle Identity Manager Design Console on a Different Machine

On the machine where you are installing and configuring Design Console, you must install the Oracle Identity and Access Management 11*g* (11.1.1.7.0) software containing Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Entitlements Server, and Oracle Identity Navigator. For information, see Section 3.2.7, "Installing Oracle Identity and Access Management (11.1.1.7.0).".

Before you can configure Oracle Identity Manager Design Console by running the Oracle Identity Manager Configuration Wizard, you should have configured the Oracle Identity Manager Server, as described in Section 5.6, "Configuring Oracle Identity Manager Server" on a local or remote machine. In addition, the Oracle Identity Manager Server should be up and running.

---

**Note:** Oracle Identity Manager Design Console is supported on Windows operating systems only. If you are installing and configuring only Design Console on a machine, you do not need to install Oracle WebLogic Server and create a Middleware Home directory before installing the Oracle Identity and Access Management software.

---

#### 5.4.1.3 Prerequisites for Configuring Only Oracle Identity Manager Remote Manager on a Different Machine

On the machine where you are installing and configuring Remote Manager, you must install the Oracle Identity and Access Management 11*g* (11.1.1.7.0) software containing Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Entitlements Server, and Oracle Identity Navigator. For information, see Section 3.2.7, "Installing Oracle Identity and Access Management (11.1.1.7.0)".

Before you can configure Oracle Identity Manager Remote Manager by running the Oracle Identity Manager Configuration Wizard, you should have configured the Oracle Identity Manager Server, as described in Section 5.6, "Configuring Oracle Identity Manager Server". In addition, the Oracle Identity Manager Server should be up and running.

---

**Note:** If you are installing and configuring only Remote Manager on a machine, you do not need to install Oracle WebLogic Server and create a Middleware Home directory before installing the Oracle Identity and Access Management software.

---

### 5.4.2 Oracle Identity Manager Configuration Scenarios

The Oracle Identity Management 11*g* Configuration Wizard enables you to configure Oracle Identity Manager Server, Design Console (Windows only), and Remote Manager.

If you are configuring Oracle Identity Manager Server, you must run this configuration wizard on the machine where the Administration Server is running.

You must complete this additional configuration for Oracle Identity Manager components after configuring Oracle Identity Manager in a new or existing WebLogic administration domain.

**Note:** You can run the Oracle Identity Manager Configuration Wizard to configure Oracle Identity Manager Server only once during the initial setup. After the initial setup, you cannot run the Oracle Identity Manager Configuration Wizard again to modify the configuration of Oracle Identity Manager Server, Design Console, or Remote Manager. For such modifications, you must use Oracle Enterprise Manager Fusion Middleware Control.

This section discusses the following topics:

- Scope of Configuration Using the Oracle Identity Manager 11g Configuration Wizard
- Scenario 1: Oracle Identity Manager Server and Design Console on Different Machines
- Scenario 2: Oracle Identity Manager Server and Remote Manager on Different Machines
- Scenario 3: Oracle Identity Manager Server, Design Console, and Remote Manager on a Single Windows Machine

#### 5.4.2.1 Scope of Configuration Using the Oracle Identity Manager 11*g* Configuration Wizard

You can use the Oracle Identity Manager 11*g* Configuration Wizard to configure the non-J2EE components and elements of Oracle Identity Manager. Most of the J2EE configuration is done automatically in the domain template for Oracle Identity Manager.

#### 5.4.2.2 Scenario 1: Oracle Identity Manager Server and Design Console on Different Machines

In this scenario, you configure Oracle Identity Manager Server on one machine, and install and configure only Oracle Identity Manager Design Console on a different Windows machine (a development or design system).

Perform the following tasks:

1. Install and configure Oracle Identity Manager Server on a machine after completing all of the prerequisites, as described in Section 5.6, "Configuring Oracle Identity Manager Server". Ensure that the Oracle Identity Manager Server is up and running.
2. On the Windows machine on which the Design Console is to be installed, install a JDK in a path without a space such as `c:/jdk1.6.0_24`.
3. Create a `Middleware_Home` folder such as `c:/oracle/Middleware`.
4. Run `setup.exe` from the installation media `disk1` and follow the prompts selecting the `Middleware_Home` created above.

**Note:** When you specify the location of the Middleware_Home, you will see a message "Specified middleware home is not valid. If you continue with this installation only Remote Manager and Design Console can be configured." This is a valid message if you intend to install only the Design Console.

5. The installer will install the Oracle Identity and Access Management suite needed to install the Design Console.
6. On the Windows machine where you installed the Oracle Identity and Access Management 11*g* software, run the Oracle Identity Manager Configuration Wizard to configure only Design Console. Note that you must provide the Oracle Identity Manager Server information, such as host and URL, when configuring Design Console. For more information, see Section 5.7, "Optional: Configuring Oracle Identity Manager Design Console".

#### 5.4.2.3 Scenario 2: Oracle Identity Manager Server and Remote Manager on Different Machines

In this scenario, you configure Oracle Identity Manager Server on one machine, and install and configure only Oracle Identity Manager Remote Manager on a different machine.

The following are the high-level tasks in this scenario:

1. Install and configure Oracle Identity Manager Server on a machine after completing all of the prerequisites, as described in Section 5.6, "Configuring Oracle Identity Manager Server". Ensure that the Oracle Identity Manager Server is up and running.
2. On a different machine, install the Oracle Identity and Access Management 11*g* software containing Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Entitlements Server, and Oracle Identity Navigator. For information, see Section 3.2.7, "Installing Oracle Identity and Access Management (11.1.1.7.0)".
3. On the machine where you installed the Oracle Identity and Access Management 11*g* software, run the Oracle Identity Manager Configuration Wizard to configure only Remote Manager. Note that you must provide the Oracle Identity Manager Server information, such as host and URL, when configuring Remote Manager. For more information, see Section 5.8, "Optional: Configuring Oracle Identity Manager Remote Manager".

#### 5.4.2.4 Scenario 3: Oracle Identity Manager Server, Design Console, and Remote Manager on a Single Windows Machine

In this scenario, suitable for test environments, you install and configure Oracle Identity Manager Server, Design Console, and Remote Manager on a single Windows machine.

The following are the high-level tasks in this scenario:

1. Install and configure Oracle Identity Manager Server on a machine after completing all the prerequisites, as described in Section 5.6, "Configuring Oracle Identity Manager Server". Ensure that the Oracle Identity Manager Server is up and running.
2. On the same machine, configure Design Console, as described in Section 5.7, "Optional: Configuring Oracle Identity Manager Design Console".
3. On the same machine, configure Remote Manager, as described in Section 5.8, "Optional: Configuring Oracle Identity Manager Remote Manager".

## 5.5 Starting the Oracle Identity Manager 11*g* Configuration Wizard

To start the Oracle Identity Manager 11*g* Configuration Wizard, execute the `<IAM_Home>/bin/config.sh` script (on UNIX) on the machine where the Administration Server is running. (`<IAM_Home>\bin\config.bat` on Windows). The Oracle Identity Management 11*g* Configuration Wizard starts, and the Welcome Screen appears.

---

**Note:** If you have extended an existing WebLogic domain to support Oracle Identity Manager, you must restart the Administration Server before starting the Oracle Identity Manager Configuration Wizard to configure Oracle Identity Manager Server, Design Console, or Remote Manager.

---

## 5.6 Configuring Oracle Identity Manager Server

This topic describes how to install and configure only Oracle Identity Manager Server. It includes the following sections:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure
- Completing the Prerequisites for Enabling LDAP Synchronization
- Running the LDAP Post-Configuration Utility
- Verifying the LDAP Synchronization
- Post-Configuration Steps
- Setting oamEnabled Parameter for Identity Virtualization Library
- Enabling LDAP Sync after Installing and Configuring Oracle Identity Manager Server at a Later Point

### 5.6.1 Appropriate Deployment Environment

Perform the configuration in this topic if you want to install Oracle Identity Manager Server on a separate host.

### 5.6.2 Components Deployed

Performing the configuration in this section deploys only Oracle Identity Manager Server.

### 5.6.3 Dependencies

The installation and configuration in this section depends on Oracle WebLogic Server, on Oracle SOA Suite, and on the installation of Oracle Identity and Access Management 11*g* software. For more information, see Preparing to Install and Installing Oracle Identity and Access Management (11.1.1.7.0).

### 5.6.4 Procedure

Perform the following steps to configure only Oracle Identity Manager Server:

1. Ensure that all the prerequisites, described in Section 5.4.1.1, "Prerequisites for Configuring Oracle Identity Manager Server", are satisfied. In addition, see Section 5.1, "Important Notes Before You Start Configuring Oracle Identity Manager".
2. On the machine where the Administration Server is running, start the Oracle Identity Manager Configuration Wizard, as described in Section 5.5, "Starting the Oracle Identity Manager 11g Configuration Wizard". The Welcome screen appears.
3. On the Welcome screen, click **Next.** The Components to Configure screen appears.

   On the Components to Configure screen, ensure that only the **OIM Server** option is selected. It is selected, by default. Click **Next**. The Database screen appears.
4. On the Database screen, enter the full path, listen port, and service name for the database in the **Connect String** field. For a single host instance, the format of connect string is `hostname:port:servicename`. For example, if the hostname is `aaa.bbb.com`, port is 1234, and the service name is `xxx.bbb.com`, then you must enter the connect string for a single host instance as follows:

   ```
   aaa.bbb.com:1234:xxx.bbb.com
   ```

   If you are using a Real Application Cluster database, the format of the database connect string is as follows:

   ```
   hostname1:port1^hostname2:port2@servicename
   ```

   **Note:** You can use the same database or different databases for creating the Oracle Identity Manager schema and the Metadata Services schema.
5. In the **OIM Schema User Name** field, enter the name of the schema that you created for Oracle Identity Manager using the Oracle Fusion Middleware Repository Creation Utility (RCU). For more information, see Section 3.2.3, "Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)".
6. In the **OIM Schema Password** field, enter the password for the Oracle Identity Manager schema that you set while creating the schema using the Oracle Fusion Middleware Repository Creation Utility (RCU).
7. If you want to use a different database for the Metadata Services (MDS) schema, select the **Select different database for MDS Schema** check box.
8. If you choose to use a different database for MDS schema, in the **MDS Connect String** field, enter the full path, listen port, and service name for the database associated with the MDS schema. For the format of the connect string, see Step 4.

   In the **MDS Schema User Name** field, enter the name of the schema that you created for AS Common Services - Metadata Services using the Oracle Fusion Middleware Repository Creation Utility (RCU). For more information, see Section 3.2.3, "Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)".

   In the **MDS Schema Password** field, enter the password for the AS Common Services - Metadata Services schema that you set while creating the schema using the Oracle Fusion Middleware Repository Creation Utility (RCU). Click **Next**. The WebLogic Admin Server screen appears.

9. On the WebLogic Admin Server screen, in the **WebLogic Admin Server URL** field, enter the URL of the WebLogic Administration Server of the domain in the following format:

   `t3://hostname:port`

   In the **UserName** field, enter the WebLogic administrator user name of the domain in which the Oracle Identity Manager application and the Oracle SOA Suite application are deployed. If you are setting up integration between Oracle Identity Manager and Oracle Access Manager, the Oracle Access Manager application is also configured in the same domain.

   In the **Password** field, enter the WebLogic administrator password of the domain in which the Oracle Identity Manager application and the Oracle SOA Suite application are deployed. Click **Next**.

   The OIM Server screen appears. The OIM Server screen enables you to set a password for the system administrator (`xelsysadm`).

10. On the OIM Server screen, in the **OIM Administrator Password** field, enter a new password for the administrator. A valid password contains at least 6 characters; begins with an alphabetic character; includes at least one number, one uppercase letter, and one lowercase letter. The password cannot contain the first name, last name, or the login name for Oracle Identity Manager.

11. In the **Confirm User Password** field, enter the new password again.

12. In the **OIM HTTP URL** field, enter the http URL that front-ends the Oracle Identity Manager application.

    The URL is of the format: `http(s)://<oim_host>:<oim_port>`. For example, `https://localhost:7002`.

13. In the **KeyStore Password** field, enter a new password for the keystore. A valid password can contain 6 to 30 characters, begin with an alphabetic character, and use only alphanumeric characters and special characters like Dollar ($), Underscore (_), and Pound (#). The password must contain at least one number.

14. In the **Confirm Keystore Password** field, enter the new password again. Click **Next**. The OIM Server screen appears.

15. Optional: To enable LDAP Sync, you must select the **Enable LDAP Sync** option on the OIM Server screen.

    ---

    **Note:** If you want to enable LDAP Sync, before enabling LDAP Sync you must complete the steps, as described in Section 5.6.5, "Completing the Prerequisites for Enabling LDAP Synchronization".

    Once LDAP Sync is enabled on the OIM Server screen and prerequisites are completed, you must continue to configure the Oracle Identity Manager Server. After you have configured the Oracle Identity Manager Server and exited the Oracle Identity Management Configuration Wizard, you must run the LDAP post-configuration utility as described in Section 5.6.6, "Running the LDAP Post-Configuration Utility".

    ---

16. After making your selections, click **Next** on the OIM Server screen. If you chose to enable LDAP Sync, the LDAP Server screen appears.

    The LDAP Server screen enables you to specify the following information:

- **Directory Server Type** - Select the desired Directory Server from the dropdown list. You have the following options:
  - OID
  - ACTIVE_DIRECTORY
  - IPLANET
  - OVD

  **Notes:**

  - IPLANET is also referred to as Oracle Directory Server Enterprise Edition (ODSEE) in this guide.
  - If you choose to use OID, ACTIVE_DIRECTORY or IPLANET as the Directory Server and if you want to integrate Oracle Identity Manager and Oracle Access Manager, you must set the `oamEnabled` parameter to `true`. To set the `oamEnabled` parameter to `true` in case of Identity Virtualization Library, see Section 5.6.9, "Setting oamEnabled Parameter for Identity Virtualization Library".

- **Directory Server ID** - enter the Directory Server ID. It can be any unique value.

  For example: `oid1` for OID, `iplanet1` for IPLANET, and `ad1` for ACTIVE_DIRECTORY
- **Server URL** - enter the LDAP URL in the format `ldap://oid_host:oid_port`.
- **Server User** - enter the user name for Directory Server administrator.

  For example: `cn=oimAdminUser,cn=systemids,dc=mycompany,dc=com`
- **Server Password** - enter the Oracle Identity Manager admin password.
- **Server SearchDN** - enter the Distinguished Names (DN). For example, `dc=exampledomain, dc=com`. This is the top-level container for users and roles in LDAP, and Oracle Identity Manager uses this container for reconciliation.

Click **Next**. The LDAP Server Continued screen appears.

17. On the LDAP Server Continued screen, enter the following LDAP information:
    - **LDAP RoleContainer** - enter a name for the container that will be used as a default container of roles in the LDAP directory. You can configure isolation rules in Oracle Identity Manager to create roles in different containers in LDAP. For example, `cn=groups, dc=mycountry, dc=com`.
    - **LDAP RoleContainer Description** - enter a description for the default role container.
    - **LDAP Usercontainer** - enter a name for the container that will be used as a default container of users in the LDAP directory. You can configure isolation rules in Oracle Identity Manager to create users in different containers in LDAP. For example, `cn=users, dc=mycountry, dc=com`.
    - **LDAP Usercontainer Description** - enter a description for the default user container.

- **User Reservation Container** - enter a name for the container that will be used for reserving user names in the LDAP directory while their creation is being approved in Oracle Identity Manager. When the user names are approved, they are moved from the reservation container to the user container in the LDAP directory. For example, `cn=reserve, dc=mycountry, dc=com`.

After enabling LDAP synchronization and after running the LDAP post-configuration utility, you can verify it by using the Oracle Identity Manager Administration Console. For more information, see Section 5.6.7, "Verifying the LDAP Synchronization". Click **Next**. The Configuration Summary screen appears.

18. If you did not choose the **Enable LDAP Sync** option on the OIM Server screen, the Configuration Summary screen appears after you enter information in the OIM Server screen.

    The Configuration Summary screen lists the applications you selected for configuration and summarizes your configuration options, such as database connect string, OIM schema user name, MDS schema user name, WebLogic Admin Server URL, WebLogic Administrator user name, and OIM HTTP URL.

    Review this summary and decide whether to start the configuration. If you want to modify any of the configuration settings at this stage, select a topic in the left navigation page and modify your choices. To continue installing this configuration of the Oracle Identity Manager Server, click **Configure**.

    > **Note:** Before configuring an application, you can save your configuration settings and preferences in a response file. Response files are text files that you can create or edit in a text editor. You can use response files to perform a silent installation or use as templates or customized settings for your environment. For more information, see Appendix F.4, "Performing a Silent Installation".

    After you click **Configure**, the Configuration Progress screen appears. Click **Next**.

    A configuration log is saved to the `logs` directory under Oracle Inventory directory. For information about the log files, see Appendix G.2, "Installation Log Files". If the Configuration Progress screen displays any errors, click **Abort** to stop the installation and restart the Oracle Identity Manager Configuration Wizard.

19. Click **Finish**.

20. Restart the WebLogic Administration Server and SOA Managed Server, as described in Appendix C.3, "Restarting Servers".

    > **Note:** If the configuration fails, click **Abort** to stop the installation and restart the Oracle Identity Manager Configuration Wizard, as described in Section 5.5, "Starting the Oracle Identity Manager 11g Configuration Wizard".

## 5.6.5 Completing the Prerequisites for Enabling LDAP Synchronization

You must complete the following prerequisites:

- Preconfiguring the Identity Store
- Creating Adapters in Oracle Virtual Directory

#### 5.6.5.1 Preconfiguring the Identity Store

Before you can use your LDAP directory as an Identity store, you must preconfigure it.

---

**Note:** Follow the steps in this section if you are using any one of the Directory Servers mentioned below for LDAP Synchronization:

- OID
- Active Directory
- iPlanet/ODSEE
- OVD

---

You must complete the following steps to preconfigure the Identity Store if you have not configured already:

1. Create User, Group and Reserve Containers.
2. Create the proxy user for OIM, namely `oimadminuser` in the Directory Server outside the search base used for OIM reconciliation. This OIM proxy user should not be reconciled into OIM Database.
3. Create the `oimadmingroup` and assign the `oimadminuser` to the group.
4. Add the ACIs to the group and user container for the OIM proxy user to have access to all entries in those containers.
5. Extend OIM Schema for non-OID Directory Servers.
   - For Active Directory
     - The OIM Schema for Active Directory is in the following location:

       ```
       $MW_HOME/oracle_common/modules/oracle.ovd_
       11.1.1/oimtemplates
       ```

     - Run the following command to extend Active Directory schema:

       On Windows:

       ```
       extendadschema.bat -h AD_host -p AD_port -D <adminis-
       trator@mydomain.com> -q -AD <dc=mydomain,dc=com> -OAM
       true -schemaFiles adUpgradeOrclIDXPerson.ldif
       ```

       On UNIX:

       ```
       sh extendadschema.sh -h AD_host -p AD_port -D adminis-
       trator@mydomain.com -q -AD dc=mydomain,dc=com -OAM true
       -schemaFiles adUpgradeOrclIDXPerson.ldif
       ```

   - For ODSEE/iPlanet
     - The OIM Schema for iPlanet (also known as ODSEE) is in the following location:

       ```
       $MW_HOME/oracle_common/modules/oracle.ovd_
       11.1.1/oimtemplates/sunOneSchema.ldif
       ```

     - Run the following command to extend ODSEE schema:

       ```
       ldapmodify -h <ODSEE Server> -p <ODSEE port> -D <ODSEE
       Admin ID> -w <ODSEE Admin password> -f sunOne-
       Schema.ldif
       ```

6. If you want to enable OAM-OIM integration, extend the following OAM Schema:
   - For OID
     - To extend OAM Schema for OID, locate the following files:

       ```
       $IAM_HOME/oam/server/oim-intg/ldif/oid/schema/OID_
       oblix_pwd_schema_add.ldif
       ```

       ```
       $IAM_HOME/oam/server/oim-intg/ldif/oid/schema/OID_
       oblix_schema_add.ldif
       ```

       ```
       $IAM_HOME/oam/server/oim-intg/ldif/oid/schema/OID_oim_
       pwd_schema_add.ldif
       ```

       ```
       $IAM_HOME/oam/server/oim-intg/ldif/oid/schema/OID_
       oblix_schema_index_add.ldif
       ```

     - Use ldapmodify from the command line to load the four LDIF files:

       ```
       cd $IAM_HOME/oam/server/oim-intg/ldif/oid/schema/
       ```

       ```
       ldapmodify -h <OID Server> -p <OID port> -D <OID Admin
       ID> -w <OID Admin password> -f OID_oblix_pwd_schema_
       add.ldif
       ```

       ```
       ldapmodify -h <OID Server> -p <OID port> -D <OID Admin
       ID> -w <OID Admin password> -f OID_oblix_schema_
       add.ldif
       ```

       ```
       ldapmodify -h <OID Server> -p <OID port> -D <OID Admin
       ID> -w <OID Admin password> -f OID_oim_pwd_schema_
       add.ldif
       ```

       ```
       ldapmodify -h <OID Server> -p <OID port> -D <OID Admin
       ID> -w <OID Admin password> -f OID_oblix_schema_index_
       add.ldif
       ```

   - For Active Directory
     - To extend OAM Schema for Active Directory, locate the following files:

       ```
       $IAM_HOME/oam/server/oim-intg/ldif/ad/schema/ADUser-
       Schema.ldif
       ```

       ```
       $IAM_HOME/oam/server/oim-intg/ldif/ad/schema/AD_oam_
       pwd_schema_add.ldif
       ```

       In both the above files, replace the domain-dn with the appropriate domain-dn value.

     - Use ldapadd from the command line to load the two LDIF files, as follows:

       ```
       cd $IAM_HOME/oam/server/oim-intg/ldif/ad/schema/
       ```

       ```
       ldapadd -h <activedirectoryhostname> -p <activedirecto-
       ryportnumber> -D <AD_administrator> -q -c -f ADUser-
       Schema.ldif
       ```

       ```
       ldapadd -h <activedirectoryhostname> -p <activedirecto-
       ryportnumber> -D <AD_administrator> -q -c -f AD_oam_
       pwd_schema.ldif
       ```

       where AD_administrator is a user which has schema extension privileges to the directory.

       For example:

```
ldapadd -h activedirectoryhost.mycompany.com -p 389 -D admin-
user -q -c -f ADUserSchema.ldif
```

- For ODSEE/iPlanet
  - To extend OAM Schema for ODSEE, locate the following files:

```
$IAM_
HOME/oam/server/oim-intg/ldif/iplanet/schema/iPlanet7_
user_index_add.ldif
```

```
$IAM_
HOME/oam/server/oim-intg/ldif/iplanet/schema/iPlanet7_
user_index_generic.ldif
```

```
$IAM_
HOME/oam/server/oim-intg/ldif/iplanet/schema/iPlanet_
oam_pwd_schema_add.ldif
```

```
$IAM_
HOME/oam/server/oim-intg/ldif/iplanet/schema/iPlanet_
user_schema_add.ldif
```

```
$IAM_
HOME/oam/server/oim-intg/ldif/iplanet/schema/iPlanet_
user_index_add.ldif
```

**Note:** If you are not sure about the which `index-root` you should use, instead of `iPlanet7_user_index_add.ldif`, please use `iPlanet7_user_index_generic.ldif` file which also has step by step instructions on finding `index-root`.

  - Use ldapmodify from the command line to load the four LDIF files:

```
cd $IAM_HOME/oam/server/oim-intg/ldif/iplanet/schema/
```

```
ldapmodify -h <ODSEE Server> -p <ODSEE port> -D <ODSEE
Admin ID> -w <ODSEE Admin password> -f iPlanet_oam_pwd_
schema_add.ldif
```

```
ldapmodify -h <ODSEE Server> -p <ODSEE port> -D <ODSEE
Admin ID> -w <ODSEE Admin password> -f iPlanet_user_
schema_add.ldif
```

```
ldapmodify -h <ODSEE Server> -p <ODSEE port> -D <ODSEE
Admin ID> -w <ODSEE Admin password> -f iPlanet_user_
index_add.ldif
```

7. If you are using Oracle Directory Server Enterprise Edition (ODSEE), you must enable `moddn` and `Changelog` properties in the ODSEE Directory Server.

   Skip this step if you are using Oracle Internet Directory (OID) or Active Directory.

**Note:** The preconfiguration differs, depending on the directory store you wish to use to hold your identity information. For a sample procedure of preconfiguring the Identity Store, refer to Appendix D, "Preconfiguring Oracle Directory Server Enterprise Edition (ODSEE)".

#### 5.6.5.2 Creating Adapters in Oracle Virtual Directory

Oracle Virtual Directory communicates with other directories through adapters.

Before you can start using Oracle Virtual Directory as an identity store, you must create adapters to each of the directories you want to use.The procedure is slightly different, depending on the directory you are connecting to.

---

**Note:** This procedure is applicable only if you are using OVD as the Directory Server. If you choose to use OID, Active Directory or Oracle Directory Server Enterprise Edition (ODSEE) as the Directory Server, the required adapters are created and configured while installing and configuring the Oracle Identity Manager server. For more information on managing the adapters, see "Managing Identity Virtualization Library (libOVD) Adapters" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

The User Management and Changelog adapters for Identity Virtualization Library configured by the Oracle Identity Manager installer are stored in `adapters.os_xml` file. The `adapters.os_xml` will be in the following location:

```
$DOMAIN_HOME/config/fmwconfig/ovd/<context>/
```

For example:

```
$DOMAIN_HOME/config/fmwconfig/ovd/oim1/adapters.os_xml
```

---

The following sections show how to create adapters for the respective directories:

- Creating Adapters for Oracle Internet Directory
- Creating Adapters for Microsoft Active Directory Server
- Creating Adapters for Oracle Directory Server Enterprise Edition (ODSEE)
- Important Notes on Changelog Plugin Configuration

##### 5.6.5.2.1 Creating Adapters for Oracle Internet Directory

**User Adapter**

Create the user adapter for Oracle Virtual Directory. Follow the steps below to create the User Adapter in Oracle Virtual Directory using Oracle Directory Services Manager.

1. Open a browser and bring up the ODSM console at `http://hostname:port/odsm`

   ---

   **Note:** The default port number is 7005.

   ---

2. Connect to Oracle Virtual Directory by using the appropriate connection entry.
3. On the Home page, click the **Adapter** tab.
4. Start the New Adapter Wizard by clicking **Create Adapter** at the top of the adapter window.
5. Create a new adapter using the New Adapter Wizard, with the following parameters:

*Table 5–1 Parameters for User Adapter Creation*

| Screen | Field | Value/Step |
|---|---|---|
| Type | **Adapter Type** | `LDAP` |
| | **Adapter Name** | `User Adapter` |
| | **Adapter Template** | `User_OID` |
| Connection | **Use DNS for Auto Discovery** | No |
| | **Host** | `idstore.mycompany.com` |
| | **Port** | 389 |
| | **Server Proxy Bind DN** | `cn=oimAdminUser,cn=systemids,dc=mycompany,dc=com` |
| | **Proxy Password** | Password for `oimadmin` user. |
| Connection Test | | Validate that the test succeeds. |
| Namespace | **Remote Base** | `dc=mycompany,dc=com` |
| | **Mapped Namespace** | `dc=mycompany,dc=com` |

Verify that the summary is correct and then click **Finish**.

6. Edit the User Adapter as follows:
   a. Select the User Adapter.
   b. Click the **Plug-ins** Tab.
   c. Click the **User Management** Plug-in, then click **Edit** in the plug-ins table. The plug-in editing window appears.
   d. In the Parameters table, update the parameter values as follows:

*Table 5–2 User Adapter Parameter Values*

| Parameter | Value |
|---|---|
| **directoryType** | `oid` |
| **pwdMaxFailure** | `10` |
| **oamEnabled** | `true` or `false`<br>Note that this parameter should be set to `true` only if you are setting up integration between Oracle Identity Manager and Oracle Access Manager at a later time. |
| **mapObjectclass** | container=`orclContainer` |

   e. Click **OK**.
   f. Click **Apply**.

### Change Log Adapter

Create the change log adapter for Oracle Virtual Directory. Follow the steps below to create the Change Log Adapter in Oracle Virtual Directory using Oracle Directory Services Manager.

1. Open a browser and bring up the ODSM console at `http://hostname:port/odsm`

**Note:** The default port number is 7005.

2. Connect to Oracle Virtual Directory by using the appropriate connection entry.
3. On the Home page, click on the **Adapter** tab.
4. Start the New Adapter Wizard by clicking **Create Adapter** at the top of the adapter window.
5. Create a new adapter using the New Adapter Wizard, with the following parameters:

***Table 5–3 Parameters for Change Log Adapter Creation***

| Screen | Field | Value/Step |
|---|---|---|
| Type | **Adapter Type** | `LDAP` |
| | **Adapter Name** | `Change Log Adapter` |
| | **Adapter Template** | `Changelog_OID` |
| Connection | **Use DNS for Auto Discovery** | No |
| | **Host** | `policystore.mycompany.com` |
| | **Port** | 389 |
| | **Server Proxy Bind DN** | `cn=oimAdminUser,cn=systemids,dc=mycompany,dc=com` |
| | **Proxy Password** | Password for `oimadmin` user |
| Connection Test | | Validate that the test succeeds |
| Namespace | **Remote Base** | Remote Base should be empty |
| | **Mapped Namespace** | `cn=changelog` |

Verify that the summary is correct, then click **Finish**.

6. To edit the change adapter follow the steps below:
   a. Select the OIM Change Log Adapter.
   b. Click the **Plug-ins** tab.
   c. In the Deployed Plus-ins table, click the **changelog** plug-in, then click **Edit** in the plug-ins table. The plug-in editing window appears.
   d. In the Parameters table, update the parameter values.

      Edit the Change Log Adapter to either add or modify the properties so that they match the values shown in the following table. You must add the `modifierDNFilter`, `sizeLimit`, and `targetDNFilter` properties to the adapter.

***Table 5–4 Changelog Adapter Parameter Values***

| Parameter | Value |
|---|---|
| **directoryType** | `oid` |
| **mapAttribute** | `targetGUID=orclguid` |
| **requiredAttribute** | `orclguid` |

*Table 5–4 (Cont.) Changelog Adapter Parameter Values*

| Parameter | Value |
|---|---|
| **modifierDNFilter** | !(modifiersname=cn=oimadmin,cn=systemids,<root suffix>)<br>**Note:** This is an example. This value can be of any Proxy DN that the customer defines.<br>For example: rootSuffix can be dc=mycompany,dc=com |
| **sizeLimit** | 1000 |
| **targetDNFilter** | Optional parameter.<br>For more information, see Section 5.6.5.2.4, "Important Notes on Changelog Plugin Configuration". |
| **oamEnabled** | true or false<br>Note that this parameter should be set to true only if you are setting up integration between Oracle Identity Manager and Oracle Access Manager at a later time. |
| **mapUserState** | true<br>For more information, see Section 5.6.5.2.4, "Important Notes on Changelog Plugin Configuration". |
| **virtualDITAdapterName** | Name of the OID User Management adapter.<br>For more information, see Section 5.6.5.2.4, "Important Notes on Changelog Plugin Configuration". |

e. Click **OK**.

f. Click **Apply**.

---

**Note:** For more information about these plug-in parameters, refer to the Understanding the Oracle Virtual Directory Plug-ins section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory 11g Release 1 (11.1.1)*.

---

### Restarting Oracle Virtual Directory

Restart Oracle Virtual Directory, as described in Appendix C, "Starting or Stopping the Oracle Stack".

#### 5.6.5.2.2 Creating Adapters for Microsoft Active Directory Server

### User Adapter

Create the user adapter for Oracle Virtual Directory. Follow these steps to create the User Adapter in Oracle Virtual Directory using Oracle Directory Services Manager.

1. Start the Administration Server and the ODSM Managed Server as described in Appendix C, "Starting or Stopping the Oracle Stack".
2. Open a browser and bring up the ODSM console at http://hostname:port/odsm

---

**Note:** The default port number is 7005.

---

3. Connect to Oracle Virtual Directory by using the appropriate connection entry.
4. On the Home page, click the **Adapter** tab.
5. Start the New Adapter Wizard by clicking **Create Adapter** at the top of the adapter window.
6. Create a new adapter using the New Adapter Wizard, with the following parameters:

***Table 5–5 Parameters for New User Adapter Creation***

| Screen | Field | Value/Step |
|---|---|---|
| Type | **Adapter Type** | `LDAP` |
| | **Adapter Name** | `User Adapter` |
| | **Adapter Template** | `User_ActiveDirectory` |
| Connection | **Use DNS for Auto Discovery** | No |
| | **Host** | Active Directory host/virtual name |
| | **Port** | Active Directory SSL port |
| | **Server Proxy Bind DN** | `cn=oimAdminUser,cn=systemids,dc=mycompany,dc=com` |
| | **Proxy Password** | Password for `oimadmin` user. |
| | **User SSL/TLS** | Selected |
| | **SSL Authentication Mode** | Server Only Authentication |
| Connection Test | | Validate that the test succeeds. |
| Namespace | **Remote Base** | `dc=mycompany,dc=com` |
| | **Mapped Namespace** | `dc=mycompany,dc=com` |

Verify that the summary is correct and then click **Finish**.

7. Edit the User Adapter as follows:
   a. Select the OIM User Adapter.
   b. Click the **Plug-ins** Tab.
   c. Click the **User Management** Plug-in, then click **Edit** in the plug-ins table. The plug-in editing window appears.
   d. In the Parameters table, update the parameter values as follows:

***Table 5–6 User Adapter Parameter Values***

| Parameter | Value |
|---|---|
| **directoryType** | `activedirectory` |
| **mapAttribute** | `orclguid=objectGuid` |
| **mapAttribute** | `uniquemember=member` |
| **addAttribute** | `user,samaccountname=%uid%,%orclshortuid%` |
| **mapAttribute** | `mail=userPrincipalName` |

*Table 5–6 (Cont.) User Adapter Parameter Values*

| Parameter | Value |
|---|---|
| **mapAttribute** | `ntgrouptype=grouptype` |
| **mapObjectclass** | `groupofUniqueNames=group` |
| **mapObjectclass** | `inetOrgPerson=user` |
| **mapObjectclass** | `orclidxperson=user` |
| **mapPassword** | `true` |
| **exclusionMapping** | `orclappiduser,uid=samaccountname` |
| **pwdMaxFailure** | `10` |
| **oamEnabled** | `true` or `false`<br>Note that this parameter should be set to `true` only if you are setting up integration between Oracle Identity Manager and Oracle Access Manager at a later time. |
| **oimLanguages** | For language support, you need to edit the User Management plugin to add a new configuration parameter `oimLanguages`.<br>See "Important Notes on User Management Plugin Configuration". |

e. Click **OK**.

f. Click **Apply**.

### Important Notes on User Management Plugin Configuration

**oimLanguages attribute**: For language support, you need to edit the User Management plugin to add a new configuration parameter `oimLanguages`.

For example, if the Managed Localization for the `DisplayName` while creating the User in OIM is selected as `French`, then the value for `oimLanguages` in the User Management adapter plugin should be `fr`. If you have other languages to be supported, say Japanese, then the value for the parameter should be `fr,ja`.

This parameter is functional only when the `directoryType` parameter is set to `activedirectory`.

The User Management plugin has the following configuration parameters:

`oimLanguages` , <separated list of language codes to be used in attribute language subtypes>.

*Table 5–7 Language Codes'for the MLS Enabled Attributes*

| Objectclasses | MLS Enabled Attributes | Language Codes |
|---|---|---|
| orclIDXPerson | `cn, sn, givenName, middleName, displayName, o, ou, title, postalAddress, st, description, orclGenerationQualifier` | `sq,ar,as,az,bn,bg, be,ca,zh-CN,zh-TW, hr,cs,da,nl,en,et, fi,fr,de,el,gu,he, hi,hu,is,id,it,ja, kn,kk,ko,lv,lt,mk, ms,ml,mr,no,or,pl, pt,pt-BR,pa,ro,ru, sr,sk,sl,es,sv,ta, te,th,tr,uk,uz,vi` |

*Table 5–7 (Cont.) Language Codes'for the MLS Enabled Attributes*

| Objectclasses | MLS Enabled Attributes | Language Codes |
|---|---|---|
| orclIDXGroup | cn, displayName, description | sq, ar, as, az, bn, bg, be, ca, zh-CN, zh-TW, hr, cs, da, nl, en, et, fi, fr, de, el, gu, he, hi, hu, is, id, it, ja, kn, kk, ko, lv, lt, mk, ms, ml, mr, no, or, pl, pt, pt-BR, pa, ro, ru, sr, sk, sl, es, sv, ta, te, th, tr, uk, uz, vi |

**Note:** If you are using Identity Virtualization Library, then see "Managing Identity Virtualization Library (libOVD) Adapters" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

### Change Log Adapter

Follow the steps below to create the Change Log Adapter in Oracle Virtual Directory using Oracle Directory Services Manager.

1. Open a browser and bring up the ODSM console at `http://hostname:port/odsm`

   **Note:** The default port number is 7005.

2. Connect to Oracle Virtual Directory by using the appropriate connection entry.
3. On the Home page, click on the **Adapter** tab.
4. Start the New Adapter Wizard by clicking **Create Adapter** at the top of the adapter window.
5. Create a new adapter using the New Adapter Wizard, with the following parameters:

*Table 5–8 Parameters for New Change Log Adapter Creation*

| Screen | Field | Value/Step |
|---|---|---|
| Type | **Adapter Type** | LDAP |
| | **Adapter Name** | OIM Change Log Adapter |
| | **Adapter Template** | Changelog_ActiveDirectory |
| Connection | **Use DNS for Auto Discovery** | No |
| | **Host** | Active Directory host/virtual name |
| | **Port** | 389 |

*Table 5–8 (Cont.) Parameters for New Change Log Adapter Creation*

| Screen | Field | Value/Step |
|---|---|---|
| | **Server Proxy Bind DN** | `cn=oimAdminUser,cn=systemids,dc=mycompany,dc=com` |
| | **Proxy Password** | Password for `oimadmin` user |
| Connection Test | | Validate that the test succeeds |
| Namespace | **Remote Base** | Remote Base should be empty |
| | **Mapped Namespace** | `cn=changelog` |

Verify that the summary is correct and then click **Finish**.

6. To edit the change adapter follow the steps below:
   a. Select the OIM Change Log Adapter.
   b. Click the **Plug-ins** tab.
   c. In the Deployed Plus-ins table, click the **changelog** plug-in, then click **Edit** in the plug-ins table. The plug-in editing window appears.
   d. In the Parameters table, update the parameter values.

      Edit the Change Log Adapter to either add or modify the properties so that they match the values shown in Table 5–9. You must add the `sizeLimit`, and `targetDNFilter` properties to the adapter.

*Table 5–9 Changelog Adapter Parameter Values*

| Parameter | Value |
|---|---|
| **directoryType** | `activedirectory` |
| **mapAttribute** | `targetGUID=objectGuid` |
| **requiredAttribute** | samaccountname |
| **sizeLimit** | 1000 |
| **targetDNFilter** | Optional parameter.<br>For more information, see Section 5.6.5.2.4, "Important Notes on Changelog Plugin Configuration" . |
| **oamEnabled** | `true` or `false`<br>Note that this parameter should be set to `true` only if you are setting up integration between Oracle Identity Manager and Oracle Access Manager at a later time. |
| **mapUserState** | `true`<br>For more information, see Section 5.6.5.2.4, "Important Notes on Changelog Plugin Configuration" . |
| **virtualDITAdapterName** | The name of the User adapter<br>For more information, see Section 5.6.5.2.4, "Important Notes on Changelog Plugin Configuration". |

**Note:** The parameter **modifierDNFilter** should not be added to Active Directory Changelog plugin adapter.

   e. Click **OK**.

f. Click **Apply**.

#### 5.6.5.2.3 Creating Adapters for Oracle Directory Server Enterprise Edition (ODSEE)

### User Adapter

Create the user adapter for Oracle Virtual Directory. Follow the steps below to create the User Adapter in Oracle Virtual Directory using Oracle Directory Services Manager.

1. Start the Administration Server and the ODSM Managed Server as described in Appendix C, "Starting or Stopping the Oracle Stack".
2. Open a browser and bring up the ODSM console at `http://hostname:port/odsm`

> **Note:** The default port number is 7005.

3. Connect to Oracle Virtual Directory by using the appropriate connection entry.
4. On the Home page, click on the **Adapter** tab.
5. Start the New Adapter Wizard by clicking on **Create Adapter** at the top of the adapter window.
6. Create a new adapter using the New Adapter Wizard, with the following parameters:

***Table 5–10 Parameters for New User Adapter Creation***

| Screen | Field | Value/Step |
|---|---|---|
| Type | **Adapter Type** | `LDAP` |
| | **Adapter Name** | `User Adapter` |
| | **Adapter Template** | `User_SunOne` |
| Connection | **Use DNS for Auto Discovery** | No |
| | **Host** | Sun Java System Directory Server host/virtual name |
| | **Port** | Sun Java System Directory Server port |
| | **Server Proxy Bind DN** | `cn=oimAdminUser,cn=systemids,dc=mycompany,dc=com` |
| | **Proxy Password** | Password for `oimadmin` user (`cn=oimAdminUser,cn=systemids,dc=mycompany,dc=com`) |
| Connection Test | | Validate that the test succeeds. |
| Namespace | **Remote Base** | `dc=mycompany,dc=com` |
| | **Mapped Namespace** | `dc=mycompany,dc=com` |

Verify that the summary is correct and then click **Finish**.

**Note:** For information about creating Oracle Identity Manager user adapter by using Oracle Directory Services Manager, refer to the "Creating LDAP Adapters" topic in the *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.

7. Edit the User Adapter as follows:
   a. Select the OIM User Adapter.
   b. Click the **Plug-ins** Tab.
   c. Click the **User Management** Plug-in, then click **Edit** in the plug-ins table. The plug-in editing window appears.
   d. In the Parameters table, update the parameter values as follows:

***Table 5–11 User Adapter Parameter Values***

| Parameter | Value |
|---|---|
| **directoryType** | `sunone` |
| **mapAttribute** | `orclGUID=nsUniqueID` |
| **mapObjectclass** | `container=nsContainer` |
| **pwdMaxFailure** | `10` |
| **oamEnabled** | `true` or `false`<br>Note that this parameter should be set to `true` only if you are setting up integration between Oracle Identity Manager and Oracle Access Manager at a later time. |

   e. Click **OK**.
   f. Click **Apply**.

### Change Log Adapter

Follow the steps below to create the Change Log Adapter in Oracle Virtual Directory using Oracle Directory Services Manager.

1. Open a browser and bring up the ODSM console at `http://hostname:port/odsm`

**Note:** The default port number is 7005.

2. Connect to Oracle Virtual Directory by using the appropriate connection entry.
3. On the Home page, click on the **Adapter** tab.
4. Start the New Adapter Wizard by clicking on **Create Adapter** at the top of the adapter window.
5. Create a new adapter using the New Adapter Wizard, with the following parameters:

***Table 5–12 Parameters for New Change Log Adapter Creation***

| Screen | Field | Value/Step |
|---|---|---|
| Type | **Adapter Type** | `LDAP` |

*Table 5–12 (Cont.) Parameters for New Change Log Adapter Creation*

| Screen | Field | Value/Step |
|---|---|---|
| | **Adapter Name** | `OIM Change Log Adapter` |
| | **Adapter Template** | `Changelog_SunOne` |
| Connection | **Use DNS for Auto Discovery** | No |
| | **Host** | Sun Java System Directory Server host virtual name |
| | **Port** | Sun Java System Directory Server port |
| | **Server Proxy Bind DN** | `cn=oimAdminUser,cn=systemids,dc=mycompany,dc=com` |
| | **Proxy Password** | Password for `oimadmin` user.<br>(`cn=oimAdminUser,cn=systemids,dc=mycompany,dc=com`) |
| Connection Test | | Validate that the test succeeds. |
| Namespace | **Remote Base** | |
| | **Mapped Namespace** | `cn=changelog` |

Verify that the summary is correct, then click **Finish**.

---

**Note:** For information about creating Oracle Identity Manager user adapter by using Oracle Directory Services Manager, refer to the "Creating LDAP Adapters" topic in the *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.

---

6. To edit the change adapter follow the steps below:
   a. Select the OIM Change Log Adapter.
   b. Click the **Plug-ins** tab.
   c. In the Deployed Plus-ins table, click the **changelog** plug-in, then click **Edit** in the plug-ins table. The plug-in editing window appears.
   d. In the Parameters table, update the parameter values.

      Edit the Change Log Adapter to either add or modify the properties so that they match the values shown in the following table. You must add the `mapObjectclass`, `modifierDNFilter`, `sizeLimit`, and `targetDNFilter` properties to the adapter.

*Table 5–13 Changelog Adapter Parameter Values*

| Parameter | Value |
|---|---|
| **directoryType** | `sunone` |
| **mapAttribute** | `targetGUID=targetUniqueID` |
| **mapObjectclass** | `changelog=changelogentry` |

*Table 5–13 (Cont.) Changelog Adapter Parameter Values*

| Parameter | Value |
|---|---|
| **modifierDNFilter** | `!(modifiersname=cn=oimadmin,cn=systemids,<root suffix>)`<br>Note : This is an example. This value can be of any Proxy DN that the customer defines.<br>For example: rootSuffix can be `dc=mycompany,dc=com` |
| **sizeLimit** | 1000 |
| **virtualDITAdapterName** | Name of the iPlanet User Management adapter.<br>For more information, see Section 5.6.5.2.4, "Important Notes on Changelog Plugin Configuration". |
| **targetDNFilter** | Optional parameter.<br>For more information, see Section 5.6.5.2.4, "Important Notes on Changelog Plugin Configuration". |
| **oamEnabled** | `true` or `false`<br>Note that this parameter should be set to `true` only if you are setting up integration between Oracle Identity Manager and Oracle Access Manager at a later time. |
| **mapUserState** | `true`<br>For more information, see Section 5.6.5.2.4, "Important Notes on Changelog Plugin Configuration". |

**e.** Click **OK**.

**f.** Click **Apply**.

---

**Note:** For more information about these plug-in parameters, refer to the Understanding the Oracle Virtual Directory Plug-ins section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory 11g Release 1 (11.1.1)*.

---

#### 5.6.5.2.4 Important Notes on Changelog Plugin Configuration

- The **virtualDITAdapterName** parameter must be added after the changelog adapter is created.

  **virtualDITAdapterName** identifies the corresponding user profile adapter name. For example, in a single-directory deployment, you can set this parameter value to `A1`, which is the user adapter name.

  If you set this parameter **virtualDITAdapterName** to `A1`, the plug-in fetches the **mapAttribute** and **mapObjectclass** configuration in the UserManagementPlugin of adapter `A1`, so you do not have to duplicate those configurations.

  This configuration is a must for **directoryType**=`ActiveDirectory` for the GUID mapping to happen in the case of incremental reconciliation to avoid the missing required attribute exception. (`LDAP GUID=null`).

  Add the attribute **virtualDITAdapterName** and set it to the value of the Active Directory User Management adapter name in the Active Directory changelog plugin. This is required to pick up the attribute mappings set in the Active Directory User Management adapter plugin as the Active Directory schema and OIM schema are different.

- **targetDNFilter** attribute should be set if you want to perform reconciliation from a certain user container and group container instead of from the root suffix.

  These values should be the ones entered for User Container and Role Container during the configuration of Oracle Identity Manager when LDAP Sync is enabled.

  For example:

  targetDNFilter : `cn=Users,dc=mycountry,dc=mycompany,dc=com`

  targetDNFilter : `cn=Groups,dc=mycountry,dc=mycompany,dc=com`

  These settings would pull in/reconcile all users and groups from the above mentioned containers in the backend Directory Server.

- The changelog adapter plugin should always have the attribute **mapUserState** set to `true` for the attribute **orclaccountenabled** to return in the search result.

> **Note:** If you are using Identity Virtualization Library, then see "Managing Identity Virtualization Library (libOVD) Adapters" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.
>
> For more information about these plug-in parameters, refer to the "Understanding the Oracle Virtual Directory Plug-ins" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory 11g Release 1 (11.1.1)*.

## 5.6.6 Running the LDAP Post-Configuration Utility

You must run the LDAP post-configuration utility after you have configured the Oracle Identity Manager Server and exited the Oracle Identity Management Configuration Wizard. The LDAP configuration post-setup script enables all the LDAP Sync-related incremental Reconciliation Scheduler jobs, which are disabled by default.

> **Note:** This procedure is applicable to all the Directory Server options. The LDAP post-configuration utility must be run after configuring Oracle Identity Manager server. This procedure is required only if you chose to enable and configure LDAP Sync during the Oracle Identity Manager Server configuration.

### Setting Up Environment Variables

Before you run the LDAP post-configuration utility, you must ensure that the following environment variables are set:

- *APP_SERVER* - is set to the application server on which Oracle Identity Manager is running. Set `APP_SERVER` to `weblogic`.
- *JAVA_HOME* - is set to the directory where the JDK is installed on your machine.
- *MW_HOME* - is set to the Middleware home path provided during the Oracle Identity Manager installation.
- *OIM_ORACLE_HOME* - is set to the directory where Oracle Identity Manager is deployed.

  For example:

On UNIX, it is the <MW_HOME>/IAM_Home directory.

On Windows, it is the <MW_HOME>\IAM_Home directory.

- *WL_HOME* - is set to the wlserver_10.3 directory under your Middleware Home.

  For example:

  On UNIX, it is the <MW_HOME>/wlserver_10.3 directory.

  On Windows, it is the <MW_HOME>\wlserver_10.3 directory.

- *DOMAIN_HOME* - is set to the domain of the WebLogic Server.

  For example:

  On UNIX, it is the <MW_HOME>/user_projects/domains/base_domain directory.

  On Windows, it is the <MW_HOME>\user_projects\domains\base_domain directory.

### Running the LDAP Post-Configuration Utility

Run the LDAP post-configuration utility as follows:

1. Open the ldapconfig.props file in a text editor. This file is located in the server/ldap_config_util directory under the IAM_Home for Oracle Identity and Access Management.
2. In the ldapconfig.props file, set values for the following parameters:
   - **OIMServerType** - Specify the application server on which Oracle Identity Manager is deployed.

     For example:

     ```
     OIMServerType=WLS
     ```

   - **OIMProviderURL** - Specify the URL for the OIM provider.

     If the OIMServerType is WLS, then

     ```
     OIMProviderURL=t3://localhost:ManagedServerPort
     ```

     For example:

     ```
     OIMProviderURL=t3://localhost:14000
     ```

   - **LDAPURL** - Specify the URL for the OVD instance.

     If OVD server is selected during Oracle Identity Manager installation, then provide value for LDAPURL. If OVD server is not selected during Oracle Identity Manager installation, then leave LDAPURL blank.

     ```
     LDAPURL=ldap://<OVD server>:<OVD Port>
     ```

     For example:

     ```
     LDAPURL=ldap://OVDserver.examplehost.exampledomain.com:650
     1
     ```

**Note:** If you have selected Active Directory or ODSEE as the directory server during Oracle Identity Manager installation, after enabling LDAPSync, do not specify the value for the `LDAPURL` parameter. Leave `LDAPURL` blank. For example: `LDAPURL=`

Enter OVD server and OVD port number and specify the URL as value only if you are using Oracle Virtual Directory (OVD) as the directory server.

- **LDAPAdminUsername** - Specify the user name for the OVD Administrator.

  If OVD server is selected during Oracle Identity Manager installation, then provide the Admin user name to connect to LDAP/OVD Server.

  For example:

  ```
  LDAPAdminUsername=cn=oimAdminUser,cn=systemids,dc=mycompan
  y,dc=com
  ```

  **Notes:**

  - `LDAPAdminUsername` is the name of user used to connect to Identity Store. For example: `cn=oimAdminUser,cn=systemids,dc=mycompany,dc=com`

    This `LDAPAdminUsername` should not be located in the user container where customer's user accounts reside. For example: `cn=Users,cn=oracleAccounts,dc=mycompany,dc=com`. This user should be outside the search scope in order to avoid reconciliation of this user into OIM.

  - If you have selected Active Directory or ODSEE as the directory server during Oracle Identity Manager installation, after enabling LDAPSync, do not specify the value for the `LDAPAdminUsername` parameter. Leave `LDAPAdminUsername` blank. For example: `LDAPAdminUsername=`

    Enter the OVD user admin name as value only if you are using Oracle Virtual Directory (OVD) as the directory server.

- **LIBOVD_PATH_PARAM** - Specify the configuration directory path of libOVD.

  If OVD server is not selected during Oracle Identity Manager installation, then provide the following value for this parameter:

  ```
  LIBOVD_PATH_PARAM=<Middleware_Home>/user_
  projects/domains/base_domain/config/fmwconfig/ovd/oim
  ```

**Notes:**

- If you have selected Active Directory or ODSEE as the directory server during Oracle Identity Manager installation, after enabling LDAPSync, specify the value for this property similar to the example given above.
- If OVD server is selected during Oracle Identity Manager installation, then leave this parameter blank. For example: `LIBOVD_PATH_PARAM=`

- **ChangeLogNumber** - Leave this parameter blank.

3. Ensure the required environment variables are set, as described in "Setting Up Environment Variables".
4. Start the Oracle Identity Manager Managed Server. For more information, see Section 5.3, "Starting the Servers".
5. The utility and the properties files are located in the `server/ldap_config_util` directory under your `IAM_Home`. `IAM_Home` is the Oracle Identity and Access Management home directory for Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Entitlements Server, and Oracle Identity Navigator.

   On the command line, run the LDAP configuration post-setup script as follows:

   On Windows:

   `LDAPConfigPostSetup.bat` <location of the directory containing the `ldapconfig.props` file>

   For example:

   ```
   LDAPConfigPostSetup.bat c:\Oracle\Middleware\IAM_
   Home\server\ldap_config_util
   ```

   On UNIX:

   `LDAPConfigPostSetup.sh` <location of the directory containing the `ldapconfig.props` file>

   For example:

   ```
   LDAPConfigPostSetup.sh <MW_Home>/IAM_Home/server/ldap_config_
   util
   ```

6. When prompted, enter the OIM administrator's password and the LDAP administrator password as applicable.

**Notes:**

- If you have selected Active Directory or ODSEE as the directory server during Oracle Identity Manager installation, then after enabling LDAPSync when you run this utility, it will prompt only for the **OIM admin password**. This OIM admin password is the `xelsyadm` password.
- If you have selected OVD as the directory server during Oracle Identity Manager installation, then after enabling LDAPSync when you run this utility, it will prompt for following passwords:

  **LDAP admin password**- LDAP admin password is the OVD server's admin password.

  **OIM admin password**- LDAP admin password is the `xelsyadm` password.

### 5.6.7 Verifying the LDAP Synchronization

To verify the configuration of LDAP with Oracle Identity Manager, complete the following steps:

1. Ensure that the WebLogic Administration Server is up and running.
2. Invoke the Oracle Identity Manager Administration Console (`http://<host>:<port>/oim`), which is deployed on the Administration Server.
3. In this console, click **Search** under **Configurations** -> **Manage IT Resource**. If the LDAP information is correct, the resource information is displayed.

   For more information, see "Managing IT Resources" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
4. Create a normal user using the same console.
5. If a user is created, verify the creation in the chosen LDAP store or OVD using any ldap client.

**Note:** Ensure that the chosen Directory server or OVD and Oracle Identity Manager are up and running.

### 5.6.8 Post-Configuration Steps

After installing and configuring Oracle Identity Manager Server, you must complete the following manual steps:

- Set the *XEL_HOME* variable in the setenv script (`setenv.bat` on Windows, and `setenv.sh` on UNIX) as follows:

  On Windows: Open the `<IAM_Home>\server\bin\setenv.bat` file and search for *XEL_HOME* variable. Update the path of the *XEL_HOME* variable to the absolute path of `<IAM_Home>\server`. For example, if your IDM_Home is the `C:\oracle\Middleware\IAM_Home` directory, then set *XEL_HOME* in the `setenv.bat` file to the `C:\oracle\Middleware\IAM_Home\server` directory.

  On UNIX: Open the `<IAM_Home>/server/bin/setenv.sh` file and search for *XEL_HOME* variable.Update the path of the *XEL_HOME* variable to the absolute

path of <IAM_Home>/server. For example, if your IDM_Home is the /test/Middleware/IAM_Home directory, then set *XEL_HOME* in the setenv.sh file to the /test/Middleware/IAM_Home/server directory.

### 5.6.9 Setting oamEnabled Parameter for Identity Virtualization Library

Follow these steps for setting oamEnabled parameter. You must set oamEnabled parameter to true only if you want to integrate Oracle Identity Manager and Oracle Access Manager at a later time. This procedure applies only if you use Identity Virtualization Library.

1. Log in into Oracle Enterprise Manager Fusion Middleware Control at

   http://adminvhn.mycompany.com:7001/em as user weblogic.

2. Right click on **Oim(11.1.1.3.0)**, and click **System Mbean Browser**.
3. Go to: **Application defined MBeans** -> **com.oracle** -> **Domain:base_domain** -> **OVD**
4. There are two **AdaptersConfig** options. Click on the one that has a plus (+) symbol, indicating a subtree. Then click on **OVDAdaptersConfig**. You should see **CHANGELOG_oid1** and **oid1**.
5. Configure **oamenabled** in both the adapters.

   Follow these steps to configure oamenabled in the **Changelog** adapter:

   a. Click on **CHANGELOG_oid1** and keep going down the tree until the very end. You should see **changelog** with a bean symbol. Double click on **changelog**.

   b. Click on the **operations** subtab.

   c. Click on **removeParam operation**.

   d. Enter oamEnabled in the textbox and click **invoke**. It should give you a **false** or a **true**.

   e. Return to the original page with **operations**.

   f. Click on **AddParam** operation.

   g. Edit the names and values to contain **oamEnabled** and **true**.

   h. Click **invoke** to complete the addParam operation.

   Follow these steps to configure oamenabled in the **Usermanagement** adapter:

   a. Click on **oid1** and keep going down the tree until the very end. You should see **oid1** with a bean symbol. Double click on **oid1**.

   b. Click on the **operations** subtab.

   c. Click on **removeParam operation**.

   d. Enter oamEnabled in the textbox and click **invoke**. It should give you a **false** or a **true**.

   e. Return to the original page with **operations**.

   f. Click on **AddParam** operation.

   g. Edit the names and values to contain **oamEnabled** and **true**.

   h. Click **invoke** to complete the addParam operation.

6. Restart Oracle Identity Manager Managed Server and SOA Managed Server.

### 5.6.10 Enabling LDAP Sync after Installing and Configuring Oracle Identity Manager Server at a Later Point

LDAP Sync can be enabled at any point after installing and configuring Oracle Identity Manager Server. For more infromation on enabling LDAP Sync after installing and configuring Oracle Identity Manager Server, see "Enabling LDAP Synchronization" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

## 5.7 Optional: Configuring Oracle Identity Manager Design Console

This topic describes how to install and configure only Oracle Identity Manager Design Console, which is supported on Windows operating systems only.

It includes the following sections:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure
- Post-Configuration Steps
- Updating the xlconfig.xml File to Change the Port for Design Console
- Configuring Design Console to Use SSL

### 5.7.1 Appropriate Deployment Environment

Perform the installation and configuration in this topic if you want to install Oracle Identity Manager Design Console on a separate Windows machine where Oracle Identity Manager Server is not configured. For more information, see Section 5.4.2.2, "Scenario 1: Oracle Identity Manager Server and Design Console on Different Machines".

### 5.7.2 Components Deployed

Performing the installation and configuration in this section deploys only Oracle Identity Manager Design Console on the Windows operating system.

### 5.7.3 Dependencies

The installation and configuration in this section depends on the installation of Oracle Identity and Access Management 11*g* software and on the configuration of Oracle Identity Manager Server. For more information, see Section 3.2.7, "Installing Oracle Identity and Access Management (11.1.1.7.0)" and Section 5.6, "Configuring Oracle Identity Manager Server".

### 5.7.4 Procedure

Perform the following steps to install and configure only Oracle Identity Manager Design Console on the Windows operating system:

1. Ensure that all the prerequisites, described in Section 5.4.1.2, "Prerequisites for Configuring Only Oracle Identity Manager Design Console on a Different Machine", are satisfied. In addition, see Section 5.1, "Important Notes Before You Start Configuring Oracle Identity Manager".

2. On the Windows machine where Oracle Identity Manager Design Console should be configured, start the Oracle Identity Manager Configuration Wizard, as described in Section 5.5, "Starting the Oracle Identity Manager 11g Configuration Wizard". The Welcome screen appears.
3. On the Welcome screen, click **Next.** The Components to Configure screen appears.

   On the Components to Configure screen, select only the **OIM Design Console** check box. Click **Next**. The OIM Server Host and Port screen appears.
4. On the OIM Server Host and Port screen, enter the host name of the Oracle Identity Server Manager Server in the **OIM Server Hostname** field. In the **OIM Server Port** field, enter the port number for the Oracle Identity Manager Server on which the Oracle Identity Manager application is running. Click **Next**. The Configuration Summary screen appears.

   The Configuration Summary screen lists the application that you selected for configuration and summarizes your configuration options, such as OIM Server host name and port.

   Review this summary and decide whether to start the configuration. If you want to modify any of the configuration settings at this stage, select a topic in the left navigation page and modify your choices. To continue installing this configuration of the Oracle Identity Management Design Console, click **Configure**.

   **Note:** Before configuring an application, you can save your configuration settings and preferences in a response file. Response files are text files that you can create or edit in a text editor. You can use response files to perform a silent installation or use as templates or customized settings for your environment. For more information, see Appendix F.4, "Performing a Silent Installation".

   After you click **Configure**, the Configuration Progress screen appears. A configuration log is saved to the `logs` directory under Oracle Inventory directory. For information about the log files, see Appendix G.2, "Installation Log Files". If the Configuration Progress screen displays any errors, click **Abort** to stop the installation and restart the Oracle Identity Manager Configuration Wizard.
5. Click **Finish**.

   **Note:** If the configuration fails, click **Abort** to stop the installation and restart the Oracle Identity Manager Configuration Wizard, as described in Section 5.5, "Starting the Oracle Identity Manager 11g Configuration Wizard".

### 5.7.5 Post-Configuration Steps

Complete the following steps after configuring the Oracle Identity Manager Design Console on the Windows operating system:

1. On the machine where Oracle WebLogic Server is installed (the machine where Oracle Identity Manager Server is installed), create the `wlfullclient.jar` file as follows:
   a. Use the `cd` command to move from your present working directory to the `<MW_HOME>\wlserver_10.3\server\lib` directory.
   b. Ensure that *JAVA_HOME* is set, as in the following example:

`D:\oracle\<MW_HOME>\jdk160_24`

To set this variable, right-click the **My Computer** icon and select **Properties**. The System Properties screen is displayed. Click the **Advanced** tab and click the **Environment Variables** button. The Environment Variables screen is displayed. Ensure that the *JAVA_HOME* variable in the **User Variables** section is set to the path of the JDK directory installed on your machine.

After setting the *JAVA_HOME* variable, select the **Path** variable in the System Variables section on the same Environment Variables screen, and click **Edit**. The Edit System Variable dialog box is displayed. In the **variable value** field, enter the complete path to your *JAVA_HOME*, such as `D:\oracle\<MW_HOME>\jdk160_24`, preceded by a semicolon (**;**). The semicolon is used as the delimiter for multiple paths entered in this field.

**c.** After verifying the values, click **OK**.

2. Use the following steps to create a `wlfullclient.jar` file for JDK 1.6 client application:

   **a.** Change directories to the `server/lib` directory.

   `cd` WL_HOME`/server/lib`

   **b.** Use the following command to create `wlfullclient.jar` in the `server/lib` directory:

   ```
   java -jar wljarbuilder.jar
   ```

   This command generates the `wlfullclient.jar` file.

3. Copy the `wlfullclient.jar` file to the `<IAM_Home>\designconsole\ext\` directory on the machine where Design Console is configured.
4. Ensure that the Administration Server and the Oracle Identity Manager Managed Server are started. For information about starting the servers, see Starting the Stack.
5. Start the Design Console client by running the `xlclient.cmd` executable script, which is available in the `<IAM_Home>\designconsole\` directory.
6. Log in to the Design Console with your Oracle Identity Manager user name and password.

## 5.7.6 Updating the xlconfig.xml File to Change the Port for Design Console

To update the `xlconfig.xml` file and start the Design Console on a new port as opposed to what was set during configuration, complete the following steps:

1. In a text editor, open the `<IAM_Home>\designconsole\config\xlconfig.xml` file.
2. Edit the following tags:
   - `ApplicationURL`
   - `java.naming.provider.url`
3. Change the port number.
4. Restart the Design Console.

**Note:** You do not have to perform this procedure during installation. It is required if you want to change ports while using the product. You must ensure that the Oracle Identity Manager server port is changed to this new port before performing these steps.

### 5.7.7 Configuring Design Console to Use SSL

To configure the Design Console to use SSL, complete the following steps:

1. Add the WebLogic Server jar files required to support SSL by copying the `webserviceclient+ssl.jar` file from the `<WL_HOME>/server/lib` directory to the `<IAM_Home>/designconsole/ext` directory.
2. Use the server trust store in Design Console as follows:
   a. Log in to the Oracle WebLogic Administration Console using the WebLogic administrator credentials.
   b. Under **Domain Structure**, click **Environment** > **Servers**. The Summary of Servers page is displayed.
   c. Click on the Oracle Identity Manager server name (for example, `oim_server1`). The Settings for `oim_server1` is displayed.
   d. Click the **Keystores** tab.
   e. From the **Trust** section, note down the path and file name of the trust keystore.
3. Set the `TRUSTSTORE_LOCATION` environment variable as follows:
   - If Oracle Identity Manager Design Console and Oracle Identity Manager Server are installed and configured on the same machine, set the `TRUSTSTORE_LOCATION` environment variable to the location of the trust keystore that you noted down.

     For example, `setenv TRUSTSTORE_LOCATION=/test/DemoTrust.jks`
   - If Oracle Identity Manager Design Console and Oracle Identity Manager Server are installed and configured on different machines, copy the trust keystore file to the machine where Design Console is configured. Set the `TRUSTSTORE_LOCATION` environment variable to the location of the copied trust keystore file on the local machine.
4. If the Design Console was installed without SSL enabled, complete the following steps:
   a. Open the `<IAM_Home>/designconsole/config/xlconfig.xml` file in a text editor.
   b. Edit the `<ApplicationURL>` entry to use HTTPS, T3S protocol, and SSL port to connect to the server, as in the following example:

```
<ApplicationURL>https://<host>:<sslport>/xlWebApp/loginWorkflowRenderer.do</ApplicationURL>
```

**Note:** For a clustered installation, you can send an https request to only one of the servers in the cluster, as shown in the following element:

```
<java.naming.provider.url>t3s://<host>:<sslport></ja
va.naming.provider.url>
```

c. Save the file and exit.

5. Specify Java permissions for Crypto-J librairies as follows:

   a. Open the *IAM_HOME*/designconsole/config/xl.policy file in a text editor.

   b. Add the following at the end and save the file.

```
grant codeBase "file:MW_HOME/modules/cryptoj.jar"{permission
java.security.AllPermission;};
```

## 5.8 Optional: Configuring Oracle Identity Manager Remote Manager

This topic describes how to install and configure only Oracle Identity Manager Remote Manager. It includes the following sections:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

### 5.8.1 Appropriate Deployment Environment

Perform the installation and configuration in this topic if you want to install Oracle Identity Manager Remote Manager on a separate machine. For more information, see Section 5.4.2.3, "Scenario 2: Oracle Identity Manager Server and Remote Manager on Different Machines".

### 5.8.2 Components Deployed

Performing the installation and configuration in this section deploys only Oracle Identity Manager Remote Manager.

### 5.8.3 Dependencies

The installation and configuration in this section depends on the installation of Oracle Identity and Access Management 11*g* software and on the configuration of Oracle Identity Manager Server. For more information, see Section 3.2.7, "Installing Oracle Identity and Access Management (11.1.1.7.0)" and Section 5.4.1.3, "Prerequisites for Configuring Only Oracle Identity Manager Remote Manager on a Different Machine".

### 5.8.4 Procedure

Perform the following steps to install and configure only Oracle Identity Manager Remote Manager:

1. Ensure that all the prerequisites, described in Section 5.4.1.3, "Prerequisites for Configuring Only Oracle Identity Manager Remote Manager on a Different

Machine", are satisfied. In addition, see Section 5.1, "Important Notes Before You Start Configuring Oracle Identity Manager".

2. On the machine where Oracle Identity Manager Remote Manager should be configured, start the Oracle Identity Manager Configuration Wizard, as described in Section 5.5, "Starting the Oracle Identity Manager 11g Configuration Wizard". The Welcome screen appears.
3. On the Welcome screen, click **Next.** The Components to Configure screen appears.

   On the Components to Configure screen, select only the **OIM Remote Manager** check box. Click **Next**. The Remote Manager screen appears.
4. On the Remote Manager screen, enter the service name in the **Service Name** field. Oracle Identity Manager Remote Manager will be registered under this service name. The service name is used with the Registry URL to a build fully qualified service name, such as `rmi://host:RMI Registry Port/service name`.
5. In the **RMI Registry Port** field, enter the port number on which the RMI registry should be started. The default port number is 12345.
6. In the **Listen Port (SSL)** field, enter the port number on which a secure socket is opened to listen to client requests. The default port number is 12346. Click **Next**. The Keystore Password screen appears.
7. On the KeyStore Password screen, in the **KeyStore Password** field, enter a new password for the keystore. A valid password contains 6 to 30 characters, begins with an alphabetic character, and uses only alphanumeric characters and special characters like Dollar ($), Underscore (_), and Pound (#). The password must contain at least one number. In the **Confirm KeyStore Password** field, enter the new password again. Click **Next**. The Configuration Summary screen appears.
8. The Configuration Summary screen lists the application that you selected for configuration and summarizes your configuration options, such as Remote Manager Service Name, RMI Registry Port, and Remote Manager Listen Port (SSL).

   Review this summary and decide whether to start the configuration. If you want to modify any of the configuration settings at this stage, select a topic in the left navigation page and modify your choices. To continue installing this configuration of the Oracle Identity Manager Remote Manager, click **Configure**.

   ---

   **Note:** Before configuring an application, you can save your configuration settings and preferences in a response file. Response files are text files that you can create or edit in a text editor. You can use response files to perform a silent installation or use as templates or customized settings for your environment. For more information, see Appendix F.4, "Performing a Silent Installation".

   ---
9. After you click **Configure**, the Configuration Progress screen appears. A configuration log is saved to the `logs` directory under Oracle Inventory directory. For information about the log files, see Appendix G.2, "Installation Log Files". If the Configuration Progress screen displays any errors, click **Abort** to stop the installation and restart the Oracle Identity Manager Configuration Wizard.
10. Click **Finish**.

**Note:** Oracle Identity Manager Server certificates, such as `xlserver.cert`, are created in the `DOMAIN_HOME/config/fmwconfig/` directory. You can use these certificates if you require server-side certificates for configuring Oracle Identity Manager Remote Manager.

If the configuration fails, click **Abort** to stop the installation and restart the Oracle Identity Manager Configuration Wizard, as described in Section 5.5, "Starting the Oracle Identity Manager 11g Configuration Wizard".

## 5.9 Verifying the Oracle Identity Manager Installation

Before you can verify the Oracle Identity Manager installation, ensure that the following servers are up and running:

- Administration Server for the domain in which the Oracle Identity Manager application is deployed
- Managed Server hosting Oracle Identity Manager
- Managed Server hosting the Oracle SOA 11*g* suite

You can verify your Oracle Identity Manager installation by:

- Checking the Oracle Identity Manager Server URL, such as `http://<Hostname>:<Port>/oim/faces/faces/pages/Admin.jspx`.
- Checking the Identity Management shell, such as `http://<Hostname>:<Port>/admin/faces/pages/Admin.jspx`. This shell is used for Users and Role Management tasks.
- Checking the Oracle Identity Manager Self Service URL, such as `http://<Hostname>:<Port>/oim`.
- Verifying the configuration between Oracle Identity Manager and Oracle SOA (BPEL Process Manager) as follows:
  - **a.** Log in to the Oracle Identity Manager Administration Console, with `xelsysadm`:

    `http://<host>:<oim_port>/oim/faces/pages/Admin.jspx`
  - **b.** Create a Request, such as modifying a user profile.
  - **c.** Log in to the SOA Infrastructure to verify whether the composite applications are displayed.

    `http://<host>:<bpel_port>/soa-infra`
  - **d.** Log in to the BPEL Worklist application, with `xelsysadm`:

    `http://<host>:<soa_port>/integration/worklistapp`
  - **e.** In the list of tasks, verify whether the request has come for approval.
  - **f.** Click on the task, and click **Approve** in the **Actions** tab.
  - **g.** Click on the refresh icon. The request comes back. Approve it again.
  - **h.** Go to `http://<host>:<oim_port>/oim/faces/pages/Admin.jspx` and verify whether the request is completed.

i. Go to `http://<host>:<oim_port>/admin/faces/pages/Admin.jspx` and verify whether the user profile is modified.

- Logging in to the Design Console, `xelsysadm`, and the appropriate password. A successful login indicates that the installation was successful.
- Starting the Remote Manager service by running `remotemanager.sh` or `remotemanager.bat`, as appropriate. (`remotemanager.sh` on UNIX or remotemanager.bat on Windows resides in your Oracle Home directory under a folder named `remote_manager`.

## 5.10 Setting Up Integration with Oracle Access Manager

For information about setting up integration between Oracle Identity Manager and Oracle Access Manager, see "Integrating Oracle Access Manager and Oracle Identity Manager" in the *Oracle Fusion Middleware Integration Guide for Oracle Access Manager*.

## 5.11 List of Supported Languages

Oracle Identity Manager supports the following languages:

Arabic, Brazilian Portuguese, Czech, Danish, Dutch, Finnish, French, German, Greek, Hebrew, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Romanian, Russian, Simplified Chinese, Slovak, Spanish, Swedish, Thai, Traditional Chinese, and Turkish

## 5.12 Using the Diagnostic Dashboard

Diagnostic Dashboard is a stand-alone application that helps you validate some of the Oracle Identity Manager prerequisites and installation.

You must have the appropriate system administrator permissions for your Application Server and Oracle Identity Manager environments to use this tool. You need DBA-level permissions to execute some database-related tests.

---

**Note:** The Diagnostic Dashboard and Oracle Identity Manager must be installed on the same application server.

For more information about installing and using the Diagnostic Dashboard for Oracle Identity Manager, see the "Working with the Diagnostic Dashboard" topic in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*.

---

## 5.13 Getting Started with Oracle Identity Manager After Installation

After installing Oracle Identity Manager, refer to *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

# 6

# Configuring Oracle Access Manager

This chapter explains how to configure Oracle Access Manager. It includes the following topics:



## 6.1 Important Note Before You Begin

Before you start installing and configuring Oracle Identity and Access Management products in any of the scenarios discussed in this chapter, note that **IAM_Home** is used to refer to the Oracle Home directory that includes Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Entitlements Server, and Oracle Identity Navigator. You can specify any name for this Oracle Home directory.

## 6.2 Oracle Access Manager Domain Configuration Template

When configuring Oracle Access Manager in a new or existing WebLogic administration domain, you must choose **Oracle Access Manager with Database Policy Store - 11.1.1.3.0 [Oracle_IDM2]** as the domain configuration template on the Select Domain Source screen in the Oracle Fusion Middleware Configuration Wizard.

A database policy store offers more security measures that can be layered based on the storage, thereby ensuring higher resiliency to corruption and better high availability.

To configure Oracle Access Manager with a database policy store, choose the **Oracle Access Manager with Database Policy Store - 11.1.1.3.0 [Oracle_IDM2]** option on the Select Domain Source screen in the Oracle Fusion Middleware Configuration Wizard.

**Note:** It is recommended that you use a database policy store in production environments.

## 6.3 Oracle Access Manager in a New WebLogic Domain

This topic describes how to configure Oracle Access Manager in a new WebLogic domain.

It includes the following sections:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

### 6.3.1 Appropriate Deployment Environment

Perform the configuration in this topic if you want to install only Oracle Access Manager in an environment where you may add other Oracle Identity and Access Management 11*g* components, such as Oracle Identity Navigator, Oracle Identity Manager, and Oracle Adaptive Access Manager at a later time in the same domain.

### 6.3.2 Components Deployed

Performing the configuration in this section deploys the following:

- WebLogic Administration Server
- Managed Server for Oracle Access Manager
- Oracle Access Manager Console on the Administration Server

### 6.3.3 Dependencies

The configuration in this section depends on the following:

- Oracle WebLogic Server 11*g* Release 1 (10.3.6) or Oracle WebLogic Server 11*g* Release 1 (10.3.5).
- Installation of the Oracle Identity and Access Management 11*g* Release 1 (11.1.1.7.0) software.
- Database schemas for Oracle Access Manager. For more information, see Section 3.2.3, "Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)".

### 6.3.4 Procedure

Perform the following steps to configure Oracle Access Manager in a new WebLogic domain:

1. Start the Oracle Fusion Middleware Configuration Wizard by running the `<IAM_Home>/common/bin/config.sh` script (on UNIX), or `<IAM_Home>\common\bin\config.cmd` (on Windows). The Welcome screen of the Oracle Fusion Middleware Configuration Wizard appears.

> **Note:** `IAM_Home` is used as an example here. You must run this script from your Oracle Identity and Access Management Home directory that contains Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Entitlements Server, and Oracle Identity Navigator.

2. On the Welcome screen, select the **Create a new WebLogic domain** option. Click **Next**. The Select Domain Source screen appears.
3. On the Select Domain Source screen, ensure that the **Generate a domain configured automatically to support the following products:** option is selected. Select **Oracle Access Manager with Database Policy Store - 11.1.1.3.0 [Oracle_IDM2]**, and click **Next**. The Select Domain Name and Location screen appears.

   > **Note:** When you select the **Oracle Access Manager with Database Policy Store - 11.1.1.3.0 [Oracle_IDM2]** option, the **Oracle JRF 11.1.1.0 [Oracle_Common]** option is also selected, by default.

4. Enter a name and a location for the domain to be created, and click **Next**. The Configure Administrator User Name and Password screen appears.
5. Configure a user name and a password for the administrator. The default user name is `weblogic`. Click **Next**.
6. The Configure Server Start Mode and JDK screen appears. Choose a JDK from the **Available JDKs** and select a **WebLogic Domain Startup Mode**. Click **Next**.
7. On the Configure JDBC Component Schema screen, select a component schema, such as the OAM Infrastructure Schema that you want to modify.

   You can set values for Schema Owner, Schema Password, Database and Service, Host Name, and Port. Click **Next**. The Test JDBC Component Schema screen appears. After the test succeeds, the Select Optional Configuration screen appears.
8. On the Select Optional Configuration screen, you can configure the **Administration Server** and **Managed Servers, Clusters, and Machines**. Click **Next**.
9. Optional: Configure the following Administration Server parameters:
   - Name
   - Listen address
   - Listen port
   - SSL listen port
   - SSL enabled or disabled
10. Optional: Configure Managed Servers, as required.

    > **Note:** If you want to configure the Managed Server on the same machine, ensure that the port is different from that of the Administration Server.

11. Optional: Configure Clusters, as required.

For more information about configuring clusters for Oracle Identity and Access Management products, see the "Configuring High Availability for Identity Management Components" topic in the guide *Oracle Fusion Middleware High Availability Guide*.

12. Optional: Assign Managed Servers to clusters, as required.
13. Configure Machines, as needed. This step is useful when you want to run the Administration Server on one machine and Managed Servers on another physical machine.

    **Tip:** Before configuring a machine, use the `ping` command to verify whether the machine or host name is accessible.

14. If the Administration Server is not assigned to a machine, you can assign it to a machine.

    Note that deployments, such as applications and libraries, and services that are targeted to a particular cluster or server are selected, by default.

15. Assign the newly created Managed Server, such as `oam_server1`, to a machine.
16. On the Configuration Summary screen, review the domain configuration, and click **Create** to start creating the domain.

A new WebLogic domain to support Oracle Access Manager is created in the `<MW_HOME>\user_projects\domains` directory (on Windows). On UNIX, the domain is created in the `<MW_HOME>/user_projects/domains` directory.

## 6.4 Starting the Servers

After configuring Oracle Access Manager in a new or existing domain, you must start the Oracle WebLogic Administration Server and various Managed Servers, as described in Appendix C.1, "Starting the Stack".

## 6.5 Optional Post-Installation Tasks

After installing and configuring Oracle Access Manager, you can perform the following optional tasks:

- Configure your own LDAP to use instead of the default embedded LDAP, which comes with Oracle WebLogic Server.
- Configure a policy store to protect resources.
- Add more Managed Servers to the existing domain.
- Add a Managed Server instance.

For more information, see the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service*.

## 6.6 Verifying the Oracle Access Manager Installation

After completing the installation process, including post-installation steps, you can verify the installation and configuration of Oracle Access Manager as follows:

1. Ensure that the Administration Server and the Managed Server are up and running.

2. Log in to the Administration Console for Oracle Access Manager using the URL: `http://<adminserver-host>:<adminserver-port>/oamconsole`

   When you access this Administration Console running on the Administration Server, you are prompted to enter a user name and password. Note that you must have Administrator's role and privileges.

3. Verify the Oracle WebLogic Server Administration Console. If the installation and configuration of Oracle Access Manager is successful, this console shows the Administration Server (for example, `oam_admin`) and the Managed Server (for example, oam_server) in the running mode. In addition, if you check Application Deployments in this console, both `oam_admin` and oam_server must be in active state.

## 6.7 Setting Up Oracle Access Manager Agents

For information about setting up Oracle Access Manager agents, see *Oracle Fusion Middleware Installing Webgates for Oracle Access Manager*.

## 6.8 Setting Up Integration with Oracle Identity Manager

For information about setting up integration between Oracle Access Manager and Oracle Identity Manager, see "Integrating Oracle Access Manager and Oracle Identity Manager" in the *Oracle Fusion Middleware Integration Guide for Oracle Access Manager*.

## 6.9 Getting Started with Oracle Access Manager After Installation

After installing Oracle Access Manager, refer to the "Getting Started with Administering Oracle Access Manager" chapter in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager*.

# 7

# Configuring Oracle Adaptive Access Manager

This chapter explains how to configure Oracle Adaptive Access Manager. It includes the following topics:



## 7.1 Overview

For Oracle Identity and Access Management 11.1.1.7.0, Oracle Adaptive Access Manager includes two components:

- Oracle Adaptive Access Manager (Online)
- Oracle Adaptive Access Manager (Offline)

> **Note:** Oracle Adaptive Access Manager (Offline) is included in the Oracle Identity and Access Management Suite. When you are installing Oracle Identity and Access Management 11.1.1.7.0, Oracle Adaptive Access Manager (Offline) is also installed along with Oracle Adaptive Access Manager. For configuring Oracle Adaptive Access Manager (Offline), see Configuring Oracle Adaptive Access Manager (Offline).

## 7.2 Important Note Before You Begin

Before you start installing and configuring Oracle Identity and Access Management products in any of the scenarios discussed in this chapter, note that **IAM_Home** is used to refer to the Oracle Home directory that includes Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Entitlements Server,

and Oracle Identity Navigator. You can specify any name for this Oracle Home directory.

## 7.3 Configuring Oracle Adaptive Access Manager in a New WebLogic Domain

This topic describes how to configure Oracle Adaptive Access Manager in a new WebLogic administration domain. It includes the following sections:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

### 7.3.1 Appropriate Deployment Environment

Perform the configuration in this topic if you want to install Oracle Adaptive Access Manager in an environment where you may install other Oracle Identity and Access Management 11*g* components, such as Oracle Identity Navigator, Oracle Access Manager, or Oracle Identity Manager at a later time in the same domain.

You can use the Oracle Identity Navigator interface and dashboard to discover and launch the Oracle Adaptive Access Manager console from within Oracle Identity Navigator.

### 7.3.2 Components Deployed

Performing the configuration in this section deploys the following:

- WebLogic Administration Server
- Managed Servers for Oracle Adaptive Access Manager, depending on the Oracle Adaptive Access Manager Domain Configuration template you choose.
- Oracle Adaptive Access Manager Console and Oracle Identity Navigator application on the Administration Server.

### 7.3.3 Dependencies

The configuration in this section depends on the following:

- Oracle WebLogic Server 11*g* Release 1 (10.3.6) or Oracle WebLogic Server 11*g* Release 1 (10.3.5).
- Installation of the Oracle Identity and Access Management 11*g* software.
- Database schema for Oracle Adaptive Access Manager. For more information about schemas specific to Oracle Adaptive Access Manager, see Section 3.2.3, "Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)".

### 7.3.4 Procedure

Perform the following steps to configure only Oracle Adaptive Access Manager in a new WebLogic domain:

1. Start the Oracle Fusion Middleware Configuration Wizard by running the `<IAM_Home>/common/bin/config.sh` script (on UNIX), or `<IAM_`

Home>\common\bin\config.cmd (on Windows). The Welcome screen of the Oracle Fusion Middleware Configuration Wizard appears.

> **Note:** IAM_Home is used as an example here. You must run this script from your Oracle Identity and Access Management Home directory that contains Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Entitlements Server, and Oracle Identity Navigator.

2. On the Welcome screen, select the **Create a new WebLogic domain** option. Click **Next**. The Select Domain Source screen appears.
3. On the Select Domain Source screen ensure that the **Generate a domain configured automatically to support the following products:** option is selected. Select **Oracle Adaptive Access Manager Admin Server - 11.1.1.3.0 [Oracle_IDM2]**, which is mandatory.

   In addition, you can select **Oracle Adaptive Access Manager - Server Offline - 11.1.1.3.0**, which is optional. Click **Next**. The Select Domain Name and Location screen appears.

   > **Note:** When you select the **Oracle Adaptive Access Manager Admin Server - 11.1.1.3.0 [Oracle_IDM2]**, the following options are also selected, by default:
   >
   > - **Oracle Enterprise Manager 11.1.1.0 [oracle_common]**
   > - **Oracle JRF 11.1.1.0 [oracle_common]**
   > - **Oracle Identity Navigator - 11.1.1.3.0 [Oracle_IDM2]**

4. Enter a name and a location for the domain to be created, and click **Next**. The Configure Administrator User Name and Password screen appears.
5. Configure a user name and a password for the administrator. The default user name is weblogic. Click **Next**.
6. The Configure Server Start Mode and JDK screen appears. Choose a JDK from the **Available JDKs** and select a **WebLogic Domain Startup Mode**. Click **Next**.
7. On the Configure JDBC Component Schema screen, select a component schema, such as the **OAAM Admin Server Schema** or the **OAAM Admin MDS Schema**, that you want to modify.

   You can set values for Schema Owner, Schema Password, Database and Service, Host Name, and Port. Click **Next**. The Test JDBC Component Schema screen appears. After the test succeeds, click **Next**. The Select Optional Configuration screen appears.
8. On the Select Optional Configuration screen, you can configure the **Administration Server** and **Managed Servers, Clusters, and Machines**, and **Deployments and Services,** and **RDBMS Security Store**. Click **Next**.
9. Optional: Configure the following Administration Server parameters:
   - Name
   - Listen address
   - Listen port

- SSL listen port
- SSL enabled or disabled

10. On the Select Optional Configuration screen, select **Managed Servers, Clusters and Machines** to configure the managed server. For more information, see "Configure Managed Servers" in the *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard*.
11. Optional: Configure Clusters, as required.

    For more information about configuring clusters for Oracle Identity and Access Management products, see the "Configuring High Availability for Identity Management Components" topic in the guide *Oracle Fusion Middleware High Availability Guide*.
12. Optional: Assign Managed Servers to Clusters, as required.
13. Optional: Configure Machines, as needed. This step is useful when you want to run the Administration Server on one machine and Managed Servers on another physical machine.

    **Tip:** Before configuring a machine, use the `ping` command to verify whether the machine or host name is accessible.
14. Optional: Assign the Administration Server to a machine.
15. Optional: Select Deployments, such as applications and libraries, and Services to target them to a particular cluster or server.
16. Optional: Configure RDBMS Security Store, as required.
17. On the Configuration Summary screen, review the domain configuration, and click **Create** to start creating the domain.

A new WebLogic domain to support Oracle Adaptive Access Manager is created in the `<MW_HOME>\user_projects\domains` directory (on Windows). On UNIX, the domain is created in the `<MW_HOME>/user_projects/domains` directory.

## 7.4 Configuring Oracle Adaptive Access Manager (Offline)

This topic describes how to configure Oracle Adaptive Access Manager (Offline) in a new WebLogic domain. It includes the following topics:

- Components Deployed
- Dependencies
- Procedure

### 7.4.1 Components Deployed

Performing the configuration in this section deploys the following:

- WebLogic Administration Server
- Oracle Adaptive Access Manager (Offline) application on the Administration Server

### 7.4.2 Dependencies

The configuration in this section depends on the following:

- Oracle WebLogic Server 11*g* Release 1 (10.3.6) or Oracle WebLogic Server 11*g* Release 1 (10.3.5).
- Installation of the Oracle Identity and Access Management 11*g* software.
- Database schema for Oracle Adaptive Access Manager (Offline).

### 7.4.3 Procedure

Perform the following steps to configure Oracle Adaptive Access Manager (Offline) in a new WebLogic domain:

1. Start the Oracle Fusion Middleware Configuration Wizard by running the `<IAM_Home>/common/bin/config.sh` script (on UNIX), or `<IAM_Home>\common\bin\config.cmd` (on Windows). The Welcome screen of the Oracle Fusion Middleware Configuration Wizard appears.

   **Note:** `IAM_Home` is used as an example here. You must run this script from your Oracle Identity and Access Management Home directory that contains Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Entitlements Server, and Oracle Identity Navigator.

2. On the Welcome screen, select the **Create a new WebLogic domain** option. Click **Next**. The Select Domain Source screen appears.
3. On the Select Domain Source screen, ensure that the **Generate a domain configured automatically to support the following products:** option is selected.

   Select the **Oracle Adaptive Access Manager Offline - 11.1.3.0 [Oracle_IDM2]** option. When you select this option, the following options are also selected by default:

   - **Oracle Enterprise Manger - 11.1.1.0 [oracle_common]**
   - **Oracle Identity Navigator - 11.1.1.3.0 [Oracle_IDM2]**
   - **Oracle JRF 11.1.1.0 [oracle_common]**

   Click **Next**. The Specify Domain Name and Location screen appears.
4. Enter a name and a location for the domain to be created, and click **Next**. The Configure Administrator User Name and Password screen appears.
5. Configure a user name and a password for the administrator. The default user name is `weblogic`. Click **Next**. The Configure Server Start Mode and JDK screen appears.
6. Choose a JDK and **Production Mode** in the Configure Server Start Mode and JDK screen. Click **Next**. The Configure JDBC Component Schema screen is displayed.
7. On the Configure JDBC Component Schema screen, select a component schema, such as the OAAM Offline MDS Schema or the OAAM Offline Schema that you want to modify. You can set values for Schema Owner, Schema Password, Database and Service, Host Name, and Port. Click **Next**. The Test JDBC Component Schema screen appears. After the test succeeds, click **Next**. The Select Optional Configuration screen appears.
8. On the Select Optional Configuration screen, you can configure the **Administration Server**, **Managed Servers**, **Clusters**, **Machines**, **Deployments and**

**Services**, and **RDBMS Security Store**. Select the relevant check boxes and click **Next**.

- Optional: Configure the following Administration Server parameters:
  - Name
  - Listen Address
  - Listen Port
  - SSL Listen Port
  - SSL Enabled
- Optional: Add and configure Managed Servers, as required. Note that Oracle Entitlements Server does not require a Managed Server because the application is deployed on the WebLogic Administration Server.
- Optional: Configure Clusters, as required.

  For more information about configuring clusters for Oracle Identity and Access Management products, see the "Configuring High Availability for Identity Management Components" topic in the *Oracle Fusion Middleware High Availability Guide*.
- Optional: Configure Machines, as needed. This step is useful when you want to run the Administration Server on one machine and Managed Servers on another physical machine.

  **Tip:** Before configuring a machine, use the `ping` command to verify whether the machine or host name is accessible.
- Optional: Assign the Administration Server to a machine.
- Optional: Select Deployments, such as applications and libraries, and Services to target them to a particular cluster or server.
- Optional: Configure RDBMS Security Store Database, as required.

9. On the Configuration Summary screen, review the domain configuration, and click **Create** to start creating the domain.

A new WebLogic domain to support Oracle Adaptive Access Manager (Offline) is created in the `<MW_HOME>\user_projects\domains` directory (on Windows). On UNIX, the domain is created in the `<MW_HOME>/user_projects/domains` directory.

## 7.5 Starting the Servers

After installing and configuring Oracle Adaptive Access Manager, you must run the Oracle WebLogic Administration Server and various Managed Servers, as described in Appendix C.1, "Starting the Stack".

## 7.6 Post-Installation Steps

After installing and configuring Oracle Adaptive Access Manager, you must complete the following tasks:

1. Create Oracle WebLogic Server Users as follows:
   a. Log in to the Oracle WebLogic Administration Console for your WebLogic administration domain.

b. Click on **Security Realms**, and then click on your security realm.

c. Click the **Users and Groups** tab, and then click the **Users** tab under it.

d. Create a user, such as `user1`, in the security realm.

e. Assign the user `user1` to rule administrators and environment administrators groups.

2. Set up and back up Oracle Adaptive Access Manager Encryption Keys, as described in the "Setting Up Encryption and Database Credentials for OAAM" topic in the *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*. Ensure that you have a backup of the Oracle Adaptive Access Manager Encryption Keys; they are required if you want to re-create the Oracle Adaptive Access Manager domain.

3. Import Snapshot of Policies as follows:

   A full snapshot of policies, dependent components and configurations is shipped with Oracle Adaptive Access Manager. The snapshot is in the `oaam_base_snapshot.zip` file and located in the `MW_HOME/IAM_ORACLE_HOME/oaam/init` directory.

   It contains the following items that must be imported into Oracle Adaptive Access Manager:

   - Challenge questions for English (United States)

     During registration, which could be enrollment, opening a new account, or another events such as a reset, the user selects different questions from a list of questions and enters answers to them. These questions, called challenge questions, are used to authenticate users.

     Questions for the languages you want to support must be in the system before users can be asked to register. These questions may also be required to log in to Oracle Adaptive Access Manager Server.

   - Entity definitions

     The actors that are tracked during authentication are called authentication entities and include user, city, device, and so on. These base entities are required to enable conditions that are used for patterns.

   - Out-of-the-box patterns

     Patterns are used by Oracle Adaptive Access Manager to either define one bucket or dynamically create buckets. Oracle Adaptive Access Manager collects data and populates these buckets with members based on pattern parameters, and rules perform risk evaluations on dynamically changing membership and distributions of the buckets.

   - Out-of-the-box configurable actions

     Configurable actions are actions that are triggered based on the result action or risk scoring or both after a checkpoint execution. The configurable actions are built using action templates.

---

**Note:** If you are upgrading from Oracle Adaptive Access Manager 10.1.4.5 to Oracle Adaptive Access Manager 11*g*, you will see that the names and descriptions of the out-of-the-box action templates are slightly different, since the action templates in Oracle Adaptive Access Manager 11*g* are globalized and hence the difference.

---

- Out-of-the-box policies

  Policies are designed to help evaluate and handle business activities or potentially risky activities that are encountered in day-to-day operation.

- Any groups

  Collections of items used in rules, user groups, and action and alert groups are shipped with Oracle Adaptive Access Manager.

---

**Note:** If you need to customize any properties, you should import the snapshot into your new test system, make the changes, export the snapshot, and import it into your new system. Alternatively you can import the snapshot on the new system and make the property changes directly, thereby eliminating the test system completely.

---

For upgrading policies, components, and configurations, perform a backup, and then import the separate file. The following are available:

- Default questions are shipped in the `oaam_kba_questions_<locale>.zip` files, which are located in the *<MW_HOME>*`/`*<IAM_ORACLE_HOME>*`/oaam/init/kba_questions` directory. The locale identifier <locale> specifies the language version.
- Base policies are shipped in the `oaam_sample_policies_for_uio_integration.zip` file, which is located in the *<MW_HOME>*`/`*<IAM_ORACLE_HOME>*`/oaam/init` directory.
- Configurable action templates are shipped in the `OOTB_Configurable_Actions.zip` file, which is located in the *<MW_HOME>*`/`*<IAM_ORACLE_HOME>*`/oaam/init` directory.
- Base-authentication required entities are shipped in the `Auth_EntityDefinition.zip` file, which is located in the *<MW_HOME>*`/`*<IAM_ORACLE_HOME>*`/oaam/init` directory.

---

**Note:** For more information about policies, see "Importing the OAAM Snapshot" and "Managing Policies, Rules, and Conditions" topics in the *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.

---

4. Load Location Data into the Oracle Adaptive Access Manager database as follows:

   a. Configure the IP Location Loader script, as described in the topics "OAAM Command Line Interface Scripts" and "Importing IP Location Data" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.

   b. Make a copy of the `sample.bharosa_location.properties` file, which is located under the `<MW_HOME>/<IAM_Home>/oaam/cli` directory. Enter location data details in the `location.data` properties, as in the following examples:

   ```
   location.data.provider=quova

   location.data.file=/tmp/quova/EDITION_Gold_2008-07-22_v374.dat.gz
   ```

```
location.data.ref.file=/tmp/quova/EDITION_Gold_2008-07-22_
v374.ref.gz

location.data.anonymizer.file=/tmp/quova/anonymizers_
2008-07-09.dat.gz
```

c. Run the loader on the command line as follows:

On Windows: `loadIPLocationData.cmd`

On UNIX: `./loadIPLocationData.sh`

Ensure that the Oracle Middleware Home (*MW_HOME*) environment variable is set before running the `loadIPLocationData` script.

---

**Note:** If you wish to generate CSF keys or passwords manually, see the "Setting Up Encryption and Database Credentials for OAAM" topic in the *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.

---

## 7.7 Verifying the Oracle Adaptive Access Manager Installation

After completing the installation process, including post-installation steps, you can verify the installation and configuration of Oracle Adaptive Access Manager as follows:

1. Start the Administration Server to register the newly created managed servers with the domain. To start the Administration Server, run the following command:
   - On Windows: At the command prompt, run the `startWebLogic` script to start the Administration Server, as in the following example:

     ```
     \middleware\user_projects\domains\base_
     domain\bin\startWebLogic
     ```

   - On UNIX: At the $ prompt, run the startWebLogic.sh script, as in the following example:

     ```
     sh /MW_HOME/user_projects/domains/base_
     domain/bin/startWebLogic.sh
     ```

2. Start the Managed Server, as described in Appendix C.1, "Starting the Stack".

   Wait for the Administration Server and the Managed Server to start up.

3. Log in to the Administration Server for Oracle Adaptive Access Manager, using the admin server username and password. Log in to the Administration Server using the following URL:

   ```
   http://<host>:<oaam_admin_server1_port>/oaam_admin
   ```

4. Log in to the Oracle Adaptive Access Managed Server using the following URL:

   ```
   https://<host>:<oaam_server_server1_sslport>:oaam_server
   ```

## 7.8 Migrating Policy and Credential Stores

You begin policy and credential store migration by creating the JPS root and then you reassociate the policy and credential store with Oracle Internet Directory.

Migrating policy and credential stores involves the following steps:

1. Creating JPS Root

2. Reassociating the Policy and Credential Store

### 7.8.1 Creating JPS Root

Create the jpsroot in Oracle Internet Directory using the command line `ldapadd` command as shown in these steps:

1. Create an `ldif` file similar to this:

```
dn: cn=jpsroot_iam
cn: jpsroot_iam_iam
objectclass: top
objectclass: orclcontainer
```

2. Use *ORACLE_HOME*`/bin/ldapadd` to add these entries to Oracle Internet Directory. For example:

```
ORACLE_HOME/bin/ldapadd -h oid.mycompany.com -p 389 -D cn="orcladmin" -w
welcome1 -c -v -f jps_root.ldif
```

### 7.8.2 Reassociating the Policy and Credential Store

To reassociate the policy and credential store with Oracle Internet Directory, use the WLST `reassociateSecurityStore` command. Follow these steps:

1. From IAMHOST1, start the `wlst` shell from the *ORACLE_HOME*`/common/bin` directory. For example:

```
./wlst.sh
```

2. Connect to the WebLogic Administration Server using the `wlst connect` command shown below.

```
connect('AdminUser',"AdminUserPassword",t3://hostname:port')
```

For example:

```
connect("weblogic_iam,"welcome1","t3://iamhost-vip.mycompany.com:7001")
```

3. Run the `reassociateSecurityStore` command as shown below:

Syntax:

```
reassociateSecurityStore(domain="domainName",admin="cn=orcladmin",
password="orclPassword",ldapurl="ldap://LDAPHOST:LDAPPORT",servertype="OID",
jpsroot="cn=jpsRootContainer")
```

For example:

```
wls:/IAMDomain/serverConfig> reassociateSecurityStore(domain="IAMDomain",
admin="cn=orcladmin",password="password",
ldapurl="ldap://oid.mycompany.com:389",servertype="OID",
jpsroot="cn=jpsroot_iam_iamhost1")
```

The output for the command is as follows:

```
{servertype=OID, jpsroot=cn=jpsroot_iam, admin=cn=orcladmin,
domain=IAMDomain, ldapurl=ldap://oid.mycompany.com:389, password=password}
Location changed to domainRuntime tree. This is a read-only tree with
DomainMBean as the root.
For more help, use help(domainRuntime)
```

```
Starting Policy Store reassociation.
LDAP server and  ServiceConfigurator setup done.

Schema is seeded into LDAP server
Data is migrated to LDAP server
Service in LDAP server after migration has been tested to be available
Update of jps configuration is done
Policy Store reassociation done.
Starting credential Store reassociation
LDAP server and  ServiceConfigurator setup done.
Schema is seeded into LDAP server
Data is migrated to LDAP server
Service in LDAP server after migration has been tested to be available
Update of jps configuration is done
Credential Store reassociation done
Jps Configuration has been changed. Please restart the server.
```

4. Restart the Administration Server after the command completes successfully. For information about restarting the Administration Server, see Appendix C.3, "Restarting Servers".

## 7.9 Getting Started with Oracle Adaptive Access Manager After Installation

After installing Oracle Adaptive Access Manager, refer to the *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.

# 8

# Installing and Configuring Oracle Entitlements Server

This chapter describes how to install and configure Oracle Entitlements Server 11*g* Release 1 (11.1.1).

It discusses the following topics:

- Important Note Before You Begin
- Overview of Oracle Entitlements Server 11g Installation
- Installation and Configuration Roadmap for Oracle Entitlements Server
- Creating Schemas for Oracle Entitlement Server Policy Store (For Apache Derby Only)
- Configuring Oracle Entitlements Server Administration Server
- Installing Oracle Entitlements Server Client
- Configuring Oracle Entitlements Server Client
- Getting Started with Oracle Entitlements Server After Installation

## 8.1 Important Note Before You Begin

Before you start installing and configuring Oracle Identity and Access Management products in any of the scenarios discussed in this chapter, note that **IAM_Home** is used to refer to the Oracle Home directory that includes Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Entitlements Server, and Oracle Identity Navigator. You can specify any name for this Oracle Home directory.

## 8.2 Overview of Oracle Entitlements Server 11*g* Installation

Oracle Entitlements Server, formerly AquaLogic Enterprise Security, is a fine-grained authorization and entitlement management solution that can be used to precisely control the protection of application resources. It simplifies and centralizes security for enterprise applications and SOA by providing comprehensive, reusable, and fully auditable authorization policies and a simple, easy-to-use administration model. For more information, see "Introducing Oracle Entitlements Server" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Entitlements Server*.

Oracle Entitlements Server 11*g* includes two distinct components:

- Oracle Entitlements Server Administration Server (Authorization Policy Manager)

- OES Client (Security Module)

**Oracle Entitlements Server Administration Server (Authorization Policy Manager)**

This component is included in the Oracle Identity and Access Management 11*g* Release 1 (11.1.1.7.0) installation and requires Oracle WebLogic Server that creates the Middleware Home directory.

**OES Client (Security Module)**

This component has its own installer and it is not included in the Oracle Identity and Access Management 11*g* Release 1 (11.1.1.7.0) installation. The OES Client does not require Oracle WebLogic Server.

## 8.3 Installation and Configuration Roadmap for Oracle Entitlements Server

Table 8–1 lists the tasks for installing and configuring Oracle Entitlements Server.

***Table 8–1 Installation and Configuration Flow for Oracle Entitlements Server***

| No. | Task | Description |
|---|---|---|
| 1 | Review installation concepts in the Installation Planning Guide. | Read the *Oracle Fusion Middleware Installation Planning Guide*, which describes the process for various users to install or upgrade to Oracle Fusion Middleware 11*g* (11.1.1) depending on the user's existing environment. |
| 2 | Review the system requirements and certification documents to ensure that your environment meets the minimum installation requirements for the components you are installing. | For more information, see Section 2.1, "Reviewing System Requirements and Certification". |
| 3 | Obtain the Oracle Fusion Middleware Software. | For more information, see Section 3.2.1, "Obtaining the Oracle Fusion Middleware Software" |
| 4 | Install one of the following database for the Oracle Entitlements Server policy store:<br>■ Oracle Database<br>■ Apache Derby 10.5.3.0, an evaluation database included in your Oracle WebLogic Server installation | Oracle recommends to install Oracle Database. If you are installing Oracle Database, see Section 3.2.2, "Reviewing Database Requirements". |
| 5 | Create and load the appropriate schemas for Oracle Entitlements Server. | Depending on the policy store you choose for Oracle Entitlements Server, complete one of the following:<br>■ If you are using Oracle Database for Oracle Entitlements Server policy store, then you must create schemas for Oracle Entitlements Server using the Oracle Fusion Middleware Repository Creation Utility (RCU).<br>For more information, see Section 3.2.3, "Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)".<br>■ If you are using Apache Derby for Oracle Entitlements Server policy store, you must create schemas for Oracle Entitlements Server as described in Section 8.4, "Creating Schemas for Oracle Entitlement Server Policy Store (For Apache Derby Only)". |

*Table 8–1 (Cont.) Installation and Configuration Flow for Oracle Entitlements Server*

| No. | Task | Description |
|---|---|---|
| 6 | Review WebLogic Server and Middleware Home requirements. | For more information, see Section 3.2.4, "Reviewing WebLogic Server and Middleware Home Requirements". |
| 7 | Start the Oracle Identity and Access Management Installer. | For more information, see Section 3.2.6, "Starting the Oracle Identity and Access Management Installer". |
| 8 | Install the Oracle Identity and Access Management 11*g* software. | Oracle Entitlements Server is included in the Oracle Identity and Access Management Suite. You can use the Oracle Identity and Access Management 11*g* Installer to install Oracle Identity and Access Management Suite.<br>For more information, see Section 3.2.7, "Installing Oracle Identity and Access Management (11.1.1.7.0)". |
| 9 | Run the Oracle Fusion Middleware Configuration Wizard to configure Oracle Entitlements Server Administration Server. | For more information, see Section 8.5, "Configuring Oracle Entitlements Server Administration Server". |
| 10 | Install the Oracle Entitlements Server Client software. | For more information, see Section 8.6, "Installing Oracle Entitlements Server Client". |
| 11 | Configure Oracle Entitlements Server Client. | For more information, see Section 8.7, "Configuring Oracle Entitlements Server Client". |
| 12 | Get started with Oracle Entitlements Server. | For more information, see Section 8.8, "Getting Started with Oracle Entitlements Server After Installation". |

## 8.4 Creating Schemas for Oracle Entitlement Server Policy Store (For Apache Derby Only)

If you are using Apache Derby for Oracle Entitlements Server policy store, then you must complete the following:

1. Open `setNetworkServerCP` (Located at `wlserver_10.3/common/derby/bin` on UNIX) or `setNetworkServerCP.bat` (Located at `wlserver_10.3\common\derby\bin` on Windows) in a text editor and specify the `DERBY_HOME` as shown in the following example:

   ```
   DERBY_HOME="Oracle/Middleware/wlserver_10.3/common/derby"
   ```

2. Start the Apache Derby database by running the following commands:

   - `setNetworkServerCP` (UNIX) or `setNetworkServerCP.bat` (Windows).
   - `startNetworkServer` (Located at `wlserver_10.3/common/derby/bin` on UNIX) or `startNetworkServer.bat` (Located at `wlserver_10.3\common\derby\bin` on Windows).

   You can also run `startDerby.sh` (Located at `wlserver_10.3/common/bin`) or `startDerby.cmd` (Located at `wlserver_10.3\common\bin`) to start the Apache Derby database. The Apache Derby database also starts automatically when you start Oracle WebLogic Server.

3. Test the network server connection, by running `ij`(Located at `wlserver_10.3/common/derby/bin` on UNIX) or `ij.bat` (Located at `wlserver_10.3\common\derby\bin` on Windows) as follows:

   ```
   bin/ij
   ```

4. Connect to the Apache Derby Server, as shown in the following example:

```
ij> connect 'jdbc:derby://127.0.0.1:1527/data/oesdb;create=true';
```

`oesdb` is the name of database and `data` is the relative path (based on the directory where you start the server. In this example, it is `Oracle/Middleware/wlserver_10.3/common/derby/bin` where the database files will be saved.

5. Open `opss_user.sql` (Located at `RCU_HOME/rcu/integration/apm/sql/derby`) in a text editor and replace `&&1` with the schema user name.

   Repeat the above steps for the following SQL files (Located at `RCU_HOME/rcu/integration/apm/sql/derby`):

   - `opss_tables.sql`
   - `opss_version.sql`
   - `opss_gencatalog.sql`

   **Note:** This is the schema name you will specify when you configure the Oracle Entitlements Server described in Configuring Oracle Entitlements Server Administration Server.

6. Run the following SQL files (Located at `RCU_HOME/rcu/integration/apm/sql/derby`) in the ij console:

   - `run'opss_user.sql';`
   - `run'opss_tables.sql';`
   - `run'opss_version.sql';`
   - `run'opss_gencatalog.sql';`

   **Note:** Ensure that you run the SQL files in the same order listed above and make a note of the schema owner and password that you have created.

## 8.5 Configuring Oracle Entitlements Server Administration Server

This topic describes how to configure Oracle Entitlements Server in a new WebLogic domain. It includes the following sections:

- Components Deployed
- Prerequisites
- Configuring Oracle Entitlements Server in a New WebLogic Domain
- Starting the Administration Server
- Post-Configuration
- Verifying Oracle Entitlements Server Administration Server Configuration

### 8.5.1 Components Deployed

Performing the configuration in this section deploys the following:

- WebLogic Administration Server

- Oracle Entitlements Server application on the Administration Server

## 8.5.2 Prerequisites

The following are the prerequisites for configuring Oracle Entitlements Server 11*g* Release 1 (11.1.1):

- Installing Oracle Entitlements Server
- Extracting Apache Derby Template (Optional)

### 8.5.2.1 Installing Oracle Entitlements Server

You must install Oracle Entitlements Server Administration Server as described in Section 8.3, "Installation and Configuration Roadmap for Oracle Entitlements Server".

### 8.5.2.2 Extracting Apache Derby Template (Optional)

If you are using Apache Derby, then you must extract the `oracle.apm_11.1.1.3.0_template_derby.zip` file (Located at `IDM_HOME/common/templates/applications`) and save the `oracle.apm_11.1.1.3.0_template_derby.jar` file to the following location:

```
IAM_HOME\common\templates\applications
```

## 8.5.3 Configuring Oracle Entitlements Server in a New WebLogic Domain

Perform the following steps to configure Oracle Entitlements Server in a new WebLogic domain:

> **Note:** You must have a dedicated Oracle WebLogic Server domain for Oracle Entitlements Server. Do not configure any other Oracle Identity and Access Management components in this domain.

1. Run the `IAM_HOME/common/bin/config.sh` script (on UNIX), or `IAM_HOME\common\bin\config.cmd` (on Windows).

   The Fusion Middleware Configuration Wizard appears.

2. On the Welcome screen, select the **Create a new WebLogic domain** option. Click **Next**.

   The Select Domain Source screen appears.

3. On the Select Domain Source screen, ensure that the **Generate a domain configured automatically to support the following products:** option is selected.

   Select the **Oracle Entitlements Server - 11.1.1.0 [IAM_Home]** option, and click **Next**.

> **Notes:**
>
> - When you select the **Oracle Entitlements Server - 11.1.1.0 [IAM_Home]** option, the **Oracle JRF 11.1.1.0 [Oracle_Common]** option is also selected, by default.
> - If you using Apache Derby, then select the Oracle Entitlements Server Derby template.

The Specify Domain Name and Location screen appears.

4. Enter a name and a location for the domain to be created, and click **Next**.

   The Configure Administrator User Name and Password screen appears.

5. Enter a user name and a password for the administrator. The default user name is `weblogic`. Click **Next**.

   The Configure Server Start Mode and JDK screen appears.

   **Note:** When you enter the user name and the password for the administrator, be sure to remember them.

6. Choose a JDK from the **Available JDKs** and then select a **WebLogic Domain Startup Mode**. Click **Next**.

   **Note:** Ensure that the JDK version you select is Java SE 6 Update 24 or higher.

   The Configure JDBC Component Schema screen is displayed.

7. On the Configure JDBC Component Schema screen, select the Oracle Entitlements Server schema and the MDS Schema, then specify the Schema Owner, Schema Password, Database and Service, Host Name, and Port. Click **Next**.

   **Note:** You get the Schema information from the procedure you completed in step 5 of Table 8–1, " Installation and Configuration Flow for Oracle Entitlements Server".

   The Test JDBC Component Schema screen appears.

8. Select the component schema you want to test, and click **Test Connections**. After the test succeeds, click Next.

   The Select Optional Configuration screen appears.

9. On the Select Optional Configuration screen, you can configure the **Administration Server**, **Managed Servers**, **Clusters**, **Machines**, **Deployments and Services**, and **RDBMS Security Store**. Select the relevant check boxes, and click **Next**.

   **Note:** This step is optional.

10. On the Configuration Summary screen, review the domain configuration, and click **Create** to start creating the domain.

A new WebLogic domain to support Oracle Entitlements Server is created in the `<MW_HOME>\user_projects\domains` directory (on Windows). On UNIX, the domain is created in the `<MW_HOME>/user_projects/domains` directory.

### 8.5.4 Starting the Administration Server

You must start the Administration Server by running the following command on the command line:

**Windows**

```
MW_HOME\user_projects\domains\domain_name\bin\startWebLogic.cmd
```

**UNIX**

```
MW_HOME/user_projects/domains/domain_name/bin/startWebLogic.sh
```

### 8.5.5 Post-Configuration

To complete the configuration, run the following command in the command line:

> **Note:** Ensure that your Administration Server is up and running.

1. Run `wlst.sh` (located at `IDM_HOME/common/bin`).
2. Connect to your Administration Server using the following command:

   ```
   connect('weblogic-username', 'weblogic-password','t3://host:port')
   ```

3. Run the following WLST(online) command depending on your policy store:

   **Oracle Database**

   ```
   configureOESAdminServer(servertype="DB_ORACLE");
   ```

***Table 8–2 WLST Command Oracle Database***

| Argument | Definition |
|---|---|
| `domain` | Name of the Oracle Entitlements Server domain. The default value is `oes_domain`. |
| jpsroot | Specifies the root node in the target repository under which all data is migrated. The default value is `cn=jpsroot`. |
| datasourcename | Name of the data source. The default value is `jdbc/APMDBDS`. |
| servertype | Name of the target database server. Enter `DB_ORACLE`. |

> **Note:** You can enter `domain`, `jpsroot`, and `datasourcename` arguments on the command line if you want to change the default values. For example, `configureOESAdminServer(domain="oes_domain", servertype="DB_ORACLE", jpsroot="cn=jpsroot", datasourcename="jdbc/APMDBDS")`

**Apache Derby**

```
configureOESAdminServer(servertype="DB_DERBY");
```

***Table 8–3 WLST Command Apache Derby***

| Argument | Definition |
|---|---|
| `domain` | Name of the Oracle Entitlements Server domain. The default value is `oes_domain`. |
| jpsroot | Specifies the root node in the target repository under which all data is migrated. The default value is `cn=jpsroot`. |

*Table 8–3 (Cont.) WLST Command Apache Derby*

| Argument | Definition |
|---|---|
| datasourcename | Name of the data source. The default value is `jdbc/APMDBDS`. |
| servertype | Name of the target database server. Enter `DB_DERBY`. |

**Note:** You can enter `domain`, `jpsroot`, and `datasourcename` arguments in the command line, if you want to change the default values. For example,

```
configureOESAdminServer(domain="farm",
servertype="DB_DERBY", jpsroot="cn=root",
datasourcename="jdbc/APMDBDS");.
```

For more information about WLST command, see *Oracle Fusion Middleware Oracle WebLogic Scripting Tool* and *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

4. Restart the Oracle Entitlements Server Administration Server as described in Appendix C.3, "Restarting Servers".

### 8.5.6 Verifying Oracle Entitlements Server Administration Server Configuration

To verify that your Oracle Entitlements Server Administration Server configuration was successful, use the following URL to log in to the Oracle Entitlements Server Administration Console:

```
http://hostname:port/apm/
```

Where `hostname` is the DNS name or IP address of the Administration Server and `port` is the address of the port on which the Administration Server listens for requests.

For more information, see the section "Logging In to and Signing Out of the User Interface" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Entitlements Server*.

## 8.6 Installing Oracle Entitlements Server Client

This section contains the following topic:

- Prerequisites
- Obtaining Oracle Entitlements Server Client Software
- Installing Oracle Entitlements Server Client
- Verifying Oracle Entitlements Server Client Installation

### 8.6.1 Prerequisites

You must install and configure Oracle Entitlements Server Administration Server, as described in Section 8.3, "Installation and Configuration Roadmap for Oracle Entitlements Server".

### 8.6.2 Obtaining Oracle Entitlements Server Client Software

For more information on obtaining OES Client 11*g* software, see *Oracle Fusion Middleware Download, Installation, and Configuration ReadMe*.

### 8.6.3 Installing Oracle Entitlements Server Client

To install Oracle Entitlements Server 11*g* Release 1 (11.1.1.7.0) installation, extract the content of `oesclient.zip` to your local directory and then run `setup.exe` (for **Windows**) or `./runInstaller` (for **UNIX**) from the `Disk1` directory.

---

**Note:** The installer prompts you to enter the absolute path of the JDK that is installed on your system. When you install Oracle WebLogic Server, the `jdk160_24` directory is created under your Middleware Home. You must enter the absolute path of the JRE folder located in this JDK when launching the installer. For example, on Windows, if the JRE is located in `C:\oracle\Middleware\jdk160_24`, then launch the installer from the command prompt as follows:

```
C:\setup.exe -jreLoc C:\oracle\Middleware\jdk160_
24\jre
```

You must specify the `-jreLoc` option on the command line when using the JDK to avoid installation issues.

---

Follow the instructions in Table 8–4 to install OES Client.

If you need additional help with any of the installation screens, click **Help** to access the online help.

***Table 8–4 Installation Flow for the OES Client***

| No. | Screen | Description and Action Required |
|---|---|---|
| 1 | Welcome | Click **Next** to continue. |
| 2 | Prerequisite Checks | If all prerequisite checks pass inspection, then click **Next** to continue. |
| 3 | Specify Installation Location | In the **Oracle Home Directory** field, enter the directory where you want to save the OES client installation to. This directory is also referred to as `OES_Client_Home` in this book.<br>Oracle Entitlements Server Client does not require a Middleware Home with the Oracle WebLogic Server installed.<br>Oracle recommends that you save the OES client installation in a separate directory in the same Middleware Home where the Oracle Entitlements Server Administration server is installed. For example, `MW_HOME/Oracle_OESClient`.<br>Click **Next** to continue. |

*Table 8–4 (Cont.) Installation Flow for the OES Client*

| No. | Screen | Description and Action Required |
|---|---|---|
| 4 | Installation Summary | The Installation Summary Page screen displays a summary of the choices that you made. Review this summary and decide whether to start the installation. If you want to modify any of the configuration settings at this stage, select a topic in the left navigation page and modify your choices. To continue installing OES Client Management, click **Install**. |
| 5 | Installation Progress | If you are installing on a UNIX system, you may be asked to run the *ORACLE_HOME*/`oracleRoot.sh` script to set up the proper file and directory permissions.<br>Click **Next** to continue. |
| 8 | Installation Complete | Click **Finish** to dismiss the installer.<br>This installation process copies the Identity Management software to your system and creates an IDM_Home directory under your Middleware Home. You must proceed to create a WebLogic Domain, by running the Oracle Fusion Middleware Configuration Wizard. In addition, you must configure the Administration Server settings while creating the domain. |

### 8.6.4 Verifying Oracle Entitlements Server Client Installation

To verify that your OES Client install was successful, go to your Oracle Home directory which you specified during installation and verify that the OES Client installation files are created.

## 8.7 Configuring Oracle Entitlements Server Client

OES Client distributes policies to individual Security Modules that protect applications and services. Policy data is distributed in a *controlled* manner or in a *non-controlled* manner. The distribution mode is defined in the `jps-config.xml` configuration file for each Security Module. The specified distribution mode is applicable for all Application Policy objects bound to that Security Module.

> **Note:** Oracle recommends that you to configure OES Client in the controlled distribution mode.

This section describes how to configure the following:

- Configuring Security Modules in a Controlled Mode (Quick Configuration)
- Configuring Distribution Modes
- Configuring Security Module
- Creating the OES Client Domain
- Locating Security Module Instances
- Using the Java Security Module

### 8.7.1 Configuring Security Modules in a Controlled Mode (Quick Configuration)

These section describes how to configure the Security Module quickly using pre-existing `smconfig.prp` files.

- Configuring Java Security Module in a Controlled Mode

- Configuring RMI Security Module in a Controlled Mode
- Configuring Web Service Security Module in a Controlled Mode
- Configuring Oracle WebLogic Server Security Module in a Controlled Mode

#### 8.7.1.1 Configuring Java Security Module in a Controlled Mode

To configure Java Security Module instance in a controlled distribution mode, do the following:

1. Open `smconfig.java.controlled.prp` file (Located at, `OES_CLIENT_HOME/oessm/SMConfigTool`) in a text editor, and then specify the parameters described in Table 8–5.
2. Run the `config.sh` (Located at `OES_CLIENT_HOME/oessm/bin` on UNIX) or config.cmd (Located at `OES_CLIENT_HOME\oessm\bin` on Windows) as follows:

   ```
   config.sh -smConfigId <SM_NAME> -prpFileName OES_CLIENT_
   HOME/oessm/SMConfigTool/smconfig.java.controlled.prp
   ```

3. When prompted, specify the following:
   - Oracle Entitlements Server user name (This is the Administration Server's user name).
   - Oracle Entitlements Server password (This is the Administration Server's password)
   - New key store password for enrollment

#### 8.7.1.2 Configuring RMI Security Module in a Controlled Mode

To configure RMI Security Module instance in a controlled distribution mode, then do the following:

1. Open `smconfig.rmi.controlled.prp` file (Located at `OES_CLIENT_HOME/oessm/SMConfigTool`) in a text editor, and then specify the parameters described in Table 8–5.
2. Run the `config.sh` (Located at `OES_CLIENT_HOME/oessm/bin` on UNIX) or `config.cmd` (Located at `OES_CLIENT_HOME\oessm\bin` on Windows) as follows:

   ```
   config.sh -smConfigId <SM_NAME> -RMIListeningPort <RMISM_PORT> -prpFileName
   OES_CLIENT_HOME/oessm/SMConfigTool/smconfig.rmi.controlled.prp
   ```

3. When prompted, specify the following:
   - Oracle Entitlements Server user name (This is the Administration Server's user name)
   - Oracle Entitlements Server Password (This is the Administration Server's password)
   - New key store password for enrollment

#### 8.7.1.3 Configuring Web Service Security Module in a Controlled Mode

To configure Webservice Security Module instance in a controlled distribution mode, do the following:

1. Open `smconfig.ws.controlled.prp` file (Located at `OES_CLIENT_HOME/oessm/SMConfigTool`) in a text editor, and then specify the parameters described in Table 8–5.

2. Run the `config.sh` (Located at `OES_CLIENT_HOME/oessm/bin` on UNIX) or `config.cmd` (Located at `OES_CLIENT_HOME\oessm\bin` on Windows) as follows:

```
config.sh -smConfigId <SM_NAME> -WSListeningPort <WSSM_PORT> -prpFileName OES_
CLIENT_HOME/oessm/SMConfigTool/smconfig.ws.controlled.prp
```

3. When prompted, specify the following:
   - Oracle Entitlements Server user name (This is the Administration Server's user name)
   - Oracle Entitlements Server password (This is the Administration Server's password)
   - Key store password for enrollment

#### 8.7.1.4 Configuring Oracle WebLogic Server Security Module in a Controlled Mode

To configure Oracle WebLogic Server Security Module instance in a controlled distribution mode, do the following:

1. Open `smconfig.wls.controlled.prp` file (Located at `OES_CLIENT_HOME/oessm/SMConfigTool`) in a text editor, and then specify the parameters described in Table 8–5.
2. Run the `config.sh` (Located at `OES_CLIENT_HOME/oessm/bin` on UNIX) or `config.cmd` (Located at `OES_CLIENT_HOME\oessm\bin` for Windows) as follows:

```
config.sh -smConfigId <SM_NAME> -prpFileName $OES_CLIENT_
HOME/oessm/SMConfigTool/smconfig.wls.controlled.prp -serverLocation <Location
of Web Logic Server Home
```

3. Create a OES Client, as described in Section 8.7.4, "Creating the OES Client Domain".

### 8.7.2 Configuring Distribution Modes

For more information about distribution modes, see the section "Defining Distribution Modes" in the *Oracle Fusion Middleware Developer's Guide for Oracle Entitlements Server*.

The following sections explains how to configure distribution modes.

- Configuring Controlled Distribution
- Configuring Non-Controlled and Controlled Pull Distribution Mode

#### 8.7.2.1 Configuring Controlled Distribution

To configure a controlled Distribution mode, open the `smconfig.prp` file (Located at `OES_CLIENT_HOME/oessm/SMConfigTool`) in a text editor, and edit the following parameters described in Table 8–5.

***Table 8–5 smconfig.prp File Parameters (Controlled Distribution)***

| Parameter | Description |
|---|---|
| `oracle.security.jps.runtime.pd.client.policyDistributionMode` | Accept the default value `controlled-push` as the distribution mode. |

*Table 8–5 (Cont.) smconfig.prp File Parameters (Controlled Distribution)*

| Parameter | Description |
|---|---|
| `oracle.security.jps.runtime.pd.client.RegistrationServerHost` | Enter the address of the Oracle Entitlements Server Administration Server. |
| `oracle.security.jps.runtime.pd.client.RegistrationServerPort` | Enter the SSL port number of the Oracle Entitlements Server Administration Server. You can find the SSL port number from the WebLogic Administration console. |

### 8.7.2.2 Configuring Non-Controlled and Controlled Pull Distribution Mode

Open the `smconfig.prp` file (Located at `OES_CLIENT_HOME/oessm/SMConfigTool`) in a text editor and edit the following parameters described in Table 8–6.

*Table 8–6 smconfig.prp File Parameters Non- Controlled Distribution*

| Parameter | Description |
|---|---|
| `oracle.security.jps.runtime.pd.client.policyDistributionMode` | Enter non-`controlled` or `controlled-pull` as the distribution mode. |
| `oracle.security.jps.policystore.type` | Specify the policy store type. For example, `DB` for Oracle Database, `OID` for Oracle Internet Directory, and `Derby` for Apache Derby. |
| `jdbc.url` | Specify your database policy store JDBC URL. |
| `ldap.url` | Specify your LDAP URL. |
| `oracle.security.jps.farm.name` | Specify your domain name. The default value is `cn=oes_domain`. |
| `oracle.security.jps.ldap.root.name` | Specify the root name of jps context. The default value is `cn=jpsroot`. |

When prompted, specify the following:

- Oracle Entitlements Server user name (This is the Administration Server's user name).
- Oracle Entitlements Server password (This is the Administration Server's password)
- New key store password for enrollment

## 8.7.3 Configuring Security Module

OES Client includes the following Security Modules:

- Java Security Module
- Multi-Protocol Security Module
- WebLogic Security Module

For more information, see "Understanding the Types of Security Modules" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Entitlements Server*.

### 8.7.3.1 Creating Java Security Module

The Java Security Module is a generic Policy Decision Point that provides authorization decisions using Java API. This Security Module can be configured on:

- Java Standard Edition (JSE)
- IBM WebSphere

### Java Standard Edition (JSE)

To create a Java Security Module instance, you must run the `config.sh` (Located at `OES_CLIENT_HOME/oessm/bin` on UNIX) or `config.cmd` (Located at `OES_CLIENT_HOME\oessm\bin` on Windows) as follows:

> **Note:** If you are using Java Security Module in the proxy mode with Web Service Security Module or RMI Security Module, then you must use `oes-ws-client.jar` or `oes-rmi-client.jar` and ensure that you do not use `oes-client.jar`.

```
config.sh -smType java -smConfigId mySM_Java_Controlled -pdServer <oes_server_
address> -pdPort <oes_server_ssl_port>
```

In controlled push mode, you will be prompted for the Oracle Entitlements Server Administration Server username, password, and a new key store password for enrollment.

In non-controlled and controlled pull modes, you will be prompted for Oracle Entitlements Server schema username, and Password.

Table 8–7 describes the parameters you specify on the command line.

***Table 8–7 JSE Security Module Parameters***

| Parameter | Distribution Mode | Description |
|---|---|---|
| `smType` | All | Type of security module instance you want to create. For example, `java`. |
| `smConfigId` | All | Name of the security module instance. For example, `mySM_java`. |
| `pdServer` | `controlled-push` | The address of the Oracle Entitlements Server Administration Server. |
| `pdPort` | `controlled-push` | The SSL port number of the Oracle Entitlements Server Administration Server. For example, `7002`. |

The Java Security Module Instance is created at `OES_CLIENT_HOME/oes_sm_instances/mySM_java`. If you use the default values described in Table 8–7.

### IBM WebSphere

To configure Java Security Module on IBM WebSphere, complete the following steps:

1. Create a new application server using the IBM WebSphere console and name it `OesServer`.
2. Start the Oracle Entitlements Server (OesServer) you created for IBM WebSphere.
3. Deploy `was-client.war` (Located at `OES_CLIENT_HOME/oessm/pd`) to the Oracle Entitlements Server you created.
4. Open the `smconfig.prp` file in a text editor and specify the pd client port and the pd app client context. The pd client port number is the SSL port number of the

IBM WebSphere application server and pd app client contex is the location where the was-client.jar is deployed. For example:

```
oracle.security.jps.pd.was.client.appcontext=pd-client
oracle.security.jps.pd.clientPort=8002
```

5. Run the `config.sh` command as follows:

```
$OES_CLIENT_HOME/oessm/bin/config.sh -smType was -smConfigId mySM_WAS -pdServer
<oes_admin_server> -pdPort <oes_admin_port> -serverNodeName <was_node_name>
-serverName <server_name> -serverLocation WAS_HOME -profileName <dmgr_
profileName>
```

`WAS_HOME` is the location of the IBM WebSphere Application Server.

For any distribution mode you choose, you must specify the IBM WebSphere server user name and password, when prompted.

In controlled push mode, you will be prompted for Oracle Entitlements Server Administration Server user name, Oracle Entitlements Server Administration Server password, and a new key store password for enrollment.

In non-controlled and controlled-pull modes, you will be prompted for Oracle Entitlements Server schema user name and password.

Table 8–8 describes the parameters you specify on the command line.

***Table 8–8 IBM WebSphere Security Module Parameter***

| Parameter | Distribution Mode | Description |
|---|---|---|
| `smType` | All | Type of security module instance you want to create. For example, `was`. |
| `smConfigId` | All | Name of the security module instance. For example, `mySM_WAS`. |
| `pdServer` | controlled-push | The address of the Oracle Entitlements Server Administration Server. |
| `pdPort` | controlled-push | The SSL port number of the Oracle Entitlements Server Administration Server. For example, `7002`. |
| `serverLocation` | All | Location of the IBM WebSphere Server. |

6. Configure SSL for the IBM WebSphere application server as follows:

   a. Import the Oracle WebLogic Server demo trust certificate into IBM WebSphere node default trust keystore and cell default trust keystore by using keytool to export WLS demo trust certificate from WLS demo trust keystore file, or `OES trust.jks` file into a `.der`, as shown in the following example:

   ```
   keytool -exportcert -keystore $OES_CLIENT_HOME/oessm/enroll/DemoTrust.jks
   -alias wlscertgencab -file ~/was.der
   ```

   b. Import the `was.der` file into WAS node default trust keystore and cell default trust keystore. as follows:

      – You may find the import in IBM WebSphere Administration Server console:

security->SSL certificate and key management -> Key stores and certificates -> <NodeDefaultTrustStore> <CellDefaultTrustStore> (here you need to choose one name) -> Signer certificates.

- Click **Add**.
- Enter an alias. For example, **WLS**.
- Choose the `.der` file that you exported earlier, and select data type as **DER**.

**c.** Import the issued private key into the IBM WebSphere node default keystore as follows:

- You may find the import in IBM WebSphere Administration Server console:

  security->SSL certificate and key management -> Key stores and certificates -> NodeDefaultKeyStore -> Personal certificates.

- Click **Import**.
- Select Keystore and enter the path to the keystore file (Located at `OES_CLIENT_HOME/oes_sm_instances/mySM_WAS/security/identity.jks`)
- Select **JKS** as type and enter the password you used to create the keystore file.
- The certificate alias name is the same name as the hostname.

---

**Note:** You must import demo trust certificate into two trust stores for the WAS ND edition. For the private key, you must import one keystore.

---

**d.** Enable Inbound SSL for the server running IBM WebSphere Security Module as follows:

- In the IBM WebSphere administration console, go to **Security >SSL certificate and key management -> Manage endpoint security configurations**.
- Expand inbound tree to get:Inbound->DefaultCell(CellDefaultSSLSettings) -> nodes -> DefaultCellFederatedNode -> servers -> <server name running IBM WebSphere Security Module> and select the server.
- In the General Properties page, select **Override inherited values**.
- From the **SSL configuration** list, select **NodeDefaultSSLSettings**.
- Click **Update certificate alias list** button and then choose the new imported private key alias in the **Certificate alias in key store** list.
- Click **Apply**.

**e.** Enable Out bound SSL for the server running IBM WebSphere Security Module, follows:

- In the IBM WebSphere administration console, go to **Security >SSL certificate and key management -> Manage endpoint security configurations**.

- Expand inbound tree to get:Outbound->DefaultCell(CellDefaultSSLSettings) -> nodes -> DefaultCellFederatedNode -> servers -> <server name running IBM WebSphere Security Module> and select the server.
- In the General Properties page, select **Override inherited values**.
- From the **SSL configuration** list, select **NodeDefaultSSLSettings**.
- Click **Update certificate alias list** and choose the new imported private key alias in the **Certificate alias in key store** list.
- Click **Apply**.

### 8.7.3.2 Creating Multi-Protocol Security Module

The Multi-Protocol Security Module is an authorization service (based on service-oriented architecture principles) wrapped around a generic Java Security Module. This section describes how to configure Multi-Protocol Security Module using:

- RMI
- Web Service

#### RMI

To configure a RMI Security Module Instance, you must run the `config.sh` (Located at `OES_CLIENT_HOME/oessm/bin` for UNIX) or config.cmd (Located at `OES_CLIENT_HOME\oessm\bin` for Windows) as follows:

```
config.sh -smType rmi -smConfigId mySM_Rmi_Controlled -pdServer <oes_server_
address> -pdPort <oes_server_ssl_port> -RMIListeningPort 9405
```

In controlled push mode, when prompted, specify the Oracle Entitlements Server Administration Server user name, Oracle Entitlements Server Administration Server password, and a new key store password for enrollment.

In non-controlled and controlled-pull distribution modes when prompter specify the Oracle Entitlements Server schema username and password.

Table 8–9 describes the parameters you specify on the command line.

***Table 8–9 RMI Security Module Parameters***

| Parameter | Distribution Mode | Description |
|---|---|---|
| `smType` | All | The type of security module instance you want to create. For example, `rmi`. |
| `smConfigId` | All | The name of the security module instance. For example, `mySM_rmi_Controlled`. |
| `pdserver` | controlled-push | The address of the Oracle Entitlements Server Administration Server. |
| `pdPort` | controlled-push | The SSL port of the Oracle Entitlements Server Administration Server. For example, `7002`. |
| `RMIListeningPort` | All | The RMI listening port. For example, `9405`. |

This command also creates client configuration for the RMI Security Module Instance.

#### Web Service

To create a Webservice Security Module instance, you must run the `config.sh` (Located at `OES_CLIENT_HOME/oessm/bin` for UNIX) or config.cmd (Located at `OES_CLIENT_HOME\oessm\bin` for Windows) as follows:

```
config.sh -smType ws -smConfigId mySM_Ws_Controlled -pdServer <oes_server_address>
-pdPort <oes_server_ssl_port> -WSListeningPort 9410
```

In controlled push mode, when prompted, specify the Oracle Entitlements Server Administration Server user name, Oracle Entitlements Server Administration Server password, and a new key store password for enrollment.

In non-controlled and controlled-pull distribution modes when prompted, specify the Oracle Entitlements Server schema user name and password.

Table 8–10 describes the parameters you specify on the command line.

***Table 8–10 Web Service Security Module Parameter***

| Parameters | Distribution Mode | Description |
|---|---|---|
| `smType` | All | Type of security module instance you want to create. For example, `ws`. |
| `smConfigId` | All | Name of the security module instance. For example, `mySM_ws_Controlled`. |
| `pdserver` | controlled-push | The address of the Oracle Entitlements Server Administration Server. |
| `pdPort` | controlled-push | The SSL port of the Oracle Entitlements Server Administration Server. For example, 7002. |
| `WSListeningPort` | All | The web service listening port. For example, `9410`. |

This command also creates client configuration for Webservice Security Module Instance.

### 8.7.3.3 Creating WebLogic Security Module

The WebLogic Security Module is a custom Java Security Module that includes both a Policy Decision Point and a Policy Enforcement Point. It can receive requests directly from the WebLogic Server without the need for explicit authorization API calls. It will only run on the WebLogic Server container.

To configure a WebLogic Server Security Module instance, you must run the `config.sh` (Located at `OES_CLIENT_HOME/oessm/bin` on UNIX) or config.cmd (Located at `OES_CLIENT_HOME\oessm\bin` on Windows) as follows:

```
config.sh -smType wls -smConfigId mySM_WLS -pdServer <oes server> -pdPort <oes_
server_ssl_port>  -serverLocation MW_HOME/wlserver_10.3/
```

In non-controlled and controlled-pull distribution modes, when prompted, specify the Oracle Entitlements Server schema user name and password.

Table 8–11 described the parameters you specify on the command line.

*Table 8–11 Oracle WebLogic Server Security Module Parameters*

| Parameter | Distribution Mode | Description |
|---|---|---|
| smType | All | Type of security module instance you want to create. For example, WLS. |
| smConfigId | All | Name of the security module instance. For example, mySM_WLS_Controlled. |
| pdServer | controlled-push | Address of the Oracle Entitlements Server Administration server. |
| pdPort | controlled-push | The SSL port of the Oracle Entitlements Server Administration server. For example, 7002. |
| serverLocation | All | Location of the Oracle WebLogic Server. |

The Configuration Wizard is displayed. Create a OES Client as described in Section 8.7.4, "Creating the OES Client Domain".

#### 8.7.3.4 Configuring the PDP Proxy Client

Configure a PDP Proxy Client for your web service Security Module or RMI Security Module, as described in Table 8–12:

*Table 8–12 PDP Proxy Client Security Module Parameters*

| Parameter | Description |
|---|---|
| oracle.security.jps.pdp.isProxy | Specify true as the value. |
| oracle.security.jps.pdp.PDPTransport | Specify Web Service (WS) or RMI. |
| oracle.security.jps.pdp.proxy.PDPAddress | Specify http://hostname:port (WS) or rmi://hostname:port (RMI). |

You must run the config.sh (Located at OES_CLIENT_HOME/oessm/bin on UNIX) or config.cmd (Located at OES_CLIENT_HOME\oessm\bin on Windows) as shown in the following example:

For Java Security Module:

```
OES_CLIENT_HOME/oessm/bin/config.sh -smType <SM_TYPE> -smConfigId <SM_NAME>
```

The SM_TYPE can be java, wls, or was. and for SM_NAME enter an appropriate name.

### 8.7.4 Creating the OES Client Domain

To create the OES Client domain, complete the following steps:

> **Note:** You can extend an existing Oracle WebLogic Server domain for Oracle Entitlements Server. Any existing domain with JRF is not supported.

1. The Fusion Middleware Configuration Wizard appears after you invoke the Security Module configuration tool.

2. On the Welcome screen, select the **Create a new WebLogic domain** option. Click **Next**.

   The Select Domain Source screen appears.

3. On the Select Domain Source screen, ensure that the **Generate a domain configured automatically to support the following products:** option is selected.

   Select the **Oracle Entitlements Server WebLogic Security Module - 11.1.1.0 [OESCLIENT]** option. Click **Next**.

   **Note:** Ensure that you do not select the domain template associated with the Oracle Entitlements Server Administration Server from the `IDM_HOME`.

   The Specify Domain Name and Location screen appears.

4. Enter a name and a location for the domain to be created, and click **Next**.

   The Configure Administrator User Name and Password screen appears.

5. Enter a user name and a password for the administrator. The default user name is `weblogic`. Click **Next**.

   The Configure Server Start Mode and JDK screen appears.

   **Note:** When you enter the user name and the password for the administrator, be sure to remember them.

6. Choose a JDK from the **Available JDKs** and then select a **WebLogic Domain Startup Mode**. Click **Next**.

   **Note:** Ensure that the JDK version you select is Java SE 6 Update 24 or higher.

   The Select Optional Configuration screen is displayed.

7. On the Select Optional Configuration screen, select **Administration Server** and **Managed Servers**, **Clusters and Machines**, **Deployments and Services** check boxes and click **Next**.

   The Configure the Administration Servers screen is displayed.

8. In the Configure the Administration Servers screen, enter the following details:

   - Name: Valid server names are a string of characters (alphabetic and numeric). The name must be unique in the domain. For example, `AdminServer`.
   - Listen address: From the drop-down list, select a value for the listen address. See Specifying the Listen Address for information about the available values.
   - Listen port—Enter a valid value for the listen port to be used for regular, nonsecure requests (through protocols such as HTTP and T3). The default value is the next available listen port. If you leave this field blank, the default value is used. For example, 8001.
   - SSL enabled—Select this check box to enable the SSL listen port. By default, SSL is disabled for all new servers.

- SSL listen port—Enter a valid value to be used for secure requests (through protocols such as HTTPS and T3S). The default value is the next available listen port. If you leave this field blank, the default value is used. For example, 8002.

**Note:** After you specify the SSL listen port value, you must update the `oracle.security.jps.pd.clientPort` property in the `smconfig.wls.controlled.prp` file or `smconfig.prp` file with the SSL listen port value. You must then run the `smconfig` tool for Oracle WebLogic Server Security Module and set the Administration Server SSL port to the port specified in `oracle.security.jps.pd.clientPort`.

9. In the Configure Managed Servers screen, click **Add** and create two Managed Servers. Enter the following information:
   - Name: Enter `OES_ManagedServer_1` and OES_ManagedServer_2.
   - Listen address: From the drop-down list, select a value for the listen address for `OES_ManagedServer_1` and OES_ManagedServer_2.
   - Listen port—Enter a valid value for the listen port to be used for `OES_ManagedServer_1` and OES_ManagedServer_2. The default value is the next available listen port. If you leave this field blank, the default value is used. The valid listen port range is 1 to 65535.
   - SSL enabled—Select this check box to enable the SSL listen port. By default, SSL is disabled for all new servers.
   - SSL listen port—Enter a valid value to be used for secure requests (through protocols such as HTTPS and T3S) for `OES_ManagedServer_1` and OES_ManagedServer_2. The default value is the next available listen port. If you leave this field blank, the default value is used. The valid listen port range is 1 to 65535.

   Click **Next**.
10. The Configure Clusters screen is displayed, click Next.
11. The Configure Machines screen is displayed, click Next.
12. On the Configuration Summary screen, review the domain configuration, and click **Create** to start creating the domain.
13. Create three directories under `DOMAIN_HOME/config/oeswlssmconfig` and name them as follows:
    - **AdminServer**
    - **OES_ManagedServer_1**
    - **OES_ManagedServer_2**
14. Select and copy all the files except the new folder you created above in `DOMAIN_HOME/config/oeswlssmconfig` and paste them to the following newly created folders:
    - **AdminServer**
    - **OES_ManagedServer_1**
    - **OES_ManagedServer_2**

15. Open `jps-config.xml` (Located at `DOMAIN_HOME/config/oeswlssmconfig/OES_ManagedServer_1`) and specify the OES_ManagedServer_1 Managed Server host name and port number for `oracle.security.jps.runtime.pd.client.DistributionServiceURL`.
16. Open `jps-config.xml` (Located at `DOMAIN_HOME/config/oeswlssmconfig/OES_ManagedServer_2`) and specify the OES_ManagedServer_2 Managed Server host name and port number for `oracle.security.jps.runtime.pd.client.DistributionServiceURL`.
17. Open `setDomainEnv.sh` (UNIX) or `setDomainEnv.cmd` (Windows) in a text editor and edit the line `-Doracle.security.jps.config=${DOMAIN_HOME}/config/oeswlssmconfig/jps-config.xml` as follows:

    ```
    b.-Doracle.security.jps.config=${DOMAIN_HOME}/config/oeswlssmconfig/${SERVER_NAME}/jps-config.xml
    ```

### 8.7.5 Locating Security Module Instances

The Oracle Entitlements Server security module instances are created in the `OES_CLIENT_HOME/oes_sm_instances`. directory.

For Oracle WebLogic Server security module, the domain configuration is located at `DOMAIN_HOME/config/oeswlssmconfig`.

You can create, delete, or modify the security module instances, as required.

### 8.7.6 Using the Java Security Module

After configuring Java Security Module for your program, you must start the Java Security module for your program by completing the following:

1. Set a new Java System Property with the location of the `jps-config.xml` created at `OES_CLIENT_HOME/oes_sm_instances/<SM_NAME>/config/jps-config.xml`. as the value.
2. Enter `oes-client.jar` (Located at `OES_CLIENT_HOME/modules/oracle.oes_sm.1.1.1`) into the Classpath of the program.

## 8.8 Getting Started with Oracle Entitlements Server After Installation

After installing Oracle Entitlements Server, refer to the following documents:

- *Oracle Fusion Middleware Administrator's Guide for Oracle Entitlements Server*
- *Oracle Fusion Middleware Developer's Guide for Oracle Entitlements Server*

# 9 Lifecycle Management

This chapter explains how to address situations where a lifecycle change event occurs for an Oracle Identity and Access Management component that is integrated with one or more components.

Topics include:



## 9.1 How Lifecycle Events Impact Integrated Components

Following are ways in which certain lifecycle events, sometimes referred to as rewiring, affect a component that is already integrated with others:

- Reassociation

  The hostname or port of an integrated component is reassociated. For example, the hostname of an OVD server changes.

- Test to Production

  When entities in a test or pilot environment are migrated into a pre-installed production environment, this can affect dependent components. For example, moving Oracle Identity Manager Navigator to a new production environment.

> **Note:** For some components, "rewiring" to achieve Test to Production is not feasible, and it is advisable to simply create a new production instance of the server. Oracle Identity Federation is an example of a server that is freshly installed in the production environment rather than changing the test configuration.

## 9.2 LCM for Oracle Identity Manager

Lifecycle management events for Oracle Identity Manager include:

- reassociation when the host or port changes for these components:
  - Oracle Virtual Directory

  - Oracle SOA Suite
  - MDS
- moving metadata from a test environment to a production environment

Refer to the following sources for lifecycle management procedures relating to OIM:

- "Oracle Virtual Directory Host and Port Changes" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*
- "Changing OVD Password" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*
- "SOA Host and Port Changes" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*
- "Oracle Identity Manager Database Host and Port Changes" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*
- "Oracle Identity Manager (OIM) Rewiring with Existing Oracle Adaptive Access Manager (OAAM)" in the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*
- "Changing Oracle Identity Manager Database Password" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*
- "Configuring LDAP Adapters" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*
- "Adding a Component Link to the Product Launcher by Using Product Discovery" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*
- "Editing Adapter Plug-Ins" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*
- "Move Oracle Identity Manager to a New Target Environment" in the *Oracle Fusion Middleware Administrator's Guide*
- "Move Oracle Identity Manager to an Existing Target Environment" in the *Oracle Fusion Middleware Administrator's Guide*

## 9.3 LCM for Oracle Access Manager

Lifecycle events for Oracle Access Manager include replicating the policy configuration information from the test system into production.

Refer to the following sources for lifecycle management procedures relating to OAM:

- "Adding a Component Link to the Product Launcher by Using Product Discovery" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*
- "Moving OAM 11g Data from a Test to a Production Deployment" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager*

## 9.4 LCM for Oracle Adaptive Access Manager

Lifecycle events for Oracle Adaptive Access Manager include reassociation when the host or port changes for the following components:

- Oracle Virtual Directory
- Oracle Internet Directory
- Oracle Database

- Oracle Identity Manager

Refer to the following sources for lifecycle management procedures relating to OAAM:

- "Adding a Component Link to the Product Launcher by Using Product Discovery" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*
- "Oracle Virtual Directory (OVD) Rewiring with Existing Oracle Adaptive Access Manager (OAAM)" in the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*
- "Oracle Identity Manager (OIM) Rewiring with Existing Oracle Adaptive Access Manager (OAAM)" in the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*
- "OID Rewiring with Existing OAAM (in Cases without OVD)" in the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*
- "Database Rewiring with Existing OAAM" in the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*
- "Move Oracle Adaptive Access Manager to a New Target Environment" in the *Oracle Fusion Middleware Administrator's Guide*
- "Move Oracle Adaptive Access Manager to an Existing Target Environment" in the *Oracle Fusion Middleware Administrator's Guide*

## 9.5 LCM for Oracle Identity Navigator

Lifecycle events for Oracle Identity Navigator include migrating from test to production, and rewiring the integration with Oracle Business Intelligence Publisher.

Refer to the following sources for lifecycle management procedures relating to OIN:

- "Migrating Oracle Identity Navigator from Test to Production" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*.
- "Configuring Oracle Business Intelligence Publisher" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*.
- "Adding a Component Link to the Product Launcher by Using Product Discovery" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*
- "Migrating Oracle Identity Navigator from Test to Production" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*

## 9.6 References

For additional information about lifecycle management in Oracle Fusion Middleware, see "Part V Advanced Administration: Expanding Your Environment" in the *Oracle Fusion Middleware Administrator's Guide*.

# Part III

## Appendixes

Part IV contains the following appendixes:

- Appendix A, "Oracle Identity and Access Management 11.1.1.7.0 Software Installation Screens"
- Appendix B, "Oracle Identity Manager Configuration Screens"
- Appendix C, "Starting or Stopping the Oracle Stack"
- Appendix D, "Preconfiguring Oracle Directory Server Enterprise Edition (ODSEE)"
- Appendix E, "Deinstalling and Reinstalling Oracle Identity and Access Management"
- Appendix F, "Performing a Silent Installation"
- Appendix G, "Troubleshooting the Installation"
- Appendix H, "OAAM Partition Schema Reference"
- Appendix I, "Software Deinstallation Screens"

# A

# Oracle Identity and Access Management 11.1.1.7.0 Software Installation Screens

This appendix describes the screens of the Oracle Identity and Access Management 11*g* software Installation Wizard that enables you to install Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Entitlements Server, and Oracle Identity Navigator.

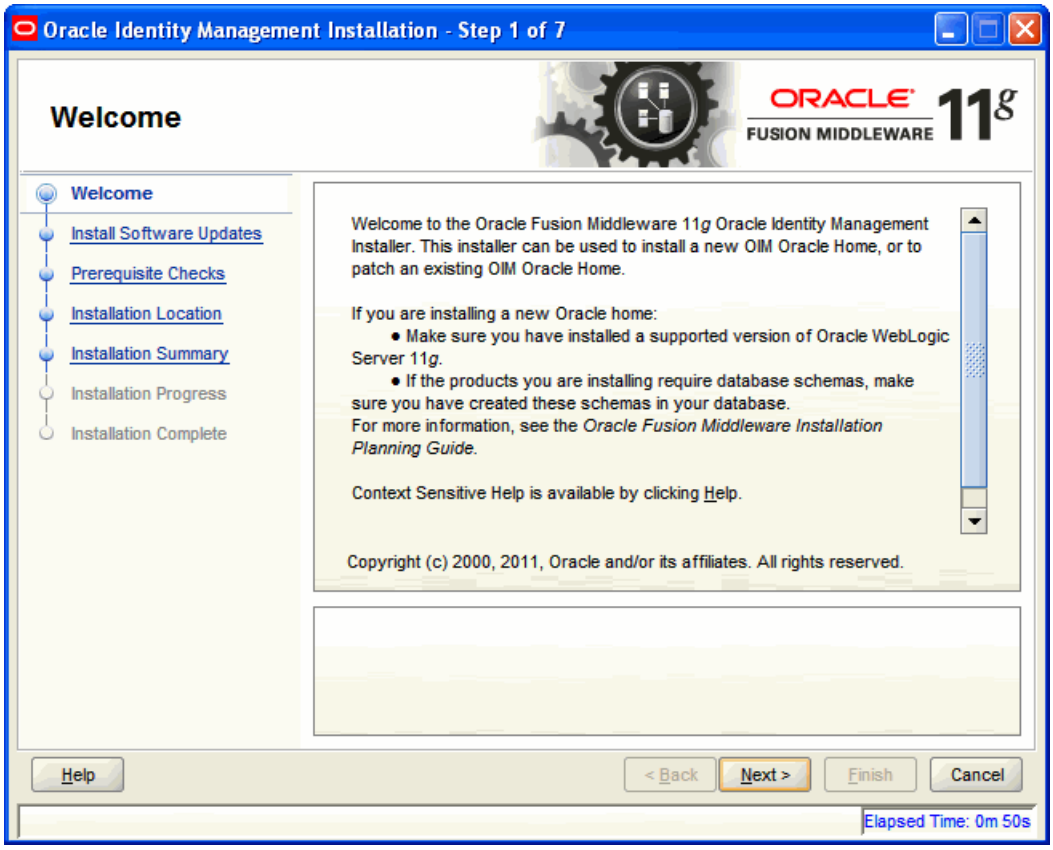
It contains the following topics:



## A.1 Welcome

The Welcome screen is displayed each time you start the Oracle Identity and Access Management 11*g* Installer wizard.

***Figure A–1 Welcome Screen***

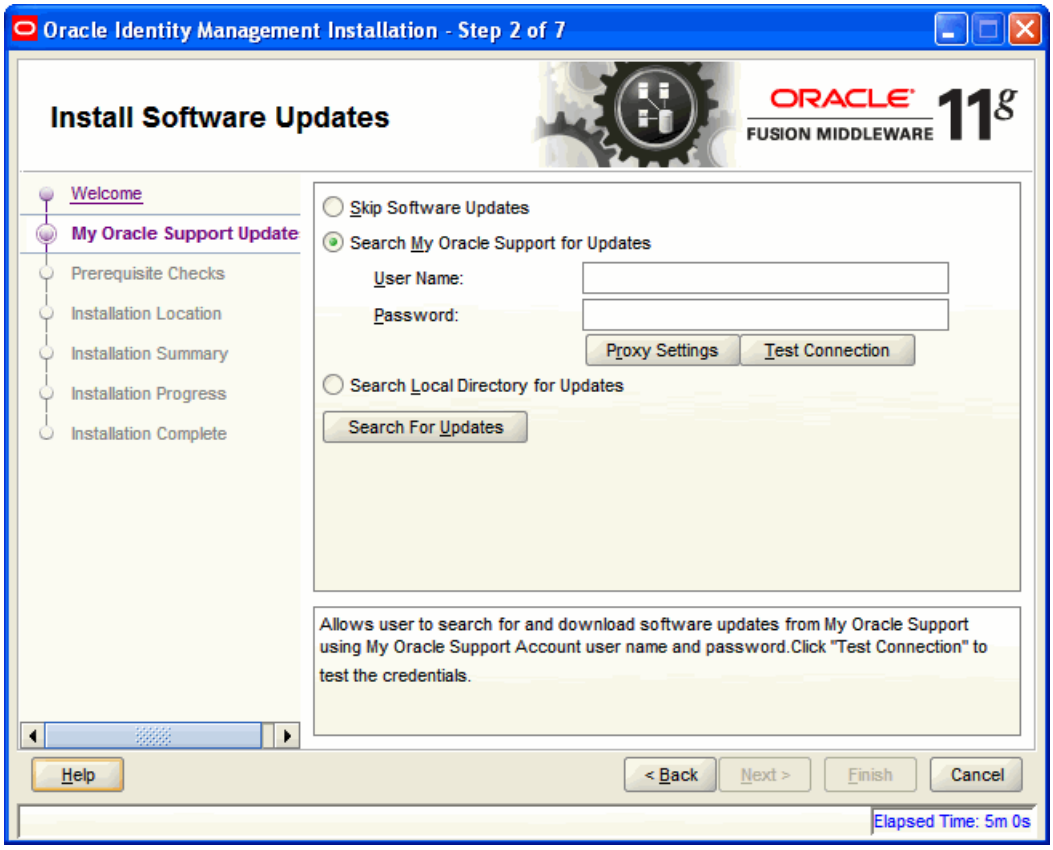



Click **Next** to continue.

## A.2 Install Software Updates

This screen helps to quickly and easily search for the latest software updates, including important security updates, via your My Oracle Support account.

*Figure A–2 Install Software Updates*

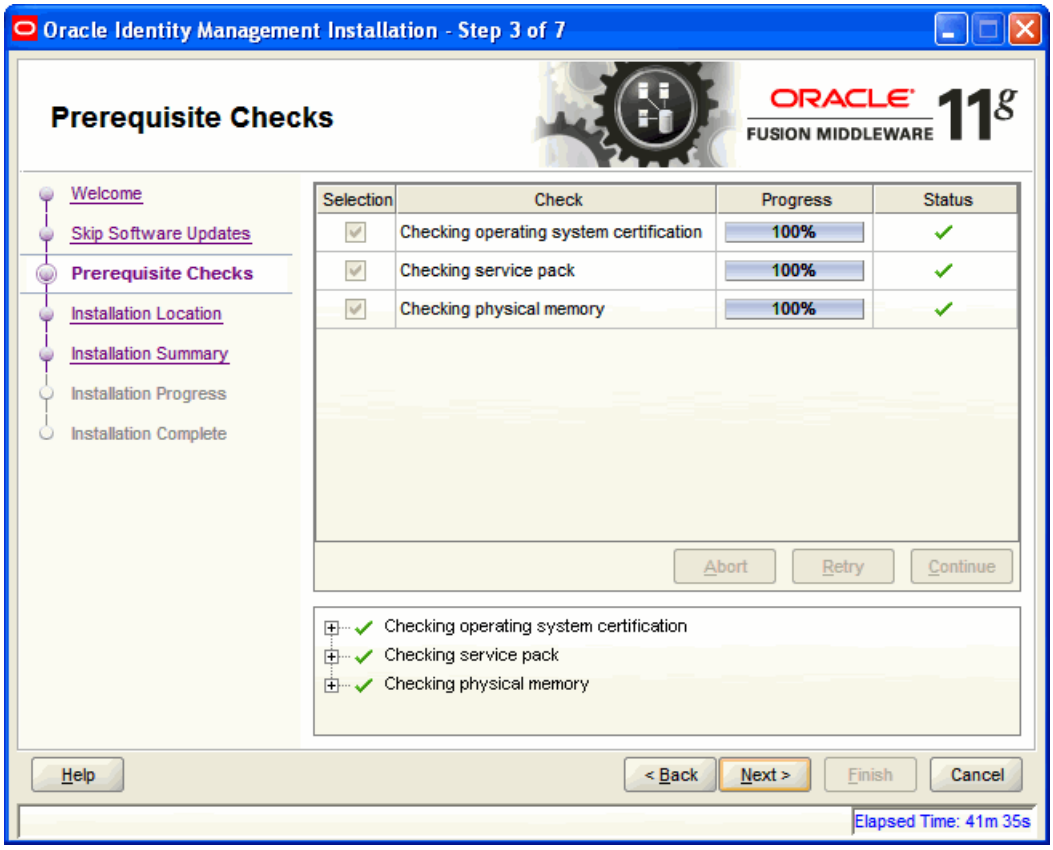



## A.3 Prerequisite Checks

The installation program ensures that you have a certified version, the correct software packages, sufficient space and memory to perform the operations that you have selected. If any issues are detected, errors appear on this page.

The following example screen applies to Windows operating systems only.

*Figure A–3 Prerequisite Checks Screen*



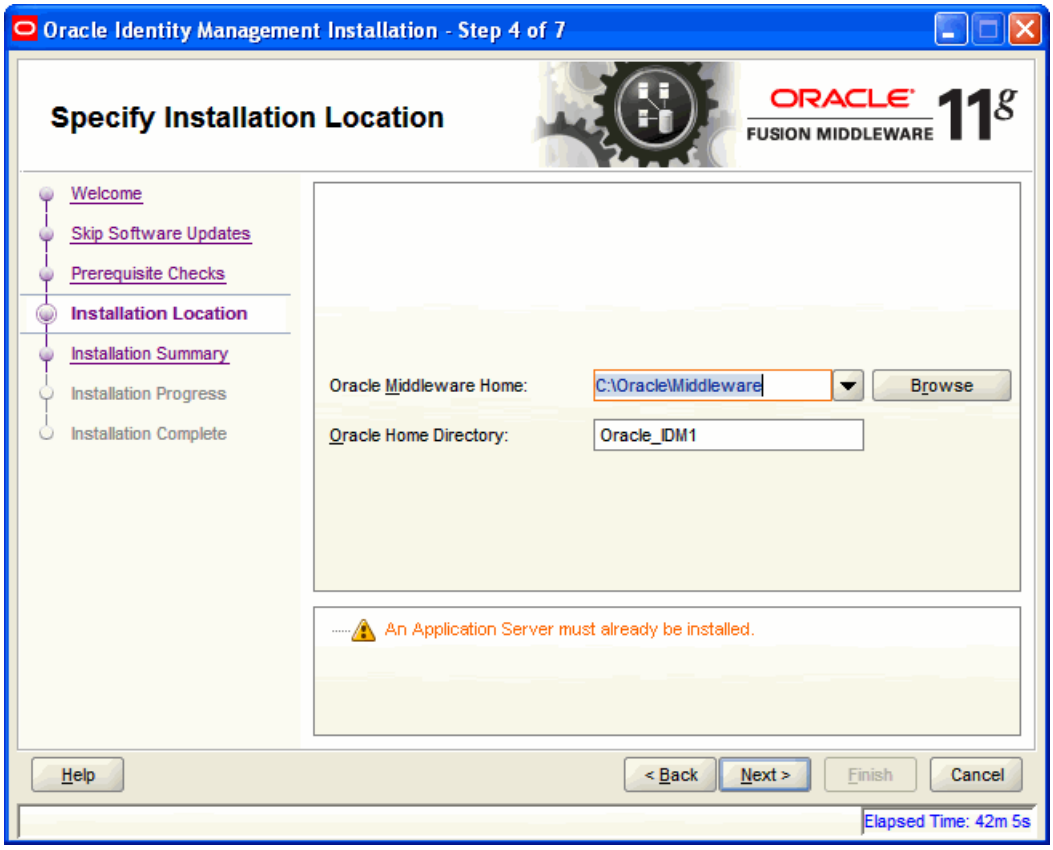

On this screen, you can select to **Abort**, **Retry**, or **Continue** with the installation.

If all the prerequisite checks pass inspection, click **Next** to continue.

## A.4 Specify Installation Location

In this screen, you enter a location for the new Oracle Identity and Access Management 11*g* software being installed.

*Figure A–4 Specify Installation Location Screen*




Ensure that Oracle WebLogic Server is already installed on your machine. Navigate to the Oracle Fusion Middleware Home directory by clicking **Browse**. Enter a name for the new Oracle Home directory for Oracle Identity and Access Management 11g components.

If the Middleware location does not exist, you must install WebLogic Server and create a Middleware Home directory, as described in Section 3.2.4, "Reviewing WebLogic Server and Middleware Home Requirements", before running the Oracle Identity and Access Management Installer.

---

**Note:** If you do not specify a valid Middleware Home directory on the Specify Installation Location screen, the Installer displays a message and prompts you to confirm whether you want to proceed with the installation of only Oracle Identity Manager Design Console and Oracle Identity Manager Remote Manager. These two components of Oracle Identity Manager do not require a Middleware Home directory.

If you want to install only Oracle Identity Manager Design Console or Remote Manager, you do not need to install Oracle WebLogic Server or create a Middleware Home directory on the machine where Design Console or Remote Manager is being configured.

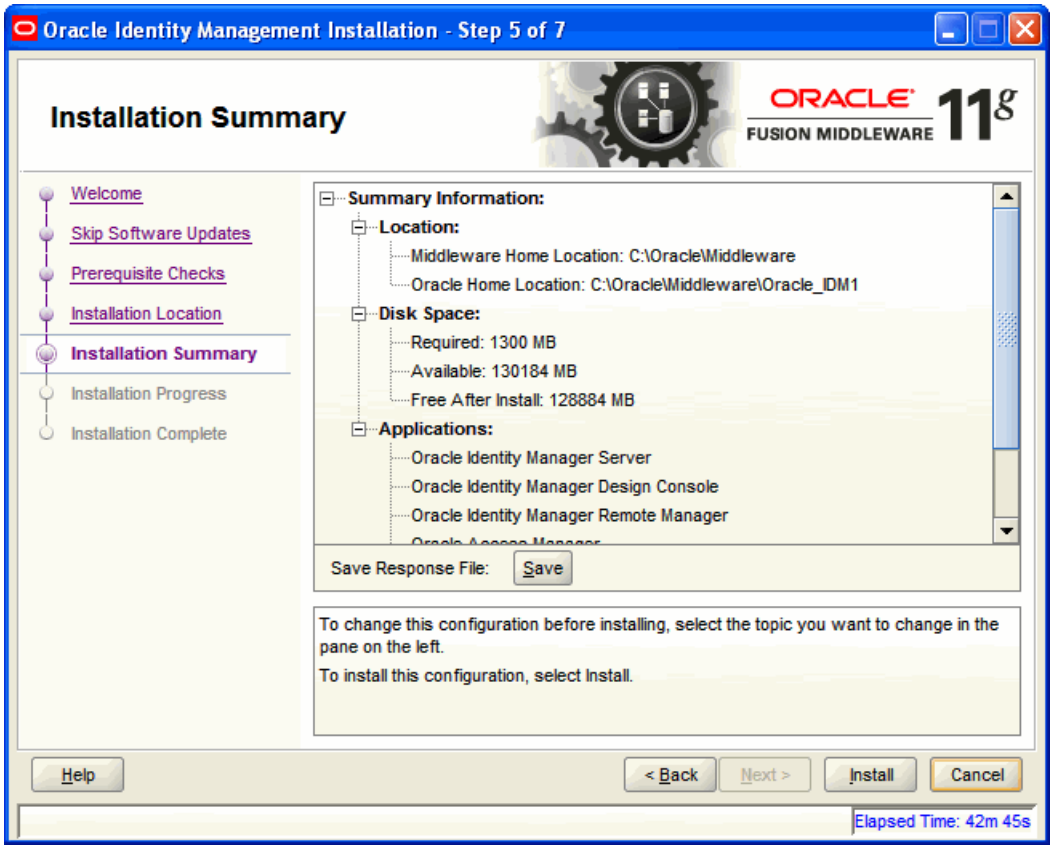
---

Click **Next** to continue.

## A.5 Installation Summary

This screen displays a summary of your Oracle Identity and Access Management 11*g* installation.

***Figure A–5 Installation Summary Screen***

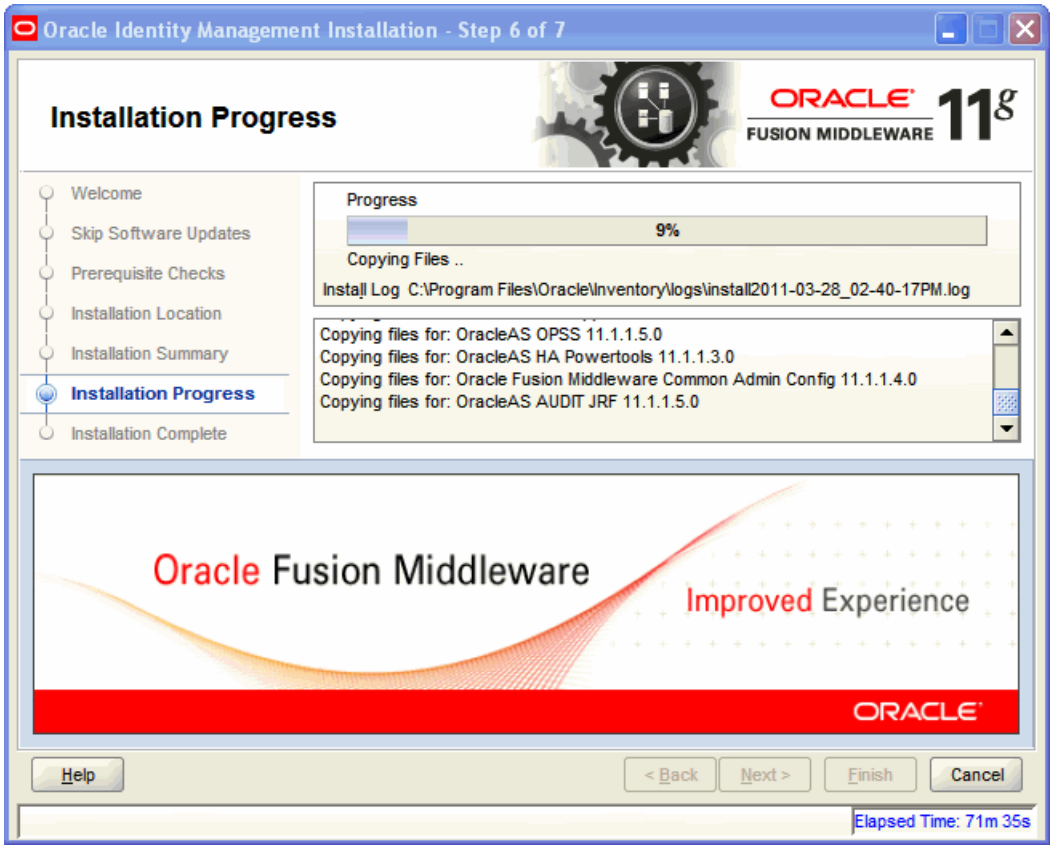



Review the contents of this screen, and click **Install** to start installing the Oracle Identity and Access Management 11*g* software.

## A.6 Installation Progress

This screen displays the progress of the Oracle Identity and Access Management installation.

*Figure A–6 Installation Progress Screen*

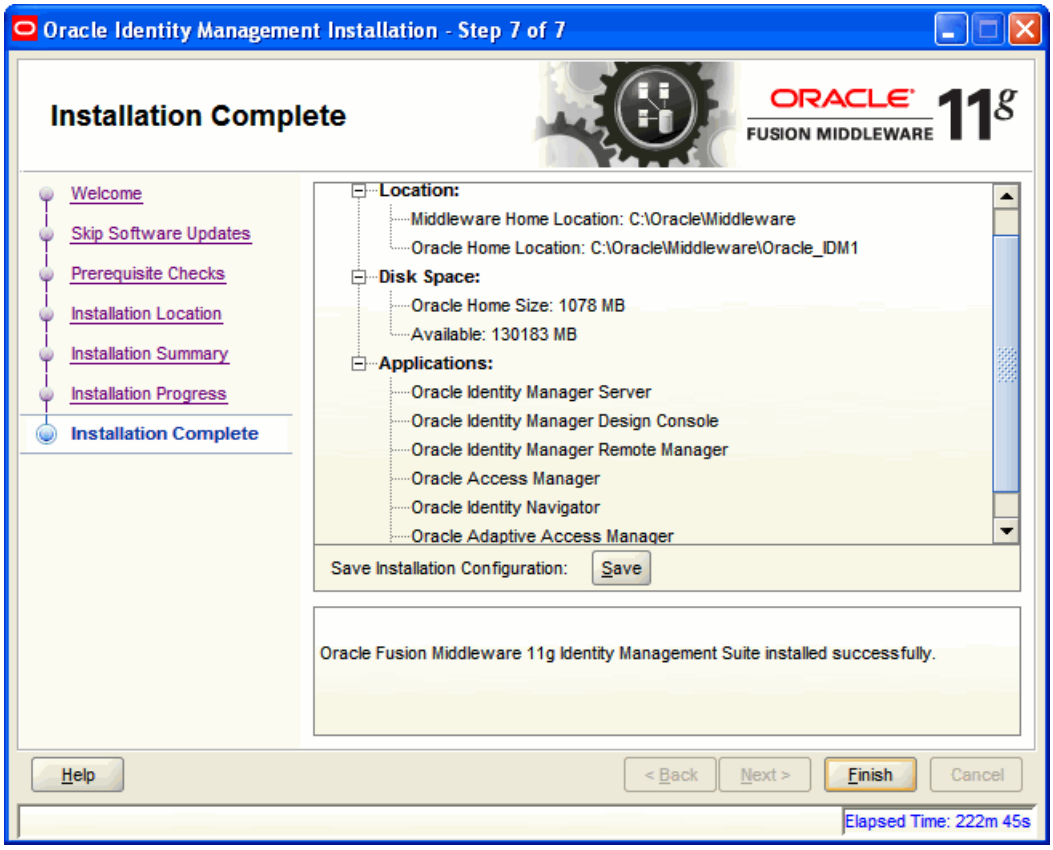



If you want to quit before the installation is completed, click **Cancel**. The installation progress indicator gives a running inventory of the files that are being installed. If you are only installing the software binaries, installation is complete after all of the binaries have been installed.

## A.7 Installation Complete

This screen displays a summary of the installation parameters, such as Location, Disk Space, and Applications. To save the installation configuration in a response file, which is used to perform silent installations, click **Save**.

*Figure A–7 Installation Complete Screen*




Click **Finish** to complete the installation process.

# B

# Oracle Identity Manager Configuration Screens

This appendix describes the screens of the Oracle Identity Manager 11*g* Configuration Wizard that enables you to configure Oracle Identity Manager Server, Oracle Identity Manager Design Console, and Oracle Identity Manager Remote Manager.

This appendix contains the following topics:



## B.1 Welcome

The Welcome screen is displayed each time you start the Oracle Identity Manager Configuration Wizard.

***Figure B–1 Welcome Screen***


You can use the Oracle Identity Manager Configuration Wizard only once during initial setup for configuring Oracle Identity Manager Server. After configuring Oracle Identity Manager Server using this wizard, you cannot re-run this wizard to modify the configuration of Oracle Identity Manager. You must use Oracle Enterprise Manager Fusion Middleware Control to make such modifications. However, you can run this wizard on other machines, where Design Console or Remote Manager is configured, as and when needed.

Ensure that you have configured Oracle Identity Manager in a new or existing WebLogic domain before launching the Oracle Identity Manager Configuration Wizard to configure Oracle Identity Manager Server, Design Console on Windows, and Remote Manager.

If you are configuring Server, you must run this wizard on the machine where the WebLogic Administration Server is running (the Administration Server for the domain in which Oracle Identity Manager is deployed). Ensure that the Administration Server is up and running before you start configuring Oracle Identity Manager Server.

If you are configuring only Design Console, you must run this wizard on the Windows machine where Design Console should be configured. If you are configuring only Remote Manager, you must run this wizard on the machine where Remote Manager is being configured. Note that the Oracle Identity Manager Server should be configured before you can configure Design Console or Remote Manager.

Click **Next** to continue.

## B.2 Components to Configure

Use this screen to select the Oracle Identity Manager components that you want to configure. Oracle Identity Manager components include Server, Design Console, and Remote Manager.

Before configuring Oracle Identity Manager Server, Design Console or Remote Manager, ensure that you have configured Oracle Identity Manager in a new or existing WebLogic domain using the Oracle Fusion Middleware Configuration Wizard.

*Figure B–2 Components to Configure Screen*

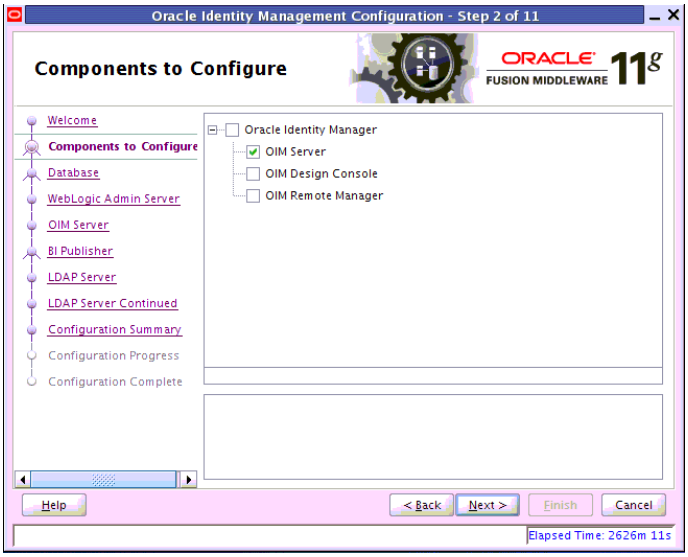



Table B–1 describes the Oracle Identity Manager components that you can choose.

*Table B–1 Oracle Identity Manager Configuration Choices*

| Option | Description |
|---|---|
| Configure all components on this screen | To configure Oracle Identity Manager Server, Design Console, and Remote Manager simultaneously on the same machine, select the **Oracle Identity Manager** option. |
| Configure only Oracle Identity Manager Server | To configure only Oracle Identity Manager Server, select the **OIM Server** option. This option is selected, by default. Note that WebLogic Administration Server for the domain (the domain in which Oracle Identity Manager is deployed) should be up and running. |
| Configure only Oracle Identity Manager Design Console | To configure only Oracle Identity Manager Design Console, select the **OIM Design Console** option. However, note that Oracle Identity Manager Server must be configured either on the local machine or on a remote machine before you can run Design Console on development machines. Design Console is supported on Windows operating systems only. |
| Configure only Oracle Identity Manager Remote Manager | To configure only Oracle Identity Manager Remote Manager, select the **OIM Remote Manager** option. However, note that Oracle Identity Manager Server must be configured either on the local machine or on a remote machine before you can run Remote Manager. |

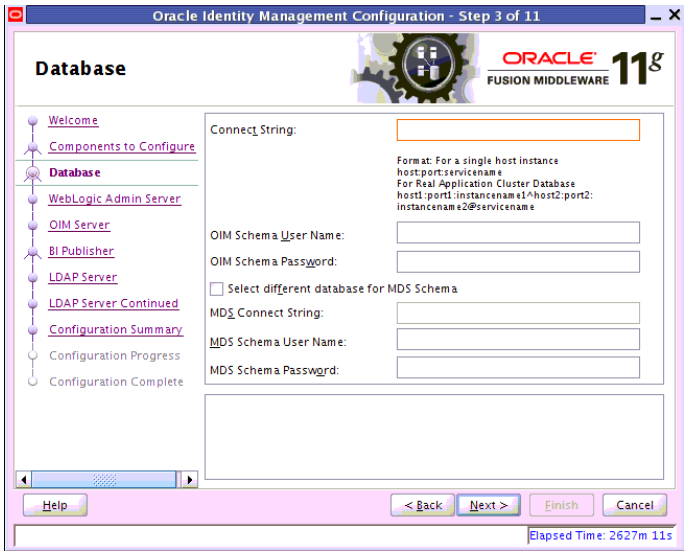
**Note:** You can also select any combination of two of the three Oracle Identity Manager components.

## B.3 Database

In this screen, you specify the database and schema information. Note that you should have created and loaded Oracle Identity Manager schemas using the Oracle Fusion Middleware Repository Creation Utility (RCU) before configuring Oracle Identity Manager Server. For information about creating and loading Oracle Identity Manager

schemas, see Section 3.2.3, "Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)".

***Figure B–3 Database Screen***




You can use the same database or different databases for creating the Oracle Identity Manager schema and the Metadata Services schema.

Table B–2 describes the database connection information that you must specify.

***Table B–2 Fields in the Database Screen***

| Field | Description |
|---|---|
| **Connect String** | Enter the full path, listen port, and service name for your Oracle database. For a single host instance, the format of connect string is `hostname:port:servicename`.<br>For example, if the hostname is aaa.bbb.com, port is 1234, and the service name is xxx.bbb.com, then you must enter the connect string for a single host instance as follows:<br>`aaa.bbb.com:1234:xxx.bbb.com`<br>If you are using a Real Application Cluster database, the format of the database connect string is as follows:<br>`hostname1:port1:instancename1^host2:port2:instancename2@servicename` |
| **OIM Schema User Name** | Enter the name of the schema user that you created for Oracle Identity Manager using the Oracle Fusion Middleware Repository Creation Utility.<br>If you upgraded your existing Oracle Identity Manager schema to 11*g* Release 1 (11.1.1), enter the user name for your existing schema. |
| **OIM Schema Password** | Enter the password for the Oracle Identity Manager schema user that you set while creating the schema using the Oracle Fusion Middleware Repository Creation Utility (RCU).<br>If you upgraded your existing Oracle Identity Manager schema to 11*g* Release 1 (11.1.1), enter the password for your existing schema. |
| **Select different database for MDS schema** | Select this check box if you want to use a different database for the Metadata Services (MDS) schema. |

*Table B–2 (Cont.) Fields in the Database Screen*

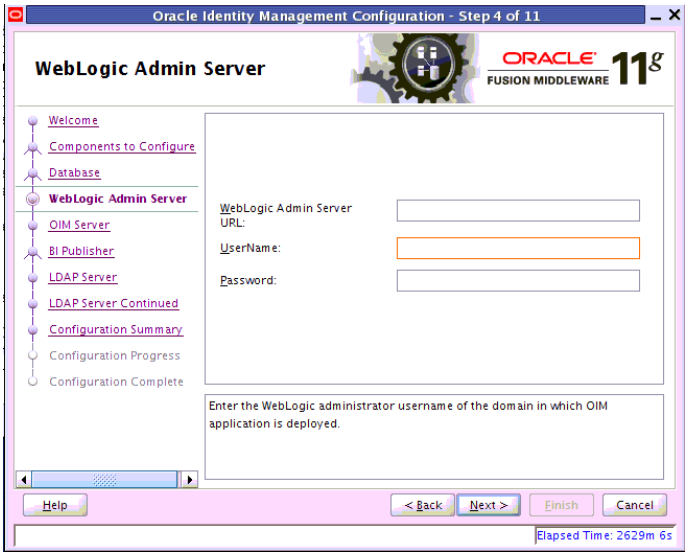
| Field | Description |
|---|---|
| **MDS Connect String** | If you are using a different database for the Metadata Services (MDS) schema, enter the full path, listen port, and service name for the database associated with the MDS schema. The format of the connect string is similar to that of the standard Connect String. |
| **MDS Schema User Name** | Enter the name of the schema user that you created for **AS Common Services - Metadata Services** by using the Oracle Fusion Middleware Repository Creation Utility (RCU).<br>If you upgraded your existing Metadata Services schema to 11*g* Release 1 (11.1.1), enter the user name for your existing schema. |
| **MDS Schema Password** | Enter the password for the **AS Common Services - Metadata Services** schema user that you set while creating the schema by using the Oracle Fusion Middleware Repository Creation Utility (RCU).<br>If you upgraded your existing Oracle Identity Manager schema to 11*g* Release 1 (11.1.1), enter the password for your existing schema. |

After entering information in the fields, click **Next** to continue.

## B.4 WebLogic Admin Server

In this screen, you specify the t3 URL, user name and password for the WebLogic administration domain in which the Oracle Identity Manager application is deployed. Ensure that the Administration Server is up and running.

*Figure B–4 WebLogic Admin Server Screen*




In the **WebLogic Admin Server URL** text box, enter the t3 URL of the Administration Server for the WebLogic domain in the following format:

```
t3://hostname:port
```

In the **UserName** text box, enter the WebLogic Administrator user name.

In the **Password** text box, enter the WebLogic Administrator password.

After entering information in the fields, click **Next** to continue.

## B.5 OIM Server

Use this screen to set a password for the for the system administrator (`xelsysadm`).

***Figure B–5 OIM Server Screen***


Table B–3 describes the Oracle Identity Manager Server parameters that you can configure.

***Table B–3 Oracle Identity Manager Server Configuration Parameters***

| Field Name | Description |
|---|---|
| **OIM Administrator Password** | Enter a new password for the administrator.<br>A valid password contains at least six characters, begins with an alphabetic character, and includes at least one number, one uppercase letter and one lowercase letter. The password cannot contain first name, last name, or login name of Oracle Identity Manager.<br>Note that you are not prompted to enter this password in upgrade scenarios. You must set a password only if you are performing a new 11*g* installation. |
| **Confirm Password** | Enter the new password again to confirm. |
| **OIM HTTP URL** | Enter the http URL that front-ends the Oracle Identity Manager application. For example, `http://localhost:7002`.<br>By default, this field contains the URL of the Oracle Identity Manager Managed Server. |
| **KeyStore Password** | Enter new password for the keystore.<br>A valid password can contain 6 to 30 characters, begin with an alphabetic character, and use only alphanumeric characters and special characters like Underscore (_), Dollar ($), Pound (#). The password must contain at least one number. |
| **Confirm KeyStore Password** | Enter the new password again to confirm. |

After entering information in the fields, click **Next** to continue.

## B.6 BI Publisher

In this screen, you can perform the following optional tasks:

- Enable synchronization of Oracle Identity Manager roles, users, and their hierarchy to an LDAP directory
- Configure Oracle Identity Manager to use Oracle BI Publisher by specifying the BI publisher URL

***Figure B–6 BI Publisher Screen***


### Enabling OIM-LDAP Synchronization

If you want to enable LDAP sync, you must first set up LDAP Sync for Oracle Identity Manager (OIM) before selecting the **Enable LDAP Sync** option on this screen. For information about setting up OIM-LDAP Sync, see Completing the Prerequisites for Enabling LDAP Synchronization. After completing the prerequisites for enabling LDAP Synchronization, select the **Enable LDAP Sync** option.

If you do not want to perform the other optional tasks, click **Next** to continue.

### Configuring Oracle Identity Manager to Use Oracle BI Publisher

Ensure that Oracle BI Publisher is installed on your local or remote machine.

To configure Oracle Identity Manager to use Oracle BI Publisher, select the **Configure BI Publisher** option, and enter the BI Publisher URL in the **BI Publisher URL** text box.

The URL is of the format: `http://hostname:port/xmlpserver`, where hostname and port are the host name and the port on which the Oracle BI Publisher server is running.

After entering information in the fields, click **Next** to continue.

## B.7 LDAP Server

This screen is displayed only if you select the **Enable LDAP Sync** option on the BI Publisher screen. In the LDAP Server screen, you should specify the authentication information for the Directory Server, as you want to synchronize Oracle Identity Manager roles, users, and their hierarchy to an LDAP directory.

*Figure B–7 LDAP Server Screen*

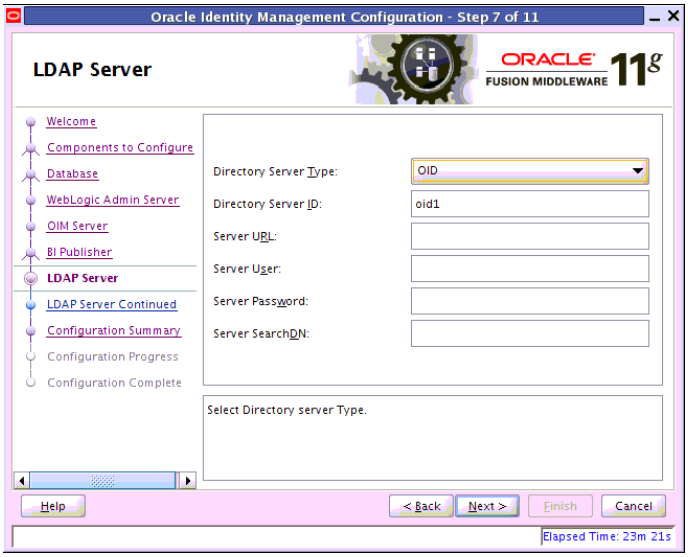



Table B–4 describes the parameters that you must specify.

*Table B–4 LDAP Server Information*

| Field Name | Description |
|---|---|
| **Directory Server Type** | Select the desired Directory Server from the dropdown list. |
| **Directory Server ID** | Enter the Directory Server ID. |
| Server URL | Enter the LDAP URL in the format:<br>`ldap://oid_host:oid_port` |
| **Server User** | Enter the user name for the Directory Server administrator.<br>For example:<br>`cn=oimAdminUser,cn=Users,dc=us,dc=oracle,dc` |
| **Server Password** | Enter the OIM admin password |
| **Server SearchDN** | Enter the Distinguished Names (DN).<br>For example, `dc=acme`, `dc=com`<br>This is the top-level container for users and roles in LDAP that is used for Oracle Identity Manager for reconciliation purposes. |

After entering information in the fields, click **Next** to continue.

## B.8 LDAP Server Continued

This screen is a continuation of the LDAP Server screen.

*Figure B–8 LDAP Server Continued Screen*

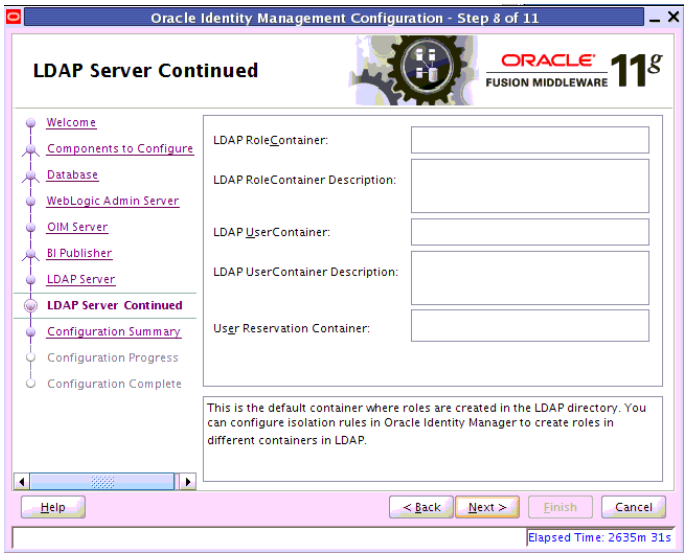



Table B–5 describes the LDAP parameters that you must specify.

*Table B–5 LDAP Server Continued Information*

| Field Name | Description |
|---|---|
| **LDAP RoleContainer** | Enter a name for the container that will be used as a default container of roles in the LDAP directory. |
| **LDAP RoleContainer Description** | Type a description for the role container. |
| **LDAP UserContainer** | Enter a name for the container that will be used as a default container of users in the LDAP directory. |
| **LDAP UserContainer Description** | Type a description for the user container. |
| **User Reservation Container** | Enter a name for the container that will be used for reserving user names in the LDAP directory while their creation is being approved in Oracle Identity Manager. When the user names are approved, they are moved from the reservation container to the user container in the LDAP directory. |

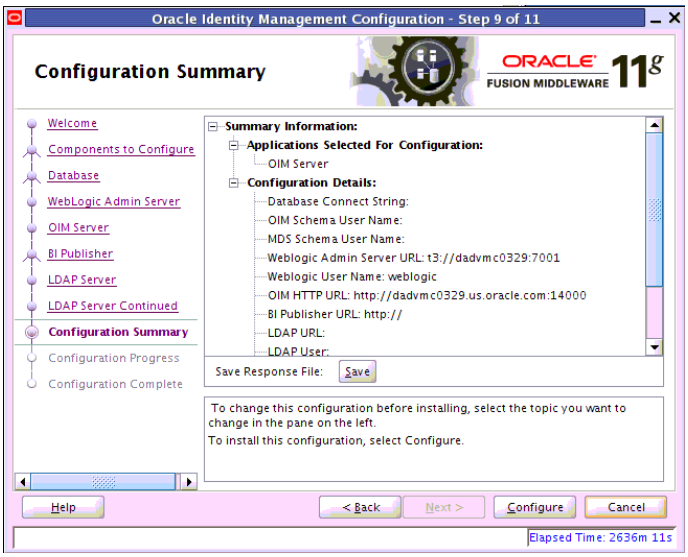
After entering information in the fields, click **Next** to continue.

## B.9 Configuration Summary

This screen displays a list of the applications or components you have selected for configuration. It includes the following information:

- Location of your installation
- Disk space that will be used for the installation
- Applications or components you have selected for configuration
- Configuration choices you made on different screens in the Oracle Identity Manager Configuration Wizard

***Figure B–9 Configuration Summary Screen***




Review this summary screen.

Additionally, you can select to create a response file from your installation selections by clicking on the **Save** button in the Save Response File field. A response file can be used for silent or non-interactive installations of software requiring no or very little user input.

Click **Configure** to start configuring the selected Oracle Identity Manager components.

# C

# Starting or Stopping the Oracle Stack

You must start or stop the components of the Oracle stack in a specific order. This appendix describes that order and contains the following topics:

- Starting the Stack
- Stopping the Stack
- Restarting Servers

---

**Note:** When executing the startManagedWebLogic and stopManagedWebLogic scripts described in the following topics:

- *SERVER_NAME* represents the name of the Oracle WebLogic Managed Server, such as wls_oif1, wls_ods1, or oam_server1.
- You will be prompted for values for *USER_NAME* and *PASSWORD* if you do not provide them as options when you execute the script.
- The value for *ADMIN_URL* will be inherited if you do not provide it as an option when you execute the script.

---

## C.1 Starting the Stack

After completing the installation and domain configuration, you must start the Administration Server and various Managed Servers to get your deployments up and running:

1. To start the Administration Server, run the `startWebLogic.sh` (on UNIX operating systems) or `startWebLogic.cmd` (on Windows operating systems) script in the directory where you created your new domain.

   On UNIX systems:

   *MW_HOME*`/user_projects/domains/`*domain_name*`/startWebLogic.sh`

   On Windows systems:

   *MW_HOME*`\user_projects\domains\`*domain_name*`\startWebLogic.cmd`

   You entered the domain name and location on the Specify Domain Name and Location Screen in the Configuration Wizard.

2. Ensure that the Node Manager is running. Oracle WebLogic Administration Server does not do this automatically. If the Node Manager is not running, start the Node Manager by executing the following command:

```
$WLS_HOME/server/bin/startNodeManager.sh
```

3. Start system components, such as Oracle Internet Directory and Oracle Virtual Directory, by executing the following command:

   ```
   ORACLE_INSTANCE/bin/opmnctl startall
   ```

   You can verify that the system components have started by executing the following command:

   ```
   ORACLE_INSTANCE/bin/opmnctl status -l
   ```

4. To start the Managed Servers, run the `startManagedWebLogic.sh` (on UNIX operating systems) or `startManagedWebLogic.cmd` (on Windows operating systems) script in the `bin` directory inside the directory where you created your domain. You must start these Managed Servers from the command line.

   This command also requires that you specify a server name. You must start the servers you created when configuring the domain, as shown in the following example:

   - `oam_server1` (Oracle Access Manager Server)
   - `oim_server1` (Oracle Identity Manager Server)

   For example, to start Oracle Access Manager Server on a UNIX system:

   ```
   MW_HOME/user_projects/domains/domain_name/bin/startManagedWebLogic.sh oam_
   server1
   ```

   On Windows systems:

   ```
   MW_HOME\user_projects\domains\domain_name\bin\startManagedWebLogic.cmd oam_
   server1
   ```

   Before the Managed Server is started, you are prompted for the WebLogic Server user name and password. These were provided on the Configure Administrator Username and Password Screen in the Configuration Wizard.

   If your Administration Server is using a non-default port, or resides on a different host than your Managed Servers (in a distributed environment), you must also specify the URL to access your Administration Server.

   On UNIX systems:

   ```
   MW_HOME/user_projects/domains/domain_name/bin/startManagedWebLogic.sh oam_
   server1 http://host:admin_server_port
   ```

   On Windows systems:

   ```
   MW_HOME\user_projects\domains\domain_name\bin\startManagedWebLogic.cmd oam_
   server1 http://host:admin_server_port
   ```

   Instead of being prompted for the Administration Server user name and password, you can also specify them directly from the command lime.

   On UNIX systems:

   ```
   MW_HOME/user_projects/domains/domain_name/bin/startManagedWebLogic.sh oam_
   server1 http://host:admin_server_port -Dweblogic.management.username=user_name
   -Dweblogic.management.password=password
   ```

   On Windows systems:

   ```
   MW_HOME\user_projects\domains\domain_name\bin\startManagedWebLogic.cmd oam_
   ```

```
server1 http://host:admin_server_port -Dweblogic.management.username=user_name
-Dweblogic.management.password=password
```

**Note:** You can use the Oracle WebLogic Administration Console to start managed components in the background. See *Oracle Fusion Middleware Introduction to Oracle WebLogic Server* for more information.

If you do not know the names of the Managed Servers that should be started, you can view the contents of the following file on UNIX systems:

```
MW_HOME/user_projects/domains/domain_name/startManagedWebLogic_readme.txt
```

On Windows systems:

```
MW_HOME\user_projects\domains\domain_name\startManagedWebLogic_readme.txt
```

Or, you can access the Administration Server console at the following URL:

```
http://host:admin_server_port/console
```

Supply the user name and password that you specified on the Configure Administrator Username and Password Screen of the Configuration Wizard. Then, navigate to **Environment > Servers** to see the names of your Managed Servers.

## C.2 Stopping the Stack

You can stop the Oracle WebLogic Administration Server and all the managed servers by using Oracle WebLogic Administration Console. See *Oracle Fusion Middleware Introduction to Oracle WebLogic Server* for more information.

To stop the stack components from the command line, perform the following steps:

1. Stop WebLogic managed components, such as Oracle Directory Integration Platform, Oracle Identity Federation, Oracle Directory Services Manager, Oracle Access Manager, Oracle Identity Manager, and Oracle Adaptive Access Manager, by executing the following command:

   ```
   MW_HOME/user_projects/domains/DOMAIN_NAME/bin/stopManagedWebLogic.sh \
   {SERVER_NAME} {ADMIN_URL} {USER_NAME} {PASSWORD}
   ```

2. Stop system components, such as Oracle Internet Directory and Oracle Virtual Directory, by executing the following command:

   ```
   ORACLE_INSTANCE/bin/opmnctl stopall
   ```

3. Stop the Oracle WebLogic Administration Server by executing the following command:

   ```
   MW_HOME/user_projects/domains/DOMAIN_NAME/bin/stopWebLogic.sh
   ```

4. If you want to stop the Node Manager, you can use the `kill` command:

   ```
   kill -9 PID
   ```

## C.3 Restarting Servers

To restart the Administration Server or Managed Servers, you must stop the running Administration Server or Managed Servers first before starting them again. For more information, see Stopping the Stack and Starting the Stack.

# D

# Preconfiguring Oracle Directory Server Enterprise Edition (ODSEE)

Before you can use your LDAP directory as an Identity store, you must preconfigure it. The procedure in this section enables you to preconfigure Oracle Directory Server Enterprise Edition (ODSEE) for using Oracle Directory Server Enterprise Edition (ODSEE) as your LDAP Identity store.

**Notes:**

- If your LDAP Identity store (Oracle Directory Server Enterprise Edition (ODSEE) or iPlanet) has been configured for the containers and oimadminuser with the schema extension, you need not follow the below mentioned configuration steps.
- The data used in the examples provided below is a sample data. Follow the examples and replace them with appropriate data as per your LDAP server configuration.
- `cn=oracleAccounts` is a sample data. It is not mandatory to use this data when you preconfigure the Identity Store.

You must complete the following steps to preconfigure the Identity Store:

1. Create a new file `iPlanetContainers.ldif`. Add the following entries and save the file.

```
dn:cn=Users,dc=mycompany,dc=com
cn:Users
objectClass:nsContainer

dn:cn=Groups,dc=mycompany,dc=com
cn:Groups
objectClass:nsContainer

dn:cn=Reserve,dc=mycompany,dc=com
cn:Reserve
objectClass:nsContainer
```

2. Import the containers into iPlanet Directory Server with `ldapadd` command. This will create the user, group and reserve containers.

```
ldapadd -h <ODSEE Server> -p <ODSEE port> -D <ODSEE Admin ID> -w <ODSEE Admin
password> -c -f ./iPlanetContainers.ldif
```

For example:

```
ldapadd -h localhost -p 1389 -D "cn=Directory Manager" -w "welcome1" -c -f
./iPlanetContainers.ldif
```

If the above gives authentication error, try the command with '-x' option with simple bind option.

```
ldapadd -h localhost -p 1389 -x -D "cn=Directory Manager" -w "welcome1" -c -f
./iPlanetContainers.ldif
```

3. Enable the `moddn` property for the rename of entries to happen between nodes.

```
..dsee7/bin/dsconf set-server-prop -h <ODSEE Server> -p <ODSEE port>
moddn-enabled:on
```

For example:

```
..dsee7/bin/dsconf set-server-prop -h localhost -p 1389 moddn-enabled:on
```

4. Enable changelog.

```
..dsee7/bin/dsconf set-server-prop -h <ODSEE Server> -p <ODSEE port>
retro-cl-enabled:on
```

For example:

```
..dsee7/bin/dsconf set-server-prop -h localhost -p 1389 retro-cl-enabled:on
```

5. Check the status.

```
..dsee7/bin/dsccsetup status
```

6. Stop and Start the ODSEE server instance.

```
..dsee7/bin/dsadm stop <ODSEE instance>
..dsee7/bin/dsadm start <ODSEE instance>
```

For example:

```
..dsee7/bin/dsadm stop /scratch/<userid>/iPlanet/dsinst1/
..dsee7/bin/dsadm start /scratch/<userid>/iPlanet/dsinst1/
```

7. Extend the Sun schema to include OIM-specific Object Classes and Attribute Types.

```
cd to $MIDDLEWARE_HOME/oracle_common/modules/oracle.ovd_11.1.1/oimtemplates
```

Run the following command to load the ldif file, `sunOneSchema.ldif`.

```
ldapmodify -h <ODSEE Server> -p <ODSEE port> -D <ODSEE Admin ID> -w <ODSEE
Admin password> -f sunOneSchema.ldif
```

For example:

```
./ldapmodify -h localhost -p 1389 -D "cn=directory manager" -w welcome1 -c -f
sunOneSchema.ldif
```

8. Enable Referential Integrity for OIM's Common Name Generation feature.

Anytime the DN or RDN is being modified, then the Referential Integrity needs to be enabled in OIM and OID/Active Directory/ODSEE.

If Referential Integrity is enabled in the Directory Server, then customers need to set the OIM property `XL.IsReferentialIntegrityEnabledInLDAP` to `TRUE` as by default it is set to `FALSE`. To set `XL.IsReferentialIntegrityEnabledInLDAP` to `TRUE`, log into OIM and go to **Advanced** > **System Management** > **System**

**Configuration**. Search for System Properties (`XL.IsReferentialIntegrityEnabled`), and set the property value to `TRUE`.

**a.** Use the following command to see the value of the referential integrity property.

```
..dsee7/bin/dsconf get-server-prop -h <ODSEE server> -p <ODSEE port>
ref-integrity-enabled
Enter "cn=Directory Manager" password:
ref-integrity-enabled : off
```

**b.** Use the following commands to enable the referential integrity property.

```
./dsconf set-server-prop -h <ODSEE server> -p <ODSEE port>
ref-integrity-enabled:on
Enter "cn=Directory Manager" password:
```

Directory Server must be restarted for changes to take effect. Restart ODSEE/iPlanet Server after enabling referential integrity property.

```
..dsee7/bin/dsadm stop <ODSEE instance>
..dsee7/bin/dsadm start <ODSEE instance>
```

For Example:

```
..dsee7/bin/dsadm stop /scratch/<userid>/iPlanet/dsinst1/
..dsee7/bin/dsadm start /scratch/<userid>/iPlanet/dsinst1/
```

**c.** Now query to see if the value has been set correctly.

```
..dsee7/bin/dsconf get-server-prop -h <ODSEE server> -p <ODSEE port>
ref-integrity-enabled
Enter "cn=Directory Manager" password:
ref-integrity-enabled : on
```

**9.** Create the OIM Admin User, Group and the ACIs. Open a new file `oimadminuser.ldif`. This oimadminuser would be used as a proxy user for OIM.

The root suffix is given as `dc=mycompany,dc=com`. This can be replaced with the appropriate root suffix of the ODSEE server.

**a.** Add the following LDAP entries and save the file `oimadminuser.ldif`. Run the following command to load the ldif file, `oimadminuser.ldif`.

```
ldapmodify -h <ODSEE Server> -p <ODSEE port> -D <ODSEE Admin ID> -w <ODSEE
Admin password> -f oimadminuser.ldif

dn: cn=systemids,dc=mycompany,dc=com
changetype: add
objectclass: nsContainer
objectclass: top
cn: systemids

dn: cn=oimAdminUser,cn=systemids,dc=mycompany,dc=com
changetype: add
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetorgperson
mail: oimAdminUser
givenname: oimAdminUser
sn: oimAdminUser
cn: oimAdminUser
```

```
uid: oimAdminUser
userPassword: welcome1

dn: cn=oimAdminGroup,cn=Groups,dc=mycompany,dc=com
changetype: add
objectclass: groupOfUniqueNames
objectclass: top
cn: oimAdminGroup
description: OIM administrator role
uniquemember: cn=oimAdminUser,cn=systemids,dc=mycompany,dc=com

dn: cn=users,dc=mycompany,dc=com
changetype: modify
add: aci
aci: (target = "ldap:///cn=users,dc=mycompany,dc=com")(targetattr =
 "*")(version 3.0; acl "Allow OIMAdminGroup add, read and write access to
 all attributes"; allow (add, read, search, compare,write, delete, import)
 (groupdn = "ldap:///cn=oimAdminGroup,cn=Groups,dc=mycompany,dc=com");)

dn: cn=Groups,dc=mycompany,dc=com
changetype: modify
add: aci
aci: (target = "ldap:///cn=Groups,dc=mycompany,dc=com")(targetattr =
 "*")(version 3.0; acl "Allow OIM AdminGroup to read and write access";
 allow (read, search, compare, add, write,delete) (groupdn =
 "ldap:///cn=oimAdminGroup,cn=Groups,dc=mycompany,dc=com");)

dn: cn=reserve,dc=mycompany,dc=com
changetype: modify
add: aci
aci: (target = "ldap:///cn=reserve,dc=mycompany,dc=com")(targetattr =
 "*")(version 3.0; acl "Allow OIM AdminGroup to read and write access";
 allow (read, search, compare, add, write,delete,export) (groupdn =
 "ldap:///cn=oimAdminGroup,cn=Groups, dc=mycompany,dc=com");)

dn: cn=changelog
changetype: modify
add: aci
aci: (target = "ldap:///cn=changelog")(targetattr = "*")(version 3.0; acl
 "Allow OIM AdminGroup to read and write access"; allow (read, search,
 compare, add, write,delete,export) (groupdn =
 "ldap:///cn=oimAdminGroup,cn=Groups, dc=mycompany,dc=com");)
```

**b.** Use the following commands to check for the entries and ACI in the LDAP:

```
ldapsearch -h <ODSEE Server> -p <ODSEE Port> -x -D "cn=Directory Manager"
 -w <ODSEE Admin Password> -b "cn=changelog" -s sub "objectclass=*" aci

ldapsearch -h <ODSEE Server> -p <ODSEE Port> -x -D "cn=Directory Manager"
 -w <ODSEE Admin Password> -b "cn=users,dc=mycompany,dc=com" -s sub
 "objectclass=*" aci

ldapsearch -h <ODSEE Server> -p <ODSEE Port> -x -D "cn=Directory Manager"
 -w <ODSEE Admin Password> -b "cn=groups,dc=mycompany,dc=com" -s sub
 "objectclass=*" aci
ldapsearch -h <ODSEE Server> -p <ODSEE Port> -x -D "cn=Directory Manager"
 -w <ODSEE Admin Password> -b "cn=reserve,dc=mycompany,dc=com" -s sub
 "objectclass=*" aci
```

# E

# Deinstalling and Reinstalling Oracle Identity and Access Management

This appendix provides information about deinstalling and reinstalling Oracle Identity and Access Management 11*g* Release 1 (11.1.1). It contains the following topics:

- Deinstalling Oracle Identity and Access Management
- Reinstalling Oracle Identity and Access Management

> **Note:** Always use the instructions provided in this appendix for removing the software. If you try to remove the software manually, you may experience problems when you try to reinstall the software. Following the procedures in this appendix ensures that the software is properly removed.

## E.1 Deinstalling Oracle Identity and Access Management

This topic contains procedures for deinstalling Oracle Identity and Access Management. It contains the following sections:

- Deinstalling the Oracle Identity and Access Management Oracle Home
- Deinstalling the Oracle Common Home

### E.1.1 Deinstalling the Oracle Identity and Access Management Oracle Home

The deinstaller attempts to remove the Oracle Home directory from which it was started. Before you choose to remove your Oracle Identity and Access Management Oracle Home directory, make sure that it is not in use by an existing domain and that you stop all running processes that use this Oracle Home.

Deinstalling Oracle Identity and Access Management will not remove any WebLogic domains that you have created—it only removes the software in the Oracle Identity and Access Management Oracle Home directory.

> **Note:** The oraInventory is required for removing instances and Oracle Home. For example, on UNIX it can be found in the following location:
>
> /etc/oraInst.loc

This section describes how to deinstall your Oracle Identity and Access Management Oracle Home using the graphical, screen-based deinstaller. However, you can also

perform a silent deinstallation using a response file. A deinstall response file template that you can customize for your deinstallation is included in the `Disk1/stage/Response` directory on UNIX, or in the `Disk1\stage\Response` directory on Windows.

Perform the following steps to deinstall your Oracle Identity and Access Management Oracle Home using the graphical, screen-based deinstaller:

1. Verify your Oracle Identity and Access Management Oracle Home is not in use by an existing domain.
2. Stop all processes that use the Oracle Identity and Access Management Oracle Home.
3. Open a command prompt and move (cd) into the *`IDM_ORACLE_HOME`*`/oui/bin directory` (UNIX) or the *`IAM_HOME`*`\oui\bin directory` (Windows).
4. Invoke the Deinstaller from command line using the `-deinstall` option. For example:

   On UNIX:

   ```
   ./runInstaller -deinstall
   ```

   On Windows:

   ```
   setup.exe -deinstall
   ```

   The Welcome screen appears.
5. Click **Next**.

   In the Deinstall Oracle Home screen, you can save a response file that contains the deinstallation settings before deinstalling. Click **Deinstall**. The Deinstall Progress screen appears. This screen shows the progress and status of the deinstallation.

   Click **Finish** after the deinstallation progresses to 100%. The Deinstallation Complete screen appears.
6. Click **Finish** on the Deinstallation Complete screen to exit the deinstaller.

## E.1.2 Deinstalling the Oracle Common Home

The *`ORACLE_COMMON_HOME`* directory located in the *`MW_HOME`* directory contains the binary and library files required for Oracle Enterprise Manager Fusion Middleware Control and Oracle Java Required Files (JRF). Before you deinstall the *`ORACLE_COMMON_HOME`* directory, ensure that no other Oracle Fusion Middleware software, such as Oracle SOA Suite, depends on *`ORACLE_COMMON_HOME`*. You cannot deinstall the *`ORACLE_COMMON_HOME`* directory until all software that depends on it has been deinstalled.

Perform the following steps to deinstall the *`ORACLE_COMMON_HOME`* directory:

1. Stop all processes that use the *`ORACLE_COMMON_HOME`* directory. To know all the processes that are using ORACLE_COMMON_HOME directory use the following commands:

   On UNIX:

   ```
   ps-ef grep <oracle_common>
   ```

   On Windows:

Use the Windows Task Manager to identify the processes that use the ORACLE_COMMON_HOME directory.

2. Deinstall your Oracle Identity and Access Management Oracle Home by performing the steps in Deinstalling the Oracle Identity and Access Management Oracle Home.

3. Open a command prompt and move (cd) into the *ORACLE_COMMON_HOME*/oui/bin/ directory (on UNIX) or the *ORACLE_COMMON_HOME*\oui\bin\ directory (on Windows).

4. Invoke the Deinstaller from command line using the -deinstall option and the -jreLoc option, which identifies the location where Java Runtime Environment (JRE) is installed. For example:

   On UNIX:

   ```
   ./runInstaller -deinstall -jreLoc FULL_PATH_TO_JRE_DIRECTORY
   ```

   On Windows:

   ```
   setup.exe -deinstall -jreLoc FULL_PATH_TO_JRE_DIRECTORY
   ```

   The Welcome screen appears.

5. Click **Next**. The Select Deinstallation Type screen appears.

6. Select the **Deinstall Oracle Home** option at the top of the Select Deinstallation Type screen.

   **Note:** The path to the *ORACLE_COMMON_HOME* directory appears in the text describing the **Deinstall Oracle Home** option.

   Click **Next**. The Deinstall Oracle Home screen appears.

7. Confirm the correct *ORACLE_COMMON_HOME* directory is listed and click **Deinstall**.

   The Deinstallation Progress screen appears, along with a Warning dialog box prompting you to confirm that you want to deinstall the *ORACLE_COMMON_HOME* directory.

8. Click **Yes** on the Warning dialog box to confirm you want to remove the *ORACLE_COMMON_HOME* directory. The deinstallation begins.

9. Click **Finish** after the deinstallation progresses to 100%. The Deinstallation Complete screen appears.

10. Click **Finish** on the Deinstallation Complete screen to exit the deinstaller.

## E.2 Reinstalling Oracle Identity and Access Management

Perform the following steps to reinstall Oracle Identity and Access Management:

1. Verify the directory you want to reinstall Oracle Identity and Access Management into, does not contain an existing Oracle Identity and Access Management instance. If it does, you must deinstall it before reinstalling. You cannot reinstall Oracle Identity and Access Management 11g Release1(11.1.1) in a directory that contains an existing Oracle Identity and Access Management instance.

2. Reinstall Oracle Identity and Access Management as if it was the first installation by performing the steps in the appropriate procedure in this guide.

# F

# Performing a Silent Installation

This appendix describes how to install Oracle Identity Management in silent mode. This appendix contains the following topics:



## F.1 What is a Silent Installation?

A silent installation eliminates the need to monitor the Oracle Identity Management installation because no graphical output is displayed and no input by the user is required.

To perform a silent Oracle Identity Management installation, you invoke the Installer with the -silent flag and provide a response file from the command line. The response file is a text file containing variables and parameter values which provide answers to the Installer prompts.

## F.2 Before Performing a Silent Installation

This topic describes tasks that may be required before you perform a silent installation. This topic includes the following sections:



### F.2.1 UNIX Systems: Creating the oraInst.loc File

The Installer uses the Oracle inventory directory to keep track of all Oracle products installed on the systems. The inventory directory is stored in a file named oraInst.loc. If this file does not already exist on your system, you must create it before starting a silent installation.

Perform the following steps to create the `oraInst.loc` file if it does not exist:

1. Log in as the root user.
2. Using a text editor such as vi or emacs, create the oraInst.loc file in any directory. The contents of the file consist of the following two lines:

```
inventory_loc=oui_inventory_directory
inst_group=oui_install_group
```

Replace *oui_inventory_directory* with the full path to the directory where you want the Installer to create the inventory directory. Replace *oui_install_group* with the name of the group whose members have write permissions to this directory.

3. Exit from the root user.

> **Note:** After you performing the silent installation on UNIX platforms, you must run the *ORACLE_HOME*/root.sh script as the root user. The root.sh script detects settings of environment variables and enables you to enter the full path of the local bin directory.

### F.2.2 Windows Systems: Creating the Registry Key

If you have not installed Oracle Identity Management on your system, you must create the following Registry key and value:

```
HKEY_LOCAL_MACHINE / SOFTWARE / Oracle / inst_loc = [inventory_directory]
```

Replace *inventory_directory* with the full path to your Installer files. For example: C:\Program Files\Oracle\Inventory

## F.3 Creating Response Files

Before performing a silent installation, you must provide information specific to your installation in a response file. Response files are text files that you can create or edit in a text editor. The Installer will fail if you attempt a silent installation using a response file that is not configured correctly.

Several default response files, which you can use as templates and customize for your environment, are included in the installation media. These default response files are located in the Disk1/stage/Response directory on UNIX, or in the Disk1\stage\Response directory on Windows.

#### Creating Response Files for Oracle Identity Management Software Installation

When you use the Oracle Identity Management Installation Wizard to install the software for the first time, you can save a summary of your installation in a response file.

To create a response file for Oracle Identity and Access Management software Installer for Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Entitlements Server, and Oracle Identity Navigator, complete the following steps:

1. On the Installation Summary screen in the installation wizard, click **Save** in the **Save Response File** field.
2. When prompted, save the file to a local directory.

#### Creating Response Files for Oracle Identity Manager Configuration

When you use the Oracle Identity Manager Configuration Wizard to configure Oracle Identity Manager Server, Design Console, or Remote Manager for the first time, you can save a summary of your configuration in a response file.

To create this response file, complete the following steps:

1. On the Configuration Summary screen in the installation wizard, click **Save** in the **Save Response File** field.
2. When prompted, save the file to a local directory.

### F.3.1 OID, OVD, ODSM, ODIP, and OIF

The following is a list of the default response files included in the installation media for the Oracle Identity Management Suite containing Oracle Internet Directory (OID), Oracle Virtual Directory (OVD), Oracle Directory Services Manager (ODSM), Oracle Directory Integration Platform (ODIP), and Oracle Identity Federation (OIF):

- im_install_only.rsp: Use this response file to install Oracle Identity Management components without configuring them.
- im_install_config.rsp: Use this response file to install and configure Oracle Identity Management components.
- im_config_only.rsp: Use this response file with the Oracle Identity Management 11g Release 1 (11.1.1) Configuration Wizard (config.sh script or config.bat) in *ORACLE_HOME*/bin/ to configure installed components.

### F.3.2 OIM, OAM, OAAM, OES, and OIN

The following is a list of the default response files included in the installation media for the Oracle Identity Management Suite containing Oracle Identity Manager (OIM), Oracle Access Manager (OAM), Oracle Adaptive Access Manager (OAAM), Oracle Entitlements Server (OES), and Oracle Identity Navigator (OIN):

- iamsuite_install_only.rsp: Use this response file to install Oracle Identity Management components without configuring them.
- iamsuite_config_only.rsp: Use this response file with the Oracle Identity Manager 11*g* Release 1 (11.1.1) Configuration Wizard (config.sh script or config.bat) in *ORACLE_HOME*/bin/ to configure Oracle Identity Manager Server, Design Console, and Remote Manager.
- deinstall_oh.rsp: Use this response file with the Oracle Identity Management 11*g* Release 1 (11.1.1) Deinstaller to deinstall installed components.

### F.3.3 Securing Your Silent Installation

Your response files contain certain passwords required by the Installer. To minimize security issues regarding these passwords in the response file, follow these guidelines:

- Set the permissions on the response files so that they are readable only by the operating system user who will be performing the silent installation.
- If possible, remove the response files from the system after the silent installation is completed.

## F.4 Performing a Silent Installation

To perform a silent Oracle Identity Management installation, you invoke the Installer with the -silent flag and provide a response file from the command line.

#### On UNIX

The following is the syntax for running the Installer from the command line on UNIX systems:

```
runInstaller [-mode] [-options] [(COMMAND_LINE_VARIABLE=VARIABLE_VALUE)*]
```

For example:

```
./runInstaller -silent -response FILE
```

### On Windows

The following is the syntax for running the Installer from the command line on Windows systems:

```
setup.exe [-mode] [-options] [(COMMAND_LINE_VARIABLE=VARIABLE_VALUE)*]
```

For example:

```
setup.exe -silent -response FILE
```

## F.5 Installer Command Line Parameters

Table F–1 lists and describes supported Installer command line parameters:

***Table F–1 Installer Command Line Parameters***

| Parameter | Description |
|---|---|
| **Installation Modes - Only One Mode Can be Specified** | |
| -i \| -install | Launches the Installer in GUI mode. This is the default mode and is used if no mode is specified on the command line. |
| -silent | Install in silent mode. The Installer must be passed either a response file or command line variable value pairs. |
| -d \| -deinstall | Launches the Installer in GUI mode for deinstallation. |
| -p \| -prerequisite | Launches the Installer in GUI mode but only checks the prerequisites. No software is installed. |
| -v \| -validate | Launches the Installer in GUI mode and performs all prerequisite and validation checking, but does not install any software. |
| -sv \| -silentvalidate | Performs all prerequisite and validation checking in silent mode. You must pass the Installer either a response file or a series of command line variable value pairs. |
| **Installation Options** | |
| -help \| --help \| --usage | Displays the usage parameters for the runInstaller command. |
| -invPtrLoc *file* | Pointer to the inventory location file. Replace file with the full path and name of the oraInst.loc file. |
| -response *file* \| -responseFile *file* | Pointer to the response file. Replace file with the full path and name of the response file. |
| -jreLoc *location* | Pointer to the location where Java Runtime Environment (JRE) is installed. Replace *location* with the full path to the jre directory where your JRE is installed. |

*Table F–1 (Cont.) Installer Command Line Parameters*

| Parameter | Description |
|---|---|
| -logLevel *level* | Specify the level of logging performed by the Installer; all messages with a lower priority than the specified level will be recorded. Valid levels are:<br>■ severe<br>■ warning<br>■ info<br>■ config<br>■ fine<br>■ finer<br>■ finest |
| -debug | Obtain debug information from the Installer. |
| -force | Allow the silent installation to proceed in a non-empty directory. |
| -printdiskusage | Log debugging information pertaining to disk usage. |
| -printmemory | Log debugging information pertaining to memory usage. |
| -printtime | Log debugging information pertaining to time usage. This command causes the timeTakentimestamp.log file to be created. |
| -waitforcompletion | Windows only - the Installer will wait for completion instead of spawning the Java engine and exiting. |
| -noconsole | Messages will not be displayed to the console window. |
| -ignoreSysPrereqs | Ignore the results of the system prerequisite checks and continue with the installation. |
| -executeSysPrereqs | Execute the system prerequisite checks only, then exit. |
| -paramFile *file* | Specify the full path to the oraparam.ini file. This file is the initialization file for the Installer. The default location of this file is Disk1/install/platform. |
| -novalidation | Disables all validation checking performed by the Installer. |
| -nodefaultinput | For the GUI install, several screens have information or default values pre-populated. Specifying this option disables this behavior so that no information or values are pre-populated. |
| **Command Line Variables** | |
| Installer Variables | Installer variables are specified using *varName=value*. For example:<br>`ORACLE_HOME=/scratch/install/IDM_Home` |
| Session Variables | Session variables are specified using session:*varName=value* |

# G

# Troubleshooting the Installation

This appendix describes solutions to common problems that you might encounter when installing Oracle Identity Management. It contains the following topics:

- General Troubleshooting Tips
- Installation Log Files
- Configuring OIM Against an Existing OIM 11g Schema
- Need More Help?

## G.1 General Troubleshooting Tips

If you encounter an error during installation:

- Consult the Oracle Fusion Middleware 11*g* Release 1 (11.1.1). You can access the Release Notes on the Oracle Technology Network (OTN) Documentation Web site. To access this Web site, go to the following URL:

  `http://www.oracle.com/technetwork/indexes/documentation/index.html`

- Verify your system and configuration is certified. See Reviewing System Requirements and Certification for more information.
- Verify your system meets the minimum system requirements. See Reviewing System Requirements and Certification for more information.
- Verify you have satisfied the dependencies for the deployment you are attempting. Each deployment documented in this guide contains a "Dependencies" section.
- If you entered incorrect information on one of the installation screens, return to that screen by clicking **Back** until you see the screen.
- If an error occurred while the Installer is copying or linking files:
  1. Note the error and review the installation log files.
  2. Remove the failed installation. See Appendix E, "Deinstalling and Reinstalling Oracle Identity and Access Management" for more information.
  3. Correct the issue that caused the error.
  4. Restart the installation.
- If an error occurred while configuring Oracle Identity Manager using the Oracle Identity Manager Configuration Wizard:
  1. Note the error and review the configuration log files.

2. Verify whether the dependencies are met. For example, Administration Server and Database should be up and running.
3. Correct the issue that caused the error.
4. Restart the Oracle Identity Manager Configuration Wizard.

## G.2 Installation Log Files

The Installer writes log files to the *ORACLE_INVENTORY_LOCATION*/logs directory on UNIX systems and to the *ORACLE_INVENTORY_LOCATION*\logs directory on Windows systems.

On UNIX systems, if you do not know the location of your Oracle Inventory directory, you can find it in the *ORACLE_HOME*/oraInst.loc file.

On Microsoft Windows systems, the default location for the inventory directory is C:\Program Files\Oracle\Inventory\logs.

The server log files are created in the <DOMAIN_HOME>/server/<servername/logs directory.

The following install log files are written to the log directory:

- install*DATE-TIME_STAMP*.log
- install*DATE-TIME_STAMP*.out
- installActions*DATE-TIME_STAMP*.log
- installProfile*DATE-TIME_STAMP*.log
- oraInstall*DATE-TIME_STAMP*.err
- oraInstall*DATE-TIME_STAMP*.log

## G.3 Configuring OIM Against an Existing OIM 11*g* Schema

In this scenario, you have created and loaded the appropriate Oracle Identity Manager (OIM) schema, installed and configured Oracle Identity Manager in a new or existing WebLogic domain. During domain configuration, you have configured JDBC Component Schemas by using the Oracle Fusion Middleware Configuration Wizard.

If you want to configure Oracle Identity Manager in a second WebLogic domain against the existing Oracle Identity Manager 11*g* schemas, you must complete the following steps when you try to configure Oracle Identity Manager using the Oracle Identity Manager Configuration Wizard:

1. When prompted, you must copy the `.xldatabasekey` file from the first WebLogic domain directory (`/<MW_HOME>/user_projects/domains/<name_of_your_first_oim_domain>/config/fmwconfig/`) to the second WebLogic domain directory (`/<MW_HOME>/user_projects/domains/<name_of_your_second_oim_domain>/config/fmwconfig/`). Proceed with the Oracle Identity Manager configuration.
2. After configuring Oracle Identity Manager using the Oracle Identity Manager Configuration Wizard, copy the `cwallet.so`, `default_keystore.jks`, and `xlserver.crt` files from the first WebLogic domain directory (`/<MW_HOME>/user_projects/domains/<name_of_your_first_oim_domain>/config/fmwconfig/`) to the second domain Home directory (`/<MW_HOME>/user_projects/domains/<name_of_your_second_oim_domain>/config/fmwconfig/`).

3. After copying the files, start the Oracle Identity Manager Managed Server, as described in Starting the Stack.

## G.4 Need More Help?

If you cannot solve a problem using the information in this appendix, look for additional information in My Oracle Support at

http://support.oracle.com.

If you cannot find a solution to your problem, open a service request.

# H

# OAAM Partition Schema Reference

This appendix provides information about tables and stored procedures used with Oracle Adaptive Access Manager with Partition support.

It contains the following topics:



## H.1 Overview

Database tables in the Oracle Adaptive Access Manager database are divided into the following categories:

- Static partition tables
- Transactional partition tables
- Non-partitioned tables

---

**Note:** All the tables contain the composite partition (RANGE, HASH). The Range partition is created using CREATE_TIME while the HASH key is defined based on application logic.

Table H–1 lists the Oracle Adaptive Access Manager partition tables. All the other tables are non-partitioned.

---

*Table H–1 OAAM Database Partition Tables*

| Table Type | Frequency | Table Name |
|---|---|---|
| Static Partition | Monthly | V_USER_QA |
| | | V_USER_QA_HIST |
| Transactional Partition | Monthly | VCRYPT_TRACKER_NODE_HISTORY |
| | | VCRYPT_TRACKER_USERNODE_LOGS |
| | | VCRYPT_TRACKER_NODE |
| | | VT_USER_DEVICE_MAP |
| | | V_MONITOR_DATA |
| | | VT_SESSION_ACTION_MAP |
| | | VT_ENTITY_ONE |
| | | VT_ENTITY_ONE_PROFILE |
| | | VT_USER_ENTITY1_MAP |
| | | VT_ENT_TRX_MAP |
| | | VT_TRX_DATA |
| | | VT_TRX_LOGS |
| Transactional Partition | Weekly | VR_POLICYSET_LOGS |
| | | VR_POLICY_LOGS |
| | | VR_RULE_LOGS |
| | | VR_MODULE_LOGS |

## H.2 Partition Add Maintenance

After the initial Oracle Adaptive Access Manager repository setup, the following stored procedures are set up as dbms_jobs to maintain the partitions on a regular basis:

- Sp_Oaam_Add_Monthly_Partition
- Sp_Oaam_Add_Weekly_Partition

### H.2.1 Sp_Oaam_Add_Monthly_Partition

This stored procedure adds partitions for tables with the monthly frequency.

The script runs at the end of each month to create partitions for the following month. To simultaneously add partitions for subsequent months, the partitions are added based on the partition of the previous month.

If this stored procedure fails to exceute (if your monthly partition is missing), you may see database errors, `"ORA-14400 and ORA-14401,"` forcing the Oracle Adaptive Access Manager application to stop.

### H.2.2 Sp_Oaam_Add_Weekly_Partition

This stored procedure adds partitions for tables with the weekly frequency.

The script runs at the end of each week to create partitions for the following week. To simultaneously add partitions for subsequent weeks, the partitions are added based on the partition of the previous week.

If this stored procedure fails to exceute (if your weekly partition is missing), you may see database errors, "ORA-14400 and ORA-14401," forcing the Oracle Adaptive Access Manager application to stop.

## H.3 Partition Maintenance Scripts

After the initial Oracle Adaptive Access Manager repository setup, use the following scripts with purging or archiving maintenance scripts to maintain the partitions on a regular basis:

- drop_monthly_partition_tables.sql
- drop_weekly_partition_tables.sql
- add_monthly_partition_tables.sql
- add_weekly_partition_tables.sql

The above mentioned scripts are located at <IDM_ORACLE_HOME>\oaam\oaam_db_maint_scripts\oaam_db_partition_maint_scripts

**Note:** You do not have to execute partition add scripts. You should only use them to create partitions manually because other automated dbms_jobs create partitions at regular intervals.

### H.3.1 drop_monthly_partition_tables.sql

You can use this script to drop partitions for tables with the monthly frequency. You should run this script at the end of each month to drop partitions older than sixth months, based on the requirements of the Oracle Adaptive Access Manager application. Note that these tables will have six partitions at a given time.

### H.3.2 drop_weekly_partition_tables.sql

You can use this script to drop partitions for tables with the weekly frequency. You should run this script either at the end of every fourteenth day or at the end of third week from the day the Oracle database was created to the dropping of partitions older than two weeks, based on the requirements of the Oracle Adaptive Access Manager application.

### H.3.3 add_monthly_partition_tables.sql

You can use this script to add partitions for tables with the monthly frequency. You should run this script at the end of each month to create partitions for the following month. To add partitions for subsequent months at the same time, run this script multiple times. When you run the script multiple times, partitions are added based on the previous month's partition.

### H.3.4 add_weekly_partition_tables.sql

You can use this script to add partitions for tables with the weekly frequency. You should run this script at the end of each month to create partitions for the following week. To add partitions for subsequent weeks at the same time, run this script multiple times. When you run the script multiple times, partitions are added based on the previous week's partition.

# Software Deinstallation Screens

This appendix describes the screens of the Oracle Fusion Middleware 11*g* Deinstallation Wizard that enables you to remove the Oracle Identity Management software from your machine. This appendix contains the following topics:



## I.1 Welcome

The Welcome screen is the first screen that appears when you start the Oracle Fusion Middleware 11*g* Deinstallation Wizard.

***Figure I–1 Welcome Screen***


Click **Next** to continue.

# I.2 Select Deinstallation Type

Select the type of deinstallation you want to perform.

***Figure I–2 Select Deinstallation Type Screen***

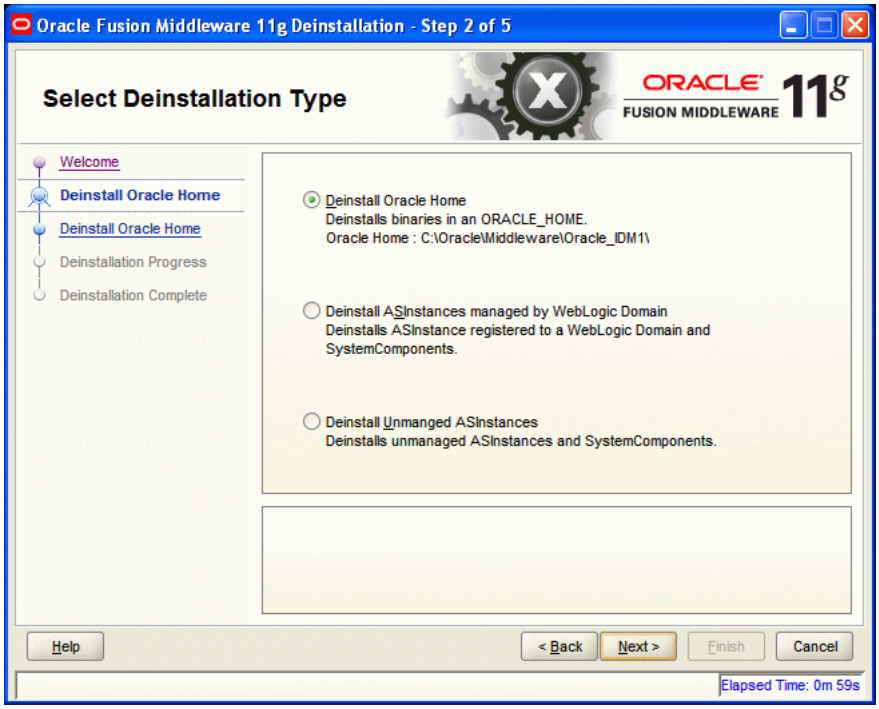



***Table I–1 Deinstallation Types***

| Type | Description |
|---|---|
| **Deinstall Oracle Home** | Select this option to deinstall the binaries contained in the listed Oracle Identity Management Oracle Home.<br>If you select this option, the Deinstall Oracle Home screen appears next, where you can save a response file that contains the deinstallation settings before deinstalling. |
| **Deinstall ASInstances managed by WebLogic Domain** - Applicable to Oracle Internet Directory and Oracle Virtual Directory only. | Select this option to deinstall the Oracle Identity Management system component instances, such as Oracle Internet Directory and Oracle Virtual Directory, that are registered in a WebLogic domain.<br>If you select this option, the Specify WebLogic Domain Detail screen appears next where you identify the administration domain containing the system components you want to deinstall. The Select Managed Instance screen appears next, where you identify the instances you want to deinstall. |
| **Deinstall Unmanaged ASInstances** - Applicable to Oracle Internet Directory and Oracle Virtual Directory only. | Select this option to deinstall the Oracle Identity Management system component instances, such as Oracle Internet Directory and Oracle Virtual Directory, that are not registered in a WebLogic domain.<br>If you select this option, the Specify Instance Location screen appears next where you identify the instances you want to deinstall. |

Click **Next** to continue.

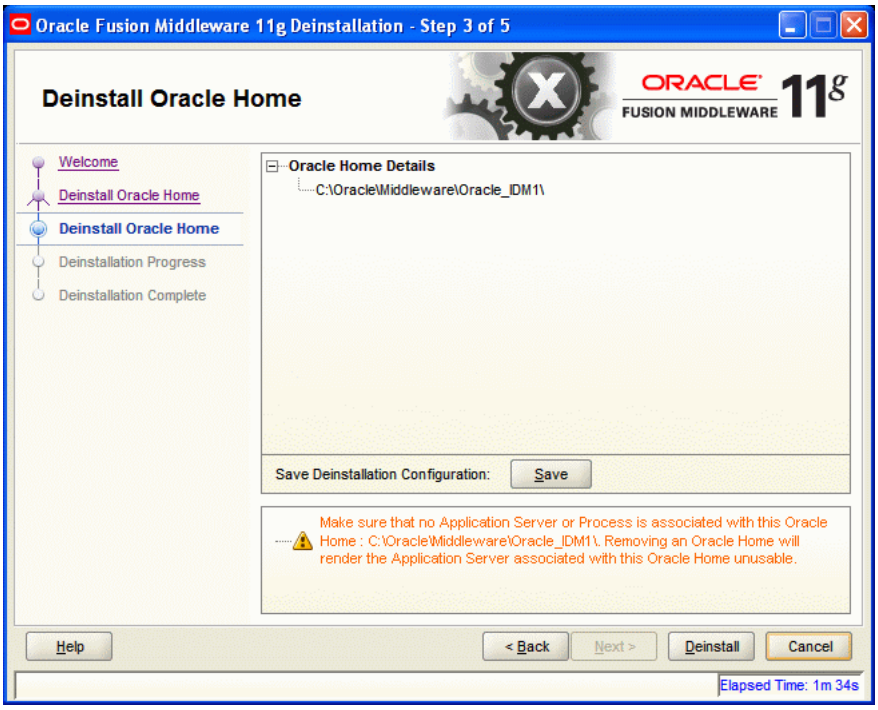
## I.2.1 Option 1: Deinstall Oracle Home

If you selected **Deinstall Oracle Home** on the Select Deinstallation Type screen, the following screen appears:

### I.2.1.1 Deinstall Oracle Home

This screen shows the Oracle Home directory that is about to be deinstalled. It is the Oracle Home directory in which the deinstaller was started.

***Figure I–3 Deinstall Oracle Home Screen***




Verify that this is the correct directory, and also verify that there are no processes associated with this Oracle Home.

Click **Deinstall** to start the deinstallation process.

## I.2.2 Option 2: Deinstall ASInstances managed by WebLogic Domain

If you selected **Deinstall ASInstances managed by WebLogic Domain** on the Select Deinstallation Type screen, the following screens appears:

- Specify WebLogic Domain Detail
- Select Managed Instance
- Deinstallation Summary (Managed Instance)

### I.2.2.1 Specify WebLogic Domain Detail

Specify the WebLogic Domain credentials:

- **Domain Host Name**

  The name of the system on which the WebLogic Domain is running.

- **Domain Port No**

Listen port number of the domain. The default port number is `7001`.

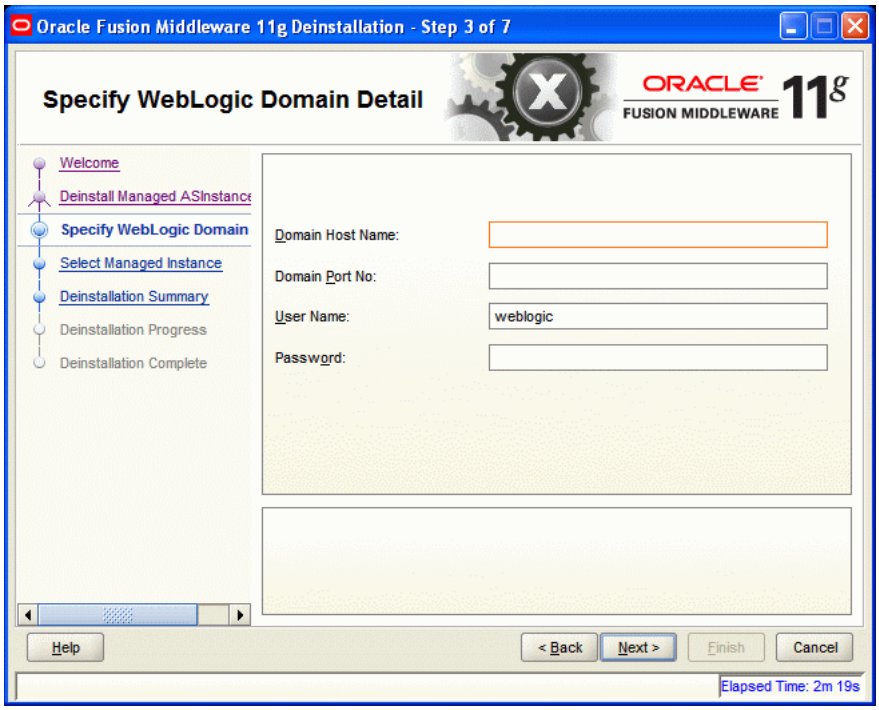
- **User Name**

  The WebLogic Domain user name.

- **Password**

  The password of the WebLogic Domain user.

***Figure I–4 Specify WebLogic Domain Detail Screen***

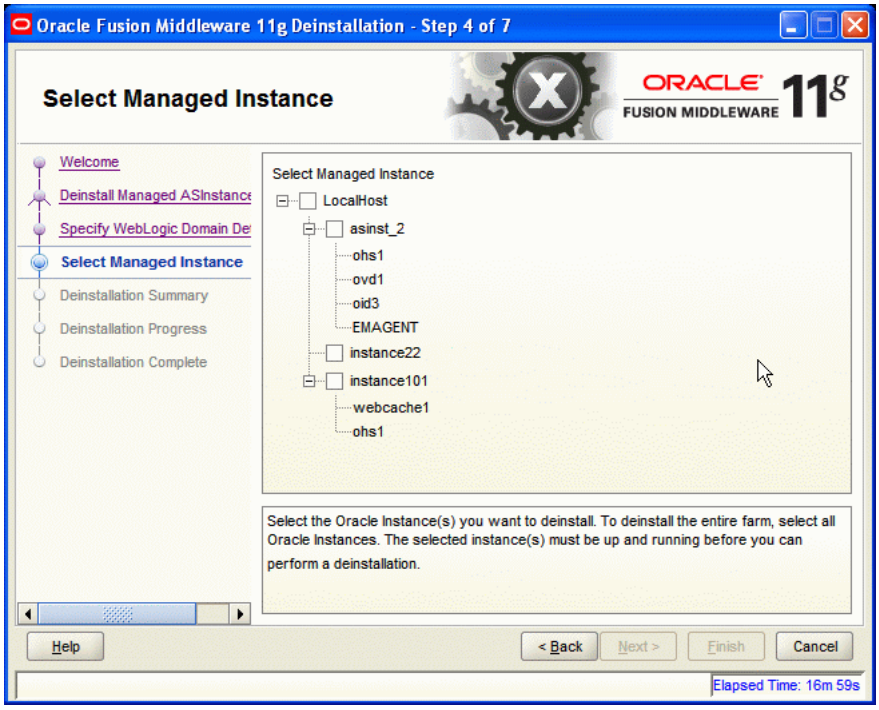



Click **Next** to continue.

### I.2.2.2 Select Managed Instance

Select the managed instance you want to deinstall.

*Figure I–5 Select Managed Instance Screen*

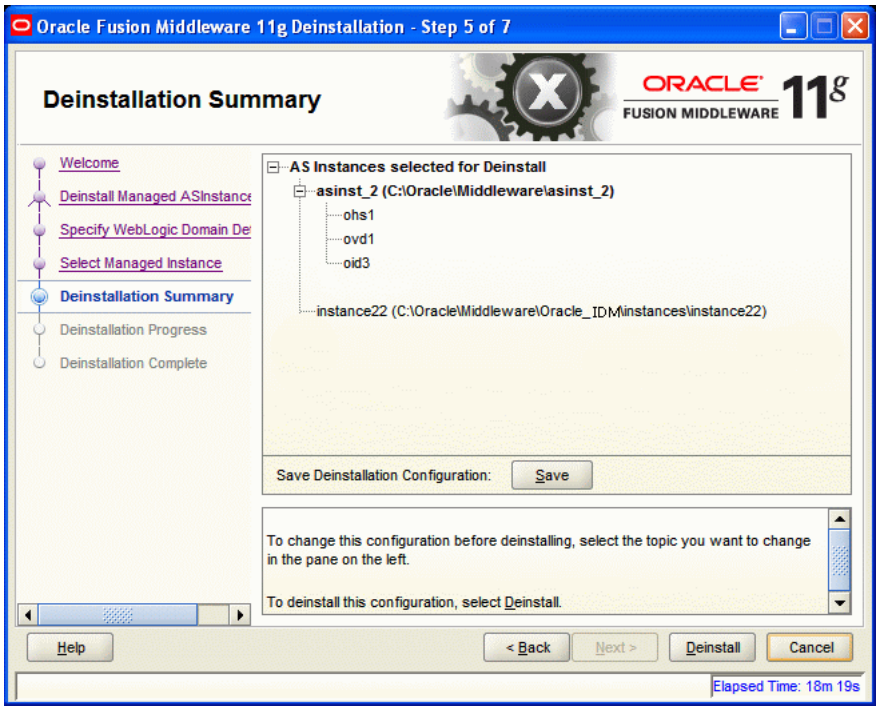



Click **Next** to continue.

### I.2.2.3 Deinstallation Summary (Managed Instance)

Verify that the specified instance is the one you want to deinstall.

*Figure I–6 Deinstallation Summary Screen*



Click **Deinstall** to start the deinstallation process.

## I.2.3 Option 3: Deinstall Unmanaged ASInstances

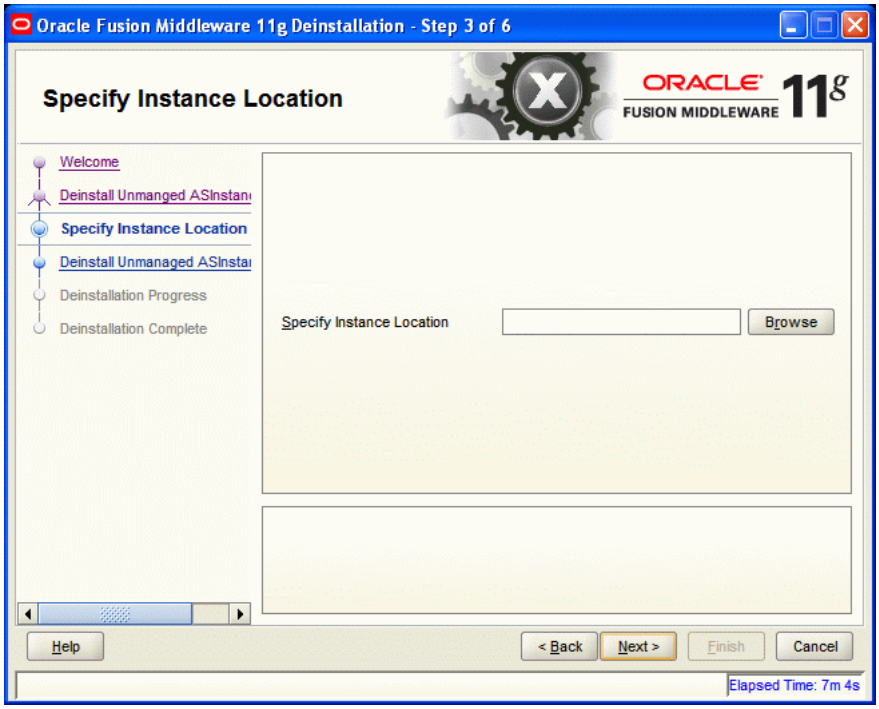
If you selected **Deinstall Unmanaged ASInstances** on the Select Deinstallation Type screen, the following screen appears:

- Specify Instance Location
- Deinstallation Summary (Unmanaged ASInstance)

### I.2.3.1 Specify Instance Location

Specify the full path to your Oracle Instance directory. If you are unsure, click **Browse** to find this directory on your system.

***Figure I–7 Specify Instance Location Screen***

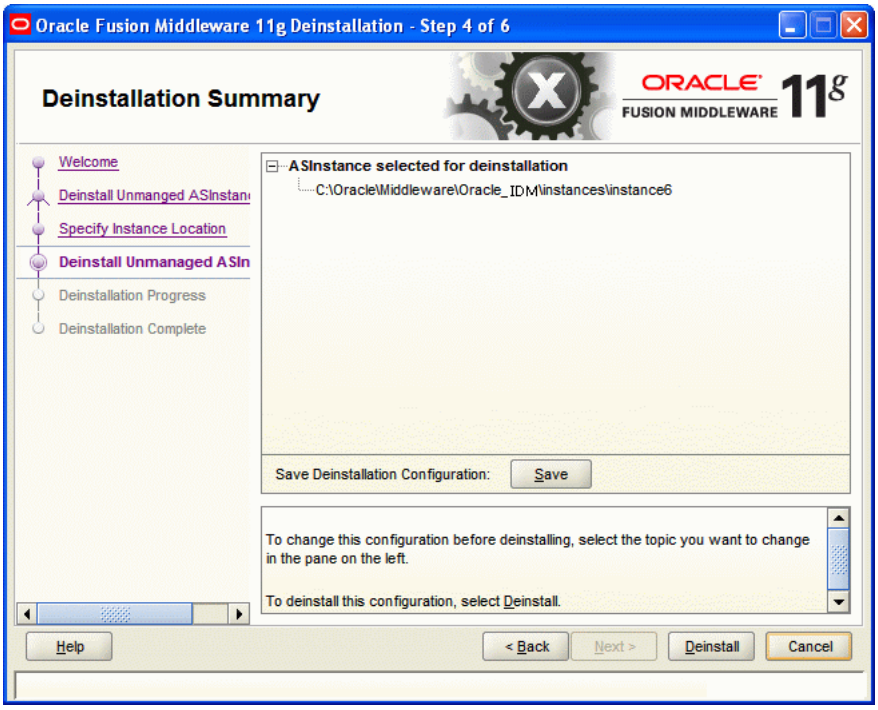



Click **Next** to continue.

### I.2.3.2 Deinstallation Summary (Unmanaged ASInstance)

Verify that the specified instance is the one you want to deinstall.

*Figure I–8 Deinstallation Summary Screen*

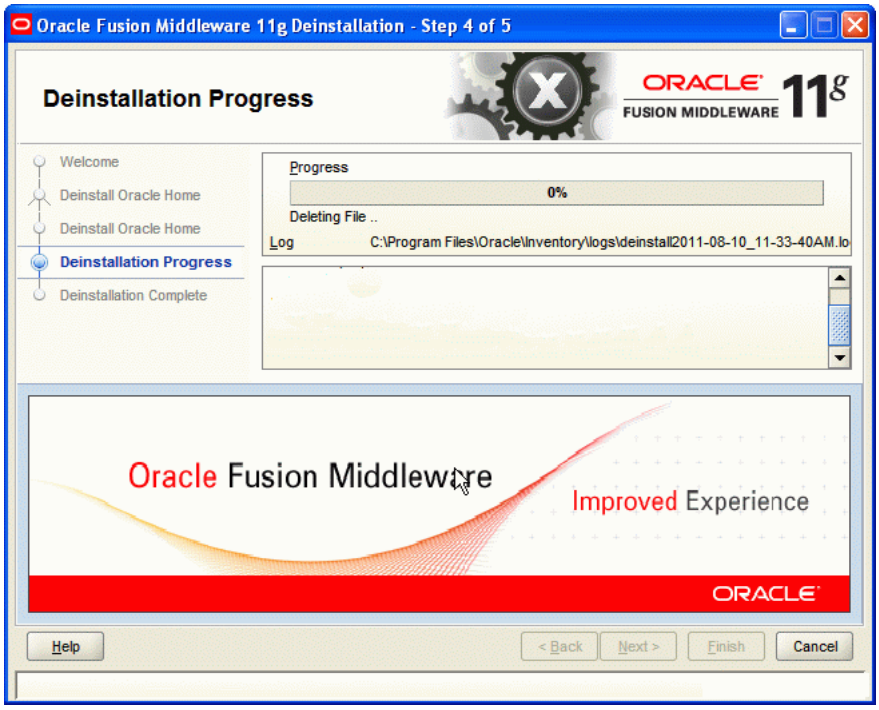



Click **Deinstall** to start the deinstallation process.

## I.3 Deinstallation Progress

This screen shows you the progress of the deinstallation.

*Figure I–9 Deinstallation Progress Screen*




If you want to quit before the deinstallation is completed, click **Cancel**.

## I.4 Deinstallation Complete

This screen summarizes the deinstallation that was just completed.

*Figure I–10 Deinstallation Complete Screen*


Click **Finish** to dismiss the deinstaller.